# Governikus – Teil der Virtuellen Poststelle des Bundes, Version 3.3 (OSCI), Sicherheitsvorgaben (ST)

**bremen online services GmbH & Co. KG**

**datenschutz nord GmbH**

**1.3**

**25.09.2009**

Zertifizierungs-ID: BSI-DSZ-CC-0563

Bestätigungs-ID: BSI.02112.TE.xx.200x

# Historie

| Version | Datum | geänderte Kapitel | Grund der Änderung | Geändert durch |
|---|---|---|---|---|
| 0.1 | 02.02.2006 | | Erstellung | Matthias Intemann<br>Sönke Maseberg |
| 0.2 | 14.03.2006 | | Einarbeitung der Kommentare von TSI, secunet und BSI; Kryptofunktionalität OSCI-Manager präzisiert | Matthias Intemann<br>Sönke Maseberg |
| 0.3 | 17.03.2006 | Fußnote 17 | kl. editorische Änderungen | Matthias Intemann<br>Sönke Maseberg |
| 0.4 | 23.05.2006 | | Integration der Kommentare von BSI und TSI vom 13.4. bzw. 28.4.2006 | Matthias Intemann<br>Sönke Maseberg |
| 1.0 | 19.11.2007 | | Verweise auf TIFF entfernt, kl. editorische Änderungen | Matthias Intemann<br>Ingo Schumann |
| 1.1 | 11.03.2008 | | Verweise auf TIFF eingefügt, kl. editorische Änderungen | Ingo Schumann |
| 1.2 | 15.08.2008 | Alle | Überarbeitung für Release Governikus 3.3.0.0 | Ingo Schumann |
| 1.21 | 19.09.2008 | FCS_COP.1.1/Hash<br>FCS_COP.1 (OSCI)<br>FCS_COP.1 (Tool) | Überarbeitung aufgrund Review-Protokoll ZK_0563_ASE_V1.0.odt: Hinweis zu SHA-1 aufgenommen, Erklärung 25: Funktionsweise Hashwertvergleich hinzugefügt. | Ingo Schumann |
| 1.22 | 24.09.2008 | 12.1 | Hinweise aus BSI_0563_ase-v11 4.12 für Schreibweise JAVA-Version umgesetzt | Ingo Schumann |
| 1.23 | 02.02.2009 | Alle | Aufnahme aller Anforderungen aus Reports der Prüfstelle; kl. editorische Änderungen | Ingo Schumann |
| 1.24 | 19.05.2009 | 5.1.2, 8.3.2 und 11 | Aufnahme aller Anforderungen aus Review des BSI V 2.2 | Ingo Schumann |
| 1.25 | 20.05.2009 | 1.1, 8.3.4 und 11 | Aktualisierung der Softwareversionsnummer, der CC-Referenzen in Absatz 187 und der Referenzen auf die Dokumente der Kartenansteuerung. | Ingo Schumann |
| 1.26 | 03.07.2009 | 11 | Referenzen zu den Dokumenten der Kartenansteuerung auf MCard 1.10.0 aktualisiert | Ingo Schumann |

| | | | | |
|---|---|---|---|---|
| 1.3 | 25.09.2009 | 11 | Referenzen zu den Dokumenten der Kartenansteuerung auf MCard 1.10.1 aktualisiert | Ingo Schumann |

## Dokumenten-Überwachungsverfahren

| | |
|---|---|
| Status: final | Prozess-/Dokumentbesitzer:<br>Ansgar Bastian (bremen online services GmbH & Co. KG)<br>Ingo Schumann (bremen online services GmbH & Co. KG) |

# Inhaltsverzeichnis

## Abbildungsverzeichnis



## Tabellenverzeichnis

# 1 ST-Einführung

## 1.1 ST-Identifikation

| | | |
|---|---|---|
| 1 | ST-Name: | Governikus – Teil der virtuellen Poststelle des Bundes, Version 3.3 (OSCI), Sicherheitsvorgaben (ST) |
| 2 | ST-Version: | 1.3 |
| 3 | Datum: | 25.09.2009 |
| 4 | Autoren: | bremen online services GmbH & Co. KG<br>datenschutz nord GmbH |
| 5 | EVG-Name: | Governikus, Version 3.3 (OSCI)<br>– abkürzend mit „OSCI-Komponente“ bezeichnet |
| 6 | EVG-Version: | 3.3.1.3 |
| 7 | CC-Version: | 2.3[1] |
| 8 | Zertifizierungs-ID: | BSI-DSZ-CC-0563 |
| 9 | Bestätigungs-ID: | BSI.02112.TE.xx.200x |

## 1.2 EVG-Übersicht

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

- 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 teilweise an.

