Virtuelle Poststelle des Bundes, Version 2.2.x.x (Verifikations-modul), Sicherheitsvorgaben (ST)

bremen online services GmbH & Co. KG

datenschutz nord GmbH

Version 1.1

11.03.2008

Zertifizierungs-ID: BSI-DSZ-CC-0504

Bestätigungs-ID: BSI.02098.TE.xx.200x

Historie

Version	Datum	geänderte Kapitel	Grund der Änderung	Geändert durch
0.1	27.03.2006		Erstellung	Matthias Intemann Sönke Maseberg
0.2	06.07.2006		Einarbeitung der Kommentare von TSI und BSI	Matthias Intemann Sönke Maseberg
0.9	11.07.2006		Finalisierung	Matthias Intemann Sönke Maseberg
0.91	24.10.2006		Präzisierung/Korrektur der Plausibilitätsprüfung bei Verifikationsanwendung und -server	Matthias Intemann Sönke Maseberg
0.92	31.10.2006		nach Rücksprache mit TSI SF2 und SF3 zusammengefasst und die Sicherheitsfunktionen neu nummeriert, das Wort „Weitere“ in Rd. Nr. 3.3 löscht sowie Rd. Nr. 160 gelöscht	Matthias Intemann Sönke Maseberg
1.0	19.11.2007		Verweise auf TIFF entfernt, kl. editorische Änderungen	Matthias Intemann Ingo Schumann
1.1	11.03.2008		Verweise auf TIFF eingefügt, kl. editorische Änderungen	Ingo Schumann

Dokumenten-Überwachungsverfahren

Status: final	Prozess-/Dokumentbesitzer: Matthias Intemann (bremen online services GmbH & Co. KG) Ingo Schumann (bremen online services GmbH & Co. KG) Sönke Maseberg (datenschutz nord GmbH)

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 ST-Einführung

1.1 ST-Identifikation

1	ST-Name:	Virtuelle Poststelle des Bundes, Version 2.2.x.x (Verifikationsmodul), Sicherheitsvorgaben (ST)
2	ST-Version:	1.1
3	Datum:	11.03.2008
4	Autoren:	bremen online services GmbH & Co. KG datenschutz nord GmbH
5	EVG-Name:	Virtuelle Poststelle des Bundes, Version 2.2.x.x (Verifikationsmodul
6	EVG-Version:	2.2.3.2
7	CC-Version:	2.3[1]
8	Zertifizierungs-ID:	BSI-DSZ-CC-0504
9	Bestätigungs-ID:	BSI.02098.TE.xx.200x

1.2 ST-Übersicht

10 Im Rahmen des Projektes BundOnline 2005 wird die Virtuelle Poststelle des Bundes entwickelt. Sie stellt als zentrales Kommunikations-Gateway Sicherheitsdienste für die gesicherte Kommunikation zwischen Behörden und externen Kommunikationspartnern (Bürgern, Wirtschaft und andere Behörden) bereit. Entsprechend den zu erwartenden Kommunikationsszenarien im E-Government soll die Virtuelle Poststelle des Bundes folgende wesentliche Funktionen serverbasiert zur Verfügung stellen:

- Signaturbildung und -prüfung;
- Verifikation von pdf-Signaturen;
- Ver- und Entschlüsselung, wobei zentral entschlüsselte Kommunikationsdaten vergleichbar der heute gängigen Praxis im Klartext weitergeleitet oder zur Weiterleitung im Hausnetz neu verschlüsselt werden;
- Abwicklung (des kryptographischen Anteils) von Authentisierungsverfahren;
- Bereitstellen von internen und externen Zeitstempeln;
- Einbindung von Virenscannern;
- Dokumentation aller Aktionen der Virtuellen Poststelle auf einem Laufzettel (VPS-Laufzettel);

[1] Dieses Dokument berücksichtigt die neue deutsche Rechtschreibung und passt die den CC entnommenen Texte teilweise an.

- Einbindung interner und externer Verzeichnisdienste;
- Bereitstellung von benutzerfreundlichen Client-Komponenten.

11 Abbildung 1 illustriert die vollständige Virtuelle Poststelle des Bundes.

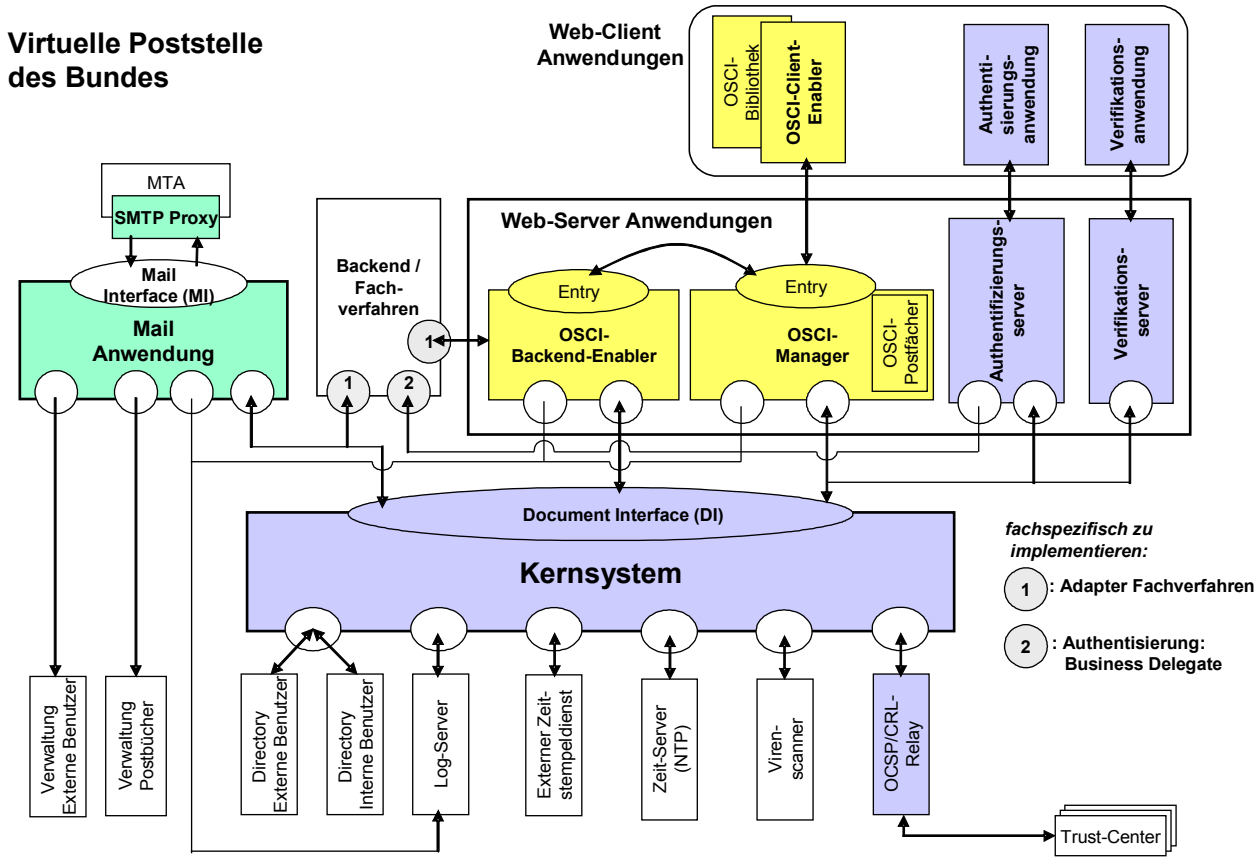

Abbildung 1: Aufbau der Virtuellen Poststelle des Bundes

12 Motivation für die Entwicklung der Virtuellen Poststelle des Bundes war, dass die Erfahrungen beim Einsatz kryptographischer Verfahren – um typische IT-Sicherheitsanforderungen wie Vertraulichkeit, Integrität und Authentizität zu erfüllen – gezeigt haben, dass diese bislang eher zögerlich genutzt werden. Idee der Virtuellen Poststelle ist, die zahlreichen praktischen Schwierigkeiten bei der ausschließlichen Anwendung von „Ende-zu-Ende-Sicherheit“ durch eine Alternative zu überwinden, die darin besteht, kryptographische Funktionen innerhalb von Behörden- und Firmennetzen serverbasiert anzubieten. Dabei darf aber nicht übersehen werden, dass es immer Kommunikationsbeziehungen oder -inhalte gibt, bei denen aufgrund ihrer Sensitivität eine zentrale kryptographische Bearbeitung nicht zweckmäßig oder sogar ausgeschlossen ist. Eine vollständige Abschaffung der Ende-zu-Ende-Sicherheit sollte also nicht das Ziel von „Zentralisierungsbemühungen“ sein.

13 Die Evaluierung der Virtuellen Poststelle des Bundes wird im Rahmen einer kompositiven Evaluierung durchgeführt, in der die VPS in drei logische Ein-

heiten aufgeteilt wird, die jeweils als ein eigenständiger Evaluationsgegenstand (EVG) evaluiert, zertifiziert und bestätigt werden. Die drei EVGs sind:

- EVG1: Virtuelle Poststelle des Bundes, Version 2.2.x.x (Basis);
- EVG2: Virtuelle Poststelle des Bundes, Version 2.2.x.x (OSCI);
- EVG3: Virtuelle Poststelle des Bundes, Version 2.2.x.x (Verifikationsmodul).

14 Die vorliegenden Sicherheitsvorgaben (Security Target – ST) fokussieren auf den Evaluationsgegenstand „Virtuelle Poststelle des Bundes, Version 2.2.x.x (Verifikationsmodul)“.

15 Der Evaluationsgegenstand stellt folgende Funktionalitäten zur Verfügung:

- mathematische Prüfung qualifizierter elektronischer Signaturen (Verifikation);
- Unterstützung bei der Statusprüfung (Validierung) qualifizierter Zertifikate;
- sichere Anzeige von signierten Daten sowie Verifikations- und Validierungsergebnissen.

16 Der Evaluationsgegenstand stellt eine Signaturanwendungskomponente nach SigG/SigV dar, die gemäß § 15 Abs. 7 und § 17 Abs. 4 SigG [SigG] sowie § 11 Abs. 3 SigV [SigV] evaluiert, zertifiziert und bestätigt werden.

17 Dementsprechend wird im Folgenden ausschließlich die für die Erfüllung des Signaturgesetzes relevante Funktionalität der Virtuellen Poststelle des Bundes – nämlich Funktionalitäten zur Signaturprüfung – betrachtet.

18 Die der Zertifizierung zu Grunde liegende Evaluierung erfolgt nach Common Criteria (CC) (ISO/IEC 15408). Für die Bestätigung werden Signaturgesetz [SigG] und -verordnung [SigV] berücksichtigt.

1.3 Postulat der Übereinstimmung mit den Common Criteria

19 Der in Abschnitt 2 beschriebene Evaluationsgegenstand (EVG) „Virtuelle Poststelle des Bundes, Version 2.2.x.x (Verifikationsmodul)“ ist zu folgenden Teilen der Common Criteria entwickelt:

- Teil 2 erweitert [CC-Teil2];
- Teil 3 mit Zusatz, EAL3 [CC-Teil3] mit den Zusätzen ADO_DEL.2, ADV_IMP.1, ADV_LLD.1, ALC_TAT.1, AVA_MSU.3 und AVA_VLA.4 (abkürzend als EAL3+ bezeichnet).

20 Dabei wird die vom EVG zur Verfügung gestellte Sicherheitsfunktionalität sowohl aus funktionalen Sicherheitskomponenten aus dem Teil 2 der CC als auch einer explizit dargelegten Sicherheitskomponente zur sicheren Anzeige hergeleitet (vgl. Abschnitt 9).

21 Hinsichtlich Teil 3 der CC soll das Verifikationsmodul als eine Signaturanwendungskomponente gemäß SigG/SigV die in Anlage 1 der Signaturverordnung [SigV] definierte Vertrauenswürdigkeitsstufe EAL3 erreichen, wobei zusätzlich folgende Anforderungen an die Schwachstellenbewertung bzw.

Mechanismenstärke formuliert sind: „Bei den Prüfstufen […] ‚EAL3' […] ist ergänzend zu den bei dieser Prüfstufe vorgeschriebenen Maßnahmen gegen ein hohes Angriffspotenzial zu prüfen und eine vollständige Missbrauchsanalyse durchzuführen" [SigV, Anlage 1]. Daraus ergibt sich, dass die Signaturanwendungskomponente insgesamt nach EAL3+ mit folgenden Vertrauenswürdigkeitskomponenten evaluiert wird:

- Vertrauenswürdigkeitskomponenten gemäß EAL3:
  - Konfigurationsmanagement:
    - ACM_CAP.3 Autorisierungskontrolle;
    - ACM_SCP.1 EVG-CM-Umfang;
  - Auslieferung und Betrieb:
    - ADO_DEL.1[2] Auslieferungsprozeduren;
    - ADO_IGS.1 Installations-, Generierungs- und Anlaufprozeduren;
  - Entwicklung:
    - ADV_FSP.1 Informelle funktionale Spezifikation;
    - ADV_HLD.2 Sicherheitsspezifischer Entwurf auf hoher Ebene;
    - ADV_RCR.1 Informeller Nachweis der Übereinstimmung;
  - Handbücher:
    - AGD_ADM.1 Systemverwalterhandbuch;
    - AGD_USR.1 Benutzerhandbuch;
  - Lebenszyklus-Unterstützung:
    - ALC_DVS.1 Identifikation der Sicherheitsmaßnahmen;
  - Testen:
    - ATE_COV.2 Analyse der Testabdeckung;
    - ATE_DPT.1 Testen – Entwurf auf hoher Ebene;
    - ATE_FUN.1 Funktionales Testen;
    - ATE_IND.2 Unabhängiges Testen – Stichprobenartig;
  - Schwachstellenbewertung:
    - AVA_MSU.1[3] Prüfung der Handbücher;
    - AVA_SOF.1 Stärke der EVG-Sicherheitsfunktionen;

[2] Diese Vertrauenswürdigkeitskomponente wird durch die höherwertige Systemkomponente ADO_DEL.2 ersetzt, vgl. [AIS27].

[3] Diese Vertrauenswürdigkeitskomponente wird durch die höherwertige Systemkomponente AVA_MSU.3 ersetzt, vgl. [AIS27].

        - AVA_VLA.1[4] Schwachstellenanalyse des Entwicklers.
    - Die Prüfung gegen ein hohes Angriffspotential (SOF-hoch) korrespondiert gemäß [CC-Teil3, Abschnitt 14.4] und [CEM, Abschnitt B.8] mit der Vertrauenswürdigkeitskomponente AVA_VLA.4, was über die Abhängigkeiten folgende zusätzliche bzw. höhere Vertrauenswürdigkeitskomponenten impliziert:
        - Entwicklung:
            - ADV_IMP.1 Teilmenge der Implementierung der TSF;
            - ADV_LLD.1 Beschreibender Entwurf auf niedriger Ebene;
            - zugehörig erweiterter Umfang von ADV_RCR.1;
        - Lebenszyklus-Unterstützung:
            - ALC_TAT.1 Klar festgelegte Entwicklungswerkzeuge;
        - Schwachstellenbewertung:
            - AVA_VLA.4 Hohe Widerstandsfähigkeit.
    - Die vollständige Missbrauchsanalyse wird durch die folgenden Vertrauenswürdigkeitskomponenten realisiert:
        - Auslieferung und Betrieb:
            - ADO_DEL.2 Erkennung von Modifizierungen;
        - Schwachstellenbewertung:
            - AVA_MSU.3 Analysieren und Testen auf unsichere Zustände.

22 Diese Vertrauenswürdigkeitskomponenten entsprechen den Anforderungen aus den im Entwurf vorliegenden „Anwendungshinweisen und Interpretationen zum Schema (AIS)“ Nr. 27 [AIS27]. In AIS 27 werden Vertrauenswürdigkeitskomponenten aufgeführt, die zusätzlich zu den in den EAL-Stufen der Common Criteria ausgewählten Komponenten auszuwählen – d. h. zu augmentieren – sind, um den Anforderungen der ITSEC zu genügen. Relevant für diese Sicherheitsvorgaben sind die in Anlage 1 der Signaturverordnung [SigV] beschriebenen Anforderungen hinsichtlich der Stärke der Sicherheitsmechanismen, die mit „hoch“ bewertet werden müssen.

2 EVG-Beschreibung

2.1 Kompositive Evaluierung

23 Die Evaluierung der Virtuellen Poststelle des Bundes (VPS) wird im Rahmen einer kompositiven Evaluierung durchgeführt, in der die VPS in drei logische Einheiten aufgeteilt wird, die jeweils als ein eigenständiger Evaluationsgegenstand (EVG) evaluiert, zertifiziert und bestätigt werden.

[4] Diese Vertrauenswürdigkeitskomponente wird durch die höherwertige Systemkomponente AVA_VLA.4 ersetzt.

24 Die drei EVGs sind in Abbildung 2 illustriert:

- EVG1: Virtuelle Poststelle des Bundes, Version 2.2.x.x (Basis);
- EVG2: Virtuelle Poststelle des Bundes, Version 2.2.x.x (OSCI);
- EVG3: Virtuelle Poststelle des Bundes, Version 2.2.x.x (Verifikationsmodul).

25 Diese Sicherheitsvorgaben fokussieren auf den EVG „Virtuelle Poststelle des Bundes, Version 2.2.x.x (Verifikationsmodul)“.

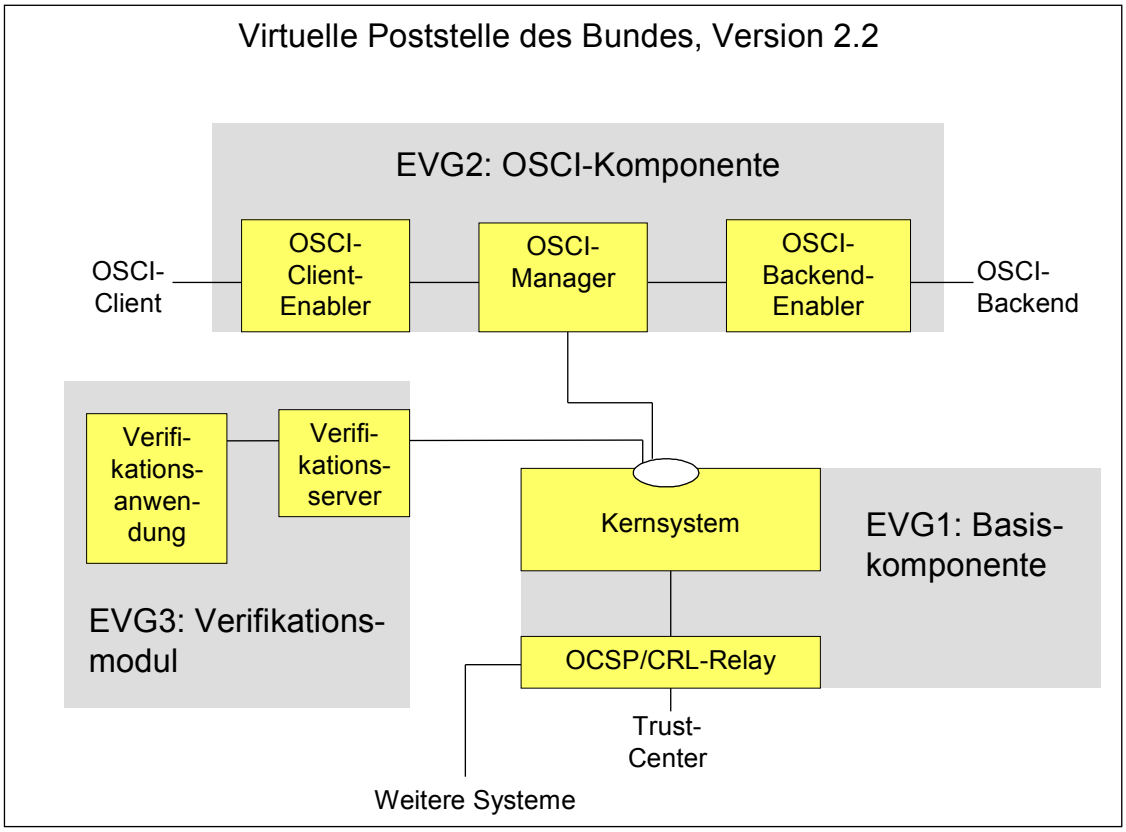

Abbildung 2: EVG-Übersicht

2.2 EVG-Umfang

26 Der Evaluationsgegenstand „Virtuelle Poststelle des Bundes, Version 2.2.x.x (Verifikationsmodul)“ stellt folgende Funktionalitäten bereit:

- mathematische Prüfung qualifizierter elektronischer Signaturen (Verifikation);
- Unterstützung bei der Statusprüfung (Validierung) qualifizierter Zertifikate;
- sichere Anzeige von zu signierenden und signierten Daten sowie Verifikations- und Validierungsergebnissen.

27 Der EVG ist eine Signaturanwendungskomponente, also insbesondere eine Software, die auf geeigneter Hardware mit geeigneten Betriebsmitteln (etwa Zertifikaten) betrieben wird.

28 Der EVG nutzt Funktionalitäten einer SigG-konformen Basiskomponente der Virtuellen Poststelle des Bundes mit Kernsystem und OCSP/CRL-Relay, die ebenfalls innerhalb der kompositiven Evaluierung der Virtuellen Poststelle des Bundes evaluiert, zertifiziert und bestätigt wird. Funktionalitäten und Eigenschaften der Basiskomponente sind in [bos_Basis-ST] näher beschrieben.

29 Der EVG besteht aus den folgenden Teilsystemen:

- Verifikationsanwendung;
- Verifikationsserver

30 Bei der Verifikationsanwendung handelt es sich um eine Java Web Start-Anwendung, die über einen Link von einem Download-Server geladen und anschließend auf einem Rechner an einem Arbeitsplatz – beispielsweise in einem Büro – (in einem „geschützten Einsatzbereich (Regelfall/Standardlösung)“ [BNetzA2005]) betrieben wird.

