Governikus – Teil der virtuellen Poststelle des Bundes, Version 3.3 (Basis), Sicherheitsvorgaben (ST)

bremen online services GmbH & Co. KG

Version 1.21

22.11.2010

Zertifizierungs-ID: BSI-DSZ-CC-0654-20xx

Bestätigungs-ID: BSI.02121.TE.xx.20xx

Historie

Version	Datum	geänderte Kapitel	Grund der Änderung	Geändert durch
0.9	19.07.2005		Erstellung	Matthias Intemann Sönke Maseberg
0.91	09.09.2005		Berücksichtigung des Dokumentenchecks von TSI vom 29.07.2005 sowie des Review-Protokolls vom BSI vom 23.08.2005 Nennung Zertifizierungs- und Bestätigungs-Ids	Matthias Intemann Sönke Maseberg
0.92	10.10.2005		Berücksichtigung des Projektmeetings vom 14.09.2005 sowie des Dokumentenchecks von TSI vom 29.07.2005 und des Review-Protokolls vom BSI vom 23.08.2005	Matthias Intemann Sönke Maseberg
0.93	18.10.2005	Rd. 214	Begründung zu Abhängigkeiten von FMT_MSA.2 präzisiert	Matthias Intemann Sönke Maseberg
0.94	09.03.2006	inhaltliche Änderungen: Tabellen 1, 8-11 und Rd.-Nr. 30, 67; hinzugefügt wurden Rd.-Nr. 133 und 134; geändert wurden Rd.-Nr. 191 (vormals 189), 201 (199), 213 (211), 234 (232)	Nach positiver Evaluierung der Version 0.93 wurde der Funktionsumfang des Kernsystems erweitert – Verifikation der Antworten des OCSP/CRL-Relays, sofern beide Komponenten nicht zusammen in einem vertrauenswürdigen Netz betrieben werden –, was in dieser Version nachgezogen wurde. Dabei wurden im ETR enthaltene „Anmerkungen der Evaluatoren“ berücksichtigt.	Matthias Intemann Sönke Maseberg
0.95	22.06.2006	Rd.-Nr. 128, 130, 132, 134; Kapitel 10	Aufnahme der Hashfunktion RIPEMD-160	Matthias Intemann Sönke Maseberg
1.0	21.11.2007		Kleinere editorische Änderungen	Ulrich Horst Ingo Schumann
1.1	15.08.2008	Alle	Überarbeitung für das Release Governikus 3.3.0.0	Ingo Schumann
1.11	10.09.2008	Kapitel 8.2	Abschnitt 8.2.2 eingefügt	Ingo Schumann
1.12	19.09.2008	2.3 (NetSigner-Beschreibung) und 5.1.1 (Fußnote zu SHA-1)	Anmerkungen aus Review-Protokoll vom BSI vom 15.09.2008 entsprechend eingearbeitet.	Ingo Schumann

1.13	02.02.2009	Alle	Finale Version: Aktualisierung Dokument, Anmerkungen der Evaluatoren berücksichtig,	Ingo Schumann
1.2	24.09.2009		Aktualisierung Versionsnummern und Referenzen Kartenansteuerung	Ingo Schumann
1.21	22.11.2010	1.1; 10	Aktualisierung IDs, Versionsnummer der Software und Referenzen Kartenansteuerung	Ingo Schumann

Dokumenten-Überwachungsverfahren

Status: final	Prozess-/Dokumentbesitzer: Ingo Schumann (bremen online services GmbH & Co. KG)

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 ST-Einführung

1.1 EVG-Identifikation

1	ST-Name:	Governikus - Teil der virtuellen Poststelle des Bundes, Version 3.3 (Basis), Sicherheitsvorgaben (ST)
2	ST-Version:	1.21
3	Datum:	22.11.2010
4	Autoren:	bremen online services GmbH & Co. KG datenschutz nord GmbH
5	EVG-Name:	Governikus, Version 3.3 (Basis) – abkürzend mit „Basiskomponente“ bezeichnet
6	EVG-Version:	3.3.1.3
7	CC-Version:	2.3[1]
8	Zertifizierungs-ID:	BSI-DSZ-CC-0654-20xx
9	Bestätigungs-ID:	BSI.02121.TE.xx.20xx

1.2 EVG-Übersicht

10 Im Rahmen des Projektes BundOnline 2005 wurde die Virtuelle Poststelle des Bundes entwickelt. Sie stellt als zentrales Kommunikations-Gateway Sicherheitsdienste für die gesicherte Kommunikation zwischen Behörden und externen Kommunikationspartnern (Bürger, Wirtschaft und andere Behörden) bereit. Sie ist „baugleich“ zur Software Governikus und wurde unter dieser Produktbezeichnung weiterentwickelt. Entsprechend den zu erwartenden Kommunikationsszenarien im E-Government soll Governikus folgende wesentliche Funktionen serverbasiert zur Verfügung stellen:

- Signaturbildung und -prüfung;
- 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 von Governikus auf einem Laufzettel;

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

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

11 Abbildung 1 illustriert den Aufbau von Governikus.

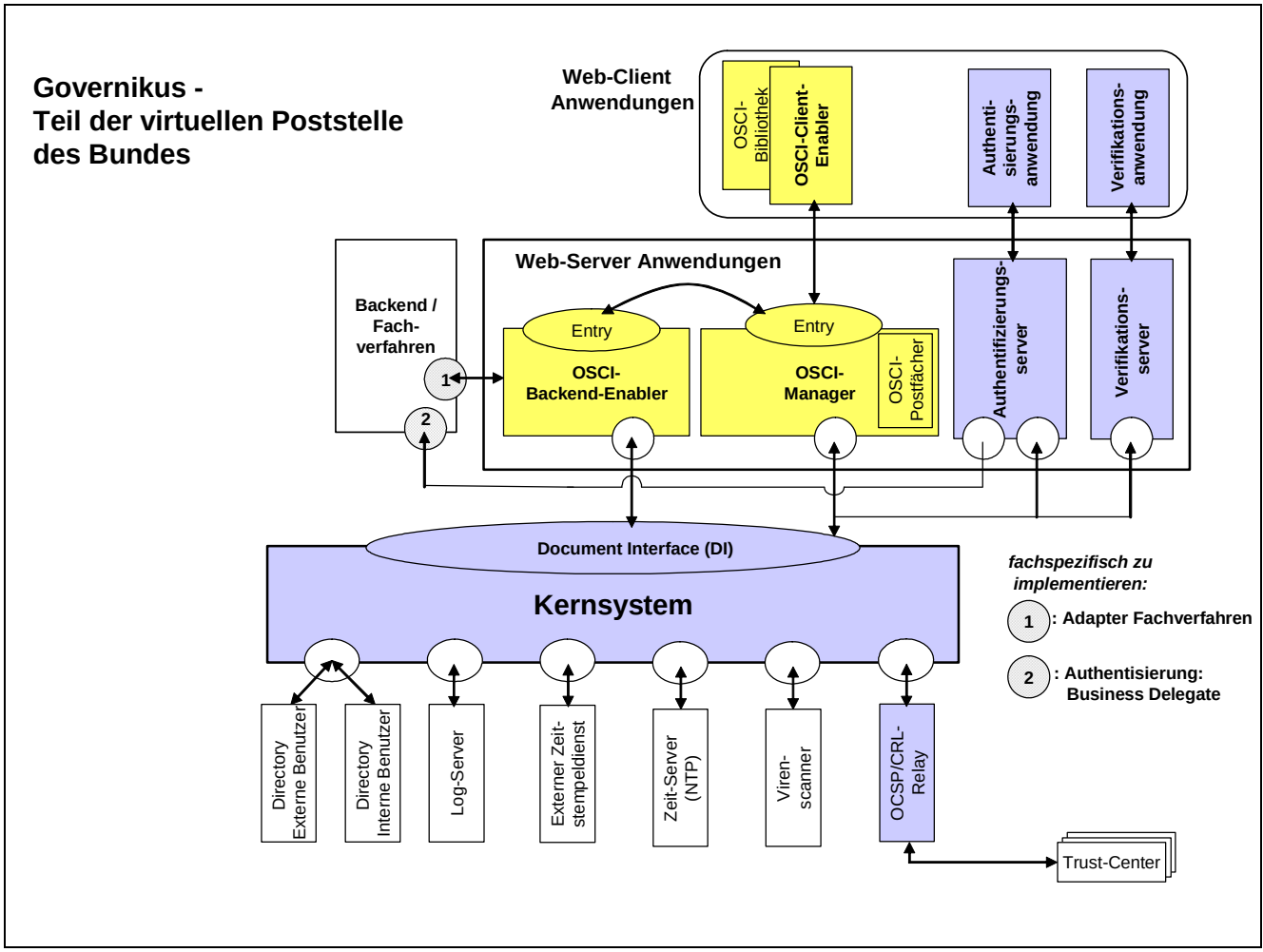

Abbildung 1: Aufbau von Governikus

12 Die Re-Evaluierung von Governikus wird im Rahmen einer kompositiven Evaluierung durchgeführt, in der Governikus in drei logische Einheiten aufgeteilt wird, die jeweils als ein eigenständiger Evaluationsgegenstand (EVG) evaluiert, zertifiziert und bestätigt werden. Die drei EVGs sind:

- EVG1: Governikus, Version 3.3 (Basis);
- EVG2: Governikus, Version 3.3 (OSCI);
- EVG3: Governikus, Version 3.3 (Verifikationsmodul).

13 Die vorliegenden Sicherheitsvorgaben (Security Target – ST) fokussieren auf den Evaluationsgegenstand „Governikus, Version 3.3 (Basis)“ – abkürzend als Basiskomponente bezeichnet.

14 Der Evaluationsgegenstand stellt Basisfunktionalitäten für andere Systeme von Governikus zur Verfügung:

- Unterstützung bei der Erzeugung qualifizierter elektronischer (Batch-) Signaturen[2];
- mathematische Prüfung qualifizierter elektronischer Signaturen (Verifikation);
- Statusprüfung qualifizierter Zertifikate (Validierung).

15 Der Evaluationsgegenstand stellt als Teil einer Signaturanwendungskomponente nach SigG/SigV eine Funktionsbibliothek – und damit eine Basis für weitere Signaturanwendungskomponenten – dar, die gemäß § 15 Abs. 7 und § 17 Abs. 4 SigG [SigG] sowie § 11 Abs. 3 SigV [SigV] evaluiert, zertifiziert und bestätigt werden.

16 Dementsprechend werden im Folgenden ausschließlich die für die Erfüllung des Signaturgesetzes relevanten Funktionalitäten von Governikus – die Funktionalitäten zur Signaturbildung und -prüfung – betrachtet.

17 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

18 Der in Abschnitt 2 beschriebene Evaluationsgegenstand (EVG) „Governikus, Version 3.3.x.x (Basis)“ ist zu folgenden Teilen der Common Criteria entwickelt:

- konform zu Teil 2 [CC-Teil2];
- konform zu 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).

19 Dabei wird die vom EVG zur Verfügung gestellte Sicherheitsfunktionalität vollständig aus funktionalen Sicherheitskomponenten aus dem Teil 2 der CC hergeleitet.

20 Hinsichtlich Teil 3 der CC soll die Basiskomponente als Teil einer 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

[2] Eine Batchsignatur ist eine serverbasiert erzeugte SigG-konforme qualifizierte elektronische Signatur gemäß [BNetzA_FAQ18], bei der „eine große Anzahl praktisch gleicher Vorgänge – z. B. Rechnungen, die sich ‚nur’ im Betrag und der Zustelladresse unterscheiden – […] in einer besonders gesicherten Umgebung automatisiert abgearbeitet“ werden.

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[3] 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[4] Prüfung der Handbücher
    - AVA_SOF.1 Stärke der EVG-Sicherheitsfunktionen
    - AVA_VLA.1[5] Schwachstellenanalyse des Entwicklers

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

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

- 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 Vertrauenswürdigkeitskomponente realisiert:
  - Auslieferung und Betrieb
    - ADO_DEL.2 Erkennung von Modifizierungen
  - Schwachstellenbewertung
    - AVA_MSU.3 Analysieren und Testen auf unsichere Zustände

2 EVG-Beschreibung

2.1 Kompositive Evaluierung

21 Die Evaluierung von Governikus wird im Rahmen einer kompositiven Evaluierung durchgeführt, in der Governikus in drei logische Einheiten aufgeteilt wird, die jeweils als ein eigenständiger Evaluationsgegenstand (EVG) evaluiert, zertifiziert und bestätigt werden.

22 Die drei EVGs sind in Abbildung 2 illustriert:

- EVG1: Governikus, Version 3.3 (Basis);
- EVG2: Governikus, Version 3.3 (OSCI);
- EVG3: Governikus, Version 3.3 (Verifikationsmodul).

23 Diese Sicherheitsvorgaben fokussieren auf den EVG „Governikus, Version 3.3“ – abkürzend als Basiskomponente bezeichnet.

---

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

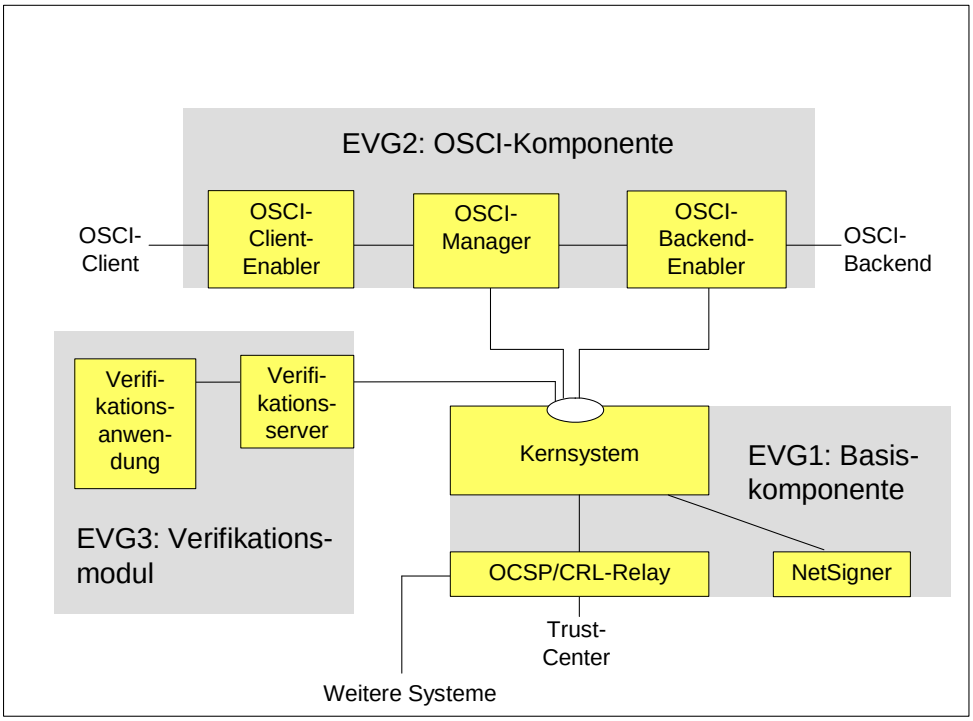

Abbildung 2: EVG-Übersicht

2.2 EVG-Umfang

24 Der Evaluationsgegenstand „Governikus, Version 3.3 (Basis)“ stellt Basisfunktionalitäten für andere Systeme der VPS zur Verfügung:

- Unterstützung bei der Erzeugung qualifizierter elektronischer (Batch-) Signaturen[2];
- mathematische Prüfung qualifizierter elektronischer Signaturen (Verifikation) [6];
- Statusprüfung qualifizierter Zertifikate (Validierung).

[6] Die Statusprüfung einer qualifizierten elektronischen Signatur, bei der geprüft wird, ob
- der Signaturzeitpunkt (vgl. Glossar) im Gültigkeitszeitraum des Zertifikats liegt, in dem der Prüfschlüssel enthalten ist,
- das Zertifikat zum Signaturzeitpunkt vorhanden und bereits freigegeben war und
- das Zertifikat zum Signaturzeitpunkt gesperrt war,

wird nicht vollständig vom EVG umgesetzt: Während die erste Prüfung beim anfordernden System erfolgt – die erforderlichen Statusinformationen sind durch die Angaben zum Gültigkeitszeitraum statisch im Zertifikat enthalten – stellt der EVG die Funktionalitäten zur Statusprüfung qualifizierter Zertifikate zur Verfügung.

25 Der EVG ist als Teil einer Signaturanwendungskomponente[7] eine Funktionsbibliothek und stellt damit eine Basis für weitere Signaturanwendungskomponenten dar.

26 Der EVG ist eine Software, die auf geeigneter Hardware mit geeigneten Betriebsmitteln betrieben wird – insbesondere mit SigG-konformen Chipkartenlesern, sicheren Signaturerstellungseinheiten (in diesen Fall Signaturkarten[8]) sowie auf den EVG zugreifenden Systemen, die die Anforderungen von SigG und SigV an Signaturanwendungskomponente erfüllen.

27 Die Basiskomponente wird auf Servern in einem „geschützten Einsatzbereich (Regelfall/Standardlösung)“ [BNetzA2005] betrieben und über jeweilige Web-Oberflächen (Graphical User Interface – GUI) von Administratoren konfiguriert. Nachdem eine Signaturkarte für die Erzeugung von Batchsignaturen[2] vom Signaturschlüssel-Inhaber freigeschaltet wurde, arbeitet die Basiskomponente im Produktivbetrieb automatisiert und ohne menschliche Interaktionen.

28 Der Evaluationsgegenstand stellt folgende Funktionen zur Verfügung:

- Der EVG erhält von außen über eine Schnittstelle die Anforderung[9], Daten serverbasiert mit einer Batchsignatur[2] zu versehen. Der EVG führt die zu signierenden Daten einer angeschlossenen sicheren Signaturerstellungseinheit zu (vgl. Einsatzszenario in Abschnitt 2.4.4) und liefert das Ergebnis (Signatur oder Fehlermeldung) zurück.

  Es können mehrere Chipkartenleser angeschlossen sein, die Karten unterschiedlicher Signaturschlüssel-Inhaber enthalten können.

- Der EVG erhält von außen über eine Schnittstelle die Anforderung[9], die mathematische Korrektheit einer qualifizierten elektronischen Signatur zu prüfen. Der EVG führt eine Signaturprüfung durch, d. h. der EVG prüft die mathematische Korrektheit der Signatur mittels zugehörigem Prüfschlüssel (öffentlichem Schlüssel aus qualifiziertem Zertifikat) und geeigneten kryptographischen Verfahren, und liefert das mit einer elektronischen

[7] Der Begriff „Teil einer Signaturanwendungskomponente“ wird in der Auflistung der Produkte für qualifizierte elektronische Signaturen auf der Web-Site der Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (Bundesnetzagentur) unter www.bundesnetzagentur.de –- in Abgrenzung zu einer „vollständigen Signaturanwendungskomponente“ – verwendet und in Funktionsbibliotheken und Chipkartenleser unterteilt.

[8] Sichere Signaturerstellungseinheiten gemäß SigG/SigV werden in diesem Kontext ausschließlich als Chipkarten, also Signaturkarten, realisiert, so dass die Begriffe synonym genutzt werden.

[9] Der EVG wird unter der Annahme betrieben, dass ein anforderndes System, das auf diesen EVG zugreift, die Anforderungen von SigG und SigV an Signaturanwendungskomponente erfüllt.

Signatur versehene Ergebnis der Verifikation (korrekte oder nicht korrekte Signatur oder Fehlermeldung) zurück[10].

- Der EVG erhält von außen über eine Schnittstelle die Anforderung[9], die Gültigkeit eines qualifizierten Zertifikats zu einem übermittelten Zeitpunkt bzw. – sofern kein expliziter Zeitpunkt übermittelt wurde – zum Prüfzeitpunkt[11] festzustellen. Der EVG stellt fest, ob das qualifizierte Zertifikat zum angegebenen Zeitpunkt bzw. zum Prüfzeitpunkt vorhanden und nicht gesperrt war und der Gültigkeitszeitraum des qualifizierten Zertifikats zum angegebenen Zeitpunkt bzw. Prüfzeitpunkt bereits begonnen und noch nicht abgelaufen war, und liefert das mit einer elektronischen Signatur versehene Ergebnis der Validierung in Form einer Interpretation (gültig und nicht gesperrt, unbekannt oder gesperrt) zurück. Zusätzlich werden die Ergebnisse der Verzeichnisdienste zurückgeliefert.