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

11 Abbildung 1 illustriert den Aufbau von Governikus.

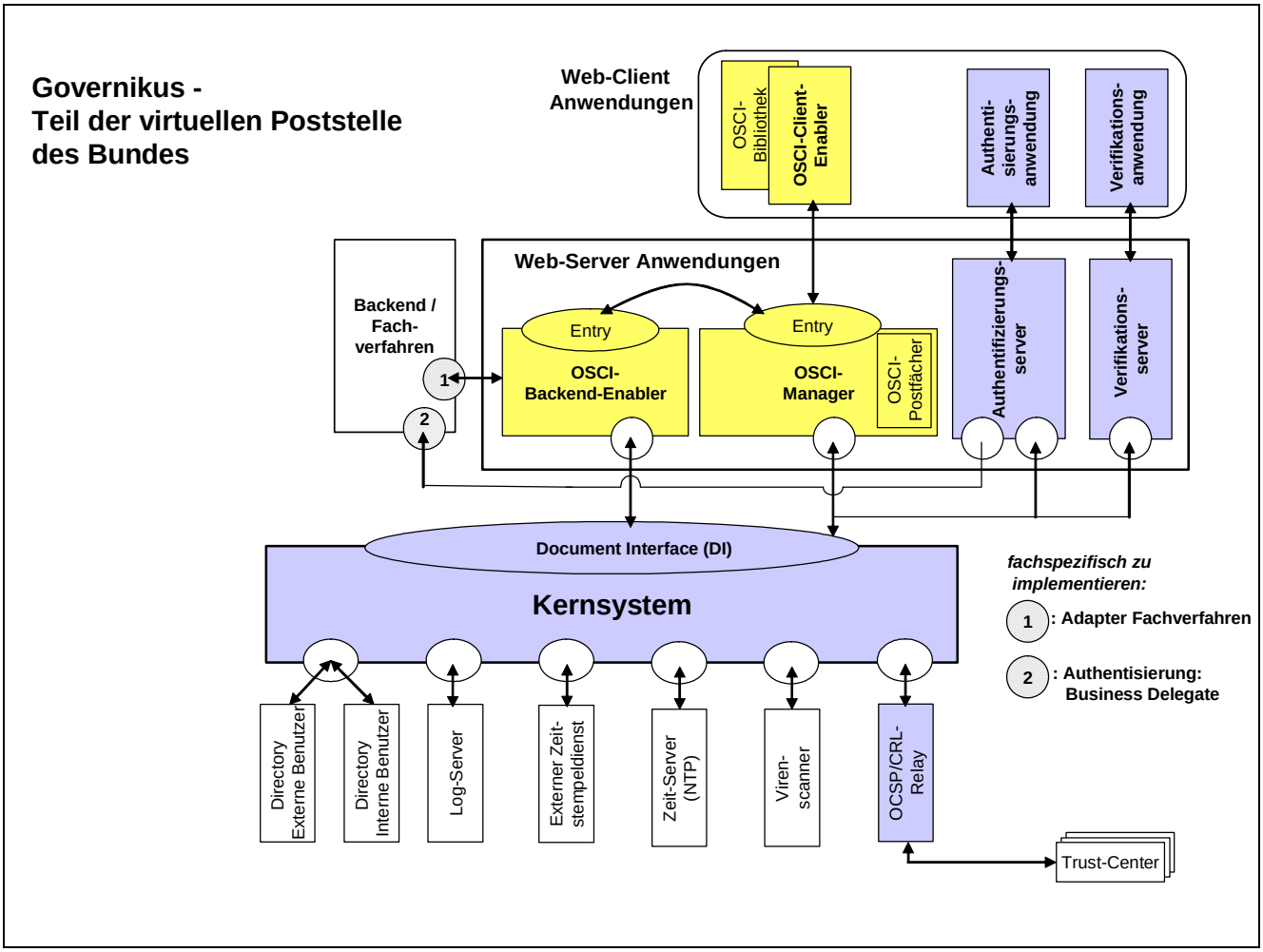


**Abbildung 1: Aufbau von Governikus**

12 Die vorliegenden Sicherheitsvorgaben (Security Target – ST) fokussieren auf den Evaluationsgegenstand[2] „Governikus, Version 3.3 (OSCI)“ – abkürzend als OSCI-Komponente bezeichnet.

[2] 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. Die drei EVGs sind:

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

13 Der Evaluationsgegenstand stellt folgende Funktionalitäten zur Verfügung:

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

14 Der Evaluationsgegenstand stellt als Teil einer Signaturanwendungskomponente nach SigG/SigV eine Funktionsbibliothek[3] – 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.

15 Dementsprechend wird im Folgenden ausschließlich die für die Erfüllung des Signaturgesetzes relevante Funktionalität von Governikus – nämlich Funktionalitäten zur Signaturbildung und -prüfung – betrachtet.

16 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

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

- Teil 2 erweitert [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).

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

19 Hinsichtlich Teil 3 der CC soll die OSCI-Komponente 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

[3] 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 http://www.bundesnetzagentur.de – in Abgrenzung zu einer „vollständigen Signaturanwendungskomponente“ – verwendet und in Funktionsbibliotheken und Chipkartenleser unterteilt. Die Funktionsbibliothek wird von Client- und Serversystemen genutzt.

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[4] 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[5] Prüfung der Handbücher;
    - AVA_SOF.1 Stärke der EVG-Sicherheitsfunktionen;
    - AVA_VLA.1[6] Schwachstellenanalyse des Entwicklers.

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

[5] 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 Vertrauenswürdigkeitskomponenten 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

20 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.

21 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).

22 Diese Sicherheitsvorgaben fokussieren auf den EVG „Governikus, Version 3.3 (OSCI)“ – abkürzend als OSCI-Komponente bezeichnet.