31 Beim Verifikationsserver handelt es sich um eine Java-Anwendung, die auf einem Server in einem Rechenzentrum (in einem „geschützten Einsatzbereich (Regelfall/Standardlösung)“ [BNetzA2005]) betrieben und mit jeweiligen Web-Oberflächen (GUIs) von Administratoren konfiguriert wird. Der Verifikationsserver arbeitet im Produktivbetrieb automatisiert und ohne menschliche Aktivitäten.

32 Der Evaluationsgegenstand stellt folgende Funktionen zur Verfügung:

- Die Verifikationsanwendung prüft auf Anforderung des Benutzers die mathematische Korrektheit einer qualifizierten elektronischen Signatur. Die Verifikationsanwendung führt eine Signaturprüfung durch, d. h. prüft die mathematische Korrektheit der Signatur mittels zugehörigem Prüfschlüssel (öffentlichem Schlüssel aus qualifiziertem Zertifikat) und geeigneten kryptographischen Verfahren und visualisiert das Verifikationsergebnis (gültige oder ungültige Signatur oder Fehlermeldung).

  Zusätzlich wird bei jeder Verifikation (mathematische Prüfung) eine Validierung (Statusprüfung) des zugehörigen Zertifikats durchgeführt (s. u.). Die eigentliche Statusprüfung wird an den Verifikationsserver weitergeleitet, der mit einem Validierungsergebnis antwortet (s. u.). Die Verifikationsanwendung prüft anschließend die elektronische Signatur der Antwort, führt eine Plausibilitätsprüfung durch – in der festgestellt wird, ob das validierte Zertifikat der zu prüfenden qualifizierten Signatur zugeordnet ist – und visualisiert das Validierungsergebnis.

  Der Benutzer kann den Prüfzeitpunkt des Zertifikats angeben (s. u.).

- Die Verifikationsanwendung führt auf Anforderung des Benutzers die Statusprüfung eines qualifizierten Zertifikats durch. Die eigentliche Statusprüfung wird an den Verifikationsserver weitergeleitet, der mit einem Validierungsergebnis antwortet (s. u.). Die Verifikationsanwendung prüft an-

schließend die elektronische Signatur der Antwort und visualisiert das Validierungsergebnis.

Der Benutzer kann den Prüfzeitpunkt des Zertifikats angeben, wobei ein Default-Wert angegeben wird:

- Bei einer OSCI-Nachricht ist der Default-Wert der Eingangszeitpunkt auf dem OSCI-Intermediär.
- Ist ein Zeitpunkt in der Nachricht enthalten, wird dieser als Default-Wert genutzt.
- In allen anderen Fällen wird der aktuelle Zeitpunkt als Default-Wert genutzt.

Die Verifikationsanwendung führt eine Plausibilitätsprüfung durch, bei der festgestellt wird, ob der Zertifikatsstatus zum angefragten Prüfzeitpunkt ermittelt wurde.

- Der Verifikationsserver stellt auf Anforderung der Verifikationsanwendung die Gültigkeit eines qualifizierten Zertifikats unter Zuhilfenahme einer Basiskomponente mit Kernsystem und OCSP/CRL-Relay zu einem Prüfzeitpunkt (s. o.) fest.

  Sofern in der Anforderung der Verifikationsanwendung ein Prüfzeitpunkt übermittelt wurde, führt der Verifikationsserver eine Plausibilitätsprüfung durch, bei der festgestellt wird, ob der Prüfzeitpunkt in der Anfrage konsistent enthalten ist.[5]

  Die Basiskomponente stellt dabei fest, ob das qualifizierte Zertifikat zum Prüfzeitpunkt vorhanden und nicht gesperrt war und der Gültigkeitszeitraum des qualifizierten Zertifikats zu diesem Zeitpunkt bereits begonnen und noch nicht abgelaufen war, und übergibt das Ergebnis der Validierung in Form der Verzeichnisdienst-Ergebnisse sowie einer Interpretation (gültig und nicht gesperrt, unbekannt oder gesperrt) an den Verifikationsserver. Die Antwort ist vom OCSP/CRL-Relay signiert.

33 Die Kommunikation zwischen Verifikationsserver und Basiskomponente erfolgt derart abgesichert, dass die tatsächliche Anforderung bearbeitet und zutreffende Ergebnisse zurückliefert werden. Hinsichtlich der Sicherheit der Kommunikation zwischen Verifikationsanwendung und -server werden keine Annahmen getroffen, da die Antwort, die die Verifikationsanwendung erhält, mit einer elektronischen Signatur versehen und dadurch abgesichert ist.

34 Der EVG wurde ISIS-MTT-konform entwickelt ([ISIS-MTT_SigG]).

35 Zum EVG-Umfang gehört darüber hinaus ein Prüftool zum Schutz vor unbefugter Veränderung an der Verifikationsanwendung; darüber hinaus werden die Konfigurationsdaten der Verifikationsanwendung abgesichert (vgl. Abschnitt 2.6).

[5] Hintergrund: Durch diese Plausibilitätsprüfung sollen etwaige Manipulation am Prüfzeitpunkt für die Verifikationsanwendung festgestellt und erkennbar gemacht werden.

2.3 Technische Realisierung

36 Das Verifikationsmodul besteht aus den Teilsystemen

- Verifikationsanwendung und
- Verifikationsserver

inklusive einer Administrationsanwendung als Graphical User Interface (GUI) zur Administration des Verifikationsservers. Abbildung 3 illustriert die Teilsysteme des Verifikationsmoduls.

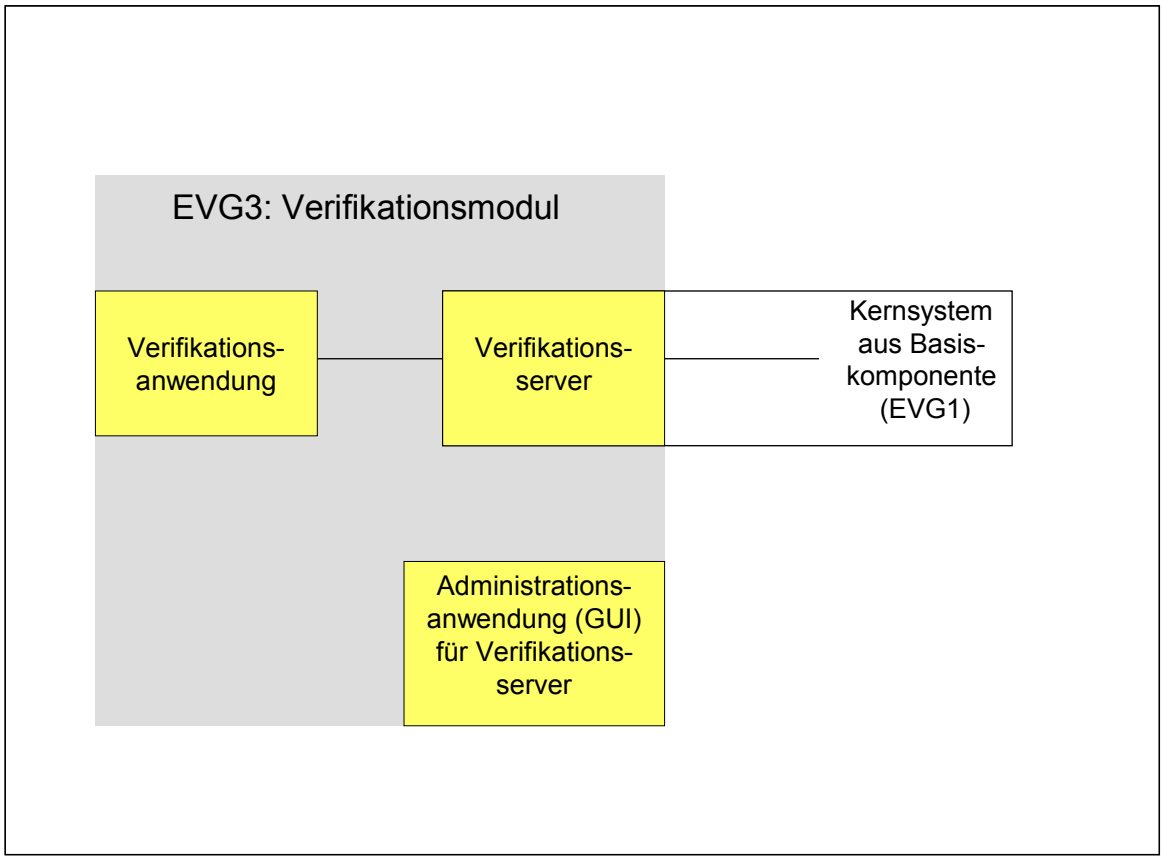

Abbildung 3: Teilsysteme des EVG

37 Verifikationsanwendung und -server können voneinander getrennt betrieben werden, d. h. nicht innerhalb eines LANs (Local Area Networks), sondern über ein Weitverkehrsnetz (Wide Area Network – WAN) verbunden sein.

38 Die wesentlichen Aufgaben der Teilsysteme:

- Verifikationsanwendung: [6]

[6] Weitere Funktionalitäten, die allerdings nicht Bestandteil der Zertifizierung und Bestätigung sind, sind in Abschnitt 1.2 aufgeführt – beispielsweise die Verifikation von pdf-Signaturen.

- Verifizieren: Die Verifikationsanwendung verifiziert qualifizierte elektronische Signaturen und zeigt das Verifikationsergebnis (gültige oder ungültige Signatur oder Fehlermeldung) sowie die signierte Daten an.

  Zusätzlich wird bei jedem Verifizieren eine Validierung (Statusprüfung) durchgeführt (siehe nächster Spiegelstrich), wobei der Prüfzeitpunkt des zugehörigen Zertifikats konfigurierbar ist; ein Default-Wert wird angegeben (s. u.).

- Validieren: Die Verifikationsanwendung führt die Statusprüfung eines qualifizierten Zertifikats durch, wobei der Prüfzeitpunkt konfiguriert werden kann; ein Default-Wert wird angegeben:

  - Bei einer OSCI-Nachricht ist der Default-Wert der Eingangszeitpunkt auf dem OSCI-Intermediär.
  - Ist ein Zeitpunkt in der Nachricht enthalten, wird dieser als Default-Wert genutzt.
  - In allen anderen Fällen wird der aktuelle Zeitpunkt als Default-Wert genutzt.

  Die Verifikationsanwendung validiert nicht selber, sondern nutzt dazu den Verifikationsserver, von dem die Verifikationsanwendung anschließend das Ergebnis der Validierung erhält, welches mit einer elektronischen Signatur versehen ist. Das Ergebnis der Validierung umfasst neben den Verzeichnisdienst-Ergebnissen eine Interpretation (gültig und nicht gesperrt, unbekannt oder gesperrt).

  Die Verifikationsanwendung verifiziert die elektronische Signatur des Validierungsergebnisses mit dem (System-)Zertifikat des OCSP/CRL-Relay und prüft, ob das validierte Zertifikat dasjenige Zertifikat ist, welches der Signatur entspricht, und ob der Zertifikatsstatus zum angefragten Prüfzeitpunkt ermittelt wurde (Plausibilitätscheck). Die Verifikationsanwendung visualisiert das Ergebnis der Validierung (Statusprüfung).

- Sichere Anzeige: Die Verifikationsanwendung bietet eine sichere Anzeige von folgenden signierten Daten:

  - plain-text (UTF-8-codiert);
  - tiff-Daten.

  Darüber hinaus bietet die Verifikationsanwendung eine sichere Anzeige von Verifikations- und Validierungsergebnissen und Konfigurationsdaten (Adresse des Verifikationsservers mit Proxy-Information sowie das (System-)Zertifikat des OCSP/CRL-Relays als Trust Anchor).

- Schutz der Konfigurationsdaten: Die Konfigurationsdaten[7] – Adresse des Verifikationsservers sowie Zertifikat des OCSP/CRL-Relays, die nicht vorkonfiguriert sind, sondern vom Benutzer konfiguriert werden müssen – werden derart geschützt, dass auf diese Konfigurationsdaten zusammen mit einem vom Benutzer frei zu vergebenen Passwort eine Hashfunktion angewendet wird und dieser Hashwert mit einem abgespeicherten Hashwert als Referenz verglichen wird (vgl. Abschnitt 2.6).

- Verifikationsserver:

  Der Verifikationsserver führt auf Anforderung der Verifikationsanwendung die Statusprüfung eines qualifizierten Zertifikats durch. Dazu greift der Verifikationsserver auf eine Basiskomponente (vgl. [bos_Basis-ST]) zu, welche die eigentliche Validierung durchführt. Sofern in der Anforderung der Verifikationsanwendung ein Prüfzeitpunkt übermittelt wurde, führt der Verifikationsserver zunächst nach Erhalt der Anforderung eine Plausibilitätsprüfung durch, bei der festgestellt wird, ob der Prüfzeitpunkt in der Anfrage konsistent enthalten ist.

  Der Verifikationsserver übergibt der Verifikationsanwendung das Validierungsergebnis der Basiskomponente – und damit insbesondere das vom OCSP/CRL-Relay mit einer elektronischen Signatur versehene Validierungsergebnis. Das Ergebnis der Validierung umfasst neben den Verzeichnisdienst-Ergebnissen eine Interpretation (gültig und nicht gesperrt, unbekannt oder gesperrt).

39 Kommunikationssicherheit:

- Verifikationsserver und Kernsystem der Basiskomponente werden zusammen innerhalb eines vertrauenswürdigen Netzes betrieben.
- Das Validierungsergebnis – in Form des Verzeichnisdienst-Ergebnisses sowie einer Interpretation gemäß [ISIS-MTT_SigG] – wird vom OCSP/CRL-Relay mit einer elektronischen Signatur versehen und von der Verifikationsanwendung mit dem (System-)Zertifikat des OCSP/CRL-Relays verifiziert.

40 Die Signaturen folgender Nachrichten- und Dateitypen können verifiziert werden:6

- X.509-Zertifikate;
- Signaturen nach OSCI (Online Services Computer Interface) – vgl. [bos_OSCI-ST];
- PKCS#7;
- S/MIME.

[7] Neben den sicherheitsrelevanten Konfigurationsdaten Adresse des Verifikationsserver und (System-)Zertifikat des OCSP/CRL-Relays umfassen die Konfigurationsdaten weitere Informationen – wie etwa die Proxy-Information –, die allerdings nicht abgesichert werden müssen.

41 Qualifizierte Zertifikate und (System-)Zertifikate werden dem EVG vom Dateisystem des unterliegenden Systems zur Verfügung gestellt.

42 Das Prüftool zum Schutz vor unbefugter Veränderung ist in Abschnitt 2.6 beschrieben.

2.4 Signaturgesetz (SigG) und -verordnung (SigV)

2.4.1 Rechtliche Grundlagen

43 Signaturanwendungskomponenten werden in § 2 Nr. 11 SigG definiert als „Software- und Hardwareprodukte, 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 [...]“.

44 Sicherheitsanforderungen an Signaturanwendungskomponenten werden in § 17 Abs. 2 SigG und § 15 Abs. 2 SigV formuliert:

45 § 17 SigG „Produkte für qualifizierte elektronische Signaturen“:

> „(2) Für die Darstellung zu signierender Daten sind Signaturanwendungskomponenten erforderlich, die die Erzeugung einer qualifizierten elektronischen Signatur vorher eindeutig anzeigen und feststellen lassen, auf welche Daten sich die Signatur bezieht. Für die Überprüfung signierter Daten sind Signaturanwendungskomponenten erforderlich, die feststellen lassen,

1. auf welche Daten sich die Signatur bezieht,

2. ob die signierten Daten unverändert sind,

3. welchem Signaturschlüssel-Inhaber die Signatur zuzuordnen ist,

> 4. welche Inhalte das qualifizierte Zertifikat, auf dem die Signatur beruht, und zugehörige qualifizierte Attribut-Zertifikate aufweisen und
>
> 5. zu welchem Ergebnis die Nachprüfung von Zertifikaten nach § 5 Abs. 1 Satz 2 geführt hat.
>
> Signaturanwendungskomponenten müssen nach Bedarf auch den Inhalt der zu signierenden oder signierten Daten hinreichend erkennen lassen. Die Signaturschlüssel-Inhaber sollen solche Signaturanwendungskomponenten einsetzen oder andere geeignete Maßnahmen zur Sicherheit qualifizierter elektronischer Signaturen treffen.“

46 § 15 SigV „Anforderungen an Produkte für qualifizierte elektronische Signaturen“:

> „(2) Signaturanwendungskomponenten nach § 17 Abs. 2 des Signaturgesetzes müssen gewährleisten, dass

1. bei der Erzeugung einer qualifizierten elektronischen Signatur

a) die Identifikationsdaten nicht preisgegeben und diese nur auf der jeweiligen sicheren Signaturerstellungseinheit gespeichert werden,

b) eine Signatur nur durch die berechtigt signierende Person erfolgt,

c) die Erzeugung einer Signatur vorher eindeutig angezeigt wird und

2. bei der Prüfung einer qualifizierten elektronischen Signatur

a) die Korrektheit der Signatur zuverlässig geprüft und zutreffend angezeigt wird und

b) eindeutig erkennbar wird, ob die nachgeprüften qualifizierten Zertifikate im jeweiligen Zertifikat-Verzeichnis zum angegebenen Zeitpunkt vorhanden und nicht gesperrt waren."

47 Die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (Bundesnetzagentur) fasst die Sicherheitsanforderungen in [BNetzA2005] zusammen und konkretisiert sie in Fußnoten:

48 „Erzeugung von Signaturen: Die Signaturanwendungskomponente muss beim Erzeugen einer Signatur gewährleisten, dass

- das Erzeugen einer Signatur vorher eindeutig angezeigt wird[8],
- erkennbar ist, auf welche Daten sich die Signatur bezieht[9],
- bei Bedarf der Inhalt der zu signierenden Daten hinreichend zu erkennen ist[10],
- eine Signatur nur durch die berechtigt signierende Person erfolgt[11],
- die Identifikationsdaten nicht preisgegeben und nur auf der jeweiligen „sicheren Signaturerstellungseinheit" gespeichert werden[12].

49 Prüfung einer Signatur: Die Signaturanwendungskomponente muss beim Prüfen einer Signatur gewährleisten, dass

- erkennbar wird, auf welche Daten sich die Signatur bezieht,

[8] „Z. B. durch einen Warnhinweis auf dem Bildschirm." [BNetzA2005]

[9] „Z. B. durch Anzeigen des Dateinamens." [BNetzA2005]

[10] „Z. B. bei Texten/Graphiken durch vollständige Anzeige des Inhaltes (keine „versteckten Texte") mit eindeutiger Interpretation auf Bildschirm/Ausdruck." [BNetzA2005]

[11] „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." [BNetzA2005]

[12] „Dies erfordert einen gesicherten Übertragungsweg von der Eingabe der Identifikationsdaten zur Signaturerstellungseinheit." [BNetzA2005]

- 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.

50 Schutz vor unbefugter Veränderung: Sicherheitstechnische Veränderungen an der Signaturanwendungskomponente müssen für den Nutzer erkennbar[13] werden."

2.4.2 Signaturgesetz-Anforderungen an den EVG

51 Der EVG ist eine Signaturanwendungskomponente zur Prüfung qualifizierter elektronischer Signaturen. Anforderungen von SigG und SigV hinsichtlich der Erzeugung qualifizierter elektronischer Signaturen werden vom EVG nicht abgedeckt.

52 Im Folgenden wird aufgezeigt und in Tabelle 1 zusammenfassend dargestellt, in welchem Umfang die Sicherheitsanforderungen des SigG und der SigV an Signaturanwendungskomponenten vom EVG erfüllt werden und welcher Anteil von der IT-Umgebung umgesetzt werden muss.

Zur Prüfung einer Signatur

53 Die Sicherheitsanforderungen, dass eine Signaturanwendungskomponente beim Prüfen einer Signatur gewährleisten muss, 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,"

[13] „Dies kann – abhängig von der Art des Einsatzbereiches (vgl. Abschnitt 4 [BNetzA-2005]) – 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." [BNetzA2005]

- „erkennbar wird, welchem Signaturschlüssel-Inhaber die Signatur zuzuordnen ist“,
- „erkennbar wird, welche Inhalte das qualifizierte Zertifikat, auf dem die Signatur beruht“, aufweist, [14]
- „erkennbar wird, ob die nachgeprüften qualifizierten Zertifikate im jeweiligen Zertifikatverzeichnis zum angegebenen Zeitpunkt vorhanden und nicht gesperrt waren” und
- „die Korrektheit der Signatur zuverlässig geprüft und zutreffend angezeigt wird“ ([BNetzA2005])

  werden vom EVG umgesetzt: Die Verifikationsanwendung prüft die Korrektheit qualifizierter elektronischer Signaturen. Entsprechende Anzeigen sind nur bei der Verifikationsanwendung verfügbar, da nur hier Benutzer involviert sind.

54 Die Validierung, „ob die geprüften qualifizierten Zertifikate im jeweiligen Zertifikat-Verzeichnis zum angegebenen Zeitpunkt vorhanden und nicht gesperrt waren“ (§ 15 Abs. 2 SigV) erfolgt

- hinsichtlich Validierung bei einer SigG-konformen Basiskomponente in der IT-Umgebung und beim Verifikationsserver (Plausibilitätsprüfung, bei der festgestellt wird, ob ein angegebener Prüfzeitpunkt in der Anfrage konsistent enthalten ist),
- hinsichtlich der Plausibilitätsprüfung (Gehört das validierte Zertifikat zur Signatur? Wurde der Zertifikatsstatus zu einem angefragten Prüfzeitpunkt ermittelt?) bei der Verifikationsanwendung und
- hinsichtlich der Anzeige bei der Verifikationsanwendung.