  In diesem Kontext prüft der EVG die mathematische Korrektheit der qualifizierten elektronischen Signaturen von Antworten auf Zertifikatsstatus-Anfragen (Online Certificate Status Protocol – OCSP) und Sperrlisten (Certificate Revocation Lists – CRLs), holt Zertifikate via Lightweight Directory Access Protocol (LDAP) ein und validiert Zertifikate der Zertifikatskette.

29 Die Kommunikation zum anfordernden System[12] – beispielsweise zu einem Verifikationsserver, OSCI-Manager oder OSCI-Backend-Enabler (vgl. Abbildung 2), die von außen über eine Schnittstelle auf den EVG zugreifen können – erfolgt jeweils abgesichert, so dass die tatsächliche Anforderung bearbeitet und zutreffende Ergebnisse zurückliefert werden (vgl. Abschnitt 2.4.4).

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

2.3 Technische Realisierung

31 Die Basiskomponente besteht aus den Teilsystemen

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

inklusive einer Administrationsanwendung als Graphical User Interface (GUI) zur Bedienung. Abbildung 3 illustriert die Teilsysteme der Basiskomponente.

[10] Dieser Dienst ergibt Sinn, da die Basiskomponente u. U. mehr Signaturformate als das anfordernde System unterstützt.

[11] vgl. Glossar

[12] vgl. Glossar

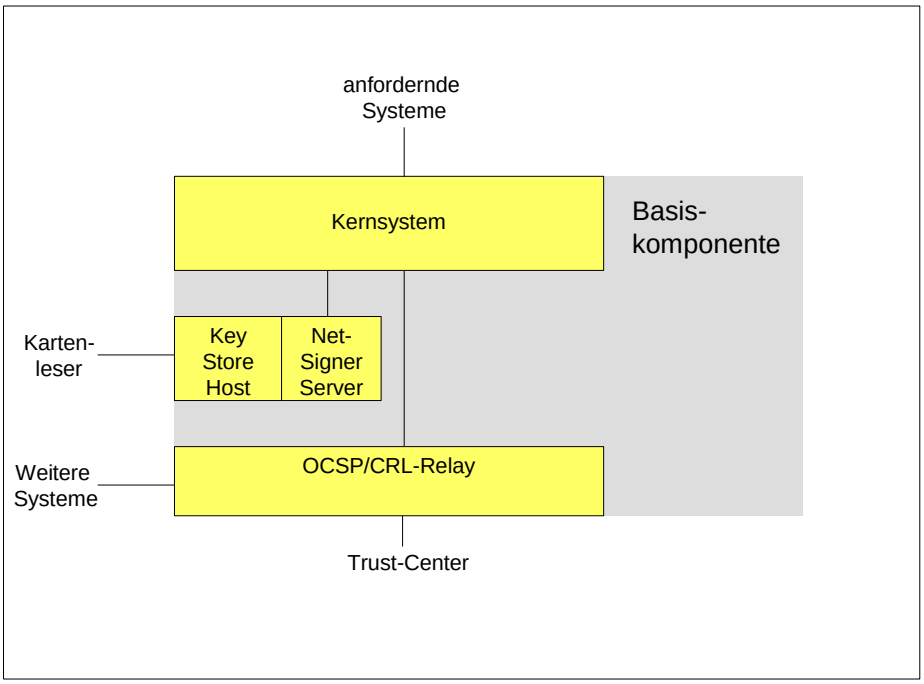

Abbildung 3: Basiskomponente

32 Kernsystem, NetSigner und OCSP/CRL-Relay können voneinander getrennt betrieben werden, d. h. nicht innerhalb eines LANs (Local Area Networks), sondern über ein Weitverkehrsnetz (Wide Area Network – WAN) verbunden. Auf ein OCSP/CRL-Relay können auch mehrere berechtigte Systeme – auch über eine zweite Schnittstelle, die ein anderes Protokoll unterstützt – zugreifen.

33 Die wesentlichen Aufgaben der Teilsysteme:

- Das Kernsystem nimmt Anforderungen von außen über eine Schnittstelle an. Die Anforderungen sind (vgl. Abschnitt 2.2):[13]
  - Unterstützung bei der Erzeugung qualifizierter elektronischer (Batch-)Signaturen[2];
  - mathematische Prüfung qualifizierter elektronischer Signaturen (Verifikation);
  - Statusprüfung qualifizierter Zertifikate (Validierung).
- Der NetSigner ist dafür zuständig, zu signierende Daten der sicheren Signaturerstellungseinheit über einen angeschlossenen Chipkartenleser zuzuführen, wobei mehrere Chipkartenleser angeschlossen sein können, die Karten unterschiedlicher Signaturschlüssel-Inhaber enthalten können. Der NetSigner selbst setzt sich aus zwei Teilkomponenten zusammen,

[13] Weitere Funktionalitäten des Kernsystems, die allerdings nicht Bestandteil der Zertifizierung und Bestätigung sind, sind in Abschnitt 1.2 aufgeführt.

der NetSigner Serverkomponente, die für Konfiguration des NetSigners und Kommunikation mit dem Kernsystem zuständig ist, sowie dem KeyStoreHost, an den die Kartenleser angeschlossen sind.

- Das OCSP/CRL-Relay stellt die Gültigkeit eines Zertifikats fest und nutzt dazu verschiedene Verzeichnisdienste.

2.4 Signaturgesetz (SigG) und -verordnung (SigV)

2.4.1 Rechtliche Grundlagen

34 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 [...]“.

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

36 § 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 3 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.“

37 § 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."

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

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

- das Erzeugen einer Signatur vorher eindeutig angezeigt wird[14],
- erkennbar ist, auf welche Daten sich die Signatur bezieht[15],
- bei Bedarf der Inhalt der zu signierenden Daten hinreichend zu erkennen ist[16],
- eine Signatur nur durch die berechtigt signierende Person erfolgt[17],
- die Identifikationsdaten nicht preisgegeben und nur auf der jeweiligen „sicheren Signaturerstellungseinheit" gespeichert werden[18].

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

- erkennbar wird, auf welche Daten sich die Signatur bezieht,
- erkennbar wird, ob die Daten unverändert sind,

---

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

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

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

[17] „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]

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

- 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.

41 Schutz vor unbefugter Veränderung: Sicherheitstechnische Veränderungen an der Signaturanwendungskomponente müssen für den Nutzer erkennbar[19] werden."

2.4.2 Batchsignatur

42 Eine Batchsignatur ist eine serverbasiert erzeugte SigG-konforme qualifizierte elektronische Signatur gemäß [BNetzA_FAQ18]. Eine Batchsignatur wird in [BNetzA_FAQ18] wie folgt definiert: „eine große Anzahl praktisch gleicher Vorgänge – z. B. Rechnungen, die sich ‚nur' im Betrag und der Zustelladresse unterscheiden – werden in einer besonders gesicherten Umgebung automatisiert abgearbeitet".

2.4.3 Signaturgesetz-Anforderungen an den EVG

43 Der EVG ist als Teil einer Signaturanwendungskomponente eine Funktionsbibliothek und stellt damit eine Basis für weitere Signaturanwendungskomponenten dar. Nicht alle Anforderungen von SigG und SigV können daher vom EVG abgedeckt werden.

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

---

[19] „Dies kann – abhängig von der Art des Einsatzbereiches (vgl. Abschnitt 4 [BNetzA2005]) – 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]

Zur Erzeugung von Signaturen

45 Der EVG erstellt Batchsignaturen für autorisierte anfordernde Systeme[20]. Von daher obliegt die Funktionalität, dass „die Erzeugung einer Signatur vorher eindeutig angezeigt wird“ (§ 15 Abs. 2 SigV), dem anfordernden System in der IT-Umgebung, welches einen Auftrag an den EVG absendet. Das anfordernde System in der IT-Umgebung erfüllt – per Annahme/Auflage – die SigG/SigV-Anforderungen an eine Signaturanwendungskomponente und damit die Sicherheitsanforderungen, die der EVG nicht realisieren kann. Durch den EVG wird einzig dem Signaturschlüssel-Inhaber vor der Freischaltung seiner Signaturkarte – also vor der PIN-Eingabe – authentisch angezeigt,

- für welches anfordernde System inkl. Zweck (Fachaufgabe) und
- innerhalb welchen Zeitfensters bzw. für welche Anzahl von Batchsignaturen

er seine Signaturkarte freischaltet (dieser Aspekt wird auch im Folgenden thematisiert). Der Signaturschlüssel-Inhaber delegiert die Signaturanforderung zur Erzeugung einer Batchsignatur an eine Person, die das berechtigte anfordernde System bedient.

46 Zur Anforderung, dass „eine Signatur nur durch die berechtigt signierende Person erfolgt“ (§ 15 Abs. 2 SigV) heißt es in [SigV_Begr]: „Die Signaturkomponente darf nicht ohne Anwendung der Identifikationsdaten genutzt werden können, es sei denn, Signaturen sollen für ein festes Zeitfenster oder eine bestimmte Anzahl ohne jeweilige Identifizierung erzeugt werden. In diesem Falle ist sicherzustellen, dass Unberechtigte keine Signaturen veranlassen können (Nummer 1 Buchst. b)). [...] Insbesondere bei der automatischen Erzeugung von Signaturen (‚Massensignaturen’) muss sichergestellt sein, dass Signaturen nur zu dem voreingestellten Zweck (z. B. Signaturen zu Zahlungsanweisungen bei Großanwendern) und durch eine zuvor geprüfte und abgenommene Anwendung vorgenommen werden können.”

In [BNetzA_FAQ18] wird der Aspekt der Einschränkung der Signierfähigkeit weiter thematisiert:

- „Es können Zeitfenster eingerichtet werden, in denen alle abzusendenden Dokumente signiert werden – pro Zeitfenster erfolgt dann eine einmalige PIN-Eingabe. Beispielsweise kann ein Verzeichnisdienst seine zu signierenden Auskünfte vollautomatisch mit einer personalisierten Karte und einmaligen PIN-Eingabe für einen Zeitraum X (z. B. 1 Stunde) erteilen.
- Es kann eine Freigabe einer bestimmten Anzahl von Signiervorgängen mittels einmaliger Eingabe der PIN erfolgen.“

Sichere Signaturerstellungseinheiten sollen gemäß § 15 Abs. 1 SigV gewährleisten, „dass der Signaturschlüssel erst nach Identifikation des Inhabers durch Besitz und Wissen oder durch Besitz und ein oder mehrere biometrische Merkmale angewendet werden kann.“ Um „den Besitz“ in diesem Sze-

[20] vgl. Glossar

nario sicherzustellen, werden Anforderungen an die Umgebung gestellt, in der die Signaturkarten genutzt werden (vgl. Abschnitt 2.4.4) und der EVG stellt sicher, dass der Signaturschlüssel-Inhaber per E-Mail informiert wird, falls seine Signaturkarte aus dem Chipkartenleser entfernt wird.

47 In diesem Zusammenhang ist für den EVG und die IT-Umgebung zu berücksichtigen:

- Der EVG muss gewährleisten, dass eine Batchsignatur nur durch ein berechtigtes anforderndes System angefordert werden darf.
- Der EVG muss gewährleisten, dass eine Batchsignatur nur innerhalb eines festen Zeitfensters oder für eine bestimmte Anzahl von Batchsignaturen ohne jeweilige PIN-Eingabe erzeugt wird.
- In der IT-Umgebung muss gewährleistet sein, dass nur eine berechtigte Person das anfordernde System bedienen kann. Das anfordernde System in der IT-Umgebung erfüllt – per Annahme/Auflage – die SigG/SigV-Anforderungen an eine Signaturanwendungskomponente und damit die Sicherheitsanforderungen, die der EVG nicht realisieren kann.
- Die Maßnahmen zur Kommunikationssicherheit, um sicherzustellen, dass Batchsignaturen nur für berechtigte Systeme erzeugt werden können, sind vom EVG und von der IT-Umgebung umzusetzen (vgl. Abschnitt 2.4.4).

48 Die beiden Anforderungen, dass sich feststellen lässt, „auf welche Daten sich die Signatur bezieht“ und dass der EVG „nach Bedarf auch den Inhalt der zu signierenden Daten hinreichend erkennen lassen“ muss (§ 17 Abs. 2 SigG), obliegen dem anfordernden System in der IT-Umgebung, das – per Annahme/Auflage – die SigG/SigV-Anforderungen an eine Signaturanwendungskomponente erfüllt und damit insbesondere die Sicherheitsanforderungen realisiert, die der EVG nicht realisieren kann.

49 Die Anforderung, dass „die Identifikationsdaten nicht preisgegeben und diese nur auf der jeweiligen sicheren Signaturerstellungseinheit gespeichert werden“ (§ 15 Abs. 2 SigV), muss von der EVG-Umgebung durch Nutzung einer sicheren Signaturerstellungseinheit und Eingabe der PIN am PIN-Pad des Chipkartenlesers gewährleistet werden.

Zur Prüfung einer Signatur

50 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,“
- „erkennbar wird, welchem Signaturschlüssel-Inhaber die Signatur zuzuordnen ist“ und

- „erkennbar wird, welche Inhalte das qualifizierte Zertifikat, auf dem die Signatur beruht, und zugehörige qualifizierte Attribut-Zertifikate aufweisen“ ([BNetzA2005])

obliegen dem anfordernden System in der IT-Umgebung, das – per Annahme/Auflage – die SigG/SigV-Anforderungen an eine Signaturanwendungskomponente erfüllt und damit die Sicherheitsanforderungen realisiert, die der EVG nicht realisieren kann.

51 Die Sicherheitsanforderungen, dass bei der Prüfung einer qualifizierten elektronischen Signatur „die Korrektheit der Signatur zuverlässig geprüft und zutreffend angezeigt wird“ (§ 15 Abs. 2 SigV) obliegt

- hinsichtlich der Anzeige ebenfalls dem anfordernden System in der IT-Umgebung, welches – per Annahme/Auflage – die SigG/SigV-Anforderungen an eine Signaturanwendungskomponente erfüllt,
- allerdings hinsichtlich der Prüfung der Korrektheit der Signatur dem EVG.

52 Die Anforderung dass „eindeutig erkennbar wird, ob die nachgeprüften qualifizierten Zertifikate im jeweiligen Zertifikat-Verzeichnis zum angegebenen Zeitpunkt vorhanden und nicht gesperrt waren“ (§ 15 Abs. 2 SigV) erfolgen

- hinsichtlich der Anzeige ebenfalls beim anfordernden System in der IT-Umgebung, welches – per Annahme/Auflage – die SigG/SigV-Anforderungen an eine Signaturanwendungskomponente erfüllt,
- allerdings hinsichtlich der Validierung beim EVG.

Schutz vor unbefugter Veränderung

53 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 der Signaturschlüssel-Inhaber per E-Mail informiert wird, sofern seine Signaturkarte aus dem Chipkartenleser entfernt wird, und dass in der IT-Umgebung die Anforderungen an den sicheren Betrieb von den Administratoren realisiert werden müssen.

2.4.4 Einsatzszenario

54 Im Folgenden wird das Szenario beschrieben, in dem die oben genannten Anforderungen des Signaturgesetzes erfüllt werden.

Vorbereitung der Batchsignaturen

55 Der zuständige Mitarbeiter, der der Signaturschlüssel-Inhaber ist, steckt die entsprechende Signaturkarte in den dafür vorgesehenen SigG-konformen Chipkartenleser und schaltet seine Karte durch Eingabe seiner PIN am PIN-Pad des Chipkartenlesers frei. Dem Signaturschlüssel-Inhaber wird vor Eingabe seiner PIN angezeigt, welches anfordernde System inkl. Zweck (Fachaufgabe) somit wie viele bzw. in welchem Zeitraum Batchsignaturen mit seiner Signaturkarte erzeugt werden können.

56 Die Chipkartenleser befinden sich in einem dedizierten, gesicherten Raum. Der Zugang zu diesem Raum ist restriktiv auf namentlich bekannte Personen beschränkt und vor Fremdzugriffen geschützt.

57 Wird eine Signaturkarte aus dem Chipkartenleser entfernt, erhält der Signaturschlüssel-Inhaber eine entsprechende Mitteilung per E-Mail. Das System, das auf die Signaturkarte zugreift, erhält eine Fehlermeldung, wenn die Signaturkarte aus dem Chipkartenleser entfernt wurde oder eine Signatur erzeugt werden soll, ohne dass eine entsprechende Signaturkarte verfügbar ist.

Einschränkung der Signiertätigkeit

58 Der EVG gewährleistet, dass nach Freischaltung der sicheren Signaturerstellungseinheit je nach Konfiguration entweder

- nur eine bestimmte Anzahl von Batchsignaturen und bzw. oder
- Batchsignaturen nur innerhalb eines Zeitfensters

59 erzeugt werden können, wobei die Konfiguration durch den Schlüssel-Administrator (Konfiguration der Voreinstellungen) und den Signaturschlüssel-Inhaber (Korrektur der Voreinstellungen, direkt vor PIN-Eingabe) erfolgt.

Systemauthentisierung/-autorisierung zur Batchsignatur

60 Der EVG stellt die Basis für weitere Signaturanwendungskomponenten dar, die nicht mehr zum EVG gehören. Es wird vorausgesetzt, dass ein anforderndes System, welches eine Batchsignatur anfordert, die SigG/SigV-Anforderungen an eine Signaturanwendungskomponente erfüllt.

61 Die Anforderung zur Erzeugung einer Batchsignatur, die der EVG von außen über eine Schnittstelle erhält, enthält insbesondere

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

und ist mit einer elektronischen Signatur versehen.

62 Die Anforderung zur Erzeugung einer Batchsignatur ist wie folgt abgesichert:

- Die Signaturanforderung wird mit einer elektronischen Signatur versehen. Dazu verfügt jedes anfordernde System, welches auf den NetSigner zugreifen darf, über einen privaten Schlüssel und ein entsprechendes (System-)Zertifikat (X.509-Zertifikat) und nutzt hinreichende kryptographische Algorithmen und Schlüssellängen (RSA mit Schlüssellängen von mindestens 2048 Bit).
- Die Basiskomponente (genauer das Kernsystem) prüft, ob das anfordernde System den NetSigner nutzen darf (Abgleich der SystemId und der OperationId mit den im Regelwerk der Basiskomponente (genauer des Kernsystems) enthaltenen Regeln, welche die Zulässigkeit von Zugriffen über eine Zuordnung (zulässige OperationId je SystemId) steuern), und lässt die Daten nach positiver Prüfung vom NetSigner signieren und sendet das Ergebnis zurück.

- Darüber hinaus stellt der NetSigner sicher, dass nur einem berechtigten System ein Zugriff auf eine zugeordnete sichere Signaturerstellungseinheit gewährt wird:
  - Es wird geprüft, dass die Signaturprüfung der Anfrage (Anfrage ist elektronisch signiert) mathematisch korrekt ist.
  - Der für die Verifikation der Anfrage benötigte öffentliche Schlüssel des anfordernden Systems liegt in Form eines (System-) Zertifikats im EVG – im Sinne eines Trust Anchors – vor. Das (System-) Zertifikat wird dabei nicht mit der Signier-Anforderung übertragen.
  - Zudem wird geprüft, dass die Zuordnung von (System-)Zertifikat der Signier-Anforderung des anfordernden Systems zur Rolle der Signaturkarte in der IT-Umgebung für die Erzeugung der Batchsignatur korrekt ist, d. h. das anfordernde System (gekennzeichnet durch das Zertifikat) darf die sichere Signaturerstellungseinheit, die die Batchsignatur erzeugen soll (gekennzeichnet durch die Rolle), nutzen.

  Dazu wird jeder Signaturkarte eindeutig eine Rolle zugeordnet. Aus Performancegründen können dabei verschiedene Signaturkarten ein und derselben Rolle zugeordnet sein. Signaturschlüssel-Inhaber können mehrere Signaturkarten besitzen. Jeder Rolle wird nun eindeutig ein anforderndes System zugeordnet – und zwar über das (System-)Zertifikat –, welches damit eine Signaturkarte dieser Rolle nutzen kann. Ein anforderndes System darf eine Signaturkarte zur Erzeugung einer Batchsignatur nur dann nutzen, wenn es im Besitz des Privatschlüssels zu dem (System-)Zertifikat der Rolle ist, der die Signaturkarte zugeordnet ist (vgl. auch Glossar).
- Eine Revokation wird wie folgt durchgeführt: Sollten die benutzten (System-)Zertifikate für die Absicherung innerhalb dieses Szenarios – die für keine anderen Zwecke benutzt werden – revoziert werden müssen, hat der Schlüssel-Administrator die Pflicht, dies manuell zu organisieren.