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

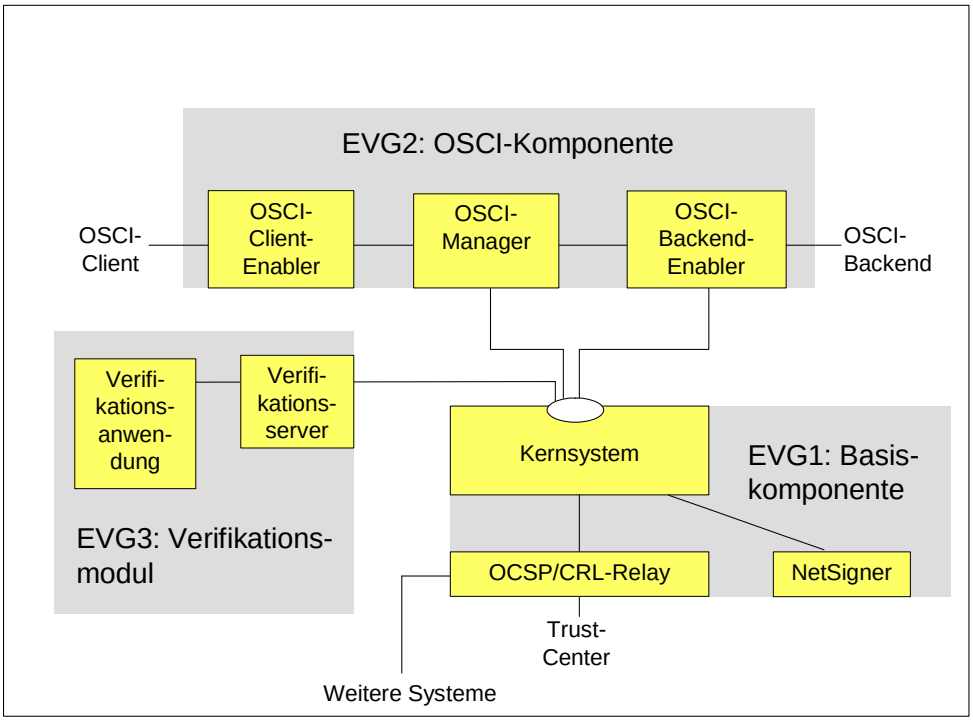


**Abbildung 2: EVG-Übersicht**

## 2.2 Online Services Computer Interface (OSCI)

23 Ein wichtiger Standard im E-Government ist das Online Services Computer Interface (OSCI) [OSCI]. Das im OSCI-Protokoll realisierte Kommunikationsmodell weist eine Architektur über zwei Ebenen auf:

- Absender- und Empfänger-Seite

  Auf Absender-Seite erzeugt ein Nutzer oder ein Fachverfahren mit Hilfe einer Client-Anwendung eine OSCI-konforme Nachricht. Die Client-Anwendung übernimmt unter anderem die Verschlüsselung von Dokumenten, die Unterstützung des Signaturschlüssel-Inhabers beim Signieren von Daten, die Visualisierung von Inhaltsdaten sowie die Verwaltung von Zertifikaten und Signaturen.

  Auf Empfänger-Seite verhält sich die Client-Anwendung spiegelbildlich: Die Client-Anwendung übernimmt die Entschlüsselung der Nachrichten, das Prüfen von Signaturen und möglicherweise die automatische Weiterleitung der eingehenden Nachrichten in ein Backend bzw. Fachverfahren, also der elektronischen Datenverarbeitung in der Behörde.

  Absender- und Empfänger-Seite wird durch einen OSCI-Client bzw. OSCI-Backend realisiert.

- OSCI-Intermediär

Die Kommunikation zwischen Absender und Empfänger wird über einen Intermediär vermittelt, der wichtige Dienste wie die Zertifikatsprüfung, eine beweiskräftige Protokollierung des Nachrichtenweges oder die Zustellung der Nachrichten nach bestimmten Regeln zentral erbringt und damit die an der Kommunikation Beteiligten entlastet.

24 Aufgrund der strikten Trennung von Nutzungs- und Inhaltsdaten (Prinzip des doppelten Umschlags nach OSCI) können beliebig viele Kommunikationsprozesse mit unterschiedlichen Beteiligten über den Intermediär abgewickelt werden, ohne den datenschutzrechtlichen Grundsatz der Datentrennung zu verletzen (Mehrmandantenfähigkeit). Der Intermediär bzw. die hinter ihm stehenden Systemadministratoren sind zu keinem Zeitpunkt in der Lage, auf übermittelte Inhaltsdaten im Klartext zuzugreifen.

25 Weitere Informationen sind unter [OSCI] zu finden.

26 Für die OSCI-Kommunikation stellt der EVG wichtige Funktionalitäten zur Verfügung:

- OSCI-Client-Enabler für einen OSCI-Client;
- OSCI-Manager für den OSCI-Intermediär[7];
- OSCI-Backend-Enabler für ein OSCI-Backend.

27 Bei der OSCI-Kommunikation wird aufgrund des doppelten Umschlags zwischen Inhalts- und Nutzungsdaten unterschieden:

- Inhaltsdaten können vom Absender mit qualifizierten elektronischen Signaturen versehen und mit dem öffentlichen Schlüssel des Empfängers verschlüsselt (innerer Umschlag) werden.
- Nutzungsdaten umfassen den inneren Umschlag sowie weitere Kommunikationsdaten – wie etwa das Zertifikat des Absenders – und können mit dem öffentlichen Schlüssel des Intermediärs verschlüsselt (äußerer Umschlag) werden, so dass der Intermediär den o. g. Mehrwert für den Empfänger erbringen kann.

Das OSCI-Transport-Protokoll erlaubt eine individuelle Konfiguration der Nutzung von Signaturen und Verschlüsselungen.

28 OSCI bedient sich für die Darstellung digitaler Signaturen des XML-Signature-Standards[8]. Darüber hinaus wurde für die flexible und performante Verarbeitung von Attachments die Realisierung als SOAP-Attachment gewählt. Das bedeutet im Wesentlichen, dass zum Anbringen von Signaturen alle zu signierenden Bereiche (bestehend aus SOAP-Attachments oder aus XML-Teil-Strukturen) über eine für die Kommunikation eindeutige ID sowie dem entsprechenden Hashwert referenziert werden. Über diese Referenzen wird ein Hashwert gebildet, der signiert wird (vgl. [OSCI-Transport, Kap. 4.1] sowie [OSCI-Transport_Korr, Kap. 2.1]).

[7] Zur Realisierung des OSCI-Intermediärs ist neben dem OSCI-Manager zusätzlich eine SigG-konformen Basiskomponente von Governikus notwendig (vgl. [bos_Basis_ST]).

[8] vgl. http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/

29 Zur Darstellung von OSCI-Nachrichten: Der OSCI-Client-Enabler bietet eine sichere Anzeige von folgenden zu signierenden und signierten Daten:[9]

- plain-text (UTF-8-codiert): In dieser Darstellung werden die in der XML-Struktur enthaltenen OSCI-Inhaltsdaten vom EVG interpretiert und angezeigt. In dieser Darstellung können in Attachments enthaltene tiff-Dateien – also Bilddaten – nicht angezeigt werden.
- tiff-Dateien: In dieser Darstellung werden Bilddaten vom EVG sicher angezeigt.