Schutz vor unbefugter Veränderung

55 Die Sicherheitsanforderungen zum Schutz vor unbefugter Veränderung – „um sicherheitstechnische Veränderungen an der Signaturanwendungskomponente“ [BNetzA2005] für den Nutzer erkennbar zu machen – sind hinsichtlich des EVG in der Weise umzusetzen, dass sowohl die Client-Komponenten am Arbeitsplatz als auch die Server-Komponenten im Serverraum in einem geschützten Einsatzbereich eingesetzt werden (vgl. nach [BNetzA2005]). Darüber hinaus wird für die Verifikationsanwendung ein Prüftool zur Verfügung gestellt (EVG-Umfang), um die Integrität der Verifikationsanwendung zu gewährleisten. Die Integrität der Konfigurationsdaten der Verifikationsanwendung wird vom EVG geschützt.

[14] Attributzertifikate werden vom EVG nicht unterstützt.

Tabelle 1: Umsetzung der SigG/SigV-Anforderungen

Sicherheitsanforderungen an Signaturanwendungskomponenten [BNetzA2005]	Umsetzung der Anforderungen aus SigG und SigV	
	in EVG	in der IT-Umgebung
Prüfung einer Signatur: Die Signaturanwendungskomponente muss beim Prüfen einer Signatur gewährleisten, dass	Verifikationsanwendung prüft qualifizierte elektronische Signaturen; Teilfunktionalitäten der Validierung erfolgen beim Verifikationsserver; Plausibilitätsprüfung bei Verifikationsanwendung und -server	
▪ erkennbar wird, auf welche Daten sich die Signatur bezieht,[15]	wird von Verifikationsanwendung angezeigt	-
▪ erkennbar wird, ob die Daten unverändert sind,[16]	die Prüfung, ob Daten unverändert sind, erfolgt bei der Verifikationsanwendung; die entsprechende Anzeige wird von der Verifikationsanwendung angezeigt	-
▪ bei Bedarf der Inhalt der signierten Daten hinreichend zu erkennen ist,[17]	wird von Verifikationsanwendung angezeigt	-
▪ erkennbar wird, welchem Signaturschlüssel-Inhaber die Signatur zuzuordnen ist,[18]	wird von Verifikationsanwendung angezeigt	-
▪ erkennbar wird, welche Inhalte das qualifizierte Zertifikat, auf dem die Signatur	wird von Verifikationsanwendung angezeigt	-

[15] vgl. „Für die Überprüfung signierter Daten sind Signaturanwendungskomponenten erforderlich, die feststellen lassen, [...] auf welche Daten sich die Signatur bezieht [...]." [§17 Abs. 2 Nr.1 SigG]

[16] vgl. „Für die Überprüfung signierter Daten sind Signaturanwendungskomponenten erforderlich, die feststellen lassen, [...] ob die signierten Daten unverändert sind [...]." [§17 Abs. 2 Nr.2 SigG]

[17] vgl. „Signaturanwendungskomponenten müssen nach Bedarf auch den Inhalt der [...] signierten Daten hinreichend erkennen lassen." [§17 Abs. 2 SigG]

[18] vgl. „Für die Überprüfung signierter Daten sind Signaturanwendungskomponenten erforderlich, die feststellen lassen, [...] welchem Signaturschlüssel-Inhaber die Signatur zuzuordnen ist [...]." [§17 Abs. 2 Nr.3 SigG]

Sicherheitsanforderungen an Signaturanwendungskomponenten [BNetzA2005]	Umsetzung der Anforderungen aus SigG und SigV	
	in EVG	in der IT-Umgebung
Prüfung einer Signatur: Die Signaturanwendungskomponente muss beim Prüfen einer Signatur gewährleisten, dass	Verifikationsanwendung prüft qualifizierte elektronische Signaturen; Teilfunktionalitäten der Validierung erfolgen beim Verifikationsserver; Plausibilitätsprüfung bei Verifikationsanwendung und -server	
beruht,14 aufweisen,[19]		
▪ erkennbar wird, ob die nachgeprüften qualifizierten Zertifikate im jeweiligen Zertifikatverzeichnis zum angegebenen Zeitpunkt vorhanden und nicht gesperrt waren,[20]	Verifikationsergebnis wird von Verifikationsanwendung angezeigt	die eigentliche Statusprüfung (Validierung) des Zertifikats erfolgt in der Basiskomponente
▪ die Korrektheit der Signatur zuverlässig geprüft und zutreffend angezeigt wird.[21]	führt Verifikationsanwendung durch	-
Schutz vor unbefugter Veränderung: Sicherheitstechnische Veränderungen an der Signaturanwendungskomponente müssen für den Nutzer erkennbar	Prüftool zum Schutz vor unbefugter Veränderung wird zur Verfügung gestellt; sichere Anzeige der	für den Verifikationsserver muss der sichere Betrieb in der (Server-)Umgebung gewährleistet wer-

[19] vgl. „Für die Überprüfung signierter Daten sind Signaturanwendungskomponenten erforderlich, die feststellen lassen, [...] welche Inhalte das qualifizierte Zertifikat, auf dem die Signatur beruht, und zugehörige qualifizierte Attribut-Zertifikate aufweisen [...].“ [§17 Abs. 2 Nr. 4 SigG]

[20] vgl. „Für die Überprüfung signierter Daten sind Signaturanwendungskomponenten erforderlich, die feststellen lassen, [...] zu welchem Ergebnis die Nachprüfung von Zertifikaten nach § 5 Abs. 1 Satz 2 geführt hat. [...].“ [§17 Abs. 2 Nr. 5 SigG] sowie „Signaturanwendungskomponenten nach § 17 Abs. 2 des Signaturgesetzes müssen gewährleisten, dass [...] bei der Prüfung einer qualifizierten elektronischen Signatur [...] eindeutig erkennbar wird, ob die nachgeprüften qualifizierten Zertifikate im jeweiligen Zertifikat-Verzeichnis zum angegebenen Zeitpunkt vorhanden und nicht gesperrt waren.“ [§ 15 Abs. 2 Nr. 2b SigV]

[21] vgl. „Signaturanwendungskomponenten nach § 17 Abs. 2 des Signaturgesetzes müssen gewährleisten, dass [...] bei der Prüfung einer qualifizierten elektronischen Signatur [...] die Korrektheit der Signatur zuverlässig geprüft und zutreffend angezeigt wird [...].“ [§ 15 Abs. 2 Nr. 2a SigV]

Sicherheitsanforderungen an Signaturanwendungskomponenten [BNetzA2005]	Umsetzung der Anforderungen aus SigG und SigV	
	in EVG	in der IT-Umgebung
Prüfung einer Signatur: Die Signaturanwendungskomponente muss beim Prüfen einer Signatur gewährleisten, dass	Verifikationsanwendung prüft qualifizierte elektronische Signaturen; Teilfunktionalitäten der Validierung erfolgen beim Verifikationsserver; Plausibilitätsprüfung bei Verifikationsanwendung und -server	
werden.”	Konfiguration der Verifikationsanwendung; Konfigurationsdaten der Verifikationsanwendung werden geschützt	den; für die Verifikationsanwendung muss der sichere Betrieb am Arbeitsplatz gewährleistet werden; zusätzliche Absicherung zum Integritätsschutz durch Prüftool

2.5 Produktbestandteile und EVG-Abgrenzung

56 Der Lieferumfang des EVG ist in Tabelle 2 aufgeführt:

Tabelle 2: Lieferumfang EVG

Liefergegenstand		Typ	Medium
Verifikationsanwendung	Anwendung (genaue Bezeichnung, Version 2.2.x.x, Datum, Größe)	Software	CD-ROM oder Archiv-Datei
	Benutzerhandbuch, Version 2.2.x.x, Datum	Dokumentation	
Verifikationsserver	Anwendung (genaue Bezeichnung, Version 2.2.x.x, Datum, Größe)	Software	CD-ROM oder Archiv-Datei
	Betriebshandbuch, Version 2.2.x.x, Datum	Dokumentation	

Liefergegenstand		Typ	Medium
Prüftool	Anwendung (genaue Bezeichnung, Version 2.2.x.x, Datum, Größe)	Software	CD-ROM oder Archiv-Datei
	Benutzerhandbuch, Version 2.2.x.x, Datum	Dokumentation	

57 Neben der in Tabelle 2 aufgeführten Software werden für den Betrieb des EVG folgende Komponenten benötigt, die somit die technische Einsatzumgebung definieren:

- geeignete Hard- und Software, auf der der EVG betrieben wird;
- qualifizierte Zertifikate;
- (System-)Zertifikat des OCSP/CRL-Relays zur Gewährleistung der Systemsicherheit;
- Download-Server für den Download der Verifikationsanwendung;
- Basiskomponente der Virtuellen Poststelle des Bundes (vgl. [bos_Basis-ST]).

Eine exakte Auflistung der technischen Einsatzumgebung findet sich im Anhang in Abschnitt 12.

2.6 Absicherung

58 Die Client-Komponente[22] des EVGs – d. h. die Verifikationsanwendung – selber sowie die Konfigurationsdaten der Verifikationsanwendung werden vor unbefugter Veränderung abgesichert, wie im Folgenden ausgeführt wird.

2.6.1 Integritätsschutz der Verifikationsanwendung

59 Die Verifikationsanwendung ist durch ein Prüftool zum Schutz vor unbefugter Veränderung (Integritätsschutz) abgesichert, das im Folgenden näher beschrieben wird.

- Das Prüftool überprüft die elektronische Signatur der JAR-Files der Verifikationsanwendung.
- Das Prüftool kennt die Dateinamen aller JAR-Files, die überprüft werden müssen.
- Die JAR-Files sind durch den Hersteller (vgl. Abschnitt 2.7) signiert. Die zugehörigen Zertifikate des Herstellers, die die öffentlichen Schlüssel zwecks Verifikation enthalten, sind im Prüftool enthalten.
- Dem Anwender wird zu jedem überprüften JAR-File der Dateiname, der Dateipfad, die Version, das jeweilige Prüfergebnis (Signatur korrekt, Sig-

[22] Hinsichtlich der Server-Komponente (Verifikationsserver) ist zu berücksichtigen, dass der Schutz vor unbefugter Veränderung durch bauliche und organisatorische Maßnahmen sichergestellt wird (vgl. A.ServerBetrieb).

natur nicht korrekt) sowie das Gesamtergebnis (Produktintegrität bestätigt, Produktintegrität nicht bestätigt) angezeigt. Entsprechende Hinweise und Maßnahmen für den Fall, dass die Produktintegrität nicht bestätigt werden kann, werden im Benutzerhandbuch beschrieben.

- Die Integritätsprüfung erfolgt bei gestarteter Verifikationsanwendung, d. h. im laufenden Betrieb.
- Den Dateipfad der JAR-Files ermittelt das Prüftool aus einem Übergabeparameter und dem in Java Web Start eingetragenen Pfad des Caches.
- Werden die JAR-Archive vom Prüftool nicht gefunden, kann der Anwender den/die Speicherort/e über den Java-File-Explorer auswählen.
- Darüber hinaus wird die JNLP (Java Network Launching Proctocol)-Datei, mit der die für die Verifikationsanwendung benötigten JAR-Archive von einer Web-Seite heruntergeladen werden können, über das Prüftool durch Hashwertvergleich abgesichert. Die entsprechenden JNLP-Dateien werden für den Integritätscheck vom Betreiber mit SHA-1 gehashed. Der Referenz-Hashwert wird dem Prüftool als Parameter übergeben.

60 Die technische Realisierung des Prüftools:

- Das Prüftool ist ein Java-Applet, das vom Hersteller signiert ist.
- Der Anwender benötigt die Java Virtual Machine und einen Browser.
- Genutzte Hashfunktion: SHA-1 (Mechanismenstärke „hoch“).
- Genutzter Verifikationsalgorithmus: RSA mit 1024 bzw. 2048 Bit[23] Schlüssellänge.

61 Für die Erzeugung der Signatur des Herstellers wird ein privater Schlüssel genutzt, der von einer Zertifizierungsinstanz für die bos KG zertifiziert wurde.

2.6.2 Schutz der Konfigurationsdaten der Verifikationsanwendung

62 Die Verifikationsanwendung wird ohne vorkonfigurierte Standardwerte vom Betreiber an den Benutzer ausgeliefert, d. h. der Benutzer konfiguriert die Verifikationsanwendung mit

- der Adresse des Verifikationsservers und
- dem Zertifikat des OCSP/CRL-Relays,

die im Dateisystem des Betriebssystem auf dem Rechner abgelegt werden, auf dem die Verifikationsanwendung betrieben wird.

63 Im Folgenden wird das Verfahren zum wirksamen Schutz der Konfigurationsdaten beschrieben, um sicherzustellen, dass der EVG jederzeit mit dem authentischen Zertifikat des OCSP/CRL-Relay arbeitet und somit der Anwender der Zertifikatstatusauskunft vertrauen kann.

64 **Erstellen der Konfigurationsdaten**

[23] Die Schlüssellänge richtet sich nach dem eingesetzten Zertifikat; Mindestlänge ist 1024 Bit.

65 Der Anwender startet den EVG und wird darauf hingewiesen, dass noch keine Konfiguration erstellt wurde. Der Anwender erstellt im Konfigurationsmenü die o. g. Konfigurationsdaten. Die authentischen Daten,

- Adresse des Verifikationsservers und
- Zertifikat des OCSP/CRL-Relay,

erhält der Anwender über den Betreiber (vgl. Abschnitt 2.7).

66 Nachdem der Anwender die Daten konfiguriert hat, wird er aufgefordert ein Passwort zum Schutz der Konfigurationsdaten einzugeben. Das Passwort wird über die Tastatur eingegeben. Das Passwort wird bei der Eingabe auf dem Bildschirm nur verdeckt durch einen „Dummy“ (Stern) für jedes eingegebene Passwortzeichen anstelle des ursprünglichen Zeichens angezeigt. Das Passwort muss einer vorgegebenen Passwortqualität bezüglich Länge (mind. 8 Zeichen) und Kombinatorik (keine trivialen Passwörter; mind. ein Zeichen pro Passwort, das kein Buchstabe ist) aufweisen. Weist das Passwort nicht die geforderte Passwortqualität auf, erhält der Anwender einen entsprechenden Hinweis und muss erneut ein Passwort eingeben. Entspricht das Passwort der geforderten Passwortqualität, erzeugt der EVG aus den Konfigurationsdaten und dem eingegebenen Passwort einen Hashwert mit der Hashfunktion SHA-1. Der Hashwert wird in einer Hashwertdatei und die Konfigurationsdaten in einer Konfigurationsdatei auf einem fest vorgegebenen File des Betriebssystems abgelegt. Das Passwort wird weder im EVG noch auf dem File dauerhaft abgespeichert. Der Speicherbereich, in dem das Passwort temporär gespeichert wurde, wird durch den EVG definiert überschrieben.

67 **Prüfen der Konfigurationsdaten**

68 Bei jedem Start des EVG werden Konfigurationsdatei und Hashwertdatei geladen. Kann eine der beiden Dateien nicht geladen werden, wird der Anwender darauf hingewiesen, dass noch keine Konfiguration erstellt wurde (s. o.). Sind beide Dateien geladen, wird der Benutzer aufgefordert, das Passwort einzugeben. Aus dem eingegebenen Passwort und der Konfigurationsdatei wird ein Hashwert (mit der Hashfunktion SHA-1) berechnet. Anschließend erfolgt ein Hashwertvergleich. Der EVG besitzt einen Fehlbedienungszähler (FBZ=3). Sind die Hashwerte nicht identisch, gilt folgendes:

- bei FBZ>1 muss der Anwender erneut das Passwort eingeben;
- bei FBZ=1 erhält der Anwender den Hinweis, dass er mit einer nicht authentischen Konfiguration arbeitet und die Konfiguration daher neu erstellen muss (s. o.).

Sind die Hashwerte identisch, arbeitet der Anwender mit einer authentischen Konfiguration; der EVG startet.

69 **Ändern der Konfigurationsdaten**

70 Eine Änderung der Konfigurationsdaten ist nur möglich, wenn das Prüfen der Konfigurationsdaten erfolgreich war (s. o.), d. h. wenn das Passwort korrekt eingegeben und der Hashwertvergleich erfolgreich durchgeführt wurde. Der Anwender kann dann ohne erneute Authentisierung die Konfiguration ändern,

wobei – wie oben ausgeführt – ein Passwort zum Schutz der Konfigurationsdaten einzugeben ist. Die Änderung wird sofort wirksam.

71 **Ändern des Passwortes**

72 Eine Änderung des Passwortes ist nur möglich, wenn das Prüfen der Konfigurationsdaten erfolgreich war (s. o.), d. h. wenn das Passwort korrekt eingegeben und der Hashwertvergleich erfolgreich durchgeführt wurde. Der Anwender kann dann ohne erneute Authentisierung das Passwort ändern. Die Änderung wird sofort wirksam. Ein Passwortwechsel wird durch den EVG nicht initiiert. Die Wiederholung alter Passwörter beim Passwortwechsel wird durch den EVG nicht verhindert (Passworthistorie).

2.7 Auslieferung

73 Die Auslieferung wird wie folgt durchgeführt, wobei an der Auslieferung Hersteller, Vertreiber, Betreiber sowie Benutzer beteiligt sind:

- Hersteller der Virtuellen Poststelle des Bundes, Version 2.2.X.X (Verifikationsmodul):

  bremen online services GmbH & Co. KG

  Am Fallturm 9

  28359 Bremen

  Der Hersteller liefert den EVG gemäß Auflistung in Tabelle 2 an den Vertreiber (s. u.) aus. Die Auslieferung erfolgt via CD-ROM oder online auf gesicherte Weise.

- Vertreiber der Virtuellen Poststelle des Bundes, Version 2.2.X.X (Verifikationsmodul):

  bremen online services GmbH & Co. KG

  Am Fallturm 9

  28359 Bremen

  Der Vertreiber erhält den EVG gemäß Auflistung in Tabelle 2 und reicht die erhaltene Auslieferung unverändert – d. h. via CD-ROM oder online – auf gesicherte Weise an den Betreiber weiter.

- Betreiber der Virtuellen Poststelle des Bundes, Version 2.2.X.X (Verifikationsmodul) sind beispielsweise Bundes- oder Landesbehörden.

  Der Betreiber erhält den EVG gemäß Auflistung in Tabelle 2 vom Vertreiber.

  Der Betreiber konfiguriert, installiert, administriert und betreibt den Verifikationsserver.

  Der Betreiber liefert die Verifikationsanwendung, das Prüftool und die zugehörige Dokumentation an den Benutzer aus. Die Auslieferung kann über ein Onlineverfahren (beispielsweise Java Web

Start) oder durch Zustellung einer einmal beschreibbaren CD-ROM auf gesicherte Weise erfolgen.

- Benutzer sind Anwender der Verifikationsanwendung und des Prüftools.

3 EVG-Sicherheitsumgebung

3.1 Rollen

74 Es gibt im Kontext des Verifikationsmoduls folgende Rollen, die hinsichtlich des Standortes differenziert werden:

75 serverseitig:

- **System-Administrator**: Ein System-Administrator ist für die Verwaltung und Organisation der grundlegenden IT-Infrastruktur zuständig, die für den EVG (Verifikationsserver) benötigt werden.[24] Typische Aktivitäten – mit dedizierter Rechtebeschränkung und Protokollierung – des System-Administrators sind:
  - Konfiguration, Betriebsüberwachung und Sicherung von Servern, Betriebssystem und Datenbank;
  - Konfiguration und Betriebsüberwachung der Netzwerkkomponenten.
- **Security-Administrator:** Der Security-Administrator ist für den EVG (Verifikationsserver) zuständig. Typische Aktivitäten – mit dedizierter Rechtebeschränkung, Protokollierung und Vier-Augen-Prinzip – des Security-Administrators sind:
  - Verwaltung (Hinzufügen, Update, Löschen) der unterschiedlichen Methoden, die der EVG zur Verfügung stellt (kryptographische Funktionen, Sicherheitsdienste, Anbindung externer Systeme);
  - Software-Updates (Einbringung von Patches, Austausch von Software-Komponenten);
  - Datensicherung (Initiieren, Prüfung des Resultats, Setzen, Ändern und Löschen von periodischen Abläufen);
  - System-Starts (Starten, Stoppen und Rücksetzen des EVGs).

  Darüber hinaus erstellt er die initiale Konfiguration für die Verifikationsanwendung.
- **Schlüssel-Administrator:** Der Schlüssel-Administrator verwaltet die in der Basiskomponente benötigten kryptographischen Schlüssel und (System-) Zertifikate zur Gewährleistung der Systemsicherheit. Der öffentliche Schlüssel des Zertifikats des OCSP/CRL-Relays wird dem Security-Administrator für die Vor-Konfiguration der Verifikationsanwendung sowie dem Benutzer zur Verfügung gestellt.
- **Revisor:** Der Revisor prüft beim EVG (Verifikationsserver) die Parameter (Adressinformationen zum Ansprechen des Kernsystems), konfiguriert die Protokollierung und wertet sie aus und begleitet den Security-Administra-

[24] Der System-Administrator kann beispielsweise ein Administrator bei einem Dienstleister sein, der die Systeme hostet.

tor zur Gewährleistung des Vier-Augen-Prinzips. Typische Aktivitäten des Revisors sind:

- Aufruf der Monitoring-Konsole zum Check des System-Status;
- Lesen von Teilen der Konfiguration; kein Ändern der Konfiguration.

76 clientseitig:

- **Benutzer:** Der Benutzer nutzt und konfiguriert die Verifikationsanwendung.

77 allgemein:

- **nicht autorisierte Person:** Eine nicht autorisierte Person ist jede Person, die weder System-, Security- oder Schlüssel-Administrator noch Revisor oder Benutzer ist.