63 Durch diese Vorgehensweise wird gewährleistet, dass nur ein zulässiges System auf eine erlaubte Signaturkarte zugreifen kann und die Authentizität und Integrität der zu signierenden Daten gesichert ist.

64 Alle Systeme, welche die Erzeugung einer Batchsignatur bei der Basiskomponente anfordern, müssen an der Schnittstelle obige Informationen (vgl. Rd-Nr. 61) zur Verfügung stellen.

2.4.5 Kommunikationssicherheit

65 Die Kommunikation zwischen den Komponenten erfolgt auf sichere Art und Weise:

- Die Komponenten, die in einem lokalen Netz (Local Area Network – LAN) aufgestellt sind, sind dadurch abgesichert, dass sie sich allesamt in einem sicheren Netz befinden. Zusätzlich gilt:

- Die Signaturanforderung zur Erzeugung einer serverbasiert erzeugten Batchsignatur wird in der in Abschnitt 2.4.3 beschriebenen Art und Weise abgesichert.
- Das Verifikationsergebnis, welches der EVG an das anfordernde System zurückgibt, wird vom Kernsystem mit einer elektronischen Signatur versehen. Kernsystem und NetSigner (Server und Kartenansteuerung) befinden sich im selben Netz. Ein anforderndes System kann die Signatur des Kernsystems durch einen Sicherheitsanker (Trust Anchor) prüfen. Ein Abgleich, ob die Antwort zur Frage passt, kann beim anfordernden System erfolgen.
- Das Validierungsergebnis – in Form des Verzeichnisdienst-Ergebnisses sowie einer Interpretation (gültig und nicht gesperrt, unbekannt oder gesperrt) – wird vom OCSP/CRL-Relay mit einer elektronischen Signatur versehen. Ein anforderndes System kann diese Signatur durch einen Sicherheitsanker (Trust Anchor) prüfen. Hier kann auch ein Abgleich erfolgen, ob die Antwort zur Anfrage passt.

- Sofern Kernsystem und OCSP/CRL-Relay nicht zusammen in einem vertrauenswürdigen Netz betrieben werden, prüft das Kernsystem (gemäß Konfiguration) die Integrität und Authentizität der Antwort des OCSP/CRL-Relays mit einem Sicherheitsanker (Trust Anchor).
- Das OCSP/CRL-Relay wird in einem sicheren Netz betrieben. Der Zugriff auf das OCSP/CRL-Relay erfolgt optional auch über Entry-Points, die in vorgelagerten Zonen installiert werden (vgl. [VPS-SiKo]).
- Kernsystem und beide Teile des NetSigners (Server und Kartenansteuerung) befinden sich auf demselben Rechner.
- Die Chipkartenleser sind physikalisch über Kabel an den Rechner, auf dem der NetSigner betrieben wird, angeschlossen.
- Wenn OCSP/CRL-Relay und Kernsystem innerhalb eines Weitverkehrsnetz (Wide Area Network – WAN) betrieben werden, wird zur Gewährleistung von Authentizität und Integrität innerhalb dieser 1:1-Beziehung SSL mit gegenseitiger Authentisierung (RSA mit 2048 Bit und ausgetauschten (System-)Zertifikaten) eingesetzt. Eine Revokation (manuelles Entfernen eines gesperrten (System-)Zertifikats) obliegt dem Schlüssel-Administrator.
- Die Auskünfte, die das OCSP/CRL-Relay von den Verzeichnisdiensten erhält – also Zertifikate, OCSP-Antworten und Sperrlisten – sind qualifiziert signiert. Das OCSP/CRL-Relay verfügt über den entsprechenden Sicherheitsanker (Trust Anchor) und prüft die Signaturen, bevor es die Informationen auswertet.

2.4.6 Fazit

66 Im Folgenden wird zusammenfassend in Tabelle 1 aufgezeigt, in welchem Umfang die Sicherheitsanforderungen des SigG und der SigV an Signaturanwendungskomponenten (gemäß [BNetzA2005]) vom EVG als Funktions-

bibliothek erfüllt werden und welcher Anteil von einem System in der IT-Umgebung erfüllt werden muss, das allerdings über die Annahmen/Auflagen gleichfalls die Anforderungen von SigG und SigV an eine Signaturanwendungskomponente erfüllen muss.

Tabelle 1: Umsetzung der SigG/SigV-Anforderungen

Sicherheitsanforderungen an Signaturanwendungskomponenten [BNetzA2005]	Umsetzung der Anforderungen aus SigG und SigV	
	in EVG	in der IT-Umgebung
„Erzeugung von Signaturen: Die Signaturanwendungskomponente muss beim Erzeugen einer Signatur gewährleisten, dass		
▪ das Erzeugen einer Signatur vorher eindeutig angezeigt wird,	EVG zeigt dem Signaturschlüssel-Inhaber das anfordernde System inkl. Zweck (Fachaufgabe) an, welches nach Freischalten der Signaturkarte diese zur Erzeugung von Batchsignaturen innerhalb eines festen Zeitfensters oder für eine bestimmte Anzahl von Batchsignaturen nutzen kann	Auslösen der Erzeugung einer Batchsignatur obliegt dem anfordernden System in der IT-Umgebung
▪ erkennbar ist, auf welche Daten sich die Signatur bezieht,	-	Anzeige der Daten, auf die sich die Batchsignatur bezieht, erfolgt beim anfordernden System
▪ bei Bedarf der Inhalt der zu signierenden Daten hinreichend zu erkennen ist,	-	erfolgt beim anfordernden System
▪ eine Signatur nur durch die berechtigt signierende Person erfolgt,	EVG gewährleistet, dass Batchsignatur nur für berechtigte anfordernde Systeme auf Anforderung innerhalb eines festen Zeitfensters oder für eine bestimmte Anzahl erfolgt – durch die in Abschnitt 2.4.4 beschriebenen Maßnahmen, insbesondere: ▪ dediziertes sicheres Netz ▪ Absicherung der Signa-	Autorisierung der Erzeugung einer Batchsignatur erfolgt unterstützend beim anfordernden System

Sicherheitsanforderungen an Signaturanwendungskomponenten [BNetzA2005]	Umsetzung der Anforderungen aus SigG und SigV	
	in EVG	in der IT-Umgebung
	turanforderung mit elektronische Signatur, Prüfung der Signatur und des (System-) Zertifikats und Revokation durch Schlüssel-Administrator ▪ Prüfung der Zulässigkeit der Aktion über die im Regelwerk abgelegten Regeln	
▪ die Identifikationsdaten nicht preisgegeben und nur auf der jeweiligen „sicheren Signaturerstellungseinheit“ gespeichert werden.	-	wird durch sichere Signaturerstellungseinheit sowie Eingabe der PIN am PIN-Pad des Chipkartenlesers gewährleistet
Prüfung einer Signatur: Die Signaturanwendungskomponente muss beim Prüfen einer Signatur gewährleisten, dass		
▪ erkennbar wird, auf welche Daten sich die Signatur bezieht,	-	erfolgt beim anfordernden System
▪ erkennbar wird, ob die Daten unverändert sind,	-	Anzeige obliegt anforderndem System
▪ bei Bedarf der Inhalt der signierten Daten hinreichend zu erkennen ist,	-	erfolgt beim anfordernden System
▪ erkennbar wird, welchem Signaturschlüssel-Inhaber die Signatur zuzuordnen ist,	-	erfolgt beim anfordernden System
▪ erkennbar wird, welche Inhalte das qualifizierte Zertifikat, auf dem die Signatur beruht, und zugehörige qualifizierte Attribut-Zertifikate aufweisen,	-	erfolgt beim anfordernden System

Sicherheitsanforderungen an Signaturanwendungskomponenten [BNetzA2005]	Umsetzung der Anforderungen aus SigG und SigV	
	in EVG	in der IT-Umgebung
▪ erkennbar wird, ob die nachgeprüften qualifizierten Zertifikate im jeweiligen Zertifikatverzeichnis zum angegebenen Zeitpunkt vorhanden und nicht gesperrt waren,	EVG führt die Validierung durch Absicherung der internen Kommunikation erfolgt durch die in Abschnitt 2.4.4 beschriebenen Maßnahmen, insbesondere: ▪ dediziertes sicheres Netz ▪ Interpretation der Relay-Auskunft signiert ▪ Kernsystem verifiziert elektronische Signatur des Validierungsergebnis des OCSP/CRL-Relays, sofern nicht in einem vertrauenswürdigen Netz ▪ anfordernde Systeme können Signatur der Verzeichnisdienst-Auskünfte mit Trust Anchor prüfen	obliegt anforderndem System
▪ die Korrektheit der Signatur zuverlässig geprüft und zutreffend angezeigt wird.	EVG führt die mathematische Prüfung der Korrektheit der Signatur durch. Absicherung der internen Kommunikation erfolgt durch die in Abschnitt 2.4.4 beschriebenen Maßnahmen, insbesondere: ▪ dediziertes sicheres Netz ▪ Auskunft elektronisch signiert	zutreffende Anzeige obliegt anforderndem System

Sicherheitsanforderungen an Signaturanwendungskomponenten [BNetzA2005]	Umsetzung der Anforderungen aus SigG und SigV	
	in EVG	in der IT-Umgebung
Schutz vor unbefugter Veränderung: Sicherheitstechnische Veränderungen an der Signaturanwendungskomponente müssen für den Nutzer erkennbar werden.”	Benachrichtigung des Signaturschlüssel-Inhabers, wenn seine Signaturkarte aus dem Chipkartenleser entfernt wird	ein sicherer Betrieb muss in der Umgebung gewährleistet werden

67 Zusammenfassend muss der EVG damit die folgenden Anforderungen umsetzen (vgl. auch organisatorische Sicherheitspolitiken in Abschnitt 3.4):

- Erzeugung von Batchsignaturen:
  - Der EVG muss beim Erzeugen einer Batchsignatur gewährleisten, dass dem Signaturschlüssel-Inhaber vor seiner PIN-Eingabe angezeigt wird, welches System inkl. Zweck (Fachaufgabe) innerhalb welchen Zeitfensters bzw. für welche Anzahl von Batchsignaturen seine sichere Signaturerstellungseinheit nutzen kann.
  - Der EVG muss beim Erzeugen einer Batchsignatur gewährleisten, dass eine Batchsignatur nur durch ein berechtigtes anforderndes System innerhalb eines festen Zeitfensters oder für eine bestimmte Anzahl erfolgt.
- Prüfung von Signaturen:
  - 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.
  - Der EVG muss beim Prüfen einer Signatur gewährleisten, dass die Korrektheit der Signatur zuverlässig geprüft wird.
- Schutz vor unbefugter Veränderung:
  - Wird die Signaturkarte im laufenden Betrieb aus dem Chipkartenleser entfernt, wird dies dem Signaturschlüssel-Inhaber mitgeteilt.

68 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):

- Erzeugung von Batchsignaturen:
  - Das anfordernde System in der IT-Umgebung muss beim Erzeugen einer Batchsignatur gewährleisten, dass das Auslösen einer Batchsignatur vorher eindeutig angezeigt wird.

- Das anfordernde System in der IT-Umgebung muss beim Erzeugen einer Batchsignatur gewährleisten, dass erkennbar ist, auf welche Daten sich die Batchsignatur bezieht.
- Das anfordernde System in der IT-Umgebung muss beim Erzeugen einer Batchsignatur gewährleisten, dass bei Bedarf der Inhalt der zu signierenden Daten hinreichend zu erkennen ist.
- Das anfordernde System in der IT-Umgebung muss beim Erzeugen einer Batchsignatur gewährleisten, dass die Autorisierung zur Erzeugung einer Batchsignatur nur durch eine berechtigte Person bzw. einen entsprechenden Prozess erfolgt.
- Sichere Signaturerstellungseinheit und Chipkartenleser müssen gewährleisten, dass die Identifikationsdaten nicht preisgegeben und nur auf der jeweiligen sicheren Signaturerstellungseinheit gespeichert werden.

- Prüfung von Signaturen:
  - Das anfordernde System in der IT-Umgebung muss beim Prüfen einer Signatur gewährleisten, dass erkennbar wird, auf welche Daten sich die Signatur bezieht.
  - Das anfordernde System in der IT-Umgebung muss beim Prüfen einer Signatur gewährleisten, dass erkennbar wird, ob die Daten unverändert sind – also eine geeignete Anzeige bereitstellen.
  - Das anfordernde System in der IT-Umgebung muss beim Prüfen einer Signatur gewährleisten, dass bei Bedarf der Inhalt der signierten Daten hinreichend zu erkennen ist.
  - Das anfordernde System in der IT-Umgebung muss beim Prüfen einer Signatur gewährleisten, dass erkennbar wird, welchem Signaturschlüssel-Inhaber die Signatur zuzuordnen ist.
  - Das anfordernde System in der IT-Umgebung muss beim Prüfen einer Signatur gewährleisten, dass erkennbar wird, welche Inhalte das qualifizierte Zertifikat, auf dem die Signatur beruht, und zugehörige qualifizierte Attribut-Zertifikate aufweisen.
  - Das anfordernde System in der IT-Umgebung 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 – also eine geeignete Anzeige bereitstellen.
  - Das anfordernde System in der IT-Umgebung muss beim Prüfen einer Signatur gewährleisten, dass die Korrektheit der Signatur zuverlässig geprüft und zutreffend angezeigt wird – also eine geeignete Anzeige bereitstellen.

- Schutz vor unbefugter Veränderung:
  - Sicherheitstechnische Veränderungen müssen für den Administrator erkennbar werden.

2.5 Produktbestandteile und EVG-Abgrenzung

69 Der Lieferumfang des EVG ist in Tabelle 2 aufgeführt:

Tabelle 2: Lieferumfang EVG

Liefergegenstand		Typ	Medium
Alle Komponenten	Betriebshandbuch	Dokumentation	CD-ROM oder Archiv-Datei
Kern-System	Kernsystem-Software	Software	CD-ROM oder Archiv-Datei
	Installationshandbuch für Administrator	Dokumentation	
	Releasebeschreibung (Funktionsbeschreibung für Administration)	Dokumentation	
	Schnittstellenbeschreibung (für Anwendungsentwickler)	Dokumentation	
	Logging der Komponenten (Log-Systematik) für Betrieb und Entwicklung	Dokumentation	
Net-Signer	NetSigner-Server-Software	Software	CD-ROM oder Archiv-Datei
	NetSigner-Kartenansteuerung-Software (Keystore-Host)	Software	
OCSP/ CRL-Relay	OCSP/CRL-Relay-Software	Software	CD-ROM oder Archiv-Datei
	Administrationshandbuch	Dokumentation	
	Installationsleitfaden für Administrator	Dokumentation	
	Releasebeschreibung (Funktionsbeschreibung für Administration)	Dokumentation	
	Schnittstellenbeschreibung (für Anwendungsentwickler)	Dokumentation	
	Logging der Komponenten (Log-Systematik) für Betrieb und Entwicklung	Dokumentation	
Administrations-anwendung	Administrationsanwendung	Software	CD-ROM oder Archiv-Datei

70 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;
- geeignete, SigG-konforme sichere Signaturerstellungseinheiten (Signaturkarten[21] mit entsprechendem Zertifikat) für die Erzeugung von Batchsignaturen (so genannte Multisignaturkarten) samt SigG-konformem Chipkartenleser (mit PIN-Pad);
- qualifizierte Zertifikate;
- geeignete, SigG-konforme Verzeichnisdienstauskünfte samt Verbindung, auf die das OCSP/CRL-Relay zur Zertifikatsprüfung zugreifen kann;
- (System-)Zertifikate und private Schlüssel zur Gewährleistung der Systemsicherheit;
- anfordernde Systeme, die von außen über eine Schnittstelle auf den EVG zugreifen – beispielsweise ein Verifikationsserver, OSCI-Manager oder OSCI-Backend-Enabler aus Abbildung 2 in der IT-Umgebung –, die Funktionalitäten des EVG[22] nutzen und die die Anforderungen des Signaturgesetzes an eine Signaturanwendungskomponente erfüllen

Eine exakte Auflistung der technischen Einsatzumgebung findet sich im Anhang in Abschnitt 11.

71 Der EVG wird in einem in [BNetzA2005] bezeichneten „geschützten Einsatzbereich (Regelfall/Standardlösung)“ eingesetzt. Dementsprechend werden „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 abgewehrt“ [BNetzA2005].

2.6 Auslieferung

72 Die Auslieferung des EVG (vgl. Tabelle 2) erfolgt auf zwei Wegen:

---

[21] Sichere Signaturerstellungseinheiten gemäß SigG/SigV werden in diesem Kontext ausschließlich als Chipkarten, also Signaturkarten, realisiert, so dass die Begriffe synonym genutzt werden.

[22] Funktionalitäten, die der EVG für anfordernde Systeme zur Verfügung stellt, sind:

- Unterstützung bei der Erzeugung qualifizierter elektronischer (Batch-) Signaturen;
- mathematische Prüfung qualifizierter elektronischer Signaturen (Verifikation);
- Statusprüfung qualifizierter Zertifikate (Validierung).

- via CD-ROM: Die Software und Dokumentation wird auf CD-ROM gebrannt und auf sicherem Wege übermittelt.
- online: Die Software und Dokumentation wird in einer gesicherten Archiv-Datei online zur Verfügung gestellt.

3 EVG-Sicherheitsumgebung

3.1 Rollen

73 Es gibt im Kontext der Basiskomponente folgende Rollen:

- **System-Administrator**: Ein System-Administrator ist für die Verwaltung und Organisation der grundlegenden IT-Infrastruktur zuständig, die für den EVG benötigt werden.[23] 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.
- Ein System-Administrator ist in der Regel auch Security-Administrator.
- **Security-Administrator ("generaladmin"):** Der Security-Administrator ist für den EVG 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);
  - Konfiguration der Authentisierungssysteme für Administration (Rechte der Rollen und Regeln im Regelwerk setzen, ändern und löschen, Administratoren-Rollen konfigurieren) – in Zusammenarbeit mit dem Revisor;
  - System-Starts (Starten, Stoppen und Rücksetzen des EVGs).
- **Schlüssel-Administrator:** Der Schlüssel-Administrator verwaltet die im EVG benötigten kryptographischen Schlüssel und die Sicherheitsanker (Trust Anchor), wobei Sicherheitsanker sowohl SigG-konforme qualifizierte Zertifikate als auch (System-)Zertifikate zur Gewährleistung der Sys-

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

temsicherheit sind. Zudem nimmt der Schlüssel-Administrator eine Voreinstellung zur Begrenzung für die Erzeugung von Batchsignaturen vor – hinsichtlich der Anzahl zu erzeugender Batchsignaturen oder des Zeitfensters, in dem Batchsignaturen erzeugt werden können – sowie die Zuordnung der Signaturkarten zu einer Rolle.

- **Signaturschlüssel-Inhaber ("keyowner"):** Im Kontext der Signaturerstellung im EVG wird automatisiert auf Anforderung eine qualifizierte elektronische Signatur generiert. Die personengebundene, aber automatisch arbeitende Signatur wird durch den Signaturschlüssel-Inhaber freigeschaltet. Der Signaturschlüssel-Inhaber kann zudem die Voreinstellung zur Begrenzung für die Erzeugung von Batchsignaturen (Anzahl zu erzeugender Batchsignaturen oder Zeitfenster, in dem Batchsignaturen erzeugt werden können) verändern.
- **Revisor ("revision"):** Der Revisor prüft die Sicherheitsparameter, konfiguriert die Protokollierung und wertet sie aus und begleitet den Security-Administrator 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.
- **nicht autorisierte Person:** Eine nicht autorisierte Person ist jede Person, die weder System-, Security- oder Schlüssel-Administrator noch Signaturschlüssel-Inhaber oder Revisor ist.