Unterstützend können die entsprechenden XML-Daten in Roh-Form, d. h. uninterpretiert, angezeigt werden.

Neben der Darstellung der Inhaltsdaten in plain-text (UTF-8-codiert) oder tiff werden weitere Informationen vom OSCI-Client-Enabler dem Benutzer angezeigt – beispielsweise das zugehörige Zertifikat sowie Verifikations- und Validierungsergebnisse.

## 2.3 EVG-Umfang

30 Der Evaluationsgegenstand „Governikus, Version 3.3 (OSCI)“ stellt zur Realisierung des OSCI-Transport-Protokolls (vgl. [OSCI]) für

- OSCI-Client,
- OSCI-Intermediär und
- OSCI-Backend

31 folgende Funktionalitäten für die OSCI-Kommunikation bereit:

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

32 Der EVG ist eine Funktionsbibliothek[3], die auf geeigneter Hardware mit geeigneten Betriebsmitteln – insbesondere mit SigG-konformem Chipkartenleser und sicheren Signaturerstellungseinheiten (in diesem Fall Signaturkarten[10]) – betrieben wird.

33 Der EVG nutzt Funktionalitäten einer SigG-konformen Basiskomponente von Governikus mit Kernsystem, OCSP/CRL-Relay und NetSigner, die ebenfalls innerhalb der kompositiven Evaluierung von Governikus evaluiert, zertifiziert

[9] Nicht im Umfang der Evaluierung enthalten sind weitere unterstützte Datenformate.

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

und bestätigt wird. Funktionalitäten und Eigenschaften der Basiskomponente sind in [bos_Basis_ST] näher beschrieben.[11]

34 Der EVG nutzt darüber hinaus Funktionalitäten von OSCI-Client und -Backend zur Identifikation und Authentisierung zum Management von Sicherheitsattributen, d. h. den kryptographischen Schlüsseln und (System-)Zertifikaten.

35 Der EVG besteht aus den folgenden Teilsystemen:

- OSCI-Client-Enabler;
- OSCI-Manager;
- OSCI-Backend-Enabler.

36 Der OSCI-Client-Enabler wird auf einem Rechner an einem Arbeitsplatz – beispielsweise in einem Büro – (in einem „geschützten Einsatzbereich (Regelfall/Standardlösung)“ [BNetzA2005]) mit einem OSCI-Client betrieben, der von einem Benutzer beispielsweise über eine GUI (Graphical User Interface) benutzt wird. Der OSCI-Client-Enabler verfügt über die Einbindung von Chipkartenlesern.

37 OSCI-Manager und -Backend-Enabler werden auf Servern in einem Rechenzentrum (in einem „geschützten Einsatzbereich (Regelfall/Standardlösung)“ [BNetzA2005]) betrieben, mit jeweiligen Web-Oberflächen (GUIs) von Administratoren konfiguriert und arbeiten im Produktivbetrieb automatisiert und ohne menschliche Aktivitäten. Der OSCI-Backend-Enabler wird von einem OSCI-Backend genutzt.

38 Die Teilsysteme können räumlich voneinander getrennt betrieben werden.

39 Der Evaluationsgegenstand stellt folgende Funktionen zur Verfügung:

- Der EVG stellt Funktionalitäten zur Unterstützung eines Signaturschlüssel-Inhabers bei der Erzeugung einer qualifizierten elektronischen Signatur (Individualsignaturen im Sinne der Bundesnetzagentur (vgl. [BNetzA_FAQ18])) bereit, die auf Anforderung des Benutzers lokal erzeugt werden sollen.

  Der Signaturschlüssel-Inhaber hat an seinem Arbeitsplatz (mit Chipkartenleser) zur Signaturerzeugung unmittelbar Zugriff auf seine Signaturkarte. Zum Signieren steckt der Benutzer seine Signaturkarte in den Chipkartenleser, bestätigt die Aktion – woraufhin die zu signierenden Daten der sicheren Signaturerstellungseinheit zugeführt werden, in der sein privater Signaturschlüssel vorgehalten wird – und autorisiert das Signieren durch Eingabe seiner PIN am PIN-Pad des Kartenlesegeräts. Anschließend wird die Signatur bzw. eine Fehlermeldung an den EVG zurückgeliefert. Der Benutzer wird durch entsprechende Anzeigen des EVG unterstützt.

- Der EVG prüft auf Anforderung des Benutzers die mathematische Korrektheit einer qualifizierten elektronischen Signatur. Der EVG führt eine

[11] Darüber hinaus wird die Basiskomponente für die Gewährleistung der Systemsicherheit genutzt (vgl. Abschnitt 2.4).

Signaturprüfung durch, d. h. prüft die mathematische Korrektheit der Signatur mittels zugehörigen Prüfschlüssels (öffentlichem Schlüssel aus qualifiziertem Zertifikat) und geeigneten kryptographischen Verfahren und visualisiert das Verifikationsergebnis (gültige oder ungültige Signatur oder Fehlermeldung).

- Der EVG führt auf Anforderung des Benutzers die Statusprüfung eines qualifizierten Zertifikats durch. Gemäß OSCI-Protokoll führt der EVG die Statusprüfung als OSCI-Intermediär durch, prüft anschließend – aufgrund der Realisierung des EVG durch u. U. räumlich getrennte Teilsysteme – das Ergebnis der Zertifikats-Statusprüfung und visualisiert das Validierungsergebnis.

  Das Ergebnis der Statusprüfung zum Zeitpunkt der Prüfung beim OSCI-Intermediär – die zeitlich vorher erfolgte – bleibt gültig: Ein zum Prüfzeitpunkt gültiges Zertifikat kann nachträglich nicht ungültig geworden sein.[12]

- Der EVG stellt als OSCI-Intermediär die Gültigkeit eines qualifizierten Zertifikats unter Zuhilfenahme einer Basiskomponente mit Kernsystem und OCSP/CRL-Relay fest.