3.2 Annahmen

78 Die in diesem Abschnitt aufgeführten Annahmen stellen die Auflagen für den Betrieb dar.

79 A.PKI Die für den Betrieb der Virtuellen Poststelle notwendigen Systemkomponenten der Public-Key-Infrastruktur (PKI) sind vorhanden:

- qualifizierte Zertifikate;
- (System-)Zertifikate (zur Gewährleistung der Systemsicherheit);
- Basiskomponente der Virtuellen Poststelle des Bundes für die Validierung von qualifizierten Zertifikaten (vgl. [bos_Basis-ST]).

  Dabei werden geeignete kryptographische Verfahren mit entsprechenden Schlüssellängen eingesetzt.

  Eine Verbindung zur Basiskomponente ist vorhanden.

  Eine Auflistung findet sich im Anhang in Abschnitt 12.

80 A.ServerBetrieb 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 der serverseitigen Komponenten des EVG (Verifikationsserver) sind vorhanden.

Es sind verschiedene Administratoren für die verschiedenen Aufgaben benannt, die einen Beitrag zur Sicherstellung einer vertraulichen und integren Betriebsumgebung des EVG leisten. Ein Vier-Augen-Prinzip mit Revisor ist für wichtige Aktivitäten organisatorisch realisiert.

Es wird gewährleistet, dass der EVG korrekt aufgebaut ist, inkl. Einhaltung der Vorgaben hinsichtlich der räumlichen Gegebenheiten 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 Sicherheitskonzept für die Kern- und Webkomponenten der Virtuellen Poststelle“ beschrieben werden [VPS-SiKo].

Die Anforderungen aus [BNetzA2005] an einen „geschützten Einsatzbereich (Regelfall/Standardlösung)“ 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“ hinsichtlich eines hohen Angriffspotentials abzuwehren:

- 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, geeignete Absicherung des LAN und durch die Verwendung geeigneter Anti-Viren-Programme;
- Auflagen zur Sicherheit der IT-Plattform und Applikationen: Es wird angenommen, dass gewährleistet wird, dass von der Hardware, auf der der EVG 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.
- Auflagen zum Schutz vor manuellem Zugriff Unbefugter und Datenaustausch per Datenträger: Es wird angenommen, dass die folgenden baulichen, personellen und organisatorischen Anforderungen umgesetzt sind:
    - Rechner, Monitor und Tastatur befinden sich in einem Betriebsraum.
    - Für die Administratoren müssen Vertreterregelungen für Krankheit und Urlaub bestehen.

- Wartungs- bzw. Reinigungspersonal erhält den Zugang zum zugriffssicheren Betriebsraum nur durch einen Administrator, der den Aufenthalt überwacht.
- Auslieferung, wie in Abschnitt 2.6 beschrieben.

81 A.ClientBetrieb Benutzer leisten einen Beitrag zur Sicherheit.

Es wird gewährleistet, dass der Rechner korrekt aufgebaut ist, inkl. Einhaltung der Vorgaben hinsichtlich der räumlichen Gegebenheiten und für die Realisierung der Netzwerkarchitektur mit Firewall etc. Vgl. dazu die Vorgaben und Auflagen zum Betrieb der Virtuellen Poststelle, die im „Generischen Sicherheitskonzept für die Kern- und Webkomponenten der Virtuellen Poststelle“ beschrieben werden [VPS-SiKo].

Die Anforderungen aus [BNetzA2005] an einen „geschützten Einsatzbereich (Regelfall/Standardlösung)“ 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“ hinsichtlich eines hohen Angriffspotentials abzuwehren:

- 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, und durch die Verwendung geeigneter Anti-Viren-Programme;
- Auflagen zur Sicherheit der IT-Plattform und Applikationen: Es wird angenommen, dass gewährleistet wird, dass von der Hardware, auf der der EVG 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, um Daten auszuforschen oder zu verändern.
- Auflagen zum Schutz vor manuellem Zugriff Unbefugter und Datenaustausch per Datenträger: Es wird angenommen, dass die folgenden baulichen, personellen und organisatorischen Anforderungen umgesetzt sind:

- Raum des Arbeitsplatzes: Es ist Sorge zu tragen, dass ein Zugriff Unbefugter ausgeschlossen ist oder zumindest mit hoher Sicherheit erkennbar wird – beispielsweise durch ein Sperren des Bildschirmes oder Verschließen des Büros bei Abwesenheit.
- Der Benutzer hat vor Gebrauch mit einem vom Hersteller zur Verfügung gestellten Prüftool die Integrität der Verifikationsanwendung zu prüfen – vgl. Abschnitt 2.6.
- Bei der Installation hat der Benutzer die Integrität und Authentizität der Verifikationsanwendung mit dem vom Hersteller zur Verfügung gestellten Prüftool zu prüfen – vgl. Abschnitt 2.6.

3.3 Bedrohungen

82 Bedrohungen ergeben sich implizit durch Nennung organisatorischer Sicherheitspolitiken.

3.4 Organisatorische Sicherheitspolitiken[25]

83 P.Anzeige Der EVG (hier: Verifikationsanwendung) muss gewährleisten, dass beim Prüfen einer Signatur

- 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, aufweist und
- erkennbar wird, ob die nachgeprüften qualifizierten Zertifikate im jeweiligen Zertifikatverzeichnis zum angegebenen Zeitpunkt vorhanden und nicht gesperrt waren.

  Darüber hinaus muss der EVG (hier: Verifikationsanwendung) gewährleisten, dass die Konfigurationsdaten (Adresse des Verifikationsservers sowie (System-) Zertifikat des OCSP/CRL-Relays) angezeigt werden können.

[25] Die für den EVG relevanten organisatorischen Sicherheitspolitiken ergeben sich aus den Anforderungen von Signaturgesetz und -verordnung (vgl. Abschnitt 2.4).

84 P.ValidZert Der EVG muss beim Prüfen einer Signatur gewährleisten, dass festgestellt wird, ob die nachgeprüften qualifizierten Zertifikate im jeweiligen Zertifikatverzeichnis zum angegebenen Zeitpunkt vorhanden und nicht gesperrt waren.

85 P.VerifySign Der EVG muss beim Prüfen einer Signatur gewährleisten, dass die Korrektheit der Signatur zuverlässig geprüft wird.

86 P.Manipulation Der EVG muss zum Schutz vor unbefugter Veränderung an der Verifikationsanwendung sowie den Konfigurationsdaten der Verifikationsanwendung gewährleisten, dass sicherheitstechnische Veränderungen festgestellt werden können.

Erklärung 1*Die organisatorischen Sicherheitspolitiken entstammen den für den EVG relevanten Anforderungen des Signaturgesetzes und der -verordnung, wie in [BNetzA2005] zusammenfassend dargestellt (vgl. Abschnitt 2.4.2 und Tabelle 1).*

4 Sicherheitsziele

4.1 EVG-Sicherheitsziele

87 O.Anzeige Der EVG (hier: Verifikationsanwendung) muss gewährleisten, dass dem Benutzer folgende Informationen angezeigt werden bzw. bei Bedarf – d. h. optional – angezeigt werden können:

- Bezug zu den Daten, auf die sich die Signatur bezieht;
- Ergebnis der Verifikation einer qualifizierten elektronischen Signatur;
- Ergebnis der Validierung eines qualifizierten Zertifikats;
- signierte Daten (optional);
- Signaturschlüssel-Inhaber der Signatur (optional);
- Zertifikatsinhalt (optional);
- Konfigurationsdaten mit Angabe der Adresse des Verifikationsservers sowie des (System-) Zertifikats des OCSP/CRL-Relays (optional).

Erklärung 2*Das Sicherheitsziel O.Anzeige deckt die organisatorische Sicherheitspolitik P.Anzeige zur sicheren und zuverlässigen Anzeige bei der Prüfung qualifizierter elektronischer Signaturen ab. Dabei wird durch die Verifikation festgestellt, ob die Daten unverändert sind. Die Anzeige umfasst nicht nur, was signiert wurde, sondern auch ergänzende Informationen zur Nachricht, wie Zertifikatsinhalt, Signaturschlüssel-Inhaber und Verifikations- und Validierungsergebnisse, sowie die Konfigurationsdaten.*

88 O.ValidZert Der EVG muss bei der Gültigkeitsprüfung eines qualifizierten Zertifikats

- die Funktionalitäten einer Basiskomponente[26] anfordern und Plausibilitätsprüfung (Prüfung, ob ein angegebener Prüfzeitpunkt in der Anfrage konsistent enthalten ist) durchführen (Verifikationsserver) und
- eine Plausibilitätsprüfung (Prüfung, ob das validierte Zertifikat zur Signatur gehört und ob der Zertifikatsstatus zu dem angefragten Prüfzeitpunkt ermittelt wurde.) sowie Verifikation des Validierungsergebnisses des OCSP/CRL-Relays (aus der Basiskomponente) bei der Verifikationsanwendung vornehmen.

Erklärung 3*Das Sicherheitsziel O.ValidZert deckt die organisatorische Sicherheitspolitik P.ValidZert zur Validierung qualifizierter Zertifikate ab und präzisiert die Aufgabenteilung. Zu berücksichtigen ist, dass die wesentlichen Aufgaben bei der Validierung in der IT-Umgebung durch die Basiskomponente (vgl. Sicherheitsziel für die IT-Umgebung OE.PKI) geleistet werden und dass zur Gewährleistung der Systemsicherheit (innerhalb des verteilten Systems) die Sicherheitsziele für die IT-Umgebung OE.ServerBetrieb und OE.ClientBetrieb benötigt werden.*

89 O.VerifySign Der EVG muss die mathematische Korrektheit einer qualifizierten elektronischen Signatur zuverlässig prüfen, indem folgende Prüfungen durchgeführt werden:

- Prüfung der Integrität: Der Hashwert des signierten Dokuments muss mit dem übermittelten Hashwert übereinstimmen.
- Prüfung der Authentizität: Dieser Hashwert muss gleich dem Ergebnis sein, das durch Anwendung des öffentlichen Signaturschlüssels auf die elektronische Signatur mit einem geeigneten kryptographischen Algorithmus berechnet wird.

Erklärung 4*Das Sicherheitsziel O.VerifySign deckt die organisatorische Sicherheitspolitik P.VerifySign zur Prüfung einer qualifizierten elektronischen Signatur ab und präzisiert, dass die Verifikation durch die Prüfung der Integrität und der Authentizität erfolgt (qualifizierte Zertifikate via Sicherheitsziel für die IT-Umgebung OE.PKI).*

90 O.Manipulation Der EVG muss zum Schutz vor unbefugter Veränderung an der Verifikationsanwendung sowie den Konfigurationsdaten der Verifikationsanwendung gewährleisten, dass durch Integritätsprüfung festgestellt werden kann, ob Veränderungen an der Verifikationsanwendung oder ihren Konfigurationsdaten vorgenommen wurden.

Erklärung 5*Das Sicherheitsziel O.Manipulation deckt die organisatorische Sicherheitspolitik P.Manipulation zum Schutz vor unbefugter Veränderung an der Verifikationsanwendung sowie ihren Konfigurationsdaten ab.*

[26] Wie bereits in Abschnitten 2.2 und 2.3 ausgeführt, wird die eigentliche Validierung von der Basiskomponente durchgeführt.

4.2 Sicherheitsziele für die Umgebung

91 Neben EVG-Sicherheitszielen sind Sicherheitsziele für die Umgebung notwendig, um die Sicherheit des EVG zu gewährleisten.

92 OE.PKI Die IT-Umgebung muss die für den Betrieb benötigten SigG-konformen Komponenten bereitstellen:

- qualifizierte Zertifikate mit geeigneten kryptographischen Parametern (Verfahren und Schlüssellängen);
- (System-)Zertifikate mit geeigneten kryptographischen Parametern (Verfahren und Schlüssellängen) zur Gewährleistung der Systemsicherheit;
- Basiskomponente der Virtuellen Poststelle des Bundes für die Validierung von qualifizierten Zertifikaten (vgl. [bos_Basis-ST]), in der die Gültigkeit eines qualifizierten Zertifikats zuverlässig festgestellt wird, indem für das angeforderte Zertifikat festgestellt wird, ob
  - das Zertifikat zum Prüfzeitpunkt (Eingang auf dem Server) vorhanden und nicht gesperrt war und
  - der Gültigkeitszeitraum des Zertifikats zum angegebenen Prüfzeitpunkt bereits begonnen und noch nicht abgelaufen war,

  und für die Zertifikate der Zertifikatskette festgestellt wird, ob
  - ein Ausstellerzertifikat zum Signierzeitpunkt des ausgestellten Zertifikats vorhanden und nicht gesperrt war und
  - der Gültigkeitszeitraum eines Ausstellerzertifikats zum Signierzeitpunkt des ausgestellten Zertifikats bereits begonnen und noch nicht abgelaufen war.

Erklärung 6*Das Sicherheitsziel für die Umgebung OE.PKI zielt auf die gleichnamige Annahme A.PKI ab, wobei zu berücksichtigen ist, dass OE.PKI auch für die organisatorischen Sicherheitspolitiken P.ValidZert (für die Gültigkeitsprüfung durch obige Funktionalitäten der Basiskomponenten, für die Existenz qualifizierter Zertifikate sowie die kryptographischen Schlüssel und (System-) Zertifikate zur Gewährleistung der Systemsicherheit) sowie P.VerifySign (für Existenz qualifizierter Zertifikate) benötigt werden.*

93 OE.ServerBetrieb Für den Betrieb muss vertrauenswürdiges Personal eingesetzt werden, das einen Beitrag zur Sicherheit leistet, und die notwendigen räumlichen Gegebenheiten sowie Hard- und Software für den sicheren Betrieb der serverseitigen Komponenten des EVG (Verifikationsserver) sind vorhanden.

Es müssen verschiedene Administratoren für die verschiedenen Aufgaben benannt sein, die einen Beitrag zur Sicherstellung einer vertraulichen und integren Betriebsumgebung des EVG leisten. Ein Vier-Augen-Prinzip mit Revisor muss für wichtige Aktivitäten organisatorisch realisiert sein.

Es muss gewährleistet sein, dass der EVG korrekt aufgebaut ist, inkl. Einhaltung der Vorgaben hinsichtlich der räumlichen Gegebenheiten 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 Sicherheitskonzept für die Kern- und Webkomponenten der Virtuellen Poststelle“ beschrieben werden [VPS-SiKo].

Die Anforderungen aus [BNetzA2005] an einen „geschützten Einsatzbereich (Regelfall/Standardlösung)“ müssen umgesetzt sein, 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“ hinsichtlich eines hohen Angriffspotentials abzuwehren:

- Auflagen zur Anbindung an das Internet/Intranet: Netzwerkverbindungen müssen so abgesichert sind, dass Angriffe erkannt bzw. unterbunden werden – z. B. durch eine geeignet konfigurierte Firewall, geeignete Absicherung des LAN und durch die Verwendung geeigneter Anti-Viren-Programme;
- Auflagen zur Sicherheit der IT-Plattform und Applikationen: Es muss gewährleistet sein, dass von der Hardware, auf der der EVG betrieben wird, keine Angriffe ausgehen. Insbesondere muss sichergestellt sein 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.
- Auflagen zum Schutz vor manuellem Zugriff Unbefugter und Datenaustausch per Datenträger: Die folgenden baulichen, personellen und organisatorischen Anforderungen müssen umgesetzt sein:

- Rechner, Monitor und Tastatur befinden sich in einem Betriebsraum.
- Für die Administratoren müssen Vertreterregelungen für Krankheit und Urlaub bestehen.
- Wartungs- bzw. Reinigungspersonal erhält den Zugang zum zugriffssicheren Betriebsraum nur durch einen Administrator, der den Aufenthalt überwacht.
- Auslieferung, wie in Abschnitt 2.6 beschrieben.

Erklärung 7*Das Sicherheitsziel für die Umgebung OE.ServerBetrieb zielt auf die gleichnamige Annahme A.ServerBetrieb ab und ist zur Realisierung der organisatorischen Sicherheitspolitik P.ValidZert (für die Gewährleistung der Systemsicherheit aufgrund der Realisierung der Validierung innerhalb des verteilten Systems) notwendig.*

94 OE.ClientBetrieb Für den Betrieb der Verifikationsanwendung muss der Benutzer einen Beitrag zur Sicherheit leisten.

Es muss gewährleistet sein, dass die Verifikationsanwendung korrekt aufgebaut ist, inkl. Einhaltung der Vorgaben hinsichtlich der räumlichen Gegebenheiten und für die Realisierung der Netzwerkarchitektur mit Firewall etc. Vgl. dazu die Vorgaben und Auflagen zum Betrieb der Virtuellen Poststelle, die im „Generischen Sicherheitskonzept für die Kern- und Webkomponenten der Virtuellen Poststelle“ beschrieben werden [VPS-SiKo].

Die Anforderungen aus [BNetzA2005] an einen „geschützten Einsatzbereich (Regelfall/Standardlösung)“ müssen umgesetzt sein, 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“ hinsichtlich eines hohen Angriffspotentials abzuwehren:

- Auflagen zur Anbindung an das Internet/Intranet: Netzwerkverbindungen müssen so abgesichert sein, dass Angriffe erkannt bzw. unterbunden werden – z. B. durch eine geeignet konfigurierte Firewall, und durch die Verwendung geeigneter Anti-Viren-Programme;
- Auflagen zur Sicherheit der IT-Plattform und Applikationen: Es muss gewährleistet sein, dass von der Hardware, auf der der EVG betrieben wird, keine Angriffe ausgehen. Insbesondere muss sichergestellt sein, 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, um Daten auszuforschen oder zu verändern.

- Auflagen zum Schutz vor manuellem Zugriff Unbefugter und Datenaustausch per Datenträger: Die folgenden baulichen, personellen und organisatorischen Anforderungen müssen umgesetzt sein:
  - Raum des Arbeitsplatzes: Es muss Sorge getragen werden, dass ein Zugriff Unbefugter ausgeschlossen ist oder zumindest mit hoher Sicherheit erkennbar wird – beispielsweise durch ein Sperren des Bildschirmes oder Verschließen des Büros bei Abwesenheit.
  - Der Benutzer hat vor Gebrauch mit einem vom Hersteller zur Verfügung gestellten Prüftool die Integrität der Verifikationsanwendung zu prüfen – vgl. Abschnitt 2.6.
  - Bei der Installation hat der Benutzer die Integrität und Authentizität der Verifikationsanwendung mit dem vom Hersteller zur Verfügung gestellten Prüftool zu prüfen – vgl. Abschnitt 2.6.

Erklärung 8*Das Sicherheitsziel für die Umgebung OE.ClientBetrieb zielt auf die gleichnamige Annahme A.ClientBetrieb ab und ist zur Realisierung der organisatorischen Sicherheitspolitik P.ValidZert (für die Gewährleistung der Systemsicherheit aufgrund der Realisierung der Validierung innerhalb des verteilten Systems – d. h. dem Management des (System-) Zertifikats in der Verifikationsanwendung zur Verifikation der Signatur des Validierungsergebnisses des OCSP/CRL-Relays) notwendig.*

5 IT-Sicherheitsanforderungen

5.1 EVG-Sicherheitsanforderungen

5.1.1 Funktionale EVG-Sicherheitsanforderungen

95 Die funktionalen Sicherheitsanforderungen sind zusammenfassend in Tabelle 3 aufgeführt und im Folgenden dargestellt. Die funktionalen EVG-Sicherheitsanforderungen entstammen überwiegend dem Teil 2 der CC [CC-Teil2]; eine EVG-Sicherheitsanforderung zur sicheren Anzeige ist explizit dargelegt (vgl. Abschnitt 9).

96 Die Notation der Sicherheitsanforderungen entspricht der in den Common Criteria vordefinierten semiformalen Sprache. In den Elementen ausgeführte Operationen Zuweisung und Auswahl sind **fett** dargestellt, während Verfeinerungen unterstrichen gedruckt sind.

Tabelle 3: Funktionale Sicherheitsanforderungen an den EVG

Funktionale Sicherheits-anforderung an den EVG	Beschreibung
FCS_COP.1 (Valid)	Kyptographischer Betrieb (für die kryptographische Operation „Verifizieren“ des Validierungsergebnisses)
FCS_COP.1 (Verify)	Kyptographischer Betrieb (für die kryptographische Operation „Verifizieren“ einer qualifizierten elektronischen Signatur)
FCS_COP.1 (Tool)	Kryptographischer Betrieb (für die kryptographische Operation „Verifikation“ im Rahmen des Prüftools)
FCS_COP.1 (Konfig)	Kryptographischer Betrieb (für die kryptographische Operation „Hashen“ im Rahmen der Absicherung der Konfigurationsdaten der Verifikationsanwendung)
FDP_SVR.1[27]	Sichere Anzeige
FDP_RIP.1	Teilweiser Schutz bei erhalten gebliebenen Informationen
FIA_UAU.7	Geschützte Authentisierungsrückmeldung
FIA_UAU.1	Zeitpunkt der Authentisierung (zum Schutz der Konfigurations-daten der Verifikationsanwendung)
FIA_UID.1	Zeitpunkt der Identifikation (zum Schutz der Konfigurationsda-ten der Verifikationsanwendung)

97 Im Folgenden werden die funktionalen Sicherheitsanforderungen für den EVG beschrieben.

98 **FCS_COP.1 (Valid) Kyptographischer Betrieb (für die kryptographische Operation „Verifizieren“ des Validierungsergebnisses)**

99 FCS_COP.1.1/Valid Die TSF müssen **im Rahmen der Gewährleistung der Systemsicherheit die kryptographische Operation „Verifizieren**“ gemäß eines spezifizierten kryptographischen Algorithmus **RSA im Zusammenhang mit der Hashfunktion SHA-1** und kryptographischer Schlüssellängen**, die entsprechend der X.509-Serverzertifikate derzeit 2048 Bit aufweisen**, die den folgenden **Normen [RSA] und [SHA-1]** [28] entsprechen, durchführen.