74 Darüber hinaus ist das **anfordernde System** zu nennen: Ein anforderndes System ist ein System in der IT-Umgebung, das eine Fachaufgabe wahrnimmt und die Vorgaben von Signaturgesetz und -verordnung an eine Signaturanwendungskomponente erfüllt. Ein anforderndes System kann folgende Anforderungen an den EVG stellen:

- Unterstützung bei der Erzeugung qualifizierter elektronischer (Batch-) Signaturen;
- mathematische Prüfung qualifizierter elektronischer Signaturen (Verifikation);
- Statusprüfung qualifizierter Zertifikate (Validierung).

Einem anfordernden System ist der voreingestellte Zweck („z. B. Signaturen zu Zahlungsanweisungen bei Großanwendern“ [SigV_Begr]) zugeordnet.

3.2 Annahmen

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

76 A.PKI Die für den Betrieb von Governikus notwendigen Systemkomponenten der Public-Key-Infrastruktur (PKI) sind vorhanden:

- SigG-konforme sichere Signaturerstellungseinheiten;

- SigG-konformer Chipkartenleser;
- qualifizierte Zertifikate und Sicherheitsanker (Trust Anchor);
- private Schlüssel (zur Gewährleistung der Systemsicherheit);
- (System-)Zertifikate (zur Gewährleistung der Systemsicherheit).

Dabei werden geeignete kryptographische Verfahren mit entsprechenden Schlüssellängen eingesetzt.

Eine Auflistung findet sich im Anhang in Abschnitt 11.

77 A.SAK Anfordernde Systeme, die von außen über eine Schnittstelle auf den EVG zugreifen und Funktionalitäten des EVG[22] nutzen, stehen zur Verfügung und erfüllen die Anforderungen von Signaturgesetz und -verordnung an eine Signaturanwendungskomponente. Insbesondere gewährleisten sie die SigG-relevanten Funktionalitäten hinsichtlich Autorisierung zur Erzeugung von Batchsignaturen und Visualisierung (vgl. Abschnitt 2.4.6).

78 A.Betrieb Für den Betrieb ist vertrauenswürdiges Personal eingesetzt, das einen Beitrag zur Sicherheit leistet, und die notwendigen räumlichen Gegebenheiten sowie Hard- und Software für den sicheren Betrieb des EVG sind vorhanden.

Das Personal beinhaltet Signaturschlüssel-Inhaber, die sich beispielsweise vergewissern, dass sie bei der Eingabe ihres Identifikationsmerkmals nicht beobachtet werden, oder die ihr Identifikationsmerkmal ändern, wenn sie den Verdacht oder die Gewissheit haben, Ihr Merkmal könnte nicht mehr geheim sein.

Darüber hinaus sind 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 (dedizierter Raum für die Chipkartenleser) und für die Realisierung der Netzwerkarchitektur und der internen Verbindungen zwischen den einzelnen Systemkomponenten mit Firewall, Demilitarisierter Zone (DMZ) etc. Vgl. dazu die Vorgaben und Auflagen zum Betrieb von Governikus, 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 der Kommunikationsstrecke bei Nutzung von Kernsystem und OCSP/CRL-Relay über ein Weitverkehrsnetz 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, der verwendete Chipkartenleser nicht böswillig manipuliert wurde, um Daten (z. B. PIN, Hashwerte etc.) 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:
    - Für die Aufbewahrung der "Signatur-Arbeitstation", bestehend aus EVG, Chipkartenleser, Signaturkarten, Monitor, Tastatur und Rechner, ist ein zugriffsicherer Betriebsraum erforderlich, so dass ein Zugriff Unbefugter ausgeschlossen ist oder zumindest mit hoher Sicherheit erkennbar wird.
    - Rechner, Chipkartenleser, Signaturkarten, Monitor und Tastatur befinden sich in einem Betriebsraum.
    - Rechner und Chipkartenleser sind durch einen sicheren Kanal verbunden

- Ein erfolgreicher Angriff auf die Signatur-Arbeitsstation muss in jedem Fall ersichtlich sein und unmittelbar angezeigt werden.
- Für die Administratoren müssen Vertreterregelungen für Krankheit und Urlaub bestehen.
- Wartungs- bzw. Reinigungspersonal erhalten den Zugang zum zugriffssicheren Betriebsraum nur durch einen Administrator, der den Aufenthalt überwacht.
- Ein Signaturschlüssel-Inhaber erhält den Zugang zum zugriffssicheren Betriebsraum nur durch den Schlüssel-Administrator, der den Aufenthalt überwacht.

79 A.DIR Ein SigG-konformer Verzeichnisdienst für Sperrlisten und Zertifikatsstatusabfragen zur Validierung von qualifizierten Zertifikaten ist vorhanden und es besteht eine Verbindung dorthin.

80 A.ZufPIN In der Einsatzumgebung zwischen SigG-konformem Chipkartenleser (mit PIN-Pad) und Signaturkarte wird gewährleistet, dass die Identifikationsdaten nicht preisgegeben und nur auf der jeweiligen sicheren Signaturerstellungseinheit gespeichert werden.

3.3 Bedrohungen

81 TE.RatePIN Falls eine nicht autorisierte Person in den Besitz der sicheren Signaturerstellungseinheit gelangt, könnte diese Person versuchen, das Identifikationsmerkmal zu erraten. Die nicht autorisierte Person kann ein hohes Angriffspotenzial aufweisen und über Fachkenntnisse verfügen.

82 TE.SpähePIN Eine nicht autorisierte Person könnte versuchen, das Identifikationsmerkmal auszuspähen. Die nicht autorisierte Person kann ein hohes Angriffspotenzial aufweisen und über Fachkenntnisse verfügen.

83 Weitere Bedrohungen ergeben sich implizit durch Nennung organisatorischer Sicherheitspolitiken.

3.4 Organisatorische Sicherheitspolitiken[24]

84 P.AnzeigeBatch Der EVG muss beim Erzeugen einer Batchsignatur gewährleisten, dass dem Signaturschlüssel-Inhaber vor seiner PIN-

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

Eingabe angezeigt wird, welches System inkl. Zweck (Fachaufgabe) innerhalb welchen Zeitfensters bzw. für welche Anzahl von Batchsignaturen seine sichere Signaturerstellungseinheit nutzen kann.

85 P.AuthSign Der EVG muss beim Erzeugen einer Batchsignatur gewährleisten, dass eine Batchsignatur nur durch ein berechtigtes anforderndes System innerhalb eines festen Zeitfensters oder für eine bestimmte Anzahl erfolgt.

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

87 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.

88 P.AnzEntfernen Wird die Signaturkarte im laufenden Betrieb aus dem Chipkartenleser entfernt, wird dies dem Signaturschlüssel-Inhaber mitgeteilt.

4 Sicherheitsziele

4.1 EVG-Sicherheitsziele

89 O.AnzeigeBatch Der EVG muss dem Signaturschlüssel-Inhaber vor Freischalten der Signaturkarte (vor Eingabe der PIN) authentisch anzeigen, welches System inkl. Zweck (Fachaufgabe) Batchsignaturen mit seiner sicheren Signaturerstellungseinheit innerhalb welchen Zeitfensters bzw. für welche Anzahl von Batchsignaturen erzeugen kann.

90 O.AuthSign Der EVG muss bei einer Anforderung zur Erzeugung einer Batchsignatur von außen gewährleisten, dass die zu signierenden Daten zuverlässig nur der jeweils zugeordneten sicheren Signaturerstellungseinheit zugeführt werden, für die das anfordernde System eine Berechtigung besitzt. Hierbei muss der EVG die temporalen bzw. quantitativen Beschränkungen der Signierfähigkeit berücksichtigen.

91 O.VerifSign 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 öffentli-

chen Signaturschlüssels auf die elektronische Signatur mit einem geeigneten kryptographischen Algorithmus berechnet wird.

92 O.ValidZert Der EVG muss die Gültigkeit eines qualifizierten Zertifikats zuverlässig feststellen, indem für das angeforderte Zertifikat festgestellt wird, ob

- das Zertifikat zum angegebenen Zeitpunkt bzw. Prüfzeitpunkt (wenn kein Zeitpunkt explizit übergeben wurde) vorhanden und nicht gesperrt war und
- der Gültigkeitszeitraum des Zertifikats zum angegebenen Zeitpunkt bzw. Prüfzeitpunkt (wenn kein Zeitpunkt explizit übergeben wurde) 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.

93 O.AnzEntfernen Wird eine freigeschaltete sichere Signaturerstellungseinheit aus einem Chipkartenleser entfernt, muss der EVG dies dem Signaturschlüssel-Inhaber per E-Mail anzeigen.

4.2 Sicherheitsziele für die Umgebung

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

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

- sichere Signaturerstellungseinheit mit geeigneten kryptographischen Parametern (Verfahren und Schlüssellängen);
- Chipkartenleser mit PIN-Pad;
- qualifizierte Zertifikate und Sicherheitsanker mit geeigneten kryptographischen Parametern (Verfahren und Schlüssellängen):

Zudem muss die IT-Umgebung die für die Systemsicherheit benötigten Komponenten bereitstellen:

- (System-)Zertifikate und private Schlüssel mit geeigneten kryptographischen Parametern (Verfahren und Schlüssellängen).

Eine Auflistung findet sich im Anhang in Abschnitt 11.

96 OE.SAK Die IT-Umgebung muss geeignete anfordernde Systeme zur Verfügung stellen, die die Anforderungen von Signaturgesetz und -verordnung an eine Signaturanwendungskomponente erfüllen, die von außen über eine Schnittstelle auf den EVG zugreifen und Funktionalitäten des EVG[22] nutzen und die insbesondere die SigG-relevanten Funktionalitäten hinsichtlich Autorisierung zur Erzeugung von Batchsignaturen und Visualisierung gewährleisten (vgl. Abschnitt 2.4.6).

97 OE.Betrieb Für den Betrieb muss vertrauenswürdiges Personal eingesetzt werden, das einen Beitrag zur Sicherheit leisten, und die notwendigen räumlichen Gegebenheiten sowie Hard- und Software für den sicheren Betrieb des EVG sind vorhanden.

Das Personal beinhaltet Signaturschlüssel-Inhaber, die sich beispielsweise vergewissern müssen, dass sie bei der Eingabe ihres Identifikationsmerkmals nicht beobachtet werden, oder die ihr Identifikationsmerkmal ändern, wenn sie den Verdacht oder die Gewissheit haben, Ihr Merkmal könnte nicht mehr geheim sein.

Darüber hinaus 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 (dedizierter Raum für die Chipkartenleser) und für die Realisierung der Netzwerkarchitektur und der internen Verbindungen zwischen den einzelnen Systemkomponenten mit Firewall, Demilitarisierter Zone (DMZ) etc. Vgl. dazu die Vorgaben und Auflagen zum Betrieb von Governikus, 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 werden, 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, geeignete Absicherung der Kommunikationsstrecke bei Nutzung von Kernsystem und OCSP/CRL-Relay über ein Weitverkehrsnetz 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 ist sicherzustellen, dass die auf dem eingesetzten Computer installierte Software nicht böswillig manipuliert oder verändert werden kann, auf dem Computer keine Viren oder Trojanischen Pferde eingespielt werden können, die Hardware des Computers nicht unzulässig verändert werden kann, der verwendete Chipkartenleser nicht böswillig manipuliert wurde, um Daten (z. B. PIN, Hashwerte etc.) 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:
    - Für die Aufbewahrung der "Signatur-Arbeitstation", bestehend aus EVG, Chipkartenleser, Signaturkarten, Monitor, Tastatur und Rechner, ist ein zugriffsicherer Betriebsraum erforderlich, so dass ein Zugriff Unbefugter ausgeschlossen ist oder zumindest mit hoher Sicherheit erkennbar wird.
    - Rechner, Chipkartenleser, Signaturkarten, Monitor und Tastatur befinden sich in einem Betriebsraum.
    - Rechner und Chipkartenleser sind durch einen sicheren Kanal verbunden
    - Ein erfolgreicher Angriff auf die Signatur-Arbeitsstation muss in jedem Fall ersichtlich sein und unmittelbar angezeigt werden.
    - Für die Administratoren müssen Vertreterregelungen für Krankheit und Urlaub bestehen.
    - Wartungs- bzw. Reinigungspersonal erhalten den Zugang zum zugriffssicheren Betriebsraum nur durch einen Administrator, der den Aufenthalt überwacht.
    - Ein Signaturschlüssel-Inhaber erhält den Zugang zum zugriffssicheren Betriebsraum nur durch den

Schlüssel-Administrator, der den Aufenthalt überwacht.

98 OE.DIR Die IT-Umgebung muss für Validierungen von qualifizierten Zertifikaten eine Verbindung zu einem geeigneten SigG-konformen Verzeichnisdienst bereitstellen.

99 OE.ZufPIN Die IT-Umgebung muss gewährleisten, dass die Identifikationsdaten zwischen SigG-konformem Chipkartenleser (mit PIN-Pad) und sicherer Signaturerstellungseinheit nicht preisgegeben und nur auf der jeweiligen sicheren Signaturerstellungseinheit gespeichert werden.

5 IT-Sicherheitsanforderungen

5.1 EVG-Sicherheitsanforderungen

5.1.1 Definition der funktionalen Sicherheitspolitik (FSP)

100 Bevor die funktionalen Sicherheitsanforderungen an den EVG aufgeführt werden, werden zwei funktionale Sicherheitspolitiken (FSP) definiert:

- funktionale Sicherheitspolitik für die Zugriffskontrolle auf die Batchsignatur (Batchsignatur-Zugriffskontrollpolitik);
- funktionale Sicherheitspolitik für die Zugriffskontrolle auf die Systemsicherheit (Systemsicherheit-Zugriffskontrolle).

Batchsignatur-Zugriffskontrollpolitik

101 Für die Durchführung einer Signier-Operation zur Erzeugung einer Batchsignatur sind folgende Subjekte, Objekte und Operationen relevant:

- Subjekte:
  - Signier-Anforderungs-Prozess (initiiert durch anforderndes System);

- Objekte:
  - zu signierende Daten[25];
- Operationen:
  - Weiterleiten zu signierender Daten zu einer sicheren Signaturerstellungseinheit (in der IT-Umgebung), in der eine Batchsignatur erzeugt wird.

102 Der EVG leitet die zu signierenden Daten einer sicheren Signaturerstellungseinheit nur dann weiter – gewährt damit also den Zugriff auf die Erzeugung einer Batchsignatur nur dann –, wenn folgende Regeln gelten:[26]

- Die Zuordnung von SystemId zu OperationId ist korrekt, d. h. das anfordernde System (gekennzeichnet durch eine SystemId) darf die Anforderung zur Erzeugung einer Batchsignatur (gekennzeichnet durch eine OperationId) ausführen.
- Die Signaturprüfung der Anfrage (Anfrage ist elektronisch signiert) ist mathematisch korrekt.
- Der für die Verifikation der Anfrage benötigte öffentliche Schlüssel des anfordernden Systems liegt in Form eines (System-)Zertifikats im EVG – im Sinne eines Trust Anchors – vor. Das (System-)Zertifikat wird dabei nicht mit der Signier-Anforderung übertragen.
- Die Zuordnung von (System-)Zertifikat der Signier-Anforderung des anfordernden Systems zu Rolle der Signaturkarte[27] in der IT-Umgebung für die Erzeugung der Batchsignatur ist korrekt, d. h. das anfordernde System (gekennzeichnet durch das (System-)Zertifikat) darf die sichere Signaturerstellungseinheit, die die Batchsignatur erzeugen soll (gekennzeichnet durch die Rolle), nutzen.
- Das Zeitfenster für die Erzeugung von Batchsignaturen ist gültig bzw. die gültige Anzahl von Batchsignaturen ist noch nicht erreicht.

---

[25] Sicherheitsattribute der zu signierenden Daten sind:

- Signatur, mit der die zu signierenden Daten abgesichert sind;
- (System-)Zertifikat des anfordernden Systems ((System-)Zertifikat liegt im EVG im Sinne eines Trust Anchors vor);
- SystemId (Identifier für anforderndes System);
- OperationId (Identifier für auszuführende Operationen);
- Rollendefinition (vgl. Glossar);
- Begrenzung (zeitlich bzw. quantitativ) zur Erzeugung von Batchsignaturen.

[26] In der IT-Umgebung muss zudem der Signaturschlüssel-Inhaber seine Signaturkarte in den Chipkartenleser eingesteckt und freigeschaltet haben.

[27] vgl. Glossar: Rollendefinition

Systemsicherheit-Zugriffskontrollpolitik

103 Im EVG werden elektronische Signaturen erzeugt und die mathematische Korrektheit elektronischer Signaturen verifiziert. Dazu werden private Schlüssel und Sicherheitsanker verwaltet.

104 Für das Management privater Schlüssel und Sicherheitsanker sind folgende Subjekte, Objekte und Operationen relevant:

- Subjekte:
  - Schlüssel-Administrator;
- Objekte:
  - private Schlüssel;
  - Sicherheitsanker (SigG-konforme qualifizierte Zertifikate und (System-)Zertifikate);
- Operationen:
  - Speichern privater Schlüsseln oder Sicherheitsanker;
  - Löschen privater Schlüsseln oder Sicherheitsanker;

105 Der Zugriff auf die Operationen Speichern und Löschen von privaten Schlüsseln und Sicherheitsanker erfolgt nur nach erfolgreicher Authentisierung des Schlüssel-Administrators.

5.1.2 Funktionale EVG-Sicherheitsanforderungen

106 Die funktionalen Sicherheitsanforderungen sind zusammenfassend in Tabelle 3 aufgeführt und im Folgenden dargestellt. Alle funktionalen EVG-Sicherheitsanforderungen entstammen dem Teil 2 der CC [CC-Teil2].

107 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 <u>unterstrichen</u> gedruckt sind.

Tabelle 3: Funktionale Sicherheitsanforderungen an den EVG

Funktionale Sicherheits-anforderung an den EVG	Beschreibung
FAU_ARP.1	Sicherheitsalarme
FAU_SAA.3	Heuristische Vorhersage einfacher Angriffe
FCO_NRO.1	Selektiver Urheberschaftsbeweis
FCS_CKM.4	Zerstörung des kryptographischen Schlüssels

Funktionale Sicherheits-anforderung an den EVG	Beschreibung
FCS_COP.1 (Verify)	Kyptographischer Betrieb (für die kryptographische Operation „Verifizieren“ einer qualifizierten elektronischen Signatur)
FCS_COP.1 (VSA[28])	Kyptographischer Betrieb (für die Verifikation der Signatur-anforderung)
FCS_COP.1 (SVVE[29])	Kyptographischer Betrieb (für die Erzeugung einer elektroni-schen Signatur für Verifikations- und Validierungsergebnisse)
FCS_COP.1 (VVE[30])	Kyptographischer Betrieb (für die Verifikation eines Validie-rungsergebnisses)
FDP_ACC.1 (Batch)	Teilweise Zugriffskontrolle (Batchsignatur-Zugriffskontrollpolitik)
FDP_ACF.1 (Batch)	Zugriffskontrolle basierend auf Sicherheitsattributen (Batch-signatur-Zugriffskontrollpolitik)
FDP_ACC.1 (Sys)	Teilweise Zugriffskontrolle (Systemsicherheit-Zugriffskontroll-politik)
FDP_ACF.1 (Sys)	Zugriffskontrolle basierend auf Sicherheitsattributen (Systemsi-cherheit-Zugriffskontrollpolitik)
FDP_ITC.1	Import von Benutzerdaten ohne Sicherheitsattribute
FIA_UID.2	Benutzeridentifikation vor jeglicher Aktion
FMT_MSA.1 (Batch)	Management der Sicherheitsattribute (Batchsignatur-Zugriffs-kontrollpolitik)
FMT_MSA.1 (Sys)	Management der Sicherheitsattribute (Systemsicherheit-Zugriffskontrollpolitik)
FMT_MSA.2	Sichere Sicherheitsattribute
FMT_MSA.3 (Batch)	Initialisierung statischer Attribute (Batchsignatur-Zugriffs-kontrollpolitik)
FMT_MSA.3 (Sys)	Initialisierung statischer Attribute (Systemsicherheit -Zugriffs-kontrollpolitik)
FMT_SMR.1 (Batch)	Sicherheitsrollen (Batchsignatur-Zugriffskontrollpolitik)
FMT_SMR.1 (Sys)	Sicherheitsrollen (Systemsicherheit -Zugriffskontrollpolitik)
FTA_TAB.1	Vorgegebene EVG-Zugriffswarnmeldung

[28] Verifikation der Signatur-Anforderung

[29] Signieren von Verifikations- und Validierungs-Ergebnissen

[30] Verifizieren eines Validierungs-Ergebnisses

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

109 Klasse FAU: Sicherheitsprotokollierung

110 FAU_ARP.1 Sicherheitsalarme

111 FAU_ARP.1.1 Die TSF müssen **die Aktion „Informiere den Signaturschlüssel-Inhaber per E-Mail“** bei Erkennen einer potentiellen Sicherheitsverletzung ausführen.