  Die Basiskomponente stellt dabei fest, ob das qualifizierte Zertifikat zum Zeitpunkt des Eingangs beim OSCI-Intermediär vorhanden und nicht gesperrt war und der Gültigkeitszeitraum des qualifizierten Zertifikats zu diesem Zeitpunkt bereits begonnen und noch nicht abgelaufen war, und übergibt das Ergebnis der Validierung in Form des Verzeichnisdienst-Ergebnisses sowie einer Interpretation (gültig und nicht gesperrt, unbekannt oder gesperrt) an den EVG.

- Der EVG erhält von einem OSCI-Backend die Anforderung[13], die mathematische Korrektheit einer qualifizierten elektronischen Signatur zu prüfen. Der EVG führt eine Signaturprüfung durch, d. h. prüft die mathematische Korrektheit der Signatur mittels zugehörigem Prüfschlüssel (öffentlichem Schlüssel aus qualifiziertem Zertifikat) und geeigneten kryptographischen Verfahren und liefert das Ergebnis (gültige oder ungültige Signatur oder Fehlermeldung) an das OSCI-Backend zurück.

- Der EVG erhält von einem OSCI-Backend die Anforderung[13], eine Statusprüfung eines qualifizierten Zertifikats durchzuführen. Während die eigentliche Statusprüfung gemäß OSCI-Protokoll vom OSCI-Intermediär durchgeführt wird, führt der EVG eine Plausibilitätsprüfung durch, in der der EVG prüft, ob das im OSCI-Laufzettel enthaltene Ergebnis der Zertifikats-Statusprüfung zum Zertifikat der OSCI-Nachricht passt, und gibt das Validierungsergebnis an das OSCI-Backend zurück.

40 Die Kommunikation zwischen OSCI-Client und OSCI-Client-Enabler sowie zwischen OSCI-Backend und OSCI-Backend-Enabler erfolgt derart abgesi-

[12] Für eine aktuelle Validierung sei auf EVG3 „Verifikationsmodul“ verwiesen.

[13] Der EVG wird unter der Annahme betrieben, dass das OSCI-Backend, welches auf diesen EVG zugreift, eine Signaturanwendungskomponente gemäß SigG/SigV darstellt.

chert, dass die tatsächliche Anforderung bearbeitet und zutreffende Ergebnisse zurückliefert werden.[14]

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

42 Zum EVG-Umfang gehört darüber hinaus ein Prüftool zum Schutz vor unbefugter Veränderung (vgl. Abschnitt 2.7).

## 2.4 Technische Realisierung

43 Die OSCI-Komponente besteht aus den Teilsystemen

- OSCI-Client-Enabler,
- OSCI-Manager und
- OSCI-Backend-Enabler

inklusive einer Administrationsanwendung als Graphical User Interface (GUI) zur Administration des OSCI-Managers.

Abbildung 3 illustriert die Teilsysteme der OSCI-Komponente.

[14] Die Kommunikation zwischen OSCI-Client-Enabler und OSCI-Intermediär sowie zwischen OSCI-Backend-Enabler und OSCI-Intermediär ist über das OSCI-Transport-Protokoll abgesichert. Das OSCI-Transport-Protokoll ist nicht Bestandteil der Evaluierung.