Erklärung 9*Die funktionale Sicherheitsanforderung FCS_COP.1 (Valid) wird für die Umsetzung des Sicherheitsziels O.ValidZert in der Weise benötigt,*

[27] Explizit dargelegte funktionale Anforderung (vgl. Abschnitt 9).

[28] Hinsichtlich des Paddings wird PKCS#1 [PKCS#1] umgesetzt.

dass die Verifikationsanwendung die Signatur des OCSP/CRL-Relays mit dem (System-)Zertifikat verifizieren muss.

Erklärung 10*Die Abhängigkeiten der funktionalen Sicherheitsanforderung FCS_COP.1 (Valid) – Schlüsselerzeugung gemäß FCS_CKM.1 oder Schlüsselimport gemäß FDP_ITC.1, Zerstörung eines Schlüssels gemäß FCS_CKM.4 und Schlüsselmanagement gemäß FMT_MSA.2) – sind in der IT-Umgebung einerseits hinsichtlich der initialen Konfiguration der Verifikationsanwendung durch den Security-Administrator auf Seiten des Betreibers und andererseits durch den Benutzer im Rahmen der Konfiguration der Verifikationsanwendung zu realisieren. Eine funktionale Sicherheitsanforderung FDP_ITC.1 ist für den EVG nicht notwendig, da vom EVG keine Zugriffskontroll- oder Informationsflusskontrolle durchgesetzt wird. Der EVG nutzt die in der IT-Umgebung verfügbaren Daten, ohne dafür eine dedizierte Prüfoperation durchzuführen; die Daten unterliegen keiner Benutzerkontrolle durch den EVG.*

100 **FCS_COP.1 (Verify) Kyptographischer Betrieb (für die kryptographische Operation „Verifizieren“ einer qualifizierten elektronischen Signatur)**

101 FCS_COP.1.1/Verify Die TSF müssen **für die Verifikation einer qualifizierten elektronischen Signatur die kryptographische Operation „Verifizieren**“ gemäß eines spezifizierten kryptographischen Algorithmus **RSA im Zusammenhang mit der Hashfunktion SHA-1** und kryptographischer Schlüssellängen**, die entsprechend der X.509-Zertifikate derzeit 1024 oder 2048 Bit aufweisen**, die den folgenden **Normen [RSA] und [SHA-1]28** entsprechen, durchführen.

Erklärung 11*Die funktionale Sicherheitsanforderung FCS_COP.1 (Verify) wird für die Umsetzung des Sicherheitsziels O.VerifySign benötigt.*

Erklärung 12*Die Abhängigkeiten der funktionalen Sicherheitsanforderung FCS_COP.1 (Verify) sind nicht erfüllt, da der für die Verifikation genutzte öffentliche Schlüssel aus dem Zertifikat – der zusammen mit der zu verifizierenden Signatur mitgeliefert wird – eine öffentlich Information ist und kein Sicherheitsattribut darstellt (keine Schlüsselerzeugung gemäß FCS_CKM.1, kein Schlüsselimport gemäß FDP_ITC.1 , keine Zerstörung eines Schlüssels gemäß FCS_CKM.4, kein Schlüsselmanagement gemäß FMT_MSA.2).*

102 **FCS_COP.1 (Tool) Kryptographischer Betrieb (für die kryptographische Operation „Verifizieren“ im Rahmen des Prüftools)**

103 FCS_COP.1.1/Tool Die TSF müssen **im Zusammenhang mit dem Prüftool die kryptographische Operation „Verifizieren**“ gemäß eines spezifizierten kryptographischen Algorithmus **RSA im Zusammenhang mit der Hashfunktion SHA-1** und kryptographischer Schlüssellängen**, die 1024 bzw. 2048 Bit aufweisen**, die den folgenden **Normen [RSA] und [SHA-1]28** entsprechen, durchführen.

Erklärung 13*Die funktionale Sicherheitsanforderung FCS_COP.1 (Tool) wird für die Umsetzung des Sicherheitsziels O.Manipulation hinsichtlich des Integritätsschutzes der Verifikationsanwendung benötigt.*

Erklärung 14*Die Abhängigkeiten der funktionalen Sicherheitsanforderung FCS_COP.1 (Tool) – Schlüsselimport gemäß FDP_ITC.1 oder Schlüsselerzeugung gemäß FCS_CKM.1, Zerstörung eines Schlüssels gemäß FCS_CKM.4 und Schlüsselmanagement gemäß FMT_MSA.2) – sind in der IT-Umgebung für das Prüftool zu realisieren, da die für die Prüfung notwendigen Zertifikate vom Hersteller in das Tool eingebracht – d. h. Teil der Implementierung sind – und mit dem Tool ausgeliefert werden; ein Management von Seiten des Benutzers des Tools ist nicht möglich.*

104 **FCS_COP.1 (Konfig) Kryptographischer Betrieb (für die kryptographische Operation „Hashen“ im Rahmen der Absicherung der Konfigurationsdaten der Verifikationsanwendung)**

105 FCS_COP.1.1/Konfig Die TSF müssen **im Zusammenhang mit der Absicherung der Konfigurationsdaten der Verifikationsanwendung die kryptographische Operation „Hashen**“ gemäß eines spezifizierten kryptographischen Algorithmus **SHA-1** und kryptographischer Schlüssellängen**, die bei einer Hashfunktion nicht relevant sind**, die der folgenden **Norm [SHA-1]** entspricht, durchführen.

Erklärung 15*Die funktionale Sicherheitsanforderung FCS_COP.1 (Konfig) wird für die Umsetzung des Sicherheitsziels O.Manipulation hinsichtlich des Integritätsschutzes der Konfigurationsdaten der Verifikationsanwendung benötigt.*

Erklärung 16*Die Abhängigkeiten der funktionalen Sicherheitsanforderung FCS_COP.1 (Konfig) sind nicht erfüllt, da keine Schlüssel involviert sind (weder Schlüsselerzeugung gemäß FCS_CKM.1 oder Schlüsselimport gemäß FDP_ITC.1 noch Zerstörung eines Schlüssels gemäß FCS_CKM.4) und daher kein Schlüsselmanagement gemäß FMT_MSA.2 notwendig ist.*

106 **FDP_SVR.1 Sichere Anzeige**

107 FDP_SVR.1.1 Die TSF müssen sicherstellen, dass der dem Benutzer angezeigte Inhalt eines Dokumentes (also die signierten Daten) entsprechend der folgenden Norm **plain-text (UTF-8-codiert) und tiff** sowie der Bezug zu den Daten, auf die sich die Signatur bezieht, das Ergebnis der Verifikation einer qualifizierten elektronischen Signatur, das Ergebnis der Validierung eines qualifizierten Zertifikats, den Signaturschlüssel-Inhaber der Signatur (optional[29]), den Zertifikatsinhalt (optional) und die Konfigurationsdaten (optional) eindeutig ist.

108 FDP_SVR.1.2 Die TSF müssen sicherstellen, dass der dem Benutzer anzuzeigende Inhalt eines Dokumentes frei von aktiven oder verdeckten Inhalten ist. Die TSF müssen sicherstellen, dass der Benutzer darüber informiert wird.

109 FDP_SVR.1.3 Die TSF müssen sicherstellen, dass der Benutzer über einen nicht darstellbaren Inhalt eines anzuzeigenden Dokumentes informiert wird.

Erklärung 17*Die funktionale Sicherheitsanforderung FDP_SVR.1 wird für die Umsetzung des Sicherheitsziels O.Anzeige benötigt.*

Erklärung 18*FDP_SVR.1 hat keine Abhängigkeiten.*

110 **FDP_RIP.1 Teilweiser Schutz bei erhalten gebliebenen Informationen**

111 FDP_RIP.1.1 Die TSF müssen sicherstellen, daß der frühere Informationsinhalt eines Betriebsmittels bei **Wiederfreigabe eines Betriebsmittels von** folgenden Objekten: **Passwort** nicht verfügbar ist.

Erklärung 19*Die funktionale Sicherheitsanforderung FDP_RIP.1 wird für die Umsetzung des Sicherheitsziels O.Manipulation hinsichtlich des Integritätsschutzes der Konfigurationsdaten der Verifikationsanwendung in der Weise benötigt, dass das vom Benutzer eingegebene Passwort vom EVG gelöscht wird (und nicht persistent erhalten bleibt).*

Erklärung 20*FDP_RIP.1 hat keine Abhängigkeiten.*

[29] „Optional“ bedeutet, dass sich der Benutzer die als optional gekennzeichneten Informationen bei Bedarf anzeigen lassen kann. Die TSF stellen sicher, dass die Darstellung dieser Informationen eindeutig ist.

112 **FIA_UAU.7 Geschützte Authentisierungsrückmeldung**

113 FIA_UAU.7.1 Die TSF müssen sicherstellen, daß während der Authentisierung nur **Sterne (ein Stern für jedes eingegebene Passwortzeichen anstelle des ursprünglichen Zeichens)** an den Benutzer bereitgestellt werden.

Erklärung 21*Die funktionale Sicherheitsanforderung FIA_UAU.7 wird für die Umsetzung des Sicherheitsziels O.Manipulation hinsichtlich des Integritätsschutzes der Konfigurationsdaten der Verifikationsanwendung in der Weise benötigt, dass das Passwort bei der Eingabe auf dem Bildschirm nur verdeckt durch einen Stern als „Dummy" für jedes eingegebene Passwortzeichen anstelle des ursprünglichen Zeichens angezeigt wird.*

Erklärung 22*FIA_UAU.7 hat die Abhängigkeit FIA_UAU.1.*

114 **FIA_UAU.1 Zeitpunkt der Authentisierung (zum Schutz der Konfigurationsdaten der Verifikationsanwendung)**

115 FIA_UAU.1.1 Die TSF müssen zum Schutz der Konfigurationsdaten der Verifikationsanwendung die Ausführung der **Erstellung der Konfigurationsdaten** für den Benutzer (hier: Benutzer der Verifikationsanwendung) erlauben, bevor dieser authentisiert wird (im Rahmen der Erstellung der Konfigurationsdaten wird das Passwort erst festgelegt).

116 FIA_UAU.1.2 Die TSF müssen zum Schutz der Konfigurationsdaten der Verifikationsanwendung erfordern, daß jeder Benutzer (hier: Benutzer der Verifikationsanwendung) erfolgreich authentisiert wurde, bevor diesem jegliche andere TSF-vermittelte Aktionen zum Schutz der Konfigurationsdaten der Verifikationsanwendung erlaubt werden (explizit muss jeder Benutzer ein Passwort eingeben zum Prüfen der Konfigurationsdaten beim Starten der Verifikationsanwendung, zum Ändern der Konfigurationsdaten und zum Ändern des Passwortes).

Erklärung 23*Die funktionale Sicherheitsanforderung FIA_UAU.1 ergibt sich aus der Abhängigkeit von FIA_UAU.7. FIA_UAU.1 wird damit implizit für die Umsetzung des Sicherheitsziels O.Manipulation hinsichtlich des Integritätsschutzes der Konfigurationsdaten der Verifikationsanwendung mittels Passworteingabe benötigt, wobei für die folgenden Aktionen zum Schutz der Konfigurationsdaten eine Passworteingabe erforderlich ist: Prüfen der Konfigurationsdaten beim Starten der Verifikationsanwendung, Ändern der Konfigurationsdaten, Ändern des Passwortes. Die Erstellung der Konfigurationsdaten ist ohne Passworteingabe möglich, wobei der Benutzer der Verifikationsanwendung hierzu die authentischen Konfigurationsdaten (Adresse des Verifikationsservers sowie (System-)Zertifikat des OCSP/CRL-Relays als Trust Anchor) benötigt (vgl. Abschnitt 2.6.2) .*

Erklärung 24*FIA_UAU.1 hat die Abhängigkeit FIA_UID.1.*

117 **FIA_UID.1 Zeitpunkt der Identifikation (zum Schutz der Konfigurationsdaten der Verifikationsanwendung)**

118 FIA_UID.1.1 Die TSF müssen zum Schutz der Konfigurationsdaten der Verifikationsanwendung die Ausführung der **Erstellung der Konfigurationsdaten** für den Benutzer (hier: Benutzer der Verifikationsanwendung) erlauben, bevor dieser identifiziert wird (im Rahmen der Erstellung der Konfigurationsdaten wird das Passwort erst festgelegt).

119 FIA_UID.1.2 Die TSF müssen zum Schutz der Konfigurationsdaten der Verifikationsanwendung erfordern, daß jeder Benutzer (hier: Benutzer der Verifikationsanwendung) erfolgreich identifiziert wurde, bevor diesem jegliche andere TSF-vermittelte Aktionen zum Schutz der Konfigurationsdaten der Verifikationsanwendung erlaubt werden (explizit muss jeder Benutzer ein Passwort eingeben zum Prüfen der Konfigurationsdaten beim Starten der Verifikationsanwendung, zum Ändern der Konfigurationsdaten und zum Ändern des Passwortes).

Erklärung 25*Die funktionale Sicherheitsanforderung FIA_UID.1 ergibt sich aus der Abhängigkeit von FIA_UAU.1. FIA_UID.1 wird damit implizit für die Umsetzung des Sicherheitsziels O.Manipulation hinsichtlich des Integritätsschutzes der Konfigurationsdaten der Verifikationsanwendung mittels Passworteingabe benötigt, wobei für die folgenden Aktionen zum Schutz der Konfigurationsdaten eine Passworteingabe erforderlich ist: Prüfen der Konfigurationsdaten beim Starten der Verifikationsanwendung, Ändern der Konfigurationsdaten, Ändern des Passwortes. Die Erstellung der Konfigurationsdaten ist ohne Passworteingabe möglich, wobei der Benutzer der Verifikationsanwendung hierzu die authentischen Konfigurationsdaten (Adresse des Verifikationsservers sowie (System-)Zertifikat des OCSP/CRL-Relays als Trust Anchor) benötigt (vgl. Abschnitt 2.6.2).*

Erklärung 26*FIA_UID.1 hat keine Abhängigkeiten.*

5.1.2 Anforderungen an die Vertrauenswürdigkeit des EVG

120 Die Anforderungen an die Vertrauenswürdigkeit des EVG sind in Tabelle 4 aufgeführt und genügen den in Abschnitt 1.3 beschriebenen Anforderungen.

121 Als Mindest-Stärke der Sicherheitsmechanismen des EVG wird SOF-hoch postuliert.

Tabelle 4: Vertrauenswürdigkeitskomponenten

Vertrauenswürdigkeitsklasse	Vertrauenswürdigkeitskomponente	
Konfigurationsmanagement	ACM_CAP.3	Autorisierungskontrolle
	ACM_SCP.1	EVG-CM-Umfang
Auslieferung und Betrieb	ADO_DEL.2	Erkennung von Modifizierungen
	ADO_IGS.1	Installations-, Generierungs- und Anlaufprozeduren
Entwicklung	ADV_FSP.1	Informelle funktionale Spezifikation
	ADV_HLD.2	Sicherheitsspezifischer Entwurf auf hoher Ebene
	ADV_IMP.1	Teilmenge der Implementierung der TSF
	ADV_LLD.1	Beschreibender Entwurf auf niedriger Ebene
	ADV_RCR.1	Informeller Nachweis der Übereinstimmung
Handbücher	AGD_ADM.1	Systemverwalterhandbuch
	AGD_USR.1	Benutzerhandbuch
Lebenszyklus-Unterstützung	ALC_DVS.1	Identifikation der Sicherheitsmaßnahmen
	ALC_TAT.1	Klar festgelegte Entwicklungswerkzeuge
Testen	ATE_COV.2	Analyse der Testabdeckung
	ATE_DPT.1	Testen – Entwurf auf hoher Ebene
	ATE_FUN.1	Funktionales Testen
	ATE_IND.2	Unabhängiges Testen – Stichprobenartig
Schwachstellenbewertung	AVA_MSU.3	Analysieren und Testen auf unsichere Zustände
	AVA_SOF.1	Stärke der EVG-Sicherheitsfunktionen
	AVA_VLA.4	Hohe Widerstandsfähigkeit

5.2 Sicherheitsanforderungen an die IT-Umgebung

122 Die funktionalen Sicherheitsanforderungen an die IT-Umgebung sind zusammenfassend in Tabelle 5 aufgeführt und im Folgenden aufgeführt bzw. referenziert. Die funktionalen EVG-Sicherheitsanforderungen entstammen dem Teil 2 der CC [CC-Teil2].

Tabelle 5: Funktionale Sicherheitsanforderungen an die IT-Umgebung

Funktionale Sicherheitsanforderung an die IT-Umgebung	Beschreibung
FCS_CKM.1[30]	Kryptographische Schlüsselgenerierung

Funktionale Sicherheits-anforderung an die IT-Umgebung	Beschreibung
FDP_ITC.130	Import von Benutzerdaten ohne Sicherheitsattribute
FCS_CKM.4	Zerstörung des kryptographischen Schlüssels
FMT_MSA.2	Sichere Sicherheitsattribute
FCO_NRO.1	Selektiver Urheberschaftsbeweis (vgl. [bos_Basis-ST])
FCS_CKM.4	Zerstörung des kryptographischen Schlüssels (vgl. [bos_Basis-ST])
FCS_COP.1 (Verify)	Kyptographischer Betrieb (für die kryptographische Operation „Verifizieren“ einer qualifizierten elektronischen Signatur) (vgl. [bos_Basis-ST])
FCS_COP.1 (SVVE[31])	Kyptographischer Betrieb (für die Erzeugung einer elektronischen Signatur für Verifikations- und Validierungsergebnisse) (vgl. [bos_Basis-ST])
FCS_COP.1 (VVE[32])	Kyptographischer Betrieb (für die Verifikation eines Validierungsergebnisses) (vgl. [bos_Basis-ST])
FDP_ACC.1 (Sys)	Teilweise Zugriffskontrolle (Systemsicherheit-Zugriffskontrollpolitik) (vgl. [bos_Basis-ST])
FDP_ACF.1 (Sys)	Zugriffskontrolle basierend auf Sicherheitsattributen (Systemsicherheit-Zugriffskontrollpolitik) (vgl. [bos_Basis-ST])
FDP_ITC.1	Import von Benutzerdaten ohne Sicherheitsattribute (vgl. [bos_Basis-ST])
FIA_UID.2	Benutzeridentifikation vor jeglicher Aktion (vgl. [bos_Basis-ST])
FMT_MSA.1 (Sys)	Management der Sicherheitsattribute (Systemsicherheit-Zugriffskontrollpolitik) (vgl. [bos_Basis-ST])
FMT_MSA.2	Sichere Sicherheitsattribute (vgl. [bos_Basis-ST])
FMT_MSA.3 (Sys)	Initialisierung statischer Attribute (Systemsicherheit -Zugriffskontrollpolitik) (vgl. [bos_Basis-ST])
FMT_SMR.1 (Sys)	Sicherheitsrollen (Systemsicherheit -Zugriffskontrollpolitik) (vgl. [bos_Basis-ST])

123 **FCS_CKM.130 Kryptographische Schlüsselgenerierung**

[30] In der IT-Umgebung ist zu realisieren, ob Schlüssel generiert (FCS_CKM.1) oder Schlüssel importiert (FDP_ITC.1) werden.

[31] Signieren von Verifikations- und Validierungs-Ergebnissen

[32] Verifizieren eines Validierungs-Ergebnisses

124 FCS_CKM.1.1 Die Sicherheitsfunktionen in der IT-Umgebung müssen die kryptographischen Schlüssel gemäß eines spezifizierten Algorithmus zur kryptographischen Schlüsselgenerierung **mit einem geeigneten Algorithmus zur kryptographischen Schlüsselgenerierung** und spezifizierte kryptographische Schlüssellängen**, die 2048 Bit aufweisen**, die den folgenden **Normen [RSA] und [SHA-1]28** entsprechen, generieren.

125 **FDP_ITC.130 Import von Benutzerdaten ohne Sicherheitsattribute**

126 FDP_ITC.1.1 Die Sicherheitsfunktionen in der IT-Umgebung müssen eine **SFP für Zugriffskontrolle und/oder Informationsflußkontrolle in der IT-Umgebung** beim Import von unter Kontrolle der SFP stehenden Benutzerdaten von außerhalb des TSC durchsetzen.

127 FDP_ITC.1.2 Die Sicherheitsfunktionen in der IT-Umgebung müssen die mit den Benutzerdaten verknüpften Sicherheitsattribute ignorieren, wenn diese von außerhalb des TSC importiert werden.

128 FDP_ITC.1.3 Die Sicherheitsfunktionen in der IT-Umgebung müssen die folgenden Regeln beim Import unter Kontrolle der SFP stehender Benutzerdaten von außerhalb des TSC durchsetzen: **zusätzliche Importkontrollregeln, sofern in der IT-Umgebung notwendig**.

129 FCS_CKM.4 Zerstörung des kryptographischen Schlüssels

130 FCS_CKM.4.1 Die Sicherheitsfunktionen in der IT-Umgebung müssen die kryptographischen Schlüssel nach einer spezifizierten Methode zur Zerstörung des kryptographischen Schlüssels **durch Löschen bzw. Entfernen aus entsprechendem Verzeichnis oder einen anderen geeigneten Mechanismus**, die […] **keiner speziellen Norm** entspricht, zerstören.

131 FMT_MSA.2 Sichere Sicherheitsattribute

132 FMT_MSA.2.1 Die Sicherheitsfunktionen in der IT-Umgebung müssen sicherstellen, daß nur sichere Werte für Sicherheitsattribute akzeptiert werden.