112 FAU_SAA.3 Heuristische Vorhersage einfacher Angriffe

113 Ist hierarchisch zu: FAU_SAA.1

114 FAU_SAA.3.1 Die TSF müssen in der Lage sein, die interne Darstellung folgender typischer Ereignisse **Ziehen einer Signaturkarte aus einem Chipkartenleser**, die eine TSP-Verletzung anzeigen, zu erhalten.

115 FAU_SAA.3.2 Die TSF müssen die typischen Ereignisse mit den Aufzeichnungen der Systemaktivitäten, die bei der Prüfung der **Systemdaten, die dem EVG intern anzeigen, welche Signaturkarten aktuell verfügbar sind,** erkannt werden, vergleichen können.

116 FAU_SAA.3.3 Die TSF müssen eine drohende TSP-Verletzung anzeigen können, wenn festgestellt wird, daß ein Systemereignis einem typischen Ereignis, welches eine potentielle TSP-Verletzung anzeigt, entspricht.

117 Klasse FCO: Kommunikation

118 FCO_NRO.1 Selektiver Urheberschaftsbeweis

119 FCO_NRO.1.1 Die TSF müssen auf Anforderung des **Verifikations- und Validierungsprozesses** für übertragene **Verifikations- bzw. Validierungsergebnisse** Urheberschaftsnachweise generieren können.

120 FCO_NRO.1.2 Die TSF müssen die **Identität des Kernsystems bzw. OCSP/CRL-Relay, Signaturschlüssel und Signier-Algorithmus des Informationsurhebers** den **Status einer durchgeführten Verifikation einer qualifizierten elektronischen Signatur bzw. durchgeführten Validierung (Statusprüfung) eines qualifizierten Zertifikats** der Informationen, auf die sich der Nachweis bezieht, zuordnen können.

121 FCO_NRO.1.3 Die TSF müssen dem **Verifikations- und Validierungsprozess** die Fähigkeit zum Verifizieren des Urheberschaftsnachweises von Informationen unter der Vor-

gabe von **Prüfbedingungen, nach denen hinsichtlich der Validierung als Gültigkeitsmodell das Kettenmodell genutzt wird (Ein Zertifikat ist zu einem angegeben Zeitpunkt bzw. Prüfzeitpunkt (wenn kein Zeitpunkt explizit übergeben wurde) gültig, wenn gilt:**

- **das angeforderte Zertifikat war zum angegebenen Zeitpunkt bzw. Prüfzeitpunkt (wenn kein Zeitpunkt explizit übergeben wurde) vorhanden und nicht gesperrt;**
- **der Gültigkeitszeitraum des Zertifikats war zum angegebenen Zeitpunkt bzw. Prüfzeitpunkt (wenn kein Zeitpunkt explizit übergeben wurde) bereits begonnen und noch nicht abgelaufen;**
- **ein Ausstellerzertifikat (in der Zertifikatskette) war zum Signierzeitpunkt des ausgestellten Zertifikats vorhanden und nicht gesperrt;**
- **der Gültigkeitszeitraum eines Ausstellerzertifikats (in der Zertifikatskette) hat zum Signierzeitpunkt des ausgestellten Zertifikats bereits begonnen und nicht abgelaufen;**
- **das angeforderte Zertifikat und keines seiner Ausstellerzertifikate zur irgendeinem Zeitpunkt kompromittierend gesperrt wurde.),**

bereitstellen.

122 Klasse FCS: Kryptographische Unterstützung

123 FCS_CKM.4 Zerstörung des kryptographischen Schlüssels

124 FCS_CKM.4.1 Die TSF müssen die kryptographischen Schlüssel (private Schlüssel und Sicherheitsanker) nach einer spezifizierten Methode zur Zerstörung des kryptographischen Schlüssels **durch Löschen bzw. aus entsprechendem Verzeichnis Entfernen**, die […] **keiner speziellen Norm** entspricht, zerstören.

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

126 FCS_COP.1.1/Verify Die TSF müssen **im Zusammenhang mit der Prüfung von qualifizierten elektronischen Signaturen die kryptographische Operation „Verifizieren**“ gemäß eines spezifizierten kryptographischen Algorithmus **RSA**

im Zusammenhang mit den Hashfunktionen RIPEMD-160 und SHA-1[31], SHA-224, SHA-256, SHA-384 sowie SHA-512 und kryptographischer Schlüssellängen**, die entsprechend qualifizierter Zertifikate derzeit mindestens 1024 Bit aufweisen**, die den folgenden **Normen [RSA], [RIPEMD-160] und [SHA] unter Berücksichtigung von [BNetzA_Algo2009][32]** entsprechen, durchführen.

127 FCS_COP.1 (VSA) Kyptographischer Betrieb (für die Verifikation der Signaturanforderung)

128 FCS_COP.1.1/VSA Die TSF müssen **im Rahmen der Absicherung der Signaturanforderung die kryptographische Operation „Verifizieren**“ gemäß eines spezifizierten kryptographischen Algorithmus **RSA im Zusammenhang mit den Hashfunktionen RIPEMD-160 und SHA-1 [31], SHA-224, SHA-256, SHA-384 SOWIE SHA-512** und kryptographischer Schlüssellängen**, die entsprechend der X.509-Serverzertifikate derzeit 2048 Bit aufweisen**, die den folgenden **Normen [RSA], [RIPEMD-160] und [SHA][32]** entsprechen, durchführen.

129 FCS_COP.1 (SVVE) Kyptographischer Betrieb (für die Erzeugung einer elektronischen Signatur für Verifikations- und Validierungsergebnisse)

130 FCS_COP.1.1/SVVE Die TSF müssen **im Rahmen der Absicherung der Verifikations- und Validierungsergebnisse mit einer elektronischen Signatur die kryptographische Operation „Signieren**“ gemäß eines spezifizierten kryptographischen Algorithmus **RSA mit den Hashfunktionen RIPEMD-160, SHA-1 [31], SHA-224, SHA-256, SHA-384 sowie SHA-512** und kryptographischer Schlüssellängen, **die entsprechend der X.509-Serverzertifikate derzeit 2048 Bit aufweisen**, die den folgenden **Normen [RSA], [RIPEMD-160] und [SHA] [32]** entsprechen, durchführen.

131 FCS_COP.1 (VVE) Kyptographischer Betrieb (für die Verifikation eines Validierungsergebnisses)

---

[31] SHA-1 wird zwecks Kompatibilität zu älteren Governikus-Versionen weiterhin technisch unterstützt. Das System akzeptiert nur solche Authentisierungssignaturen, die mit demselben Algorithmus erzeugt wurden wie die angeforderte qualifizierte Signatur.

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

132 FCS_COP.1.1/VVE Die TSF müssen **im Rahmen der Absicherung der Validierungsergebnisse mit einer elektronischen Signaturen die kryptographische Operation „Verifizieren**“ gemäß eines spezifizierten kryptographischen Algorithmus **RSA im Zusammenhang mit den Hashfunktionen RIPEMD-160 und SHA-1[31], SHA-224, SHA-256, SHA-384 SOWIE SHA-512** und kryptographischer Schlüssellängen**, die entsprechend der X.509-Serverzertifikate derzeit 2048 Bit aufweisen**, die den folgenden **Normen [RSA], [RIPEMD-160] und [SHA] unter Berücksichtigung von [BNetzA_Algo2009]**[32] entsprechen, durchführen.

133 Klasse FDP: Schutz der Benutzerdaten

134 FDP_ACC.1 (Batch) Teilweise Zugriffskontrolle (Batchsignatur-Zugriffskontrollpolitik)

135 FDP_ACC.1.1/Batch Die TSF müssen die **SFP für die Zugriffskontrolle auf die Batchsignatur (Batchsignatur-Zugriffskontrollpolitik)** für

- **die betrachteten Subjekte:**
  - **Signier-Anforderungs-Prozess (initiiert durch anforderndes System);**
- **die betrachteten Objekte:**
  - **zu signierende Daten;**
- **und die betrachteten Operationen:**
  - **Weiterleiten zu signierender Daten zu einer sicheren Signaturerstellungseinheit (in der IT-Umgebung), in der eine Batchsignatur erzeugt wird,**

durchsetzen.

136 FDP_ACF.1 (Batch) Zugriffskontrolle basierend auf Sicherheitsattributen (Batchsignatur-Zugriffskontrollpolitik)

137 FDP_ACF.1.1/Batch Die TSF müssen die **SFP für die Zugriffskontrolle auf die Batchsignatur (Batchsignatur-Zugriffskontrollpolitik)** für Objekte, die auf **den Sicherheitsattributen**

- **Signatur, mit der die zu signierenden Daten abgesichert sind,**
- **(System-)Zertifikat des anfordernden Systems, das im EVG im Sinne eines Trust Anchors vorliegt,**

- **SystemId (Identifier für anforderndes System),**
- **OperationId (Identifier für auszuführende Operationen),**
- **Rollendefinition der Signaturkarte und**
- **Begrenzung (zeitlich bzw. quantitativ) zur Erzeugung von Batchsignaturen**

basieren, durchsetzen.

138 FDP_ACF.1.2/Batch Die TSF müssen die folgenden Regeln durchsetzen, um festzustellen, ob eine Operation zwischen kontrollierten Subjekten und kontrollierten Objekten zulässig ist:

Der Zugriff auf die angeforderte sichere Signaturerstellungseinheit (Signaturkarte) zur Erzeugung einer Batchsignatur erfolgt nur dann, wenn die folgenden Regeln gelten:

- **Die Zuordnung von SystemId zu OperationId ist korrekt, d. h. das anfordernde System (gekennzeichnet durch eine SystemId) darf die Anforderung zur Erzeugung einer Batchsignatur (gekennzeichnet durch eine OperationId) ausführen.**
- **Die Signaturprüfung der Anfrage (Anfrage ist elektronisch signiert) ist mathematisch korrekt.**
- **Der für die Verifikation der Anfrage benötigte öffentliche Schlüssel des anfordernden Systems liegt in Form eines (System-)Zertifikats im EVG – im Sinne eines Trust Anchors – vor. Das (System-)Zertifikat wird nicht mit der Signier-Anforderung übertragen.**
- **Die Zuordnung von (System-)Zertifikat der Signier-Anforderung des anfordernden Systems zur Rolle der Signaturkarte in der IT-Umgebung für die Erzeugung der Batchsignatur ist korrekt, d. h. das anfordernde System (gekennzeichnet durch das (System-) Zertifikat) darf die sichere Signaturerstellungseinheit, die die Batchsignatur erzeugen soll (gekennzeichnet durch die Rolle), nutzen.**
- **Das Zeitfenster für die Erzeugung von Batchsignaturen ist gültig bzw. die gültige Anzahl von Batchsignaturen ist noch nicht erreicht.**

139 FDP_ACF.1.3/Batch Die TSF müssen den Zugriff von Subjekten auf Objekte basierend auf den folgenden zusätzlichen Regeln expli-

zit autorisieren: **Die TSF müssen hierbei keine zusätzlichen Regeln berücksichtigen**.

140 FDP_ACF.1.4/Batch Die TSF müssen den Zugriff von Subjekten auf Objekte, basierend auf **keinen zusätzlichen Regeln** explizit verweigern.

141 FDP_ACC.1 (Sys) Teilweise Zugriffskontrolle (Systemsicherheit-Zugriffskontrollpolitik)

142 FDP_ACC.1.1/Sys Die TSF müssen die **SFP für die Zugriffskontrolle auf die Systemsicherheit (Systemsicherheit-Zugriffskontrollpolitik)** für

- **die betrachteten Subjekte:**
  - **Schlüssel-Administrator;**
- **die betrachteten Objekte:**
  - **private Schlüssel;**
  - **Sicherheitsanker (qualifizierte Zertifikate und (System-)Zertifikate);**
- **und die betrachteten Operationen:**
  - **Speichern privater Schlüsseln oder Sicherheitsanker;**
  - **Löschen privater Schlüsseln oder Sicherheitsanker;**

durchsetzen.

143 FDP_ACF.1 (Sys) Zugriffskontrolle basierend auf Sicherheitsattributen (Systemsicherheit-Zugriffskontrollpolitik)

144 FDP_ACF.1.1/Sys Die TSF müssen die **SFP für die Zugriffskontrolle auf die Systemsicherheit (Systemsicherheit-Zugriffskontrollpolitik)** für Objekte, die auf **den Sicherheitsattributen Rolle, Benutzerkennzeichen und Rechte** basieren, durchsetzen.

145 FDP_ACF.1.2/Sys Die TSF müssen die folgenden Regeln durchsetzen, um festzustellen, ob eine Operation zwischen kontrollierten Subjekten und kontrollierten Objekten zulässig ist:

Speichern und Löschen der privaten Schlüssel und Sicherheitsanker erfolgt nur nach erfolgreicher Authentisierung des Schlüssel-Administrators.

146 FDP_ACF.1.3/Sys Die TSF müssen den Zugriff von Subjekten auf Objekte basierend auf den folgenden zusätzlichen Regeln expli-

		zit autorisieren: **Die TSF müssen hierbei keine zusätzlichen Regeln berücksichtigen**.
147	FDP_ACF.1.4/Sys	Die TSF müssen den Zugriff von Subjekten auf Objekte, basierend auf **keinen zusätzlichen Regeln** explizit verweigern.
148	FDP_ITC.1	Import von Benutzerdaten ohne Sicherheitsattribute
149	FDP_ITC.1.1	Die TSF müssen die **SFP für die Zugriffskontrolle auf die Systemsicherheit (Systemsicherheit-Zugriffskontrollpolitik** beim Import von unter Kontrolle der SFP stehenden Benutzerdaten von außerhalb des TSC durchsetzen.
150	FDP_ITC.1.2	Die TSF müssen die mit den Benutzerdaten (hier: Sicherheitsanker und private Schlüssel) verknüpften Sicherheitsattribute ignorieren, wenn diese von außerhalb des TSC importiert werden.
151	FDP_ITC.1.3	Die TSF müssen die folgenden Regeln beim Import unter Kontrolle der SFP stehender Benutzerdaten von außerhalb des TSC durchsetzen: **Keine zusätzliche Importkontrollregeln**.
152	**Klasse FIA: Identifikation und Authentisierung**	
153	FIA_UID.2	Benutzeridentifikation vor jeglicher Aktion
154	Ist hierarchisch zu:	FIA_UID.1
155	FIA_UID.2.1	Die TSF müssen erfordern, daß sich jeder Benutzer (hier: Security-Administrator, Schlüssel-Administrator, Revisor und Signaturschlüssel-Inhaber) identifiziert, bevor für diesen jegliche andere TSF-vermittelte Aktionen erlaubt werden.
156	**Klasse FMT: Sicherheitsmanagement**	
157	FMT_MSA.1 (Batch)	Management der Sicherheitsattribute (Batchsignatur-Zugriffskontrollpolitik)
158	FMT_MSA.1.1/Batch	Die TSF müssen die **SFP für die Zugriffskontrolle auf die Batchsignatur (Batchsignatur-Zugriffskontrollpolitik)** zur Beschränkung der Fähigkeit zum **Modifizieren und Löschen** der Sicherheitsattribute **Signatur, mit der die zu signierenden Daten abgesichert sind, (System-)Zertifikat des anfordernden Systems, SystemId, OperationId, Rollendefinition, Begrenzung zur Erzeugung von Batchsignaturen** auf **den Securi-**

ty-Administrator (zusammen mit dem Revisor), den Schlüssel-Administrator sowie den Signaturschlüssel-Inhaber (bzgl. der Begrenzung zur Erzeugung von Batchsignaturen) durchsetzen.

159 FMT_MSA.1 (Sys) Management der Sicherheitsattribute (Systemsicherheit-Zugriffskontrollpolitik)

160 FMT_MSA.1.1/Sys Die TSF müssen die **SFP für die Zugriffskontrolle auf die Systemsicherheit (Systemsicherheit-Zugriffskontrollpolitik)** zur Beschränkung der Fähigkeit zum **Modifizieren und Löschen** der Sicherheitsattribute **Rolle, Benutzerkennung und Rechte** auf **den Schlüssel-Administrator** durchsetzen.

161 FMT_MSA.2 Sichere Sicherheitsattribute

162 FMT_MSA.2.1 Die TSF müssen sicherstellen, dass nur sichere Werte für Sicherheitsattribute akzeptiert werden.

163 FMT_MSA.3 (Batch) Initialisierung statischer Attribute (Batchsignatur-Zugriffskontrollpolitik

164 FMT_MSA.3.1/Batch Die TSF müssen die **SFP für die Zugriffskontrolle auf die Batchsignatur (Batchsignatur-Zugriffskontrollpolitik)** zur Bereitstellung von vorgegebenen Standardwerten mit **einschränkenden Eigenschaften** für Sicherheitsattribute, die zur Durchsetzung der SFP benutzt werden, durchsetzen.

165 FMT_MSA.3.2/Batch Die TSF müssen dem **Security-Administrator (zusammen mit dem Revisor), dem Schlüssel-Administrator und dem Signaturschlüssel-Inhaber** gestatten, bei der Erzeugung eines Objekts oder von Informationen alternative Anfangswerte zu spezifizieren, die die vorgegebenen Standardwerte ersetzen.

166 FMT_MSA.3 (Sys) Initialisierung statischer Attribute (Systemsicherheit-Zugriffskontrollpolitik

167 FMT_MSA.3.1/Sys Die TSF müssen die **SFP für die Zugriffskontrolle auf die Systemsicherheit (Systemsicherheit-Zugriffskontrollpolitik)** zur Bereitstellung von vorgegebenen Standardwerten mit **einschränkenden Eigenschaften** für Sicherheitsattribute, die zur Durchsetzung der SFP benutzt werden, durchsetzen.

168 FMT_MSA.3.2/Sys Die TSF müssen dem **Schlüssel-Administrator** gestatten, bei der Erzeugung eines Objekts oder von Informationen alternative Anfangswerte zu spezifizieren, die die vorgegebenen Standardwerte ersetzen.

169 FMT_SMR.1 (Batch) Sicherheitsrollen (Batchsignatur-Zugriffskontrollpolitik)

170 FMT_SMR.1.1/Batch Die TSF müssen die Rollen **Security-Administrator, Schlüssel-Administrator, Revisor und Signaturschlüssel-Inhaber** erhalten.

171 FMT_SMR.1.2/Batch Die TSF müssen Benutzer mit Rollen verknüpfen können.

172 FMT_SMR.1 (Sys) Sicherheitsrollen (Systemsicherheit-Zugriffskontrollpolitik)

173 FMT_SMR.1.1/Sys Die TSF müssen die Rollen **Schlüssel-Administrator** erhalten.

174 FMT_SMR.1.2/Sys Die TSF müssen Benutzer mit Rollen verknüpfen können.

175 Klasse FTA: EVG-Zugriff

176 FTA_TAB.1 Vorgegebene EVG-Zugriffswarnmeldung

177 FTA_TAB.1.1 Vor Einrichtung einer Benutzersitzung müssen die TSF einen beratenden Warnhinweis für den nichtautorisierten Gebrauch des TOE (EVG) anzeigen.

Bevor der Signaturschlüssel-Inhaber seine sichere Signaturerstellungseinheit für die Erzeugung von Batchsignaturen freischaltet, müssen die TSF dem Signaturschlüssel-Inhaber einen entsprechenden Warnhinweis anzeigen. Dabei wird dem Signaturschlüssel-Inhaber angezeigt, welches System inkl. Zweck (Fachaufgabe) Batchsignaturen automatisiert erzeugen kann. Die Anzeige enthält die temporale bzw. quantitative Einschränkung der Signierfähigkeit.

5.1.3 Anforderungen an die Vertrauenswürdigkeit des EVG

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

179 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

180 Funktionale Sicherheitsanforderungen an die IT-Umgebung entfallen, da es keine Anforderung gibt, die über die Annahmen für die IT-Umgebung hinausgehen, und sich darüber hinaus keine Annahmen für die IT-Umgebung aus den funktionalen EVG-Sicherheitsanforderung ergeben.