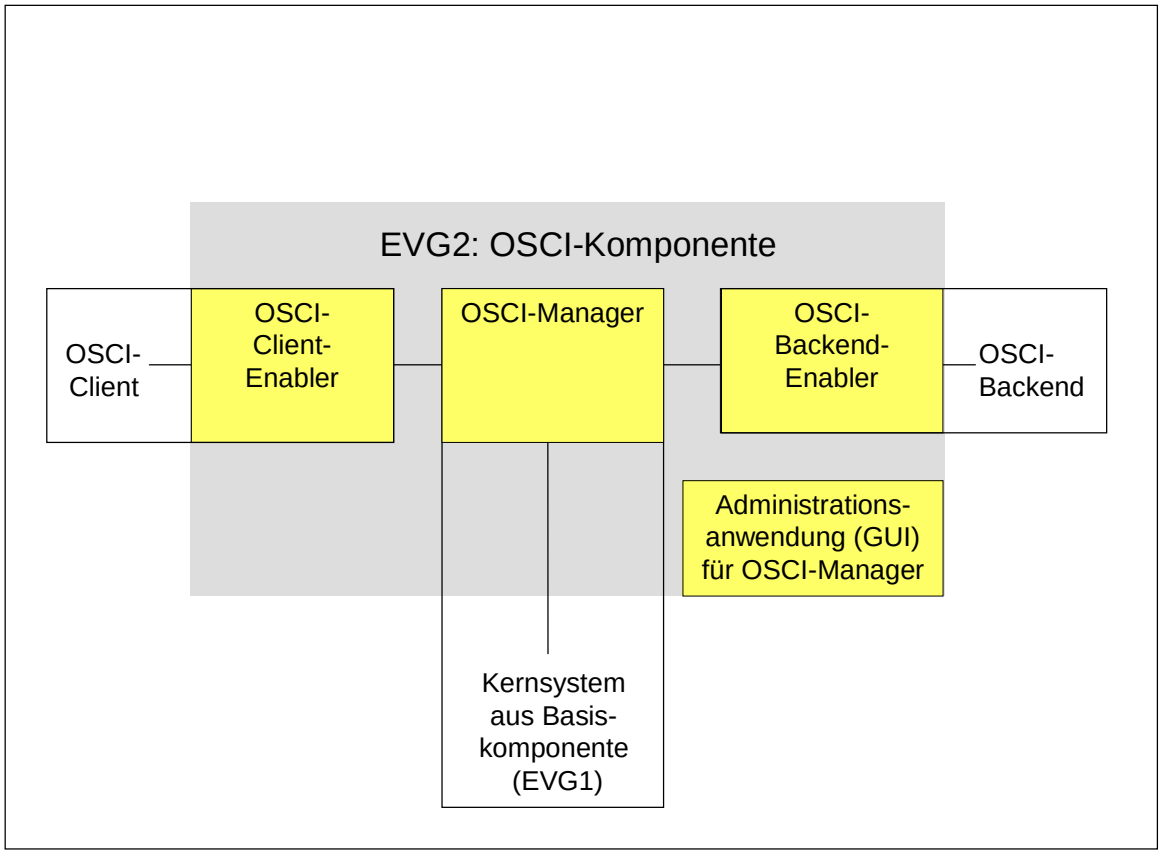


Abbildung 3: Teilsysteme des EVG

44 OSCI-Client-Enabler, -Manager und -Backend-Enabler können voneinander getrennt betrieben werden, d. h. nicht innerhalb eines LANs (Local Area Networks), sondern über ein Weitverkehrsnetz (Wide Area Network – WAN) verbunden.

45 Die wesentlichen Aufgaben der Teilsysteme:

- OSCI-Client-Enabler:[15]
  - Signieren: Der OSCI-Client-Enabler wendet auf die zu signierenden Daten eine Hashfunktion gemäß OSCI-Transport (vgl. Abschnitt 2.2) an und führt den erzeugten Hashwert einer angeschlossenen sicheren Signaturerstellungseinheit zu, die eine qualifizierte elektronische Signatur erzeugt. Am Arbeitsplatz-PC ist ein Chipkartenleser installiert. Vor jeder Signaturerzeugung erfolgt die Eingabe einer PIN. Signierte Daten werden im inneren Umschlag des OSCI-Protokolls transportiert. Daten, die dem OSCI-Client-Enabler vom OSCI-Client zum Signieren übergeben werden, sind in einer XML-Struktur codiert. Nachdem eine qualifizier-

[15] Weitere Funktionalitäten, die allerdings nicht Bestandteil der Zertifizierung und Bestätigung sind, sind in Abschnitt 1.2 aufgeführt – beispielsweise die Ver- und Entschlüsselung zur Realisierung des doppelten Umschlags gemäß OSCI.

te elektronische Signatur durch die Signaturkarte erzeugt wurde, wird die Signatur vom OSCI-Client-Enabler verifiziert; dazu wird das zum privaten Schlüssel korrespondierende Zertifikat genutzt, das sich auf der Signaturkarte befindet und das vor dem Erzeugen der Signatur angezeigt wurde.

- o Verifizieren: Der OSCI-Client-Enabler verifiziert qualifizierte elektronische Signaturen aus dem inneren Umschlag des OSCI-Protokolls und zeigt das Verifikationsergebnis sowie die signierten Daten an.
- o Validieren: Der OSCI-Client-Enabler validiert nicht selber, sondern nutzt das Ergebnis der Validierung vom OSCI-Manager, welches im OSCI-Laufzettel – mit einer elektronischen Signatur versehen – enthalten ist. Der OSCI-Client-Enabler verifiziert diese elektronische Signatur mit dem – dem OSCI-Manager zugeordneten – (System-)Zertifikat des OSCI-Managers und prüft, ob das vom OSCI-Manager validierte Zertifikat dasjenige Zertifikat ist, welches der Signatur entspricht (Plausibilitätscheck). Der OSCI-Client-Enabler visualisiert das Validierungsergebnis.

  Das Ergebnis der Statusprüfung zum Zeitpunkt der Prüfung beim OSCI-Intermediär – die zeitlich vorher erfolgte – bleibt gültig: Ein zum Prüfzeitpunkt gültiges Zertifikat kann nachträglich nicht ungültig geworden sein.
- o Sichere Anzeige: Der OSCI-Client-Enabler bietet eine sichere Anzeige von folgenden zu signierenden und signierten Daten:
  - plain-text (UTF-8-codiert);
  - tiff-Daten.

  Darüber hinaus bietet der EVG eine sichere Anzeige von Verifikations- und Validierungsergebnis und eine visuelle Unterstützung des Signier-Prozesses (insbesondere Autorisieren des Signierens).

Der OSCI-Client-Enabler als Funktionsbibliothek nutzt kryptographische Schlüssel und (System-)Zertifikate, die vom OSCI-Client zur Verfügung gestellt werden; eine geeignete Identifikation und Authentisierung zum Management dieser Sicherheitsattribute obliegt dem OSCI-Client.

- OSCI-Manager:[15]

  Der OSCI-Manager führt als OSCI-Intermediär die Statusprüfung eines qualifizierten Zertifikats durch. Dazu greift der OSCI-Manager auf eine Basiskomponente (vgl. [bos_Basis_ST])[16] zu, die die eigentliche Validierung durchführt.

[16] OSCI-Manager und Kernsystem der Basiskomponente (vgl. [bos_Basis_ST]) werden zusammen in einem vertrauenswürdigen Netz betrieben, so dass der OSCI-Manager dem Prüfergebnis des Kernsystems vertraut.

Der OSCI-Manager interpretiert die Antwort der Basiskomponente und generiert ein eigenes Ergebnis ohne die Original-Verzeichnisdienst-Auskünfte der Basiskomponente, welches der OSCI-Manager im OSCI-Laufzettel ablegt.

Der OSCI-Laufzettel wird zur Gewährleistung der Systemsicherheit mit einer elektronischen Signatur versehen: Dazu nutzt der OSCI-Manager unterstützende Sicherheitsmechanismen[17] des Kernsystems der Basiskomponente, indem das Kernsystem für den vom OSCI-Manager erzeugten und übergebenen Hashwert eine elektronische Signatur erzeugt.