Erklärung 27*Die drei funktionalen Sicherheitsanforderungen an die IT-Umgebung – FCS_CKM.1 oder FDP_ITC.1 sowie FCS_CKM.4 und FMT_MSA.2 – ergeben sich aus den Abhängigkeiten zu FCS_COP.1 (Valid) und FCS_COP.1 (Tool) und damit implizit aus den Sicherheitszielen O.ValidZert und O.Manipulation. Die Ausgestaltung der Operationen der funktionalen Sicherheitsanforderungen sowie die Abhängigkeiten dieser Anforderungen sind in der IT-Umgebung zu realisieren, da Schlüsselerzeugung, -import und -löschung sowie Management der Sicherheitsattribute in der IT-Umgebung außerhalb des EVG liegt.*

Erklärung 28*Die in Tabelle 5 referenzierten funktionalen Sicherheitsanforderungen an die IT-Umgebung FCO_NRO.1, FCS_CKM.4, FCS_COP.1 (Verify), FCS_COP.1 (SVVE), FCS_COP.1 (VVE), FDP_ACC.1 (Sys), FDP_ACF.1 (Sys), FDP_ITC.1, FIA_UID.2, FMT_MSA.1 (Sys), FMT_MSA.2,*

FMT_MSA.3 (Sys) und FMT_SMR.1 (Sys) lassen sich auf das Sicherheitsziel der IT-Umgebung OE.PKI hinsichtlich der Validierung qualifizierter Zertifikate, für die die Basiskomponente der Virtuellen Poststelle des Bundes (vgl. [bos_Basis-ST]) benötigt wird, zurückführen.

5.3 Sicherheitsanforderungen an die Nicht-IT-Umgebung

133 Sicherheitsanforderungen an die Nicht-IT-Umgebung werden nicht formuliert.

6 EVG-Übersichtsspezifikation

134 In diesem Abschnitt werden die EVG-Sicherheitsfunktionen (TSF – TOE Security Functions) dargestellt, die vom EVG zur Verfügung gestellt werden:

SF1 Verifikation einer qualifizierten elektronischen Signatur;

SF2 Verifikation einer OCSP/CRL-Relay-Antwort bei der Validierung eines qualifizierten Zertifikats;

SF3 Sichere und zuverlässige Anzeige;

SF4 Prüftool

SF5 Schutz der Konfigurationsdaten

6.1 SF1 – Verifikation einer qualifizierten elektronischen Signatur

135 Die Sicherheitsfunktion SF1 „Verifikation einer qualifizierten elektronischen Signatur“ ist wie folgt definiert:

- Die Verifikationsanwendung verifiziert eine qualifizierte elektronische Signatur.
- Die Verifikation nutzt neben der qualifizierten elektronischen Signatur das mitgelieferte zugehörige Zertifikat mit dem Prüfschlüssel sowie den Verifikationsalgorithmus RSA und die Hashfunktion SHA-1. Benutzte Schlüssellängen sind entsprechend der X.509-Zertifikate derzeit 1024 oder 2048 Bit.
- Die Verifikationsanwendung zeigt das Verifikationsergebnis via SF3 an.

6.2 SF2 – Verifikation einer OCSP/CRL-Relay-Antwort bei der Validierung eines qualifizierten Zertifikats

136 Die Sicherheitsfunktion SF2 „Verifikation einer OCSP/CRL-Relay-Antwort bei der Validierung eines qualifizierten Zertifikats“ ist wie folgt definiert:[33]

- bei der Verifikationsanwendung:

[33] Verifikationsanwendung und -server validieren nicht selber, sondern nutzen das Ergebnis der Validierung vom OCSP/CRL-Relay, welches mit einer elektronischen Signatur versehen ist.

- Die Verifikationsanwendung verifiziert die elektronische Signatur des Validierungsergebnisses mit dem (System-)Zertifikat des OCSP/CRL-Relays.
- Die Verifikationsanwendung führt einen Plausibilitätscheck durch, in der geprüft wird, ob das Ergebnis der Zertifikats-Statusprüfung zum Zertifikat der zu prüfenden Signatur passt. Es wird zusätzlich geprüft, ob tatsächlich zum angefragten Prüfzeitpunkt geprüft wurde.
- Die Verifikationsanwendung zeigt das Validierungsergebnis via SF3 an.

- beim Verifikationsserver:
  - Der Verifikationsserver greift für die Statusprüfung eines qualifizierten Zertifikats – auf Anforderung der Verifikationsanwendung – auf eine Basiskomponente in der IT-Umgebung zu, wobei der Verifikationsserver zusammen mit dem Kernsystem der Basiskomponente innerhalb eines vertrauenswürdigen Netzes betrieben wird.
  - Sofern in der Anforderung der Verifikationsanwendung ein Prüfzeitpunkt angegeben ist, führt der Verifikationsserver einen Plausibilitätscheck durch, bei dem geprüft wird, ob der Prüfzeitpunkt konsistent angegeben ist. Sind die Werte konsistent, wird fortgefahren, andernfalls wird eine Fehlermeldung an die Verifikationsanwendung gesendet.
  - Der Verifikationsserver sendet einen Request an das Kernsystem – der Request umfasst neben dem nachzuprüfenden Zertifikat die SystemID (Identifier des anfragenden Systems) des Verifikationsservers sowie die OperationID (Identifier der auszuführenden Operation) für das Validieren – und empfängt das Response mit dem Validierungsergebnis.
  - Anschließend übergibt der Verifikationsserver das Validierungsergebnis an die Verifikationsanwendung.

6.3 SF3 – Sichere und zuverlässige Anzeige

137 Die Sicherheitsfunktion SF3 „Sichere und zuverlässige Anzeige“ ist wie folgt definiert:

- Die Verifikationsanwendung bietet eine sichere Anzeige von folgenden signierten Daten:
  - plain-text (UTF-8-codiert);
  - tiff-Daten.
- Darüber hinaus bietet die Verifikationsanwendung eine sichere Anzeige weiterer signaturrelevanten Informationen;
  - Verweis, auf welche Daten sich eine Signatur bezieht;

- der Signatur zugeordnete Signaturschlüssel-Inhaber;
- Inhalte des zugehörigen qualifizierten Zertifikats.

- Die Verifikationsanwendung bietet des Weiteren hinreichende Anzeigen für folgende Prozesse:
  - Verifikationsprozess: Das Ergebnis der Verifikation wird angezeigt, d. h. es wird angezeigt, ob Daten unverändert sind.
  - Validierungsprozess: Das Ergebnis der Validierung wird angezeigt, d. h. es wird angezeigt, ob die nachgeprüften qualifizierten Zertifikate im jeweiligen Zertifikatverzeichnis zum angegebenen Zeitpunkt vorhanden und nicht gesperrt waren.
- Die Verifikationsanwendung bietet eine Anzeige der folgenden Konfigurationsparameter:
  - Adresse des Verifikationsservers mit Proxy-Information;
  - (System-)Zertifikat des OCSP/CRL-Relays.

6.4 SF4 – Prüftool

138 Die Sicherheitsfunktion SF4 „Prüftool“ zur Gewährleistung der Integrität der Verifikationsanwendung ist wie folgt definiert:

- Das Prüftool überprüft die elektronische Signatur der JAR-Files der Verifikationsanwendung.[34]
- Die zugehörigen Zertifikate des Herstellers, die die öffentlichen Schlüssel zwecks Verifikation enthalten, sind im Prüftool enthalten.
- Das Prüftool kennt die Dateinamen aller JAR-Files, die überprüft werden müssen.
- Dem Anwender wird zu jedem überprüften JAR-File der Dateiname, der Dateipfad, die Version, das jeweilige Prüfergebnis (Signatur korrekt, Signatur nicht korrekt) sowie das Gesamtergebnis (Produktintegrität bestätigt, Produktintegrität nicht bestätigt) angezeigt.
- Den Dateipfad der JAR-Files ermittelt das Prüftool aus einem Übergabeparameter und dem in Java Web Start eingetragenen Pfad des Caches.
- Werden die JAR-Archive vom Prüftool nicht gefunden, kann der Anwender den/die Speicherort/e über den Java-File-Explorer auswählen.
- Darüber hinaus wird die JNLP (Java Network Launching Proctocol)-Datei, mit der die für die Verifikationsanwendung benötigten JAR-Archive von einer Web-Seite heruntergeladen werden können, über das Prüftool durch Hashwertvergleich abgesichert. Die entsprechenden JNLP-Dateien werden für den Integritätscheck vom Betreiber mit SHA-1 gehashed. Der Referenz-Hashwert wird dem Prüftool als Parameter übergeben.

[34] Dazu wird die Verifikationsanwendung als signiertes JAR-Archiv ausgeliefert, vgl. Abschnitt 2.6.

139 Das Prüftool ist ein Java-Applet, das vom Hersteller signiert ist. Genutzte Hashfunktion ist SHA-1 (Mechanismenstärke „hoch“), genutzter Verifikationsalgorithmus ist RSA mit 1024 bzw. 2048 Bit23 Schlüssellänge.

6.5 SF5 – Schutz der Konfigurationsdaten

140 Die Sicherheitsfunktion SF5 „Schutz der Konfigurationsdaten“ zur Gewährleistung der Integrität der Konfigurationsdaten der Verifikationsanwendung,

- Adresse des Verifikationsservers,
- Zertifikat des OCSP/CRL-Relays,

ist wie folgt definiert (vgl. auch Abschnitt 2.6):

- Erstellen der Konfigurationsdaten

  Der Anwender startet den EVG und wird darauf hingewiesen, dass noch keine Konfiguration erstellt wurde. Der Anwender erstellt im Konfigurationsmenü die o. g. Konfigurationsdaten. Nachdem der Anwender die Daten konfiguriert hat, wird er aufgefordert ein Passwort zum Schutz der Konfigurationsdaten einzugeben. Das Passwort wird über die Tastatur eingegeben.

  Das Passwort wird bei der Eingabe auf dem Bildschirm nur verdeckt durch einen „Dummy“ (Stern) für jedes eingegebene Passwortzeichen anstelle des ursprünglichen Zeichens angezeigt.

  Das Passwort muss einer vorgegebenen Passwortqualität bezüglich Länge (mind. 8 Zeichen) und Kombinatorik (keine trivialen Passwörter; mind. ein Zeichen pro Passwort, das kein Buchstabe ist) aufweisen. Weist das Passwort nicht die geforderte Passwortqualität auf, erhält der Anwender einen entsprechenden Hinweis und muss erneut ein Passwort eingeben. Zur Güte des Passwortes realisiert der EVG:

  - keine Trivialpasswörter (z. B. „BBBBBBBB“ oder „12345678“);
  - mindestens ein Zeichen pro Passwort, das kein Buchstabe ist (Sonderzeichen oder Zahl);
  - mindestens 8 Zeichen lang.

  Entspricht das Passwort der geforderten Passwortqualität, erzeugt der EVG aus den Konfigurationsdaten und dem eingegebenen Passwort einen Hashwert der Hashfunktion SHA-1. Der Hashwert wird in einer Hashwertdatei und die Konfigurationsdaten (ohne Passwort!) in einer Konfigurationsdatei auf einem fest vorgegebenen File des Betriebssystems abgelegt.

  Das Passwort wird weder im EVG noch auf dem File dauerhaft abgespeichert. Der Speicherbereich, in dem das Passwort temporär gespeichert wurde, wird durch den EVG definiert überschrieben.

- Prüfen der Konfigurationsdaten

Bei jedem Start des EVG werden Konfigurationsdatei und Hashwertdatei geladen. Kann eine der beiden Dateien nicht geladen werden, wird der Anwender darauf hingewiesen, dass noch keine Konfiguration erstellt wurde (s. o.). Sind beide Dateien geladen, wird der Benutzer aufgefordert, das Passwort einzugeben. Aus dem eingegebenen Passwort und der Konfigurationsdatei wird ein Hashwert (mit der Hashfunktion SHA-1) berechnet. Anschließend erfolgt ein Hashwertvergleich. Der EVG besitzt einen Fehlbedienungszähler (FBZ=3). Sind die Hashwerte nicht identisch, gilt folgendes:

- bei FBZ>1 muss der Anwender erneut das Passwort eingeben;
- bei FBZ=1 erhält der Anwender den Hinweis, dass er mit einer nicht authentischen Konfiguration arbeitet und die Konfiguration daher neu erstellen muss (s. o.).

  Sind die Hashwerte identisch, arbeitet der Anwender mit einer authentischen Konfiguration; der EVG startet.

- Ändern der Konfigurationsdaten

  Eine Änderung der Konfigurationsdaten ist nur möglich, wenn das Prüfen der Konfigurationsdaten erfolgreich war (s. o.), d. h. wenn das Passwort korrekt eingegeben und der Hashwertvergleich erfolgreich durchgeführt wurde. Der Anwender kann dann ohne erneute Authentisierung die Konfiguration ändern, wobei – wie oben ausgeführt – ein Passwort zum Schutz der Konfigurationsdaten einzugeben ist. Die Änderung wird sofort wirksam.

- Ändern des Passwortes

  Eine Änderung des Passwortes ist nur möglich, wenn das Prüfen der Konfigurationsdaten erfolgreich war (s. o.), d. h. wenn das Passwort korrekt eingegeben und der Hashwertvergleich erfolgreich durchgeführt wurde. Der Anwender kann dann ohne erneute Authentisierung das Passwort ändern. Die Änderung wird sofort wirksam. Ein Passwortwechsel wird durch den EVG nicht initiiert. Die Wiederholung alter Passwörter beim Passwortwechsel wird durch den EVG nicht verhindert (Passworthistorie).

6.6 Maßnahmen zur Vertrauenswürdigkeit

141 Um die Vertrauenswürdigkeitsstufe EAL3+ zu erhalten, werden folgende Maßnahmen durchgeführt (vgl. Tabelle 6: Maßnahmen zur Erfüllung von EAL3+):

Tabelle 6: Maßnahmen zur Erfüllung von EAL3+

Anforderungen gemäß EAL3+		Maßnahmen der Entwickler
Konfigurations-management	ACM_CAP.3	Einsatz eines QM-Systems inklusive Konfigurationskontrolle
	ACM_SCP.1	

Anforderungen gemäß EAL3+		Maßnahmen der Entwickler
Auslieferung und Betrieb	ADO_DEL.2	Dokumentation der zum Schutz des EVG bei Auslieferung, Installation und Wartung getroffenen Maßnahmen in Form dokumentierter Auslieferungsprozeduren sowie Installations-, Generierungs- und Anlaufprozeduren
	ADO_IGS.1	
Entwicklung	ADV_FSP.1	Definition von Anforderungen gemäß CC an die Entwicklungsprozeduren und Dokumentation
	ADV_HLD.2	
	ADV_IMP.1	
	ADV_LLD.1	
	ADV_RCR.1	
Handbücher	AGD_ADM.1	Erstellung und Auslieferung eines Systemverwalter- und Benutzerhandbuchs
	AGD_USR.1	
Lebenszyklus-Unterstützung	ALC_DVS.1	Gewährleistung des Entwicklungsprozesses durch physikalische, personelle und organisatorische Sicherheitsmaßnahmen
	ALC_TAT.1	
Testen	ATE_COV.2	Verwendung eines werkzeugbasierten und automatisierten Testsystems zum Test der Sicherheitsfunktionen, Tests auf Subsystem-Ebene und Tests der funktionalen Spezifikation. Dokumentation der Ergebnisse sowie unabhängiges Testen durch den Evaluator
	ATE_DPT.1	
	ATE_FUN.1	
	ATE_IND.2	
Schwachstellenbewertung	AVA_MSU.3	Erstellung von Missbrauchsanalysen, Analyse für die sicherheitsrelevanten Mechanismen in Bezug auf die Mechanismenstärke „hoch“ sowie Schwachstellenanalyse für alle Schwachstellen des EVG
	AVA_SOF.1	
	AVA_VLA.4	

7 PP-Postulate

142 Für die Sicherheitsvorgaben (ST) zur Evaluierung der Virtuellen Poststelle des Bundes wird kein Schutzprofil (Protection Profile – PP) postuliert.

8 Erklärungen

8.1 Erklärung der organisatorischen Sicherheitspolitiken

143 Der EVG ist eine Signaturanwendungskomponente zur Prüfung elektronischer Signaturen. In Abschnitt 2.4 ist beschrieben, in welchem Umfang die

Sicherheitsanforderungen des SigG und der SigV an Signaturanwendungskomponenten vom EVG erfüllt werden und welcher Anteil von der IT-Umgebung umgesetzt werden muss.

144 Zusammenfassend muss der EVG damit die folgenden Anforderungen umsetzen, die in den organisatorischen Sicherheitspolitiken in Abschnitt 3.4 aufgeführt sind:

- Prüfung von Signaturen:
  - Die Verifikationsanwendung muss qualifizierte elektronische Signaturen prüfen.
  - Die Verifikationsanwendung und der -server müssen hinsichtlich der Validierung eine Plausibilitätsprüfung durchführen.
  - Verifikationsanwendung und -server führen die Validierung mittels Basiskomponente (vgl. [bos_Basis-ST]) durch.
  - Die Verifikationsanwendung muss beim Prüfen einer Signatur gewährleisten, dass erkennbar wird, auf welche Daten sich die Signatur bezieht.
  - Die Verifikationsanwendung muss beim Prüfen einer Signatur gewährleisten, dass erkennbar wird, ob die Daten unverändert sind.
  - Die Verifikationsanwendung muss beim Prüfen einer Signatur gewährleisten, dass bei Bedarf der Inhalt der signierten Daten hinreichend zu erkennen ist.
  - Die Verifikationsanwendung muss beim Prüfen einer Signatur gewährleisten, dass erkennbar wird, welchem Signaturschlüssel-Inhaber die Signatur zuzuordnen ist.
  - Die Verifikationsanwendung muss beim Prüfen einer Signatur gewährleisten, dass erkennbar wird, welche Inhalte das qualifizierte Zertifikat, auf dem die Signatur beruht, aufweisen.
  - Die Verifikationsanwendung muss beim Prüfen einer Signatur gewährleisten, dass erkennbar wird, ob die nachgeprüften qualifizierten Zertifikate im jeweiligen Zertifikatverzeichnis zum angegebenen Zeitpunkt vorhanden und nicht gesperrt waren.
  - Die Verifikationsanwendung muss beim Prüfen einer Signatur gewährleisten, dass die Korrektheit der Signatur zuverlässig geprüft wird.
- Schutz vor unbefugter Veränderung
  - Die Integrität der Verifikationsanwendung wird durch das Prüftool geschützt.
  - Die Integrität der Konfigurationsdaten der Verifikationsanwendung wird durch die Verifikationsanwendung geschützt.

145 In der IT-Umgebung müssen insbesondere folgende Anforderungen des SigG durch geeignete Signaturanwendungskomponenten umgesetzt werden

(vgl. Annahmen und Sicherheitsziele für die Umgebung in den Abschnitten 3.2 und 4.2):

- Prüfung von Signaturen:
  - Die Basiskomponente in der IT-Umgebung muss beim Prüfen einer Signatur gewährleisten, dass festgestellt wird, ob die nachgeprüften qualifizierten Zertifikate im jeweiligen Zertifikatverzeichnis zum angegebenen Zeitpunkt vorhanden und nicht gesperrt waren.
- Schutz vor unbefugter Veränderung:
  - Sicherheitstechnische Veränderungen am Verifikationsserver müssen für den Administrator erkennbar werden (vgl. Annahme A.ServerBetrieb).
  - Zusätzlich zur Absicherung der Integrität der Verifikationsanwendung (durch das Prüftool) und der Konfigurationsdaten der Verifikationsanwendung muss für die Verifikationsanwendung der sichere Betrieb am Arbeitsplatz gewährleistet werden (vgl. Annahme A.ClientBetrieb).

8.2 Erklärung der Sicherheitsziele

146 Im Folgenden wird dargestellt und in Tabelle 7 und Tabelle 8 zusammengefasst, wie die einzelnen Annahmen, Bedrohungen und organisatorischen Sicherheitspolitiken durch Sicherheitsziele für den EVG und die Umgebung abgedeckt werden.

- Das Sicherheitsziel für die Umgebung OE.PKI zielt auf die gleichnamige Annahme A.PKI ab, wobei zu berücksichtigen ist, dass OE.PKI auch für die organisatorischen Sicherheitspolitiken P.ValidZert (für die Gültigkeitsprüfung durch obige Funktionalitäten der Basiskomponenten, für die Existenz qualifizierter Zertifikate sowie die kryptographischen Schlüssel und (System-) Zertifikate zur Gewährleistung der Systemsicherheit) sowie P.VerifySign (für Existenz qualifizierter Zertifikate) benötigt werden
- Das Sicherheitsziel für die Umgebung OE.ServerBetrieb zielt auf die gleichnamige Annahme A.ServerBetrieb ab und ist zur Realisierung der organisatorischen Sicherheitspolitik P.ValidZert (für die Gewährleistung der Systemsicherheit aufgrund der Realisierung der Validierung innerhalb des verteilten Systems) notwendig.
- Das Sicherheitsziel für die Umgebung OE.ClientBetrieb zielt auf die gleichnamige Annahme A.ClientBetrieb ab und ist zur Realisierung der organisatorischen Sicherheitspolitik P.ValidZert (für die Gewährleistung der Systemsicherheit aufgrund der Realisierung der Validierung innerhalb des verteilten Systems – d. h. dem Management des (System-) Zertifikats in der Verifikationsanwendung zur Verifikation der Signatur des Validierungsergebnisses des OCSP/CRL-Relays) notwendig.