5.3 Sicherheitsanforderungen an die Nicht-IT-Umgebung

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

6 EVG-Übersichtsspezifikation

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

SF1 Unterstützung bei der Erzeugung qualifizierter elektronischer (Batch-) Signaturen (Zuführen zu signierender Dokumente zu einer sicheren Signaturerstellungseinheit);

SF2 Mathematische Prüfung qualifizierter Signaturen (Verifizieren);

SF3 Statusprüfung qualifizierter Zertifikate (Validieren).

183 Wie in Abschnitt 2.3 ausgeführt, besteht der EVG aus den Teilsystemen

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

6.1 SF1 – Unterstützung bei der Erzeugung qualifizierter elektronischer (Batch-)Signaturen

184 Die Sicherheitsfunktion SF1 „Unterstützung bei der Erzeugung qualifizierter elektronischer (Batch-)Signaturen (Zuführen zu signierender Dokumente zu einer sicheren Signaturerstellungseinheit)“ ist wie folgt definiert:

- Das Kernsystem erhält von außen über eine Schnittstelle die Anforderung, Daten serverbasiert mit einer Batchsignatur zu versehen:
  - Die Anforderung enthält insbesondere die zu signierenden Daten, die auszuführende Aktion (OperationId) sowie eine Kennung über das anfordernde System (SystemId) und ist mit einer elektronischen Signatur versehen.
  - Durch die elektronische Signatur der Anforderung wird die Autorisierung der Signaturanfrage zur Erzeugung einer Batchsignatur sichergestellt und gewährleistet, dass die Daten signiert werden, die das anfordernde System dem Signierprozess zuführen möchte.[33]
  - Das Kernsystem prüft, ob das anfordernde System die angeforderte Signaturkarte nutzen darf (Abgleich der SystemId und der OperationId mit den im Regelwerk des Kernsystems enthaltenen Regeln, welche die Zulässigkeit von Zugriffen steuern).
  - Zum Signieren werden die zu signierenden Daten vom Kernsystem dem NetSigner zugeführt (Am NetSigner sind die Chipkartenleser mit den Signaturkarten angeschlossen.). Anschließend emp-

[33] Der EVG wird unter der Annahme betrieben, dass ein System, das auf diesen EVG zugreift, die SigG/SigV-Anforderungen an Signaturanwendungskomponenten erfüllt.

fängt das Kernsystem die Signatur bzw. im Fehlerfall eine Fehlermeldung vom NetSigner.

- Anschließend wird die Signatur resp. die Fehlermeldung an das anfordernde System zurückgeliefert.

185 Im Kontext der Signaturerstellung wird der EVG intern wie folgt genutzt:

- Der NetSigner führt zu signierende Daten der sicheren Signaturerstellungseinheit zu:
  - Die Anforderung enthält die zu signierenden Daten (einem Hashwert). Durch die elektronische Signatur wird sichergestellt, dass die Daten signiert werden, die das anfordernde System signiert haben möchte (vgl. Abschnitt 2.4.4) und dass das anfordernde System für die Erzeugung einer Batchsignatur berechtigt ist.
  - Der NetSigner führt folgende Prüfung durch:
    - Es wird geprüft, dass die Signaturprüfung der Anfrage (Anfrage ist elektronisch signiert) mathematisch korrekt ist.
    - Der für die Verifikation der Anfrage benötigte öffentliche Schlüssel des anfordernden Systems liegt in Form eines (System-)Zertifikats im EVG – im Sinne eines Trust Anchors – vor. Das (System-)Zertifikat wird dabei nicht mit der Signier-Anforderung übertragen.
    - Zudem wird geprüft, dass die Zuordnung von (System-) Zertifikat der Signier-Anforderung des anfordernden Systems zur Rolle der Signaturkarte in der IT-Umgebung für die Erzeugung der Batchsignatur korrekt ist, d. h. das anfordernde System (gekennzeichnet durch das (System-) Zertifikat) darf die sichere Signaturerstellungseinheit, die die Batchsignatur erzeugen soll (gekennzeichnet durch die Rolle), nutzen.
    - Es wird geprüft, ob das Zeitfenster für die Erzeugung von Batchsignaturen gültig bzw. die gültige Anzahl von Batchsignaturen noch nicht erreicht ist.
  - Sind alle Prüfungen positiv verlaufen, werden zum Signieren die zu signierenden Daten der sicheren Signaturerstellungseinheit (Signaturkarte) zugeführt.
  - Anschließend wird die Signatur bzw. eine Fehlermeldung zurückgeliefert.

186 Bevor Batchsignaturen erzeugt werden können, muss der Signaturschlüssel-Inhaber initial seine sichere Signaturerstellungseinheit per PIN-Eingabe freischalten. Dazu wird ihm angezeigt, welches System inkl. Zweck (Fachaufgabe) innerhalb welchen Zeitfensters bzw. für welche Anzahl von Batchsignaturen seine sichere Signaturerstellungseinheit nutzen kann.

187 Wird eine Signaturkarte aus dem Chipkartenleser entfernt, erhält der Signaturschlüssel-Inhaber eine entsprechende Mitteilung per E-Mail.

6.2 SF2 – Mathematische Prüfung qualifizierter Signaturen

188 Die Sicherheitsfunktion SF2 „Mathematische Prüfung qualifizierter Signaturen (Verifizieren)“ ist wie folgt definiert:

- Das Kernsystem erhält von außen über eine Schnittstelle die Anforderung, die mathematische Korrektheit einer qualifizierten elektronischen Signatur zu prüfen:
  - Das Kernsystem führt eine Signaturprüfung durch.
  - Dazu prüft das Kernsystem die mathematische Korrektheit der Signatur mittels zugehörigem Prüfschlüssel (öffentlichem Schlüssel aus qualifiziertem Zertifikat) und geeigneten kryptographischen Verfahren,
  - stellt das Ergebnis (korrekte oder nicht korrekte Signatur oder Fehlermeldung) fest
  - und versieht das Ergebnis der Verifikation mit einer elektronischen Signatur. [34]
  - Anschließend wird das Ergebnis der Verifikation an das anfordernde System zurückgeliefert.

6.3 SF3 – Statusprüfung qualifizierter Zertifikate

189 Die Sicherheitsfunktion SF3 „Statusprüfung qualifizierter Zertifikate (Validieren)“ ist wie folgt definiert:

- Der EVG erhält von außen die Anforderung, die Gültigkeit eines Zertifikats festzustellen, wobei Gültigkeit gemäß SigG die Prüfung impliziert, ob ein nachgeprüftes qualifiziertes Zertifikat im jeweiligen Zertifikatsverzeichnis zum angegebenen Zeitpunkt vorhanden und nicht gesperrt war. Hierbei sind zwei Fälle zu unterscheiden:
  1. Das Kernsystem erhält diese Anforderung, welches sodann
     - zum Validieren eine entsprechende Anfrage an das OCSP/CRL-Relay sendet
     - und anschließend das mit einer elektronischen Signatur versehene Ergebnis der Validierung empfängt. Das Ergebnis der Validierung umfasst eine Interpretation der Validierung (gültig und nicht gesperrt, unbekannt oder gesperrt) und auch die Verzeichnisdienst-Auskünfte.

[34] Dieser Dienst ergibt Sinn, da das Kernsystem u. U. mehr Signaturformate als das anfordernde System unterstützt.

Das Kernsystem verifiziert das mit einer elektronischen Signatur versehene Validierungsergebnis vom OCSP/CRL-Relay, sofern Kernsystem und OCSP/CRL-Relay nicht in einem vertrauenswürdigen Netz betrieben werden,[35] und fährt bei gültiger Verifikation fort.

- Anschließend wird dieses Ergebnis der Validierung an das anfordernde System zurückgeliefert.

2. Das OCSP/CRL-Relay erhält – entweder vom Kernsystem oder einem anderen berechtigten System – die Anforderung, die Gültigkeit eines Zertifikats festzustellen. Das OCSP/CRL-Relay stellt die Gültigkeit des angefragten Zertifikats fest:

   - Das OCSP/CRL-Relay validiert das entsprechende Zertifikat entlang der Zertifikatskette. Dazu stellt das OCSP/CRL-Relay für das angeforderte qualifizierte Zertifikat fest, ob das qualifizierte Zertifikat zum angegebenen Zeitpunkt bzw. zum Prüfzeitpunkt (wenn kein Zeitpunkt explizit übergeben wurde) vorhanden und nicht gesperrt war und der Gültigkeitszeitraum des qualifizierten Zertifikats zum angegebenen Zeitpunkt bzw. Prüfzeitpunkt (wenn kein Zeitpunkt explizit übergeben wurde) bereits begonnen und noch nicht abgelaufen war. Darüber hinaus stellt das OCSP/CRL-Relay für Ausstellerzertifikate fest, ob ein Ausstellerzertifikat (in der Zertifikatskette) zum Signierzeitpunkt des ausgestellten Zertifikats vorhanden und nicht gesperrt war und der Gültigkeitszeitraum eines Ausstellerzertifikats (in der Zertifikatskette) zum Signierzeitpunkt des ausgestellten Zertifikats bereits begonnen hatte und noch nicht abgelaufen war.
   - In diesem Zusammenhang fordert das OCSP/CRL-Relay Zertifikatsstatus-Anfragen via Online Certificate Status Protocol (OCSP) und Sperrlisten via Certificate Revocation Lists (CRLs) sowie benötigte Zertifikate via Lightweight Directory Access Protocol (LDAP) an. Das OCSP/CRL-Relay prüft in diesem Kontext die mathematische Korrektheit qualifizierter elektronischer Signaturen (Zertifikate, Antworten auf OCSP-Anfragen und CRLs) und verwendet das Ergebnis (gültige oder ungültige Signatur oder Fehlermeldung) weiter.
   - Das Ergebnis der Validierung umfasst eine Interpretation der Validierung (gültig und nicht gesperrt, unbekannt oder gesperrt) und auch die Verzeichnisdienst-Auskünfte; diese beinhalten die Ergebnisse der OCSP-Anfrage bzw. optional Sperrlisten (Zertifikatsprüfungen via LDAP werden nur interpretiert zurückgeliefert). Das Ergebnis der Validierung signiert das OCSP/CRL-Relay mit einer elektronischen Signatur.

[35] Ob diese Verifikation durchgeführt wird, wird im Kernsystem konfiguriert.

- Anschließend wird dieses mit einer elektronischen Signatur versehene Ergebnis der Validierung an das anfordernde System zurückgeliefert.

6.4 Maßnahmen zur Vertrauenswürdigkeit

190 Um die Vertrauenswürdigkeitsstufe EAL3+ zu erhalten, werden folgende Maßnahmen durchgeführt (vgl. Tabelle 5: Maßnahmen zur Erfüllung von EAL3+):

Tabelle 5: 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	
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	
Schwachstellen-bewertung	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

191 Für die Sicherheitsvorgaben (ST) zur Evaluierung von Governikus wird kein Schutzprofil (Protection Profile – PP) postuliert.

8 Erklärungen

8.1 Erklärung der organisatorischen Sicherheitspolitiken

192 Der EVG ist als Teil einer Signaturanwendungskomponente eine Funktionsbibliothek und stellt damit eine Basis für weitere Signaturanwendungskomponenten dar. Nicht alle Anforderungen von SigG und SigV können daher vom EVG abgedeckt werden.

193 In Abschnitt 2.4 ist beschrieben, in welchem Umfang die Sicherheitsanforderungen des SigG und der SigV an Signaturanwendungskomponenten vom EVG als Funktionsbibliothek erfüllt werden und welcher Anteil von der IT-Umgebung umgesetzt werden muss.

194 Zusammenfassend muss der EVG damit die folgenden Anforderungen umsetzen (vgl. auch organisatorische Sicherheitspolitiken in Abschnitt 3.4):

- Erzeugung von Batchsignaturen:
  - Der EVG muss beim Erzeugen einer Batchsignatur gewährleisten, dass dem Signaturschlüssel-Inhaber vor seiner PIN-Eingabe angezeigt wird, welches System inkl. Zweck (Fachaufgabe) innerhalb welchen Zeitfensters bzw. für welche Anzahl von Batchsignaturen seine sichere Signaturerstellungseinheit nutzen kann.
  - Der EVG muss beim Erzeugen einer Batchsignatur gewährleisten, dass eine Batchsignatur nur durch ein berechtigtes anforderndes System innerhalb eines festen Zeitfensters oder für eine bestimmte Anzahl erfolgt.
- Prüfung von Signaturen:
  - 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.
  - Der EVG muss beim Prüfen einer Signatur gewährleisten, dass die Korrektheit der Signatur zuverlässig geprüft wird.
- Schutz vor unbefugter Veränderung:
  - Wird die Signaturkarte im laufenden Betrieb aus dem Chipkartenleser entfernt, wird dies dem Signaturschlüssel-Inhaber mitgeteilt.

195 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):

- Erzeugung von Batchsignaturen:
  - Das anfordernde System in der IT-Umgebung muss beim Erzeugen einer Batchsignatur gewährleisten, dass das Auslösen einer Batchsignatur vorher eindeutig angezeigt wird.
  - Das anfordernde System in der IT-Umgebung muss beim Erzeugen einer Batchsignatur gewährleisten, dass erkennbar ist, auf welche Daten sich die Batchsignatur bezieht.
  - Das anfordernde System in der IT-Umgebung muss beim Erzeugen einer Batchsignatur gewährleisten, dass bei Bedarf der Inhalt der zu signierenden Daten hinreichend zu erkennen ist.
  - Das anfordernde System in der IT-Umgebung muss beim Erzeugen einer Batchsignatur gewährleisten, dass die Autorisierung zur Erzeugung einer Batchsignatur nur durch eine berechtigte Person bzw. einen entsprechenden Prozess erfolgt.
  - Sichere Signaturerstellungseinheit und Chipkartenleser müssen gewährleisten, dass die Identifikationsdaten nicht preisgegeben und nur auf der jeweiligen sicheren Signaturerstellungseinheit gespeichert werden.
- Prüfung von Signaturen:
  - Das anfordernde System in der IT-Umgebung muss beim Prüfen einer Signatur gewährleisten, dass erkennbar wird, auf welche Daten sich die Signatur bezieht.
  - Das anfordernde System in der IT-Umgebung muss beim Prüfen einer Signatur gewährleisten, dass erkennbar wird, ob die Daten unverändert sind – also eine geeignete Anzeige bereitstellen.
  - Das anfordernde System in der IT-Umgebung muss beim Prüfen einer Signatur gewährleisten, dass bei Bedarf der Inhalt der signierten Daten hinreichend zu erkennen ist.
  - Das anfordernde System in der IT-Umgebung muss beim Prüfen einer Signatur gewährleisten, dass erkennbar wird, welchem Signaturschlüssel-Inhaber die Signatur zuzuordnen ist.
  - Das anfordernde System in der IT-Umgebung muss beim Prüfen einer Signatur gewährleisten, dass erkennbar wird, welche Inhalte das qualifizierte Zertifikat, auf dem die Signatur beruht, und zugehörige qualifizierte Attribut-Zertifikate aufweisen.
  - Das anfordernde System in der IT-Umgebung 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 – also eine geeignete Anzeige bereitstellen.

  - Das anfordernde System in der IT-Umgebung muss beim Prüfen einer Signatur gewährleisten, dass die Korrektheit der Signatur zuverlässig geprüft und zutreffend angezeigt wird – also eine geeignete Anzeige bereitstellen.

- Schutz vor unbefugter Veränderung:
  - Sicherheitstechnische Veränderungen müssen für den Administrator erkennbar werden.

8.2 Erklärung der Sicherheitsziele

8.2.1 Zuordnung der Elemente der Sicherheitsproblemdefinition zu Sicherheitszielen

196 Im Folgenden wird dargestellt und in Tabelle 6 zusammengefasst, wie die einzelnen Annahmen, Bedrohungen und organisatorischen Sicherheitspolitiken durch Sicherheitsziele abgedeckt werden.

- Die Annahmen A.PKI, A.SAK, A.Betrieb, A.DIR und A.ZufPIN werden durch die Sicherheitsziele für die IT-Umgebung OE.PKI, OE.SAK, OE.Betrieb, OE.DIR und OE.ZufPIN abgedeckt – wie auch aus den identischen Bezeichnungen hervorgeht.
- TE.RatePIN wird durch eine SigG-konforme sichere Signaturerstellungseinheit abgedeckt (vgl. OE.PKI), die nur eine begrenzte Anzahl von Fehlversuchen zur Eingabe des Identifikationsmerkmals zulässt sowie nur Merkmale mit Mindestlängen erlaubt.
- TE.SpähePIN wird durch das Sicherheitsziel OE.Betrieb abgedeckt, in dem thematisiert wird, dass der Signaturschlüssel-Inhaber hinsichtlich der Sicherheit sensibilisiert werden muss – auch durch die Auflagen und Hinweise zur Benutzung der sicheren Signaturerstellungseinheit.
- P.AnzeigeBatch wird durch O.AnzeigeBatch abgedeckt.
- P.AuthSign wird durch O.AuthSign abgedeckt. Für die Gewährleistung der Systemsicherheit, so dass also nur ein berechtigtes anforderndes System auf die Signaturkarte zugreifen kann, werden kryptographische Schlüssel und (System-)Zertifikate, ein Chipkartenleser (für die Erzeugung einer Signatur) sowie eine sichere Signaturerstellungseinheit benötigt, so dass OE.PKI vorhanden sein muss. Die Maßnahmen zur Gewährleistung eines sicheren Netzes werden durch OE.Betrieb realisiert.
- P.VerifSign wird durch O.VerifSign abgedeckt und es wird der Prozess der Verifikation präzisiert. Die Maßnahmen zur Gewährleistung eines sicheren Netzes werden durch OE.Betrieb realisiert. Für die Verifikation sind qualifizierte Zertifikate notwendig (OE.PKI). Für die Gewährleistung der Systemsicherheit werden kryptographische Schlüssel (OE.PKI) benötigt.
- P.ValidZert wird durch O.ValidZert abgedeckt und es wird der Prozess der Validierung präzisiert. Die Maßnahmen zur Gewährleistung eines sicheren Netzes werden durch OE.Betrieb realisiert. Für die Validierung

sind qualifizierte Zertifikate (OE.PKI) und Verzeichnisdienste (OE.DIR) notwendig. Für die Gewährleistung der Systemsicherheit werden kryptographische Schlüssel (OE.PKI) benötigt.

- P.AnzEntfernen wird durch das Sicherheitsziel O.AnzEntfernen umgesetzt.

Tabelle 6: Zuordnung Sicherheitsproblemdefinition zu -zielen

Sicherheitsproblemdefinition	zugehörige Sicherheitsziele
A.PKI	OE.PKI
A.SAK	OE.SAK
A.Betrieb	OE.Betrieb
A.DIR	OE.DIR
A.ZufPIN	OE.ZufPIN
TE.RatePIN	OE.PKI
TE.SpähePIN	OE.Betrieb
P.AnzeigeBatch	O.AnzeigeBatch
P.AuthSign	O.AuthSign, OE.PKI, OE.Betrieb
P.VerifSign	O.VerifSign, OE.PKI, OE.Betrieb
P.ValidZert	O.ValidZert, OE.PKI, OE.DIR, OE.Betrieb
P.AnzEntfernen	O.AnzEntfernen

8.2.2 Zuordnung Sicherheitsziele zu EVG-Sicherheitsumgebung

197 Die Sicherheitsziele werden für die Realisierung der EVG-Sicherheitsumgebung benötigt:

- O.AnzeigeBatch realisiert P.AnzeigeBatch.
- O.AuthSign realisiert P.AuthSign.
- O.VerifSign realisiert P.VerifSign.
- O.ValidZert realisiert P.ValidZert.
- O.AnzEntfernen realisiert P.AnzEntfernen.
- Das Sicherheitsziel der Umgebung OE.PKI wird für die gleichnamige Annahme (A.PKI) und die Bedrohung TE.RatePIN (SigG-konforme Signaturkarten erlauben maximal drei Fehlversuche) sowie insbesondere die organisatorischen Sicherheitspolitiken P.AuthSign, P.VerifSign und P.ValidZert benötigt, da hier sowohl Signaturkarten, Chipkartenleser als auch kryptographische Schlüssel, SigG-konforme Zertifikate und (System-)Zertifikate zur Verfügung gestellt werden.
- OE.SAK realisiert A.SAK.
- Das Sicherheitsziel der Umgebung OE.Betrieb wird für die gleichnamige Annahme (A.Betrieb) und die Bedrohung TE.SpähePIN (bauliche Maßnahmen, Sensiblisierung) sowie insbesondere die organisatorischen Sicherheitspolitiken P.AuthSign, P.VerifSign und P.ValidZert hinsichtlich des sicheren Betriebs benötigt.