Anschließend übergibt der OSCI-Manager im Rahmen des OSCI-Protokolls den OSCI-Laufzettel an den OSCI-Client-Enabler bzw. an den OSCI-Backend-Enabler.

- OSCI-Backend-Enabler:[15]
  - Verifikation: Der OSCI-Backend-Enabler verifiziert qualifizierte elektronische Signaturen aus dem inneren Umschlag des OSCI-Protokolls.[18] Der OSCI-Backend-Enabler übergibt das Verifikationsergebnis dem OSCI-Backend.
  - Validieren: OSCI-Backend-Enabler validiert nicht selber, sondern nutzt das Ergebnis der Validierung vom OSCI-Intermediär, welches im OSCI-Laufzettel – vom OSCI-Manager mit einer elektronischen Signatur versehen – enthalten ist. Der OSCI-Backend-Enabler verifiziert diese elektronische Signatur mit dem – dem OSCI-Manager zugeordneten – (System-) Zertifikat des OSCI-Managers und prüft, ob das vom OSCI-Manager validierte Zertifikat der zu prüfenden Signatur zuordenbar ist (Plausibilitätscheck).[18] Der OSCI-Backend-Enabler übergibt das Validierungsergebnis dem OSCI-Backend.

Der OSCI-Backend-Enabler als Funktionsbibliothek nutzt kryptographische Schlüssel und (System-)Zertifikate, die vom OSCI-Backend zur Verfügung gestellt werden; eine geeignete Identifikation und Authentisierung zum Management dieser Sicherheitsattribute obliegt dem OSCI-Backend.

---

[17] Das zur Gewährleistung der Systemsicherheit – in diesem Fall die Integrität und Authentizität des OSCI-Laufzettels durch eine vom Kernsystem erzeugte elektronische Signatur – notwendige Zertifikats- und Schlüssel-Management samt zugehörigen kryptographischen Verfahren wurde in [bos-Basis_ST] beschrieben. Im Rahmen der Evaluierung von EVG1 „Governikus, Version 3.3 (Basis)“ wurde geprüft und festgestellt, dass sichergestellt ist, dass

- nur autorisierte Personen auf kryptographische Schlüssel zugreifen können,
- sichere kryptographische Verfahren eingesetzt werden (vgl. Fußnote 42) und
- Kernsystem und OSCI-Manager in einem vertrauenswürdigen Netz betrieben werden.

[18] Analog zum OSCI-Client-Enabler, allerdings ohne jegliche Visualisierung.

46 Kommunikationssicherheit:

- OSCI-Client und -Enabler resp. OSCI-Backend und -Enabler kommunizieren über (Java-)Funktionsaufrufe und dadurch integer und vertraulich, da die Daten die Virtual Machine nicht verlassen. OSCI-Client und OSCI-Client-Enabler sowie OSCI-Backend und OSCI-Backend-Enabler werden jeweils zusammen auf einem Rechner betrieben.
- Der Chipkartenleser (in der IT-Umgebung) ist physikalisch über ein Kabel an den Rechner angeschlossen, auf dem der OSCI-Client-Enabler betrieben wird. Zusätzlich wird diese Kommunikation dadurch abgesichert, dass eine soeben erzeugte Signatur vom OSCI-Client-Enabler verifiziert wird.
- OSCI-Manager und Kernsystem der Basiskomponente werden zusammen innerhalb eines vertrauenswürdigen Netzes betrieben.
- Die Kommunikation zwischen OSCI-Client und -Intermediär sowie zwischen OSCI-Backend und -Intermediär ist über die Mechanismen des OSCI-Transport-Protokolls[19] abgesichert. Zusätzlich können OSCI-Backend und -Manager zusammen in einem vertrauenswürdigen Netz betrieben werden.

47 Das Prüftool zum Schutz vor unbefugter Veränderung ist in Abschnitt 2.7 beschrieben.

## 2.5 Signaturgesetz (SigG) und -verordnung (SigV)

### 2.5.1 Rechtliche Grundlagen

48 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 [...]“.

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

50 § 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,

[19] Das OSCI-Transport-Protokoll ist nicht Bestandteil der Evaluierung.

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."

51 § 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."

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

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

- das Erzeugen einer Signatur vorher eindeutig angezeigt wird[20],
- erkennbar ist, auf welche Daten sich die Signatur bezieht[21],
- bei Bedarf der Inhalt der zu signierenden Daten hinreichend zu erkennen ist[22],
- eine Signatur nur durch die berechtigt signierende Person erfolgt[23],

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

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

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

- die Identifikationsdaten nicht preisgegeben und nur auf der jeweiligen „sicheren Signaturerstellungseinheit“ gespeichert werden[24].

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

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

55 Schutz vor unbefugter Veränderung: Sicherheitstechnische Veränderungen an der Signaturanwendungskomponente müssen für den Nutzer erkennbar[25] werden.”

---

[23] „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]

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

[25] „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-Arbeitsstation“, 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]

### 2.5.2 Signaturgesetz-Anforderungen an den EVG

56 Der EVG ist eine Funktionsbibliothek zur Erzeugung und Prüfung qualifizierter elektronischer Signaturen.

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

**Zur Erzeugung von Signaturen**

58 Die Sicherheitsanforderungen, dass eine Signaturanwendungskomponente beim Erzeugen einer Signatur gewährleisten muss, dass

- „das Erzeugen einer Signatur vorher eindeutig angezeigt wird“,
- „erkennbar ist, auf welche Daten sich die Signatur bezieht“ und
- „bei Bedarf der Inhalt der zu signierenden Daten hinreichend zu erkennen ist“ ([BNetzA2005])

werden durch den EVG umgesetzt: Der OSCI-Client-Enabler unterstützt den OSCI-Client bei der Erzeugung von qualifizierten elektronischen Signaturen durch eine geeignete Anzeige der prozeduralen Abläufe. Der OSCI-Client-Enabler wendet auf die zu signierenden Daten eine Hashfunktion gemäß [OSCI-Transport (vgl. Abschnitt 2.2)] sowie [OSCI-Transport_Korr] an und nutzt eine sichere Signaturerstellungseinheit, auf die er über einen angeschlossenen Chipkartenleser zugreift. Darüber hinaus kann der OSCI-Client-Enabler dem Benutzer bei Bedarf die zu signierenden Daten anzeigen.