- Das Sicherheitsziel O.Anzeige deckt die organisatorische Sicherheitspolitik P.Anzeige zur sicheren und zuverlässigen Anzeige bei der Prüfung qualifizierter elektronischer Signaturen ab. Dabei wird durch die Verifikation festgestellt, ob die Daten unverändert sind. Die Anzeige umfasst nicht nur, was signiert wurde, sondern auch ergänzende Informationen zur Nachricht, wie Zertifikatsinhalt, Signaturschlüssel-Inhaber und Verifikations- und Validierungsergebnisse, sowie die Konfigurationsdaten.
- Das Sicherheitsziel O.ValidZert deckt die organisatorische Sicherheitspolitik P.ValidZert zur Validierung qualifizierter Zertifikate ab und präzisiert die Aufgabenteilung. Zu berücksichtigen ist, dass die wesentlichen Aufgaben bei der Validierung in der IT-Umgebung durch die Basiskomponente (vgl. Sicherheitsziel für die IT-Umgebung OE.PKI) geleistet werden und dass zur Gewährleistung der Systemsicherheit (innerhalb des verteilten Systems) die Sicherheitsziele für die IT-Umgebung OE.ServerBetrieb und OE.ClientBetrieb benötigt werden.
- Das Sicherheitsziel O.VerifySign deckt die organisatorische Sicherheitspolitik P.VerifySign zur Prüfung einer qualifizierten elektronischen Signatur ab und präzisiert, dass die Verifikation durch die Prüfung der Integrität und der Authentizität erfolgt (qualifizierte Zertifikate via Sicherheitsziel für die IT-Umgebung OE.PKI).
- Das Sicherheitsziel O.Manipulation deckt die organisatorische Sicherheitspolitik P.Manipulation zum Schutz vor unbefugter Veränderung an der Verifikationsanwendung sowie ihren Konfigurationsdaten ab.

Tabelle 7: Zuordnung Sicherheitsumgebung zu -zielen

EVG-Sicherheitsumgebung	zugehörige Sicherheitsziele
A.PKI	OE.PKI
A.ServerBetrieb	OE.ServerBetrieb
A.ClientBetrieb	OE.ClientBetrieb
P.Anzeige	O.Anzeige
P.ValidZert	O.ValidZert, OE.PKI, OE.ServerBetrieb, OE.ClientBetrieb
P.VerifySign	O.VerifySign, OE.PKI
P.Manipulation	O.Manipulation

Tabelle 8: Zuordnung Sicherheitsziele zu -umgebung

Sicherheitsziele	zugehörige EVG-Sicherheitsumgebung
O.Anzeige	P.Anzeige
O.ValidZert	P.ValidZert
O.VerifySign	P.VerifySign

Sicherheitsziele	zugehörige EVG-Sicherheitsumgebung
O.Manipulation	P.Manipulation
OE.PKI	A.PKI, P.ValidZert, P.VerifySign
OE.ServerBetrieb	A.ServerBetrieb, P.ValidZert
OE.ClientBetrieb	A.ClientBetrieb, P.ValidZert

8.3 Erklärung der Sicherheitsanforderungen

8.3.1 Erklärung zu den funktionalen Sicherheitsanforderungen

147 Wie die Sicherheitsziele, die sich auf IT beziehen, durch die funktionalen Sicherheitsanforderungen erfüllt werden, ist im Folgenden dargestellt und in Tabelle 9 und Tabelle 10 hinsichtlich des EVG und in Tabelle 11 und Tabelle 12 hinsichtlich der IT-Umgebung zusammengefasst:

- Die funktionale Sicherheitsanforderung FDP_SVR.1 wird für die Umsetzung des Sicherheitsziels O.Anzeige benötigt.
- Die funktionale Sicherheitsanforderung FCS_COP.1 (Valid) wird für die Umsetzung des Sicherheitsziels O.ValidZert in der Weise benötigt, dass die Verifikationsanwendung die Signatur des OCSP/CRL-Relays mit dem (System-)Zertifikat verifizieren muss.
- Die funktionale Sicherheitsanforderung FCS_COP.1 (Verify) wird für die Umsetzung des Sicherheitsziels O.VerifySign benötigt.
- Die funktionale Sicherheitsanforderung FCS_COP.1 (Tool) wird für die Umsetzung des Sicherheitsziels O.Manipulation hinsichtlich des Integritätsschutzes der Verifikationsanwendung benötigt.
- Die funktionale Sicherheitsanforderung FCS_COP.1 (Konfig) wird für die Umsetzung des Sicherheitsziels O.Manipulation hinsichtlich des Integritätsschutzes der Konfigurationsdaten der Verifikationsanwendung benötigt.
- Die funktionale Sicherheitsanforderung FDP_RIP.1 wird für die Umsetzung des Sicherheitsziels O.Manipulation hinsichtlich des Integritätsschutzes der Konfigurationsdaten der Verifikationsanwendung in der Weise benötigt, dass das vom Benutzer eingegebene Passwort vom EVG gelöscht wird (und nicht persistent erhalten bleibt).
- Die funktionale Sicherheitsanforderung FIA_UAU.7 wird für die Umsetzung des Sicherheitsziels O.Manipulation hinsichtlich des Integritätsschutzes der Konfigurationsdaten der Verifikationsanwendung in der Weise benötigt, dass das Passwort bei der Eingabe auf dem Bildschirm nur verdeckt durch einen Stern als „Dummy“ für jedes eingegebene Passwortzeichen anstelle des ursprünglichen Zeichens angezeigt wird.

- Die funktionale Sicherheitsanforderung FIA_UAU.1 ergibt sich aus der Abhängigkeit von FIA_UAU.7. FIA_UAU.1 wird damit implizit für die Umsetzung des Sicherheitsziels O.Manipulation hinsichtlich des Integritätsschutzes der Konfigurationsdaten der Verifikationsanwendung mittels Passworteingabe benötigt, wobei für die folgenden Aktionen zum Schutz der Konfigurationsdaten eine Passworteingabe erforderlich ist: Prüfen der Konfigurationsdaten beim Starten der Verifikationsanwendung, Ändern der Konfigurationsdaten, Ändern des Passwortes. Die Erstellung der Konfigurationsdaten ist ohne Passworteingabe möglich, wobei der Benutzer der Verifikationsanwendung hierzu die authentischen Konfigurationsdaten (Adresse des Verifikationsservers sowie (System-)Zertifikat des OCSP/CRL-Relays als Trust Anchor) benötigt (vgl. Abschnitt 2.6.2) .
- Die funktionale Sicherheitsanforderung FIA_UID.1 ergibt sich aus der Abhängigkeit von FIA_UAU.1. FIA_UID.1 wird damit implizit für die Umsetzung des Sicherheitsziels O.Manipulation hinsichtlich des Integritätsschutzes der Konfigurationsdaten der Verifikationsanwendung mittels Passworteingabe benötigt, wobei für die folgenden Aktionen zum Schutz der Konfigurationsdaten eine Passworteingabe erforderlich ist: Prüfen der Konfigurationsdaten beim Starten der Verifikationsanwendung, Ändern der Konfigurationsdaten, Ändern des Passwortes. Die Erstellung der Konfigurationsdaten ist ohne Passworteingabe möglich, wobei der Benutzer der Verifikationsanwendung hierzu die authentischen Konfigurationsdaten (Adresse des Verifikationsservers sowie (System-)Zertifikat des OCSP/CRL-Relays als Trust Anchor) benötigt (vgl. Abschnitt 2.6.2).
- Die drei funktionalen Sicherheitsanforderungen an die IT-Umgebung – FCS_CKM.1 oder FDP_ITC.1 sowie FCS_CKM.4 und FMT_MSA.2 – ergeben sich aus den Abhängigkeiten zu FCS_COP.1 (Valid) und FCS_COP.1 (Tool) und damit implizit aus den Sicherheitszielen O.ValidZert und O.Manipulation. Die Ausgestaltung der Operationen der funktionalen Sicherheitsanforderungen sowie die Abhängigkeiten dieser Anforderungen sind in der IT-Umgebung zu realisieren, da Schlüsselerzeugung, -import und -löschung sowie Management der Sicherheitsattribute in der IT-Umgebung außerhalb des EVG liegt.
- Die in Tabelle 5 referenzierten funktionalen Sicherheitsanforderungen an die IT-Umgebung FCO_NRO.1, FCS_CKM.4, FCS_COP.1 (Verify), FCS_COP.1 (SVVE), FCS_COP.1 (VVE), FDP_ACC.1 (Sys), FDP_ACF.1 (Sys), FDP_ITC.1, FIA_UID.2, FMT_MSA.1 (Sys), FMT_MSA.2, FMT_MSA.3 (Sys) und FMT_SMR.1 (Sys) lassen sich auf das Sicherheitsziel der IT-Umgebung OE.PKI hinsichtlich der Validierung qualifizierter Zertifikate, für die die Basiskomponente der Virtuellen Poststelle des Bundes (vgl. [bos_Basis-ST]) benötigt wird, zurückführen.

Tabelle 9: Zuordnung Sicherheitsziele zu Sicherheitsanforderungen an den EVG

Sicherheitsziele	funktionale Sicherheitsanforderungen an den EVG
O.Anzeige	FDP_SVR.1

O.ValidZert	FCS_COP.1 (Valid)
O.VerifySign	FCS_COP.1 (Verify)
O.Manipulation	FCS_COP.1 (Tool) FCS_COP.1 (Konfig), FDP_RIP.1, FIA_UAU.7, FIA_UAU.1, FIA_UID.1

Tabelle 10: Zuordung fkt. Sicherheitsanforderungen zu Sicherheitszielen

funktionale Sicherheitsanforderungen an den EVG	Sicherheitsziele
FCS_COP.1 (Valid)	O.ValidZert
FCS_COP.1 (Verify)	O.VerifySign
FCS_COP.1 (Tool)	O.Manipulation
FCS_COP.1 (Konfig)	O.Manipulation
FDP_SVR.1	O.Anzeige
FDP_RIP.1	O.Manipulation
FIA_UAU.7	O.Manipulation
FIA_UAU.1	O.Manipulation
FIA_UID.1	O.Manipulation

Tabelle 11: Zuordnung Sicherheitsziele zu Sicherheitsanforderungen an die IT-Umgebung

Sicherheitsziele	funktionale Sicherheitsanforderungen an die IT-Umgebung
O.Anzeige	-
O.ValidZert	FCS_CKM.1 oder FDP_ITC.1, FCS_CKM.4, FMT_MSA.2
O.VerifySign	-
O.Manipulation	FCS_CKM.1 oder FDP_ITC.1, FCS_CKM.4, FMT_MSA.2
OE.PKI	FCO_NRO.1, FCS_CKM.4, FCS_COP.1 (Verify), FCS_COP.1 (SVVE), FCS_COP.1 (VVE), FDP_ACC.1 (Sys), FDP_ACF.1 (Sys), FDP_ITC.1, FIA_UID.2, FMT_MSA.1 (Sys), FMT_MSA.2, FMT_MSA.3 (Sys) und FMT_SMR.1 (Sys)

Tabelle 12: Zuordung fkt. Sicherheitsanforderungen an die IT-Umgebung zu Sicherheitszielen

funktionale Sicherheitsanforderungen an die IT-Umgebung	Sicherheitsziele
FCS_CKM.1 oder FDP_ITC.1	O.ValidZert, O.Manipulation, OE.PKI
FCS_CKM.4	O.ValidZert, O.Manipulation, OE.PKI
FMT_MSA.2	O.ValidZert, O.Manipulation, OE.PKI
FCO_NRO.1, FCS_COP.1 (Verify), FCS_COP.1 (SVVE), FCS_COP.1 (VVE), FDP_ACC.1 (Sys), FDP_ACF.1 (Sys), FIA_UID.2, FMT_MSA.1 (Sys), FMT_MSA.3 (Sys) und FMT_SMR.1 (Sys)	OE.PKI

8.3.2 Erfüllung der Abhängigkeiten

148 Die EVG-Abhängigkeiten sind berücksichtigt, wie im Folgenden ausgeführt und in Tabelle 13 zusammenfassend dargestellt:

- FDP_SVR.1 hat keine Abhängigkeiten.
- Die Abhängigkeiten der funktionalen Sicherheitsanforderung FCS_COP.1 (Valid) – Schlüsselerzeugung gemäß FCS_CKM.1 oder Schlüsselimport gemäß FDP_ITC.1, Zerstörung eines Schlüssels gemäß FCS_CKM.4 und Schlüsselmanagement gemäß FMT_MSA.2) – sind in der IT-Umgebung einerseits hinsichtlich der initialen Konfiguration der Verifikationsanwendung durch den Security-Administrator auf Seiten des Betreibers und andererseits durch den Benutzer im Rahmen der Konfiguration der Verifikationsanwendung zu realisieren. Eine funktionale Sicherheitsanforderung FDP_ITC.1 ist für den EVG nicht notwendig, da vom EVG keine Zugriffskontroll- oder Informationsflusskontrolle durchgesetzt wird. Der EVG nutzt die in der IT-Umgebung verfügbaren Daten, ohne dafür eine dedizierte Prüfoperation durchzuführen; die Daten unterliegen keiner Benutzerkontrolle durch den EVG.
- Die Abhängigkeiten der funktionalen Sicherheitsanforderung FCS_COP.1 (Verify) sind nicht erfüllt, da der für die Verifikation genutzte öffentliche Schlüssel aus dem Zertifikat – der zusammen mit der zu verifizierenden Signatur mitgeliefert wird – eine öffentlich Information ist und kein Sicherheitsattribut darstellt (keine Schlüsselerzeugung gemäß FCS_CKM.1, kein Schlüsselimport gemäß FDP_ITC.1 , keine Zerstörung eines Schlüssels gemäß FCS_CKM.4, kein Schlüsselmanagement gemäß FMT_MSA.2).

- Die Abhängigkeiten der funktionalen Sicherheitsanforderung FCS_COP.1 (Tool) – Schlüsselimport gemäß FDP_ITC.1 oder Schlüsselerzeugung gemäß FCS_CKM.1, Zerstörung eines Schlüssels gemäß FCS_CKM.4 und Schlüsselmanagement gemäß FMT_MSA.2) – sind in der IT-Umgebung für das Prüftool zu realisieren, da die für die Prüfung notwendigen Zertifikate vom Hersteller in das Tool eingebracht – d. h. Teil der Implementierung sind – und mit dem Tool ausgeliefert werden; ein Management von Seiten des Benutzers des Tools ist nicht möglich.
- Die Abhängigkeiten der funktionalen Sicherheitsanforderung FCS_COP.1 (Konfig) sind nicht erfüllt, da keine Schlüssel involviert sind (weder Schlüsselerzeugung gemäß FCS_CKM.1 oder Schlüsselimport gemäß FDP_ITC.1 noch Zerstörung eines Schlüssels gemäß FCS_CKM.4) und daher kein Schlüsselmanagement gemäß FMT_MSA.2 notwendig ist.
- FDP_RIP.1 hat keine Abhängigkeiten.
- FIA_UAU.7 hat die Abhängigkeit FIA_UAU.1.
- FIA_UAU.1 hat die Abhängigkeit FIA_UID.1.
- FIA_UID.1 hat keine Abhängigkeiten.
- Zu den funktionalen Sicherheitsanforderungen in der IT-Umgebung:
    - Die Abhängigkeiten der drei funktionalen Sicherheitsanforderungen FCS_CKM.1 oder FDP_ITC.1, FCS_CKM.4 und FMT_MSA.2 sind in der IT-Umgebung zu realisieren, da Schlüsselerzeugung, -import und -löschung sowie Management der Sicherheitsattribute in der IT-Umgebung außerhalb des EVG liegt.
    - Die funktionalen Sicherheitsanforderungen in der IT-Umgebung, die sich aus der Nutzung der Basiskomponente zur Validierung eines qualifizierten Zertifikats ergeben – FCO_NRO.1, FCS_CKM.4, FCS_COP.1 (Verify), FCS_COP.1 (SVVE), FCS_COP.1 (VVE), FDP_ACC.1 (Sys), FDP_ACF.1 (Sys), FDP_ITC.1, FIA_UID.2, FMT_MSA.1 (Sys), FMT_MSA.2, FMT_MSA.3 (Sys) und FMT_SMR.1 (Sys) –, sind in der IT-Umgebung zu realisieren; wie [bos_Basis-ST] zu entnehmen ist, sind diese hinsichtlich der Abhängigkeiten in sich abgeschlossen.

Tabelle 13: Erfüllung der EVG-Abhängigkeiten

funktionale Sicherheitsanforderungen an den EVG	Abhängigkeiten	Bemerkung
FCS_COP.1 (Valid)	FDP_ITC.1 oder FCS_CKM.1 FCS_CKM.4 FMT_MSA.2	sind in der IT-Umgebung zu realisieren
FCS_COP.1 (Verify)	FDP_ITC.1 oder FCS_CKM.1 FCS_CKM.4	formal nicht erfüllt wg. Nutzung öffentlicher

funktionale Sicherheits-anforderungen an den EVG	Abhängigkeiten	Bemerkung
	FMT_MSA.2	Zertifikate
FCS_COP.1 (Tool)	FDP_ITC.1 oder FCS_CKM.1 FCS_CKM.4 FMT_MSA.2	sind in der IT-Umgebung zu realisieren
FCS_COP.1 (Konfig)	FDP_ITC.1 oder FCS_CKM.1 FCS_CKM.4 FMT_MSA.2	formal nicht erfüllt wg. Hashfunktion
FDP_SVR.1	-	formal erfüllt
FDP_RIP.1	-	formal erfüllt
FIA_UAU.7	FIA_UAU.1	erfüllt
FIA_UAU.1	FIA_UID.1	erfüllt
FIA_UID.1	-	formal erfüllt

8.3.3 Analyse des Zusammenwirkens der funktionalen Anforderungen

149 Aus den vorigen Ausführungen wird deutlich, dass die funktionalen Sicherheitsanforderungen eine in sich geschlossene Einheit bilden und geeignet sind, gemeinsam alle Sicherheitsziele zu erfüllen.

150 Da alle von den CC geforderten Abhängigkeiten der einzelnen Sicherheitsanforderungen – soweit auf den vorliegenden EVG anwendbar – erfüllt werden, ist das ordnungsgemäße Zusammenwirken dieser Sicherheitsanforderungen gewährleistet.

8.3.4 Analyse der Mindest-Stärkestufe

151 Gemäß SigG/SigV muss eine Signaturanwendungskomponente die in Anlage 1 der Signaturverordnung [SigV] definierte Vertrauenswürdigkeitsstufe EAL3 erreichen, wobei folgende Anforderungen an die Schwachstellenbewertung bzw. Mechanismenstärke formuliert ist: „Bei den Prüfstufen […] ‚EAL3' […] ist ergänzend zu den bei dieser Prüfstufe vorgeschriebenen Maßnahmen gegen ein hohes Angriffspotenzial zu prüfen und eine vollständige Missbrauchsanalyse durchzuführen".

152 Die Prüfung gegen ein hohes Angriffspotential (SOF-hoch) korrespondiert gemäß CC-Teil 3, Abschnitt 14.4, [CC-Teil3], und CEM, Abschnitt B.8, [CEM], mit der Vertrauenswürdigkeitskomponente AVA_VLA.4. Hierbei sind zusätzlich die Anforderungen aus den „Anwendungshinweisen und Interpretationen zum Schema (AIS)" Nr. 27 [AIS27] zu berücksichtigen. In AIS 27 werden Vertrauenswürdigkeitskomponenten aufgeführt, die zusätzlich zu den in den EAL-Stufen der Common Criteria ausgewählten Komponenten auszuwählen

– d. h. zu augmentieren – sind, um den Anforderungen der ITSEC zu genügen. Relevant für diese Sicherheitsvorgaben sind die in Anlage 1 der Signaturverordnung [SigV] beschriebenen Anforderungen hinsichtlich der Stärke der Sicherheitsmechanismen, die mit „hoch“ bewertet werden müssen.

153 Die angestrebten SOF-Stufen der einzelnen Sicherheitsfunktionen sind in Tabelle 14 aufgeführt.

Tabelle 14: Angestrebten SOF-Stufen für die Sicherheitsfunktionen

Sicherheits-funktion	Mechanismentyp	Angestrebte Stärke
SF1	Wahrscheinlichkeits- oder Permutationsmechanismen (Verifikationsalgorithmus, Hashfunktion)	SOF-hoch
SF2	Wahrscheinlichkeits- oder Permutationsmechanismen (Verifikationsalgorithmus, Hashfunktion)	SOF-hoch
SF3	deterministisch	nicht anwendbar
SF4	Wahrscheinlichkeits- oder Permutationsmechanismen (Verifikationsalgorithmus, Hashfunktion)	SOF-hoch
SF5	Wahrscheinlichkeits- oder Permutationsmechanismen (Hashfunktion)	SOF-hoch

8.3.5 Erklärung zu den Anforderungen an die Vertrauenswürdigkeit

154 Die Auswahl der Vertrauenswürdigkeitskomponenten ergibt sich direkt aus den Anforderungen von Signaturgesetz und -verordnung, wie in Abschnitt 1.3 ausführlich dargelegt wird.

8.4 Erklärung der EVG-Übersichtsspezifikation

8.4.1 Erfüllung der funktionalen Sicherheitsanforderungen

155 Die Sicherheitsfunktionen wirken mit den funktionalen Sicherheitsanforderungen wie folgt (vgl. Tabelle 15, wobei ein „X“ eine für die jeweilige Sicherheitsfunktion zutreffende funktionale Sicherheitsanforderung signalisiert):

- Für die Sicherheitsfunktion SF1 „Verifikation einer qualifizierten elektronischen Signatur“ werden folgende Komponenten benötigt:
  - Komponente FCS_COP.1 (Verify) zur Verifikation einer qualifizierten elektronischen Signatur.
- Für die Sicherheitsfunktion SF2 „Verifikation einer OCSP/CRL-Relay-Antwort bei der Validierung eines qualifizierten Zertifikats“ werden folgende Komponenten benötigt:
  - Komponente FCS_COP.1 (Valid) für die Verifikation der Validierungsergebnisse – vom OCSP/CRL-Relay signiert.

  - In der IT-Umgebung ist FCS_CKM.1 oder FDP_ITC.1, FCS_CKM.4 und FMT_MSA.2 umzusetzen.
  - In der IT-Umgebung wird die Basiskomponente zur Validierung eines qualifizierten Zertifikats benötigt; FCO_NRO.1, FCS_CKM.4, FCS_COP.1 (Verify), FCS_COP.1 (SVVE), FCS_COP.1 (VVE), FDP_ACC.1 (Sys), FDP_ACF.1 (Sys), FDP_ITC.1, FIA_UID.2, FMT_MSA.1 (Sys), FMT_MSA.2, FMT_MSA.3 (Sys) und FMT_SMR.1 (Sys) sind umzusetzen.