- OE.DIR realisiert A.DIR und wird für die Validierung (P.ValidZert) benötigt.
- OE.ZufPIN realisiert A.ZufPIN.

198 Tabelle 7 fasst zusammen, wie die Sicherheitsziele die Annahmen, Bedrohungen und organisatorischen Sicherheitspolitiken abdecken.

Tabelle 7: Zuordnung Sicherheitsziele zu -umgebung

Sicherheitsziele	zugehörige EVG-Sicherheitsumgebung
O.AnzeigeBatch	P.AnzeigeBatch
O.AuthSign	P.AuthSign
O.VerifSign	P.VerifSign
O.ValidZert	P.ValidZert
O.AnzEntfernen	P.AnzEntfernen
OE.PKI	A.PKI, TE.RatePIN, P.AuthSign, P.VerifSign, P.ValidZert
OE.SAK	A.SAK
OE.Betrieb	A.Betrieb, TE.SpähePIN, O.AuthSign, O.VerifSign, O.ValidZert
OE.DIR	A.DIR, P.ValidZert
OE.ZufPIN	A.ZufPIN

8.3 Erklärung der Sicherheitsanforderungen

8.3.1 Zuordnung Sicherheitsziele zu funktionalen Sicherheitsanforderungen

199 Wie die Sicherheitsziele, die sich auf IT beziehen, durch die funktionalen Sicherheitsanforderungen erfüllt werden, ist im Folgenden dargestellt und in Tabelle 8 zusammengefasst:

- Das Sicherheitsziel O.AnzeigeBatch wird durch die funktionale Sicherheitsanforderung FTA_TAB.1 erreicht, durch die der Signaturschlüssel-Inhaber einen Warnhinweis erhält, welches anfordernde System inkl. Zweck (Fachaufgabe) nach PIN-Eingabe seine sichere Signaturerstellungseinheit für die Erzeugung von Batchsignaturen nutzen kann. Die Anzeige umfasst die temporale bzw. quantitative Einschränkung der Signierfähigkeit. FTA_TAB.1 wird zu diesem Zweck verfeinert.
- Das Sicherheitsziel O.AuthSign wird wie folgt erreicht:
  - Der EVG kann zu signierende Daten einer angeschlossenen sicheren Signaturerstellungseinheit zur Erzeugung einer Batchsignatur genutzt werden.
  - Der EVG gewährleistet, dass nur dann Batchsignaturen erzeugt werden, sofern die Zugriffsberechtigung erfolgt. Die Zugriffskon-

trolle wird über FDP_ACC.1 (Batch) und FDP_ACF.1 (Batch) geregelt.

- In diesem Zusammenhang ist für das Management der Sicherheitsattribute FDP_ITC.1, FMT_MSA.1 (Batch), FMT_MSA.2 und FMT_MSA.3 (Batch) zuständig. Da das Management nur ausgewählten Personen möglich sein soll, sind Rollen FMT_SMR.1 (Batch) und eine Identifikation (FIA_UID.2) vorhanden.
- Für die Verifikation der Signaturanforderung wird FCS_COP.1 (VSA) benötigt. In diesem Zusammenhang ist FCS_CKM.4 für das Zerstören von kryptographischen Schlüsseln (insbesondere Sicherheitsankern) wichtig.

- O.VerifSign wird durch die funktionalen Sicherheitsanforderungen FCO_NRO.1 und FCS_COP.1 (Verify) erreicht. Letzteres beinhaltet die exakten kryptographischen Algorithmen.

  Die Absicherung des Verifikationsergebnisses an ein anforderndes System, das eine entsprechende Anforderung gestellt hat, erfolgt über eine elektronische Signatur; realisiert über FCS_COP.1 (SVVE). Hinsichtlich der Sicherheitsanker und privaten Schlüssel ist FDP_ITC.1 zum Import und FCS_CKM.4 zum Entfernen sowie FMT_MSA.2 zu den Anforderungen an sichere Werte – nämlich Sicherheitsanker und private Schlüssel – notwendig. Darüber hinaus werden FDP_ACC.1 (Sys), FDP_ACF.1 (Sys) und FMT_MSA.1 (Sys) für den Zugriff auf private Schlüssel durch den Schlüssel-Administrator (FMT_SMR.1 (Sys) und FIA_UID.2) aufgeführt.

- O.ValidZert wird durch die funktionale Sicherheitsanforderung FCO_NRO.1 erreicht, in der insbesondere das SigG-konforme Gültigkeitsmodell – das Kettenmodell – spezifiziert ist. Danach kann geprüft werden, ob das Zertifikat zum angegebenen Zeitpunkt vorhanden und nicht gesperrt war und der Gültigkeitszeitraum des Zertifikats zum angegebenen Zeitpunkt bereits begonnen und noch nicht abgelaufen war.

  Die Absicherung des Validierungsergebnisses an ein anforderndes System, das eine entsprechende Anforderung gestellt hat, erfolgt abgesichert über eine elektronische Signatur; realisiert über FCS_COP.1 (SVVE). Sofern Kernsystem und OCSP/CRL-Relay nicht in einem vertrauenswürdigen Netz betrieben werden, erfolgt die Absicherung des Validierungsergebnisses an das Kernsystem über eine elektronische Signatur; realisiert über FCS_COP.1 (SVVE) beim OCSP/CRL-Relay zur Erzeugung sowie FCS_COP.1 (VVE) beim Kernsystem zur Verifikation. Hinsichtlich der privaten Schlüssel und Sicherheitsanker ist FDP_ITC.1 zum Import und FCS_CKM.4 zum Entfernen sowie FMT_MSA.2 zu den Anforderungen an sichere Werte – nämlich privater Schlüssel und Sicherheitsanker – notwendig. Darüber hinaus werden FDP_ACC.1 (Sys), FDP_ACF.1 (Sys) und FMT_MSA.1 (Sys) für den Zugriff auf private Schlüssel und Sicher-

heitsanker durch den Schlüssel-Administrator (FMT_SMR.1 (Sys) und FIA_UID.2) aufgeführt.[36]

Im Rahmen der Validierung werden qualifizierte elektronische Signaturen verifiziert (FCS_COP.1 (Verify)).

- O.AnzEntfernen wird durch die funktionalen Sicherheitsanforderungen FAU_ARP.1 und FAU_SAA.3 erreicht, die bei Entfernen einer Signaturkarte einen Sicherheitsalarm per E-Mail auslösen.

Tabelle 8: Zuordnung Sicherheitsziele zu Sicherheitsanforderungen an den EVG

Sicherheitsziele	funktionale Sicherheitsanforderungen an den EVG
O.AnzeigeBatch	FTA_TAB.1
O.AuthSign	FCS_CKM.4, FCS_COP.1 (VSA), FDP_ACC.1 (Batch), FDP_ACF.1 (Batch), FDP_ITC.1, FMT_MSA.1 (Batch), FMT_MSA.2, FMT_MSA.3 (Batch), FMT_SMR.1 (Batch), FIA_UID.2
O.VerifSign	FCO_NRO.1, FCS_CKM.4, FCS_COP.1 (Verify), FCS_COP.1 (SVVE), FDP_ACC.1 (Sys), FDP_ACF.1 (Sys), FDP_ITC.1, FIA_UID.2, FMT_MSA.1 (Sys), FMT_MSA.2, FMT_SMR.1 (Sys),
O.ValidZert	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_SMR.1 (Sys)
O.AnzEntfernen	FAU_ARP.1, FAU_SAA.3

8.3.2 Zuordnung der funkt. Sicherheitsanforderungen zu Sicherheitszielen

200 Wie die funktionalen Sicherheitsanforderungen die Sicherheitsziele abdecken, ist den Ausführungen in Abschnitt 8.3.1 zu entnehmen und in Tabelle 9 zusammenfassend dargestellt:

Tabelle 9: Zuordnung fkt. Sicherheitsanforderungen zu Sicherheitszielen

funktionale Sicherheitsanforderungen an den EVG	Sicherheitsziele
FAU_ARP.1	O.AnzEntfernen
FAU_SAA.3	O.AnzEntfernen
FCO_NRO.1	O.VerifSign, O.ValidZert
FCS_CKM.4	O.AuthSign, O.VerifSign, O.ValidZert

[36] Sofern Kernsystem und OCSP/CRL-Relay über ein Weitverkehrsnetz kommunizieren, sind die Auflagen (vgl. A.Betrieb und OE.Betrieb) zur sicheren Kommunikation zu beachten.

funktionale Sicherheitsanforderungen an den EVG	Sicherheitsziele
FCS_COP.1 (Verify)	O.VerifSign, O.ValidZert
FCS_COP.1 (VSA)	O.AuthSign
FCS_COP.1 (SVVE)	O.VerifSign, O.ValidZert
FCS_COP.1 (VVE)	O.ValidZert
FDP_ACC.1 (Batch)	O.AuthSign
FDP_ACC.1 (Sys)	O.VerifSign, O.ValidZert
FDP_ACF.1 (Batch)	O.AuthSign
FDP_ACF.1 (Sys)	O.VerifSign, O.ValidZert
FDP_ITC.1	O.AuthSign, O.VerifSign, O.ValidZert
FIA_UID.2	O.AuthSign, O.VerifSign, O.ValidZert
FMT_MSA.1 (Batch)	O.AuthSign
FMT_MSA.1 (Sys)	O.VerifSign, O.ValidZert
FMT_MSA.2	O.AuthSign, O.VerifSign, O.ValidZert
FMT_MSA.3 (Batch)	O.AuthSign
FMT_MSA.3 (Sys)	O.VerifSign, O.ValidZert
FMT_SMR.1 (Batch)	O.AuthSign
FMT_SMR.1 (Sys)	O.VerifSign, O.ValidZert
FTA_TAB.1	O.AnzeigeBatch

8.3.3 Erfüllung der Abhängigkeiten für den EVG

201 Die EVG-Abhängigkeiten sind berücksichtigt, wie im Folgenden ausgeführt und in Tabelle 10 zusammenfassend dargestellt.

202 Die Beschreibung erfolgt für die Themenkomplexe Signieren, Verifizieren und Validieren, Batchsignatur-Zugriffskontrollpolitik, Systemsicherheit und Trust Anchor sowie Sicherheitsalarme.

Signieren, Verifizieren und Validieren

203 Selektive Urheberschaftsbeweise sind hinsichtlich von Anforderungen von außen

- für die Verifikation von qualifizierten elektronischen Signaturen und
- für die Validierung eines qualifizierten Zertifikats

sowie hinsichtlich der Systemsicherheit

- für die Erzeugung einer elektronischen Signatur für Verifikations- und Validierungsergebnisse und

- für die Verifikation einer elektronischen Signatur, die die Signier-Anforderung absichert,

relevant.

204 Diese Aspekte werden durch die funktionale EVG-Sicherheitsanforderung FCO_NRO.1 abgedeckt. Die Abhängigkeit FIA_UID.1 ist nicht anwendbar, da kein Benutzer involviert.

Batchsignatur-Zugriffskontrollpolitik

205 Ausgangspunkt dieser Betrachtung ist die funktionale EVG-Sicherheitsanforderung FDP_ACC.1 (Batch).

206 FDP_ACC.1 ist abhängig von FDP_ACF.1, so dass FDP_ACF.1 (Batch) aufgenommen wurde.

207 FDP_ACF.1 hat wiederum die Abhängigkeiten FDP_ACC.1 und FMT_MSA.3. FDP_ACC.1 (Batch) und FMT_MSA.3 (Batch) sind aufgenommen.

208 FMT_MSA.3 ist abhängig von FMT_SMR.1 und FMT_MSA.1. FMT_SMR.1 (Batch) und FMT_MSA.1(Batch) sind aufgenommen.

209 FMT_SMR.1 ist abhängig von FIA_UID.1. Da jegliche Benutzer identifiziert werden müssen, wurde die hierarchische Komponente FIA_UID.2 gewählt. FIA_UID.2 hat keine Abhängigkeiten.

210 FMT_MSA.1 hat die Abhängigkeit FDP_ACC.1 oder FDP_IFC.1 sowie FMT_SMR.1. FDP_ACC.1 (Batch) und FMT_SMR.1 (Batch) sind bereits aufgenommen; FDP_IFC.1 ist hier nicht anwendbar.

Systemsicherheit und Trust Anchor

211 Ausgangspunkt dieser Betrachtung ist die funktionale EVG-Sicherheitsanforderung FCS_COP.1. FCS_COP.1 hat die Abhängigkeit FDP_ITC.1 oder FCS_CKM.1 (für Schlüsselimport- oder -generierung) sowie FCS_CKM.4 (für Schlüsselzerstörung) und FMT_MSA.2 (für Schlüsselmanagement). Die Iterationen werden getrennt betrachtet:

- FCS_COP.1 (Verify): In diesem Kontext sind Sicherheitsanker (vertrauenswürdige qualifizierte Zertifikate) zu nennen, die von außerhalb importiert werden.
- FCS_COP.1 (VSA): In diesem Kontext sind (System-)Zertifikate (für die Systemsicherheit) zu nennen, die von außerhalb importiert werden.
- FCS_COP.1 (SVVE): In diesem Kontext sind private Schlüssel (für die Systemsicherheit) zu nennen, die von außerhalb importiert werden.
- FCS_COP.1 (VVE): In diesem Kontext ist der Sicherheitsanker (Trust Anchor) zu nennen, der von außerhalb importiert wird.

212 Gleichermaßen gilt: Da keine privaten Schlüssel im EVG generiert werden, ist FCS_CKM.1 nicht relevant. Im Folgenden werden die Abhängigkeiten zu FMT_MSA.2, FDP_ITC.1 und FCS_CKM.4 thematisiert.

213 <u>zu FMT_MSA.2:</u>

214 FMT_MSA.2 hat vier Abhängigkeiten: ADV_SPM.1, FDP_ACC.1 oder FDP_IFC.1, FMT_MSA.1 und FMT_SMR.1:

- Die Abhängigkeit zum informellen EVG-Sicherheitsmodell ADV_SPM.1 kann gemäß [CC-Teil2, H.2] entfallen, wenn eine „klare Definition der sicheren Werte“ und der „Grund, warum diese als sicher angesehen werden können, bereitgestellt“ [CC-Teil2, H.2] wird. Dies ist für die Sicherheitsattribute (Signatur, (System-)Zertifikat, SystemId, OperationId, Rollendefinition und Begrenzung zur Erzeugung von Batchsignaturen sowie Rolle, Benutzerkennung und Rechte) der Fall:
  - Für die Signatur, mit der die zu signierenden Daten abgesichert sind, sowie das (System-)Zertifikat des anfordernden Systems, das im EVG im Sinne eines Trust Anchors vorliegt, sind die in FCS_COP.1 angegebenen Normen einzuhalten.
  - Für SystemId und OperationId sind Identifier für anfordernde Systeme resp. auszuführende Operationen einzutragen.
  - Über die Rollendefinition wird u. a. der Zugriff eines Prozesses einer Fachaufgabe (in einem anfordernden System) auf eine Signaturkarte kontrolliert. Für die Rollendefinition ist die Zuordnung von Signaturkarte zu Rolle und Rolle zu anforderndem System inkl. Zweck (Fachaufgabe) herzustellen, so dass je Signaturkarte genau ein anforderndes System zugreifen darf.
  - Für die Begrenzung zur Erzeugung von Batchsignaturen sind zeitliche bzw. quantitative Angaben zu machen.
  - Hinsichtlich Rolle und Rechte sind die in Abschnitt 3.1 definierten Rollen mit Rechten einem Benutzer/Administrator über eine Benutzerkennung zuzuweisen.

  Die angegebenen Werte zu Signatur und (System-)Zertifikat können aufgrund der Sicherheit der zu Grunde liegenden Public-Key-Infrastruktur (PKI) als sicher angesehen werden. Die vom entsprechenden Security-Administrator (zusammen mit dem Revisor), Schlüssel-Administrator bzw. Signaturschlüssel-Inhaber im EVG konfigurierten Werte für die weiteren Sicherheitsattribute (SystemId, OperationId, Rollendefinition, Begrenzung, Rolle, Benutzerkennung und Rechte) werden als sicher erachtet; hinsichtlich der Zugriffskontrolle ist eine Übereinstimmung (bzw. Unterschreitung beim Sicherheitsattribut Begrenzung) zwischen übermittelten (bzw. aktuellen) und gespeicherten Daten relevant.

  Sichere Werte werden auf sichere Weise in den EVG eingespielt (vgl. weitere Abhängigkeiten).
- FDP_ACC.1 (Sys) ist aufgenommen. Die Alternative FDP_IFC.1 ist hier nicht relevant.
- FMT_MSA.1 (Sys) ist aufgenommen.
- FMT_SMR.1 (Sys) ist aufgenommen.

215 Für die Abhängigkeiten ergibt sich folgendes:

216 FDP_ACC.1 ist abhängig von FDP_ACF.1, so dass FDP_ACF.1 (Sys) aufgenommen wurde.

217 FDP_ACF.1 hat wiederum die Abhängigkeiten FDP_ACC.1 und FMT_MSA.3. FDP_ACC.1 (Sys) und FMT_MSA.3 (Sys) sind aufgenommen.

218 FMT_MSA.3 ist abhängig von FMT_SMR.1 und FMT_MSA.1. FMT_SMR.1 (Sys) und FMT_MSA.1(Sys) sind aufgenommen.

219 FMT_SMR.1 ist abhängig von FIA_UID.1. Da jegliche Benutzer identifiziert werden müssen, wurde die hierarchische Komponente FIA_UID.2 gewählt. FIA_UID.2 hat keine Abhängigkeiten.

220 FMT_MSA.1 hat die Abhängigkeit FDP_ACC.1 oder FDP_IFC.1 sowie FMT_SMR.1. FDP_ACC.1 (Sys) und FMT_SMR.1 (Sys) sind bereits aufgenommen; FDP_IFC.1 ist hier nicht anwendbar.

221 zu FCS_CKM.4:

222 FCS_CKM.4 hat die Abhängigkeiten FDP_ITC.1 (oder FCS_CKM.1, sofern Schlüssel im EVG generiert werden – hier nicht relevant) und FMT_MSA.2. Beide Abhängigkeiten sind berücksichtigt.

223 zu FDP_ITC.1:

224 FDP_ITC.1 hat die Abhängigkeiten FDP_ACC.1 oder FDP_IFC.1 sowie FMT_MSA.4. FDP_IFC.1 ist nicht anwendbar; die beiden anderen Abhängigkeiten sind berücksichtigt.

Sicherheitsalarme

225 FAU_ARP.1 hat die Abhängigkeit FAU_SAA.1. FAU_SAA.3 – hierarchisch zu FAU_SAA.1 – ist aufgenommen und hat selber keine Abhängigkeiten.