- Für die Sicherheitsfunktion SF3 „Sichere und zuverlässige Anzeige“ werden folgende Komponenten benötigt:
  - Komponente FDP_SVR.1 für die sichere Anzeige.
- Für die Sicherheitsfunktion SF4 „Prüftool“ werden folgende Komponenten benötigt:
  - Komponente FCS_COP.1 (Tool) zum Hashen von Daten.
  - Über die Abhängigkeiten ist in der IT-Umgebung – im Prüftool – FCS_CKM.1 oder FDP_ITC.1, FCS_CKM.4 und FMT_MSA.2 umzusetzen.
- Für die Sicherheitsfunktion SF5 „Schutz der Konfigurationsdaten“ werden folgende Komponenten benötigt:
  - Komponente FCS_COP.1 (Konfig) zum Hashen von Daten.
  - Komponente FDP_RIP.1 für sicheres Löschen des eingegebenen Passwortes.
  - Komponenten FIA_UAU.7, FIA_UAU.1 und FIA_UID.1 für verdeckte Passwortanzeige und Passworteingabe.

Tabelle 15: Zuordnung fkt. Sicherheitsanforderungen durch Sicherheitsfunktionen

Fkt. Sicherheitsanforderungen an EVG bzw. IT-Umgebung	SF1	SF2	SF3	SF4	SF5
FCS_COP.1 (Valid)		X			
FCS_COP.1 (Verify)	X				
FCS_COP.1 (Tool)				X	
FCS_COP.1 (Konfig)					X
FDP_SVR.1			X		
FDP_RIP.1					X
FIA_UAU.7					X
FIA_UAU.1					X
FIA_UID.1					X
FCS_CKM.1 oder FDP_ITC.1		X		X	

Fkt. Sicherheitsanforderungen an EVG bzw. IT-Umgebung	SF1	SF2	SF3	SF4	SF5
FCS_CKM.4		X		X	
FMT_MSA.2		X		X	
FCO_NRO.1, FCS_CKM.4, FCS_COP.1 (Verify), FCS_COP.1 (SVVE), FCS_COP.1 (VVE), FDP_ACC.1 (Sys), FDP_ACF.1 (Sys), FDP_ITC.1, FIA_UID.2, FMT_MSA.1 (Sys), FMT_MSA.2, FMT_MSA.3 (Sys) und FMT_SMR.1 (Sys)		X			

156 Die Sicherheitsfunktionen wirken in den beiden Teilsystemen Verifikationsanwendung und -server wie folgt (Tabelle 16):

Tabelle 16: Zuordnung von Sicherheitsfunktionen zu Teilsystemen

	Verifikations-anwendung	Verifikati-onsserver
SF1 – Verifikation einer qualifizierten elektronischen Signatur	X	
SF2 – Verifikation einer OCSP/CRL-Relay-Antwort bei der Validierung eines qualifizierten Zertifikats	X	X
SF3 – Sichere und zuverlässige Anzeige	X	
SF4 – Prüftool	X	
SF5 – Schutz der Konfigurationsdaten	X	

8.4.2 Konsistenz der Mechanismenstärke-Postulate

157 Die geforderte Stärke der Sicherheitsmechanismen von SOF-hoch findet sich in den Angaben zu den Maßnahmen zur Vertrauenswürdigkeit wieder (vgl. Tabelle 6 und Tabelle 18).

8.4.3 Analyse des Zusammenwirkens der Sicherheitsfunktionen

158 Im Folgenden ist ausgeführt und in Tabelle 17 zusammengefasst, wie die Sicherheitsfunktionen

- SF1 – Verifikation einer qualifizierten elektronischen Signatur,
- SF2 – Verifikation einer OCSP/CRL-Relay-Antwort bei der Validierung eines qualifizierten Zertifikats,
- SF3 – Sichere und zuverlässige Anzeige,

- SF4 – Prüftool,
- SF5 – Schutz der Konfigurationsdaten,

zusammenwirken, wobei ein „X“ in Tabelle 17 ein Zusammenwirken signalisiert. Tabelle 17 ist nicht symmetrisch.

159 Da bei der Verifikation einer qualifizierten elektronischen Signatur und der Validierung eines Zertifikats der Benutzer durch geeignete Anzeigen unterstützt wird, wirkt SF3 stets bei SF1 und SF2.

Tabelle 17: Zusammenwirken der Sicherheitsfunktionen

	SF1	SF2	SF3	SF4	SF5
SF1	X				
SF2		X			
SF3	X	X	X		
SF4				X	
SF5					X

8.4.4 Erklärung zu den Maßnahmen der Vertrauenswürdigkeit

160 Die Maßnahmen zur Erfüllung der Vertrauenswürdigkeitsstufe EAL3+ werden wie folgt erfüllt (vgl. Tabelle 18):

Tabelle 18: Erklärung der Maßnahmen zur Erfüllung von EAL3+

Anforderungen gemäß EAL3+	Maßnahmen der Entwickler
Konfigurationsmanagement : ▪ ACM_CAP. 3 ▪ ACM_SCP. 1	Ein Qualitätssicherungssystem mit Konfigurationskontrolle unterstützt den Entwickler bei der Entwicklung des EVG. Alle der Konfigurationskontrolle unterliegenden Objekte werden eindeutig identifiziert. Es stellt sicher, dass Unbefugte keine Modifikationen vornehmen. Das Konfigurationskontrollsystem ermöglicht eine Historie von Implementierung, Design, Tests und Dokumentation.
Auslieferung und Betrieb: ▪ ADO_DEL. 2 ▪ ADO_IGS. 1	Es werden Maßnahmen zur Umsetzung der Anforderungen hinsichtlich der Auslieferungsprozeduren sowie Installations-, Generierungs- und Anlaufprozeduren dokumentiert.

Anforderungen gemäß EAL3+	Maßnahmen der Entwickler
Entwicklung: ▪ ADV_FSP.1 ▪ ADV_HLD.2 ▪ ADV_IMP.1 ▪ ADV_LLD.1 ▪ ADV_RCR.1	Entwicklungsprozeduren und Dokumentation erfolgen in einer Weise, so dass sie den Anforderungen der CC genügen.
Handbücher: ▪ AGD_ADM.1 ▪ AGD_USR.1	Systemverwalter- und Benutzerhandbuch werden erstellt und mit dem EVG ausgeliefert.
Lebenszyklus-Unterstützung: ▪ ALC_DVS.1 ▪ ALC_TAT.1	Der Entwicklungsprozess ist durch physikalische, personelle und organisatorische Sicherheitsmaßnahmen gewährleistet. Für die Entwicklung des EVG werden festgelegte Entwicklungswerkzeuge genutzt.
Testen: ▪ ATE_COV.2 ▪ ATE_DPT.1 ▪ ATE_FUN.1 ▪ ATE_IND.2	Der Entwickler verwendet ein werkzeugbasiertes und automatisiertes Testsystem. Damit können ▪ Tests der Sicherheitsfunktionen, ▪ Tests auf Subsystem-Ebene und ▪ Tests der funktionalen Spezifikation durchgeführt und die Ergebnisse dokumentiert werden.

Anforderungen gemäß EAL3+	Maßnahmen der Entwickler
Schwachstellenbewertung: ▪ AVA_MSU.3 ▪ AVA_SOF.1 ▪ AVA_VLA.4	Basierend auf den Handbüchern werden Missbrauchsanalysen erstellt. Für die sicherheitsrelevanten Mechanismen wird eine Analyse in Bezug auf die Mechanismenstärke „hoch“ durchgeführt und dokumentiert. Es wird eine Schwachstellenanalyse für alle Schwachstellen des EVG durchgeführt.

9 Definition der Familie FDP_SVR[35]

161 Um die funktionalen IT-Sicherheitsanforderungen an den EVG zu definieren wird hier eine zusätzliche Familie (FDP_SVR) der Klasse FDP (Schutz der Benutzerdaten) definiert. Diese Familie beschreibt die funktionalen Anforderungen an eine sichere Anzeige im Umfeld elektronischer Signaturen.

162 FDP_SVR Sichere Anzeige

163 Familienverhalten

Diese Familie definiert Anforderungen an eine sichere Anzeige im Umfeld elektronischer Signaturen. In diesem Umfeld ist es erforderlich, dass der Benutzer den Inhalt des zu unterschreibenden Dokumentes eindeutig, ohne verdeckte bzw. aktive Inhalte informiert wird. Der Benutzer muss auf die nicht darstellbaren Inhalte hingewiesen werden.

164 Komponentenabstufung

FDP_SVR Sichere Anzeige --- 1

FDP_SVR.1 Sichere Anzeige erfordert von den TSF die Fähigkeit zu einer eindeutigen Anzeige der Inhalte, die frei von verdeckten oder aktiven Inhalten ist, und zur Information des Benutzers über nicht darstellbare Inhalte.

165 Management: FDP_SVR.1

Für diese Komponente sind keine Management-Aktivitäten vorgesehen.

166 Protokollierung: FDP_SVR.1

Es sind keine Ereignisse identifiziert, die protokollierbar sein sollen, wenn FAU_GEN Generierung der Sicherheitsprotokolldaten Bestandteil des PP/ der ST ist.

167 FDP_SVR.1 Sichere Anzeige

[35] aus [SignCubes]

168 Ist hierarchisch zu: Keinen anderen Komponenten

169 FDP_SVR.1.1 Die TSF müssen sicherstellen, dass der dem Benutzer angezeigte Inhalt eines Dokumentes entsprechend den folgenden Normen [Zuweisung: Normen für die Darstellung eines Inhalts] eindeutig ist.

170 FDP_SVR.1.2 Die TSF müssen sicherstellen, dass der dem Benutzer anzuzeigende Inhalt eines Dokumentes frei von aktiven oder verdeckten Inhalten ist. Die TSF müssen sicherstellen, dass der Benutzer darüber informiert wird.

171 FDP_SVR.1.3 Die TSF müssen sicherstellen, dass der Benutzer über einen nicht darstellbaren Inhalt eines anzuzeigenden Dokumentes informiert wird.

172 Abhängigkeiten: Keine Abhängigkeiten

10 Glossar

Basiskomponente	Basiskomponente der Virtuellen Poststelle des Bundes mit Kernsystem, OCSP/CRL-Relay und NetSigner (vgl. [bos_Basis-ST]).
Chipkarte	gemeint ist stets eine SigG-konforme Chipkarte
CRL	Certificate Revocation List (Sperrliste) [CRL]
LDAP	Lightweight Directory Access Protocol [LDAP]
Objekt	„Eine Einheit im TSC, die Informationen enthält oder empfängt und auf der Subjekte Operationen ausführen.“ [CC-Teil1]
OCSP	Online Certificate Status Protocol (Protokoll zur Zertifikatsstatus-Anfrage) [OCSP]
OperationId	Identifier für auszuführende Operationen
Prüfzeitpunkt	Als Prüfzeitpunkt wird der Zeitpunkt bezeichnet, an dem die aktuelle Prüfung durchgeführt wird. Die Unterscheidung zum Signaturzeitpunkt ist insbesondere von Bedeutung, weil im Laufe der Zeit die Sicherheit mathematischer Verfahren als unzureichend bewertet werden kann. Wenn der Prüfende sich über den Signaturzeitpunkt nicht sicher sein kann, kann er hilfsweise den Prüfzeitpunkt [...] als Signaturzeitpunkt annehmen. ([BSI_SigI_A6])
SAK	Signaturanwendungskomponente
SFP	funktionale Sicherheitspolitik
Sicherheitsattribut	„Informationen, die mit Subjekten, Benutzern und/oder Objekten verknüpft sind und die zur Durchsetzung der TSP benötigt werden.“ [CC-Teil1]

Signaturkarte	sichere Signaturerstellungseinheit (Die sichere Signaturerstellungseinheit gemäß SigG/SigV wird in diesem Kontext ausschließlich über eine Chipkarte, also eine Signaturkarte, realisiert. Die Begriffe werden synonym genutzt.)
Signaturzeitpunkt	Als Signaturzeitpunkt wird ein angenommener Erzeugungszeitpunkt einer digitalen Signatur bezeichnet. Der Zeitpunkt, zu dem die Signatur tatsächlich erzeugt wurde wird als objektiver Signaturzeitpunkt bezeichnet. Dieser Zeitpunkt kann von Dritten häufig nur schwer festgestellt werden. Der objektive Signaturzeitpunkt kann nur unter bestimmten Bedingungen und nur im Rahmen der technisch realisierbaren Genauigkeit durch Dritte beweissicher nachvollzogen werden, z. B. mit einer unmittelbar auf die Signaturerzeugung folgenden Zeitstempelerzeugung. Prüfende müssen in der Regel Annahmen zum Signaturzeitpunkt treffen (deshalb angenommener Erzeugungszeitpunkt). Vom Signaturzeitpunkt zu unterscheiden ist der Prüfzeitpunkt. ([BSI_SigI_A6])
Subjekt	”Eine Einheit innerhalb des TSC, die die Ausführung von Operationen bewirkt.” [CC-Teil1]
SystemId	Identifier für anforderndes System, d. h. OSCI-Manager gegenüber Basiskomponente
(System-)Zertifikat	Ein (System-)Zertifikat ist ein X.509-Zertifikat, das für die sichere Kommunikation innerhalb des EVG genutzt wird. Ein (System-)Zertifikat wird als ein Trust Anchor (Sicherheitsanker) genutzt, d. h. als ein vertrauenswürdiges Zertifikat aufgefasst, dem „vertraut“ wird und dessen Korrektheit nicht weiter geprüft zu werden braucht oder kann (etwa bei einem Selbstzertifikat).
TSC	Anwendungsbereich der TSF-Kontrolle (TSF Scope of Control): Die Menge der Interaktionen, die mit oder innerhalb eines EVG vorkommen können, werden als Anwendungsbereich der TSF-Kontrolle (TSC) bezeichnet. Der TSC umfasst eine definierte Menge von Interaktionen, basierend auf Subjekten, Objekten und Operationen innerhalb des EVG; er muss aber nicht alle Betriebsmittel eines EVG einschließen.
TSF	TOE Security Function (EVG-Sicherheitsfunktionen): „Eine Menge, die die gesamte Hardware, Software, und Firmware des TOE (EVG) umfasst, auf die Verlaß sein muss, um die TSP korrekt zu erfüllen.“ [CC-Teil1]
TSP	EVG-Sicherheitspolitik (TOE security policy, TSP) – „Eine Menge von Regeln, die angibt, wie innerhalb eines TOE (EVG) Werte verwaltet, geschützt und verteilt werden.“ [CC-Teil1]

11 Literatur

[AIS27] Bundesamt für Sicherheit in der Informationstechnik (BSI), „Application Notes and Interpretations of the Scheme (AIS), AIS 27, Version 1/20050204“, Entwurf vom 04.02.2005.

[BNetzA2005] Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (Bundesnetzagentur), „Einheitliche Spezifizierung der Einsatzkomponenten für Signaturanwendungskomponenten – Arbeitsgrundlage für Entwickler/Hersteller und Prüf-/Bestätigungsstellen“, Version 1.4, 19.07.2005.

[BNetzA_Algo2005] Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (Bundesnetzagentur), vormals Regulierungsbehörde für Telekommunikation und Post, „Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen)“, 2. Januar 2005.

[BNetzA_FAQ18] Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (Bundesnetzagentur), „FAQ, Frage 18“, www.bundesnetzagentur.de.

[bos_Basis-ST] bremen online services GmbH & Co. KG, „Virtuelle Poststelle des Bundes, Version 2.2.x.x (Basis), Sicherheitsvorgaben (ST)“, 2005.

[bos_OSCI-ST] bremen online services GmbH & Co. KG, „Virtuelle Poststelle des Bundes, Version 2.2.x.x (OSCI), Sicherheitsvorgaben (ST)“, 2008.

[BSI] Bundesamt für Sicherheit in der Informationstechnik (BSI).

[BSI_SigI_A6] Bundesamt für Sicherheit in der Informationstechnik, „Spezifikation zur Entwicklung interoperabler Verfahren und Komponenten nach SigG/SigV, Signatur-Interoperabilitätsspezifikation SigI, Abschnitt A6 Gültigkeitsmodell“, Version 1.1A, 17. Juni 1999.

[BSI-VPS_Präsentat] Bundesamt für Sicherheit in der Informationstechnik, BundOnline 2005, „Die Virtuelle Poststelle als BundOnline 2005 Basiskomponente ‚Datensicherheit’ – Informationen zu Konzept und Realisierung“, Februar 2004. Verfügbar unter http://www.bsi.bund.de/fachthem/egov/download/6_VPS_Infofolien.pdf

[CC-Teil2] „Common Criteria – Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik, Teil 2: Funktionale Sicherheitsanforderungen“, Version 2.1, August 1999.

[CC-Teil3] „Common Criteria – Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik, Teil 3:

Anforderungen an die Vertrauenswürdigkeit“, Version 2.1, August 1999.

[CEM] „Common Criteria – Common Methodology for Information Technology Security Evaluation, CEM-2001/0015R, Part 2: Evaluation Methodology“, Version 1.1, Februar 2002.

[CRL] Network Working Group: „Internet X.509 Public Key Infrastructure – Certificate and CRL Profile. Request for Comments 2459“, Januar 1999.

[Fachkonzept_v2.3.1] Bundesamt für Sicherheit in der Informationstechnik, BSI, und IBM Deutschland GmbH, IBM Global Services, „Fachkonzept für die Virtuelle Poststelle als Basiskomponente Datensicherheit von BundOnline 2005“, Version 2.3.1, 30.05.2003.

[ISIS-MTT] Common ISIS-MTT Specifications for Interoperable PKI Applications from T7 & TeleTrusT: “Specification”, Version 1.1, 16. März 2004.

[ISIS-MTT_SigG] Common ISIS-MTT Specifications for Interoperable PKI Applications from T7 & TeleTrusT: “Specification – Optional Profile – SigG-Profile”, Version 1.1, 16. März 2004.

[LDAP] Network Working Group: „Internet X.509 Public Key Infrastructure – Operational Protocols – LDAPv2. Request for Comments 2559“, April 1999.

[OCSP] Network Working Group: „Internet X.509 Public Key Infrastructure – Online Certificate Status Protocol – OCSP. Request for Comments 2560“, Juni 1999.

[OSCI] Online Services Computer Interface (OSCI), www.osci.de.

[OSCI-Transport] OSC Leitstelle, „OSCI-Transport 1.2”, 06.06.2002.

[PKCS#1] RSA, „PKCS #1 v2.1: RSA Cryptographic Standard“, 14.6.2002.

[RSA] R. Rivest, A. Shamir, L. Adleman: A method for obtaining digital signatures and public key cryptosystems, Communications of the ACM, vol. 21 no. 2, 1978.

[SHA-1] National Institute of Standards and Technology (NIST): FIPS Publication 180-2: Secure Hash Standard (SHS), August 2002 und Change Notice 1, Februar 2004.

[SigG] Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz – SigG), 16. Mai 2001.

[SignCubes] OPENLiMiT SignCubes 1.6, „Sicherheitsvorgaben (ST)“, Version 1.0, 20.7.2004.

[SigV] Verordnung zur elektronischen Signatur (Signaturverordnung – SigV), 16. November 2001.

[SigV_Begr] Begründung zum Entwurf einer Verordnung zur elektronischen Signatur in der Fassung des Kabinettbeschlusses vom 24.10.2001.

[VPS-SiKo] BundOnline 2005, Bundesamt für Sicherheit in der Informationstechnik, bremen online services GmbH & Co. KG, datenschutz nord GmbH, „Generisches Sicherheitskonzept für die Kern- und Webkomponenten der Virtuellen Poststelle“, 2004.[36]

12 Anhang: Technische Einsatzumgebung

173 Neben der in Tabelle 2 aufgeführten Software werden für den Betrieb des EVG folgende Komponenten benötigt, die somit die technische Einsatzumgebung definieren.

12.1 Hard- und Software

174 Hinsichtlich der Serverkomponenten für den Verifikations- und Download-server – auf dem die Verifikationsanwendung bereitgestellt wird – werden folgende Systemumgebungen unterstützt:

- Hardware:
  - Mind. 2 GHz i386 (Intel Xeon o.ä.) Prozessor mit mindestens 2 GB RAM und 40 GB Harddisk;
  - Sun Sparc mit mind. 300 MHz-Prozessor mit mindestens 2 GB RAM und 20 GB Harddisk;
- Betriebssysteme:
  - Linux (SuSE Linux Enterprise Server 9);
  - Windows 2003 Server;
  - Solaris 9;
- Java: SUN 1.4.2_04;
- Application Server: JBoss 3.2.5 inkl. Tomcat 5.0.26;
- Datenbank: MySQL 4.1;
- Browser zur Administration.

175 Hinsichtlich der Clientkomponenten für die Verifikationsanwendung werden folgende Systemumgebungen unterstützt:

- Hardware:
  - Mind. 1 GHz i386 (Intel Xeon o.ä.) Prozessor mit 256 MB RAM und 20 GB Harddisk;

[36] Das generische Sicherheitskonzept für die Kern- und Webkomponenten der Virtuellen Poststelle ist u.a. auf der E-Government-Seite des Bundesamtes für Sicherheit in der Informationstechnik (BSI) unter www.bsi.bund.de/fachthem/egov/vps.htm verfügbar.

- Betriebssysteme:
  - Linux (SuSE Linux Professional 9.x);
  - Windows 2000;
  - Windows XP;
- Java: SUN 1.4.2_04.

12.2 Zertifikate

176 Folgende X.509v3-Zertifikate werden unterstützt:

- SigG-konforme qualifizierte Zertifikate;
- (System-)Zertifikat des OCSP/CRL-Relays zur Gewährleistung der Systemsicherheit mit einer Mindestlänge von 2048 Bit.