Tabelle 10: Erfüllung der EVG-Abhängigkeiten

funktionale Sicherheitsanforderungen an den EVG	Abhängigkeiten	Bemerkung
FAU_ARP.1	FAU_SAA.1	erfüllt durch FAU_SAA.3, das hierarchisch zu FAU_SAA.1 ist
FAU_SAA.3	-	-
FCO_NRO.1	FIA_UID.1	formal nicht erfüllt, da keine Benutzer involviert
FCS_CKM.4	FDP_ITC.1 oder FCS_CKM.1 FMT_MSA.2.	erfüllt für FCS_ITC.1 erfüllt

funktionale Sicherheitsanforderungen an den EVG	Abhängigkeiten	Bemerkung
FCS_COP.1 (Verify)	FDP_ITC.1 oder FCS_CKM.1 FCS_CKM.4 FMT_MSA.2	erfüllt für FCS_ITC.1 erfüllt erfüllt
FCS_COP.1 (VSA)	FDP_ITC.1 oder FCS_CKM.1 FCS_CKM.4 FMT_MSA.2	erfüllt für FCS_ITC.1 erfüllt erfüllt
FCS_COP.1 (SVVE)	FDP_ITC.1 oder FCS_CKM.1 FCS_CKM.4 FMT_MSA.2	erfüllt für FCS_ITC.1 erfüllt erfüllt
FCS_COP.1 (VVE)	FDP_ITC.1 oder FCS_CKM.1 FCS_CKM.4 FMT_MSA.2	erfüllt für FCS_ITC.1 erfüllt erfüllt
FDP_ACC.1 (Batch)	FDP_ACF.1 (Batch)	erfüllt
FDP_ACC.1 (Sys)	FDP_ACF.1 (Sys)	erfüllt
FDP_ACF.1 (Batch)	FDP_ACC.1 (Batch) FMT_MSA.3 (Batch)	erfüllt erfüllt
FDP_ACF.1 (Sys)	FDP_ACC.1 (Sys) FMT_MSA.3 (Sys)	erfüllt erfüllt
FDP_ITC.1	FDP_ACC.1 oder FDP_IFC.1 FMT_MSA.3	erfüllt für FDP_ACC.1 erfüllt
FIA_UID.2	-	-
FMT_MSA.1 (Batch)	FDP_ACC.1 (Batch) oder FDP_IFC.1 FMT_SMR.1 (Batch)	erfüllt für FDP_ACC.1 erfüllt
FMT_MSA.1 (Sys)	FDP_ACC.1 (Sys) oder FDP_IFC.1 FMT_SMR.1 (Sys)	erfüllt für FDP_ACC.1 erfüllt

funktionale Sicherheitsanforderungen an den EVG	Abhängigkeiten	Bemerkung
FMT_MSA.2	ADV_SPM. FDP_ACC.1 oder FDP_IFC.1 FMT_MSA.1 FMT_SMR.1	formal nicht erfüllt, da eine klare Definition der sicheren Werte angegeben wird erfüllt für FDP_ACC.1 erfüllt erfüllt
FMT_MSA.3 (Batch)	FMT_MSA.1 (Batch) FMT_SMR.1 (Batch)	erfüllt erfüllt
FMT_MSA.3 (Sys)	FMT_MSA.1 (Sys) FMT_SMR.1 (Sys)	erfüllt erfüllt
FMT_SMR.1 (Batch)	FIA_UID.1	erfüllt durch FIA_UID.2, das hierarchisch zu FIA_UID.1 ist
FMT_SMR.1 (Sys)	FIA_UID.1	erfüllt durch FIA_UID.2, das hierarchisch zu FIA_UID.1 ist
FTA_TAB.1	-	-

8.3.4 Erfüllung der Abhängigkeiten für die IT-Umgebung

226 Es sind keine funktionalen Sicherheitsanforderungen für die IT-Umgebung formuliert.

8.3.5 Analyse des Zusammenwirkens der funktionalen Anforderungen

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

228 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.

8.3.6 Analyse der Mindest-Stärkestufe

229 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".

230 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.

8.3.7 Erklärung zu den Anforderungen an die Vertrauenswürdigkeit

231 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

232 Die Sicherheitsfunktionen wirken mit den funktionalen Sicherheitsanforderungen wie folgt (vgl. Tabelle 11, wobei ein „X" eine für die jeweilige Sicherheitsfunktion zutreffende funktionale Sicherheitsanforderung signalisiert):

- Für die Sicherheitsfunktion SF1 „Unterstützung bei der Erzeugung qualifizierter elektronischer (Batch-)Signaturen (Zuführen zu signierender Dokumente zu einer sicheren Signaturerstellungseinheit)" werden folgende Komponenten benötigt:
    - Komponente FCS_COP.1 (VSA) für die kryptographische Operation des Verifizierens der Signaturanforderungen samt der Abhängigkeiten FDP_ITC.1 (Import kryptographischer Schlüssel), FCS_CKM.4 (Zerstören kryptographischer Schlüssel) und FMT_MSA.2 (Management);
    - Komponenten FDP_ACC.1 (Batch), FDP_ACF.1 (Batch), FMT_MSA.1 (Batch), FMT_MSA.3 (Batch) sowie FMT_SMR.1 (Batch) und FIA_UID.2 für die Gewährleistung, dass der EVG eine Batchsignatur nur für berechtigte anfordernde Systeme erzeugt und die Verwaltung der Sicherheitsattribute (insbesondere

(System-)Zertifikat, SystemId, OperationId, Rollendefinition und Begrenzung zur Erzeugung von Batchsignaturen) nur durch autorisierte Benutzer erfolgt;

- Komponente FTA_TAB.1 für die Anzeige für den Signaturschlüssel-Inhaber;
- Komponenten FAU_ARP.1 und FAU_SAA.3 für die Gewährleistung, dass dem Signaturschlüssel-Inhaber mitgeteilt wird, falls seine Signaturkarte aus dem Chipkartenleser entfernt wird

- Für die Sicherheitsfunktion SF2 „Mathematische Prüfung qualifizierter Signaturen (Verifizieren)“ werden folgende Komponenten benötigt:
  - Komponente FCO_NRO.1 für die Fähigkeit des EVG, qualifizierte Signaturen zu verifizieren;
  - Komponente FCS_COP.1 (Verify) für die kryptographische Operation des Verifizierens von Signaturen samt der Abhängigkeiten FDP_ITC.1 (Import kryptographischer Schlüssel), FCS_CKM.4 (Zerstören kryptographischer Schlüssel) und FMT_MSA.2 (Management);
  - Komponente FCS_COP.1 (SVVE) für die kryptographische Operation des Signierens von Verifikationsergebnissen samt der Abhängigkeiten FDP_ITC.1, FCS_CKM.4 und FMT_MSA.2;
  - Komponenten FDP_ACC.1 (Sys), FDP_ACF.1 (Sys), FMT_MSA.1 (Sys), FMT_MSA.3 (Sys) sowie FMT_SMR.1 (Sys) und FIA_UID.2 für die Gewährleistung, dass Sicherheitsattribute (private Schlüssel und Sicherheitsanker) nur durch den Schlüssel-Administrator verwaltet werden.
- Für die Sicherheitsfunktion SF3 „Statusprüfung qualifizierter Zertifikate (Validieren)“ werden folgende Komponenten benötigt:
  - Komponente FCO_NRO.1 für die Fähigkeit des EVG, Signaturen zu validieren;
  - Komponente FCS_COP.1 (Verify) für die kryptographische Operation des Verifizierens von Signaturen – und hier insbesondere von Zertifikaten, Sperrlisten und OCSP-Statusantworten – und FDP_ITC.1 für den Import der Sicherheitsanker samt der Abhängigkeiten FCS_CKM.4 (Zerstörung kryptographischer Schlüssel) und FMT_MSA.2 (Management);
  - Komponente FCS_COP.1 (SVVE) für die kryptographische Operation des Signierens von Validierungsergebnissen samt der Abhängigkeiten FDP_ITC.1, FCS_CKM.4 und FMT_MSA.2;
  - Komponente FCS_COP.1 (VVE) für die kryptographische Operation des Verifizierens von Signaturen – hier die Verifikation des Validierungsergebnisses, das vom OCSP/CRL-Relay mit einer elektronischen Signatur versehen ist – samt der Abhängigkeiten FDP_ITC.1 (Import der Sicherheitsanker), FCS_CKM.4 (Zerstö-

rung kryptographischer Schlüssel) und FMT_MSA.2 (Management);

- Komponenten FDP_ACC.1 (Sys), FDP_ACF.1 (Sys), FMT_MSA.1 (Sys), FMT_MSA.3 (Sys) sowie FMT_SMR.1 (Sys) und FIA_UID.2 für die Gewährleistung, dass Sicherheitsattribute (private Schlüssel und Sicherheitsanker) nur durch den Schlüssel-Administrator verwaltet werden.

Tabelle 11: Zuordnung fkt. Sicherheitsanforderungen durch Sicherheitsfunktionen

Fkt. Sicherheitsanforderungen an EVG bzw. IT-Umgebung	SF1	SF2	SF3
FAU_ARP.1	X		
FAU_SAA.3	X		
FCO_NRO.1		X	X
FCS_CKM.4	X	X	X
FCS_COP.1 (Verify)		X	X
FCS_COP.1 (VSA)	X		
FCS_COP.1 (SVVE)		X	X
FCS_COP.1 (VVE)			X
FDP_ACC.1 (Batch)	X		
FDP_ACC.1 (Sys)		X	X
FDP_ACF.1 (Batch)	X		
FDP_ACF.1 (Sys)		X	X
FDP_ITC.1	X	X	X
FIA_UID.2	X	X	X
FMT_MSA.1 (Batch)	X		
FMT_MSA.1 (Sys)		X	X
FMT_MSA.2	X	X	X
FMT_MSA.3 (Batch)	X		
FMT_MSA.3 (Sys)		X	X
FMT_SMR.1 (Batch)	X		
FMT_SMR.1 (Sys)		X	X
FTA_TAB.1	X		

8.4.2 Konsistenz der Mechanismenstärke-Postulate

233 Der EVG unterstützt anfordernde Systeme bei der Erzeugung qualifizierter elektronischer (Batch-)Signaturen (Zuführen zu signierender Dokumente zu einer sicheren Signaturerstellungseinheit), führt die mathematische Prüfung qualifizierter Signaturen (Verifizieren) sowie die Statusprüfung qualifizierter Zertifikate (Validieren) durch.

234 Die geforderte Stärke der Sicherheitsmechanismen von SOF-hoch findet sich in den Angaben zu den Maßnahmen zur Vertrauenswürdigkeit wieder (vgl. Tabelle 5 und Tabelle 13).

8.4.3 Analyse des Zusammenwirkens der Sicherheitsfunktionen

235 Die Sicherheitsfunktion SF3 wirkt mit SF2 zusammen, d. h. wenn eine Validierung durchgeführt wird, werden qualifizierte elektronische Signaturen von Zertifikaten, Sperrlisten und OCSP-Antworten verifiziert (vgl. Tabelle 12, wobei ein „X“ ein Zusammenwirken signalisiert; Tabelle 12 ist nicht symmetrisch).

Tabelle 12: Zusammenwirken der Sicherheitsfunktionen

	SF1	SF2	SF3
SF1			
SF2			X
SF3			

8.4.4 Erklärung zu den Maßnahmen der Vertrauenswürdigkeit

236 Die Maßnahmen zur Erfüllung der Vertrauenswürdigkeitsstufe EAL3+ werden wie folgt erfüllt (vgl. Tabelle 13):

Tabelle 13: Erklärung der Maßnahmen zur Erfüllung von EAL3+

Anforderungen gemäß EAL3+	Maßnahmen der Entwickler
Konfigurations-management : ▪ 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.

Anforderungen gemäß EAL3+	Maßnahmen der Entwickler
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.
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.
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 Glossar

Anforderndes System	Ein anforderndes System ist ein System in der IT-Umgebung, das eine Fachaufgabe wahrnimmt und die Vorgaben von Signaturgesetz und -verordnung an eine Signaturanwendungskomponente erfüllt. Ein anforderndes System kann folgende Anforderungen an den EVG stellen: Unterstützung bei der Erzeugung qualifizierter elektronischer (Batch-) Signaturen, mathematische Prüfung qualifizierter elektronischer Signaturen (Verifikation) und Statusprüfung qualifizierter Zertifikate (Validierung). Einem anfordernden System wird der voreingestellte Zweck („z. B. Signaturen zu Zahlungsanweisungen bei Großanwendern“ [SigV_Begr]) zugeordnet (vgl. Rollendefinition).
Batchsignatur	Eine Batchsignatur ist eine serverbasiert erzeugte SigG-konforme qualifizierte elektronische Signatur gemäß [BNetzA_FAQ18]. Eine Batchsignatur wird in [BNetzA_FAQ18] wie folgt definiert: „eine große Anzahl praktisch gleicher Vorgänge – z. B. Rechnungen, die sich ‚nur’ im Betrag und der Zustelladresse unterscheiden – werden in einer besonders gesicherten Umgebung automatisiert abgearbeitet“.
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])
Rollendefinition	Über die Rollendefinition wird u. a. der Zugriff eines Prozesses einer Fachaufgabe (in einem anfordernden System) auf eine Signaturkarte kontrolliert: Jeder Signaturkarte wird eindeutig eine Rolle zugeordnet. Aus Performancegründen können dabei verschiedene Signaturkarten ein und derselben Rolle zugeordnet sein. Eine solche Rol-

	le stellt also einen Platzhalter für Signaturkarten dar. Signaturschlüssel-Inhaber können mehrere Signaturkarten besitzen. Jeder Rolle wird eindeutig ein anforderndes System inkl. Zweck (Fachaufgabe) zugeordnet – und zwar über das (System-)Zertifikat –, welches damit eine Signaturkarte dieser Rolle nutzen kann. Auf diese Weise wird gewährleistet, dass je Signaturkarte genau ein anforderndes System – also ein voreingestellter Zweck – zugreifen darf. Bsp.: Einem anfordernden System S_1 ist das (System-) Zertifikat Z_1 (für die Erzeugung von Batchsignaturen für Monatsrechnungen) und einem anfordernden System S_2 das (System-) Zertifikat Z_2 (für die Erzeugung von Batchsignaturen für Mahnungen) zugeordnet. Drei Signaturkarten sind den folgenden Rollen zugeordnet: ▪ Signaturkarten S_1 und S_2 für die Rolle R_1 zur Erstellung von Monatsrechnungen (aus Performancegründen werden zwei Karten eingesetzt); Rolle R_1 ist (System-) Zertifikat Z_1 zugeordnet; ▪ Signaturkarte S_3 für die Rolle R_2 zur Erstellung von Mahnungen; Rolle R_2 ist (System-) Zertifikat Z_2 zugeordnet. Ein anforderndes System darf eine Signaturkarte zur Erzeugung einer Batchsignatur nur dann nutzen, wenn dem benutzten (System-)Zertifikat des anfordernden Systems die Rolle zugeordnet ist, die auch der entsprechenden Signaturkarte zugeordnet ist. Eine Software kann mehrere anfordernde Systeme beinhalten.
SAK	Signaturanwendungskomponente
SFP	funktionale Sicherheitspolitik
Sicherheitsanker	Trust Anchor (siehe unten)
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]
SVVE	Signieren von Verifikations- und Validierungs-Ergebnissen[37]
SystemId	Identifier für anforderndes System
(System-)Zertifikat	Ein (System-)Zertifikat ist ein X.509-Zertifikat, das für die sichere Kommunikation zwischen anforderndem System und EVG sowie innerhalb des EVG genutzt wird.
Trust Anchor	Ein Trust Anchor (Sicherheitsanker) ist ein vertrauenswürdiges Zertifikat zur Prüfung der Authentizität und Integrität einer Kommunikation, also insbesondere ein öffentlicher Schlüssel, dem „vertraut“ wird und dessen Korrektheit nicht weiter geprüft zu werden braucht oder kann (etwa bei einem Selbstzertifikat der Wurzelzertifizierungsinstanz). In diesem Kontext gibt es zwei Arten von Trust Anchor: ▪ SigG-konforme qualifizierte Zertifikate (etwa im OCSP/CRL-Relay); ▪ (System-)Zertifikate zur Absicherung der Kommunikation (Beispielsweise werden Anforderungen zur Erzeugung einer Batchsignatur vom anfordernden System mit einer elektronischen Signatur versehen. Der für die Verifikation der Anfrage benötigte öffentliche Schlüssel des anfordernden Systems liegt in Form eines (System-) Zertifikats im EVG – im Sinne eines Trust Anchors – vor. Das (System-) Zertifikat wird dabei nicht mit der Signier-Anforderung übertragen.).
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.

[37] Diese Abkürzung wird zur Konkretisierung von FCS_COP.1 genutzt.

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]
VSA	Verifikation der Signatur-Anforderung[37]

10 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_Algo2008]	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)“, 17. Dezember 2007.
[BNetzA_Algo2009]	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)“, 17. November 2008.
[BNetzA_FAQ18]	Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (Bundesnetzagentur), „FAQ, Frage 18“, www.bundesnetzagentur.de.
[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 Ba-

siskomponente ‚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.

[HARDSOFT] bremen online services GmbH & Co. KG, „Hard- und Softwareanforderungen; Governikus – Teil der Virtuellen Poststelle des Bundes", Version 3.3.0.0, 28.07.2008.

[ISIS-MTT] Common ISIS-MTT Specifications for Interoperable PKI Applications from T7 & TeleTrusT: "Corrigenda to Specification 1.1 as of 16 March 2004", Version 1.2, 18. Januar 2008.

[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.

[Karten_Clients] bremen online services GmbH & Co. KG, „Unterstützte elektronische Signaturkarten", Karten-Leser-Ansteuerung MCARD) Version 1.11.0, 08.03.2010.

[Karten_NetSigner] bremen online services GmbH & Co. KG, „Unterstützte Signaturkarten und Chipkartenlesegeräte Governikus NetSigner", Karten-Leser-Ansteuerung MCARD) Version 1.11.0, 08.03.2010.

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

[Leser_Clients] bremen online services GmbH & Co. KG, „Unterstützte Chipkartenlesegeräte“, Karten-Leser-Ansteuerung MCARD) Version 1.11.0, 08.03.2010.

[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.

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

[RIPEMD-160] ISO/IEC 10118-3, „Information technology – Security techniques – Hash functions – Part 3: Dedicated hash functions, 2nd ed.”, 2004.

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

[SigG] Signaturgesetz vom 16. Mai 2001 (BGBl. 1 S. 876), zuletzt geändert durch Artikel 4 des Gesetzes vom 26. Februar 2007 (BGBl. I S. 179, 185).

[SigV] Verordnung zur elektronischen Signatur (Signaturverordnung – SigV), 16. November 2001 (BGBl. 1 S. 3074), zuletzt geändert durch Artikel 9 Abs. 18 des Gesetzes vom 23. November 2007 (BGBl. I S. 2631, 2671).

[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.[38]

[38] Das generische Sicherheitskonzept für die Kern- und Webkomponenten von Governikus - Teil der Virtuellen Poststelle des Bundes, ist u.a. auf der E-Government-Seite des Bundesamtes für Sicherheit in der Informationstechnik (BSI) unter http://www.bsi.bund.de/fachthem/vps/publikationen.htm verfügbar.

11 Anhang: Technische Einsatzumgebung

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

11.1 Hard- und Software

238 Folgende Systemumgebungen werden unterstützt:

- Hardware:
  - x86-Prozessor mit entsprechender Ausstattung;
  - Sun UltraSPARC mit mindestens 650 MHz-Prozessor mit entsprechender Ausstattung.
- Betriebssysteme:
  - Linux (SuSE Linux Enterprise Server 10) ;
  - Windows 2003 Server;
  - Solaris 10;
- Java: SUN 1.5
- Application Server:
  - JBoss 4.x ;
  - JBoss Enterprise Application Platform 4.2 ;
- Datenbanken:
  - MySQL 5;
  - Oracle 10gR2;

239 Detail-Informationen zu den Hard- und Softwareanforderungen werden im Dokument [HARDSOFT] mit jedem Release von Governikus veröffentlicht.

11.2 Sichere Signaturerstellungseinheiten und Chipkartenleser

240 Die vom EVG unterstützten SigG-konformen sicheren Signaturerstellungseinheiten werden in den Dokumenten [Karten_Clients] und [Karten_NetSigner] beschrieben.

241 Die vom EVG unterstützten SigG-konformen Chipkartenleser werden in den Dokumenten [Leser_Clients] und [Karten_NetSigner] beschrieben.

11.3 Zertifikate und private Schlüssel

242 Folgende X.509v3-Zertifikate werden unterstützt:

- SigG-konforme qualifizierte Zertifikate;
- (System-)Zertifikate zur Gewährleistung der Systemsicherheit.

243 Darüber hinaus werden private Schlüssel zur Gewährleistung der Systemsicherheit unterstützt.

11.4 Anfordernde Systeme

244 Anfordernde Systeme, die von außen über eine Schnittstelle auf den EVG zugreifen – beispielsweise ein Verifikationsserver, OSCI-Manager oder OSCI-Backend-Enabler in der IT-Umgebung (vgl. Abbildung 2) – müssen die Anforderungen von Signaturgesetz und -verordnung an eine Signaturanwendungskomponente erfüllen (vgl. Abschnitt 2.4.6).

11.5 Verzeichnisdienste

245 Es werden alle akkreditierten Verzeichnisdienste unterstützt (Stand 19.08.2008).