59 Die Sicherheitsanforderungen, dass eine Signaturanwendungskomponente beim Erzeugen einer Signatur gewährleisten muss, dass

- „eine Signatur nur durch die berechtigt signierende Person erfolgt“ und
- „die Identifikationsdaten nicht preisgegeben und nur auf der jeweiligen „sicheren Signaturerstellungseinheit“ gespeichert werden“ ([BNetzA2005])

obliegen Chipkartenleser und sichere Signaturerstellungseinheiten in der IT-Umgebung, die – per Annahme/Auflage – die SigG/SigV-Anforderungen erfüllen: Vom Chipkartenleser und der sicheren Signaturerstellungseinheit muss gewährleistet werden, dass eine Signatur nur durch die berechtigt signierende Person erfolgt und dass Identifikationsdaten nicht preisgegeben und nur auf der jeweiligen sicheren Signaturerstellungseinheit abgespeichert werden.

**Zur Prüfung einer Signatur**

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

- „erkennbar wird, auf welche Daten sich die Signatur bezieht,“
- „erkennbar wird, ob die Daten unverändert sind,“
- „bei Bedarf der Inhalt der signierten Daten hinreichend zu erkennen ist,“

- „erkennbar wird, welchem Signaturschlüssel-Inhaber die Signatur zuzuordnen ist“,
- „erkennbar wird, welche Inhalte das qualifizierte Zertifikat, auf dem die Signatur beruht“, aufweist, [26]
- „erkennbar wird, ob die nachgeprüften qualifizierten Zertifikate im jeweiligen Zertifikatverzeichnis zum angegebenen Zeitpunkt vorhanden und nicht gesperrt waren” und
- „die Korrektheit der Signatur zuverlässig geprüft und zutreffend angezeigt wird“ ([BNetzA2005])

werden vom EVG umgesetzt: OSCI-Client-Enabler und -Backend-Enabler prüfen die Korrektheit qualifizierter elektronischer Signaturen. Die Anzeige ist nur beim OSCI-Client-Enabler verfügbar, da nur hier Benutzer involviert sind.

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

- hinsichtlich der Validierung bei einer SigG-konformen Basiskomponente in der IT-Umgebung und beim OSCI-Manager,
- hinsichtlich der Plausibilitätsprüfung (Gehört das validierte Zertifikat zur Signatur?) bei OSCI-Client-Enabler und -Backend-Enabler und
- hinsichtlich der Anzeige beim OSCI-Client-Enabler.

**Schutz vor unbefugter Veränderung**

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

[26] Attributzertifikate werden vom EVG nicht unterstützt.

**Tabelle 1: Umsetzung der SigG/SigV-Anforderungen**

| Sicherheitsanforderungen an Signaturanwendungskomponenten [BNetzA2005] | Umsetzung der Anforderungen aus SigG und SigV | |
|---|---|---|
| | in EVG | in der IT-Umgebung |
| „Erzeugung von Signaturen: Die Signaturanwendungskomponente muss beim Erzeugen einer Signatur gewährleisten, dass | zum Erzeugen wendet der OSCI-Client-Enabler auf die zu signierenden Daten eine Hashfunktion gemäß OSCI-Transport an und führt den erzeugten Hashwert der angeschlossenen sicheren Signaturerstellungseinheit zu; eine erzeugte Signatur wird anschließend verifiziert | qualifizierte elektronische Signatur wird durch sichere Signaturerstellungseinheit erstellt |
| ▪ das Erzeugen einer Signatur vorher eindeutig angezeigt wird,[27] | der OSCI-Client-Enabler unterstützt den Benutzer durch entsprechende Anzeigen | - |
| ▪ erkennbar ist, auf welche Daten sich die Signatur bezieht,[28] | wird im OSCI-Client-Enabler angezeigt | - |
| ▪ bei Bedarf der Inhalt der zu signierenden Daten hinreichend zu erkennen ist,[29] | kann im OSCI-Client-Enabler angezeigt werden | - |
| ▪ eine Signatur nur durch die berechtigt signierende Person erfolgt,[30] | - | wird durch sichere Signaturerstellungseinheit gewährleistet |

[27] vgl. „Für die Darstellung zu signierender Daten sind Signaturanwendungskomponenten erforderlich, die die Erzeugung einer qualifizierten elektronischen Signatur vorher eindeutlich anzeigen lassen [...]“ [§ 17 Abs. 2 SigG] sowie „Signaturanwendungskomponenten nach § 17 Abs. 2 des Signaturgesetzes müssen gewährleisten, dass [...] bei der Erzeugung einer qualifizierten elektronischen Signatur [...]die Erzeugung einer Signatur vorher eindeutig angezeigt wird [...].“ [§ 15 Abs. 2 Nr. 1c SigV]

[28] vgl. „Für die Darstellung zu signierender Daten sind Signaturanwendungskomponenten erforderlich, die die Erzeugung einer qualifizierten elektronischen Signatur [...] feststellen lassen, auf welche Daten sich die Signatur bezieht.“ [§ 17 Abs. 2 SigG]

[29] vgl. „Signaturanwendungskomponenten müssen nach Bedarf auch den Inhalt der zu signierenden [...] Daten hinreichend erkennen lassen.“ [§ 17 Abs. 2 SigG]

[30] vgl. „Signaturanwendungskomponenten nach § 17 Abs. 2 des Signaturgesetzes müssen gewährleisten, dass [...] bei der Erzeugung einer qualifizierten elektronischen Signatur [...] eine Signatur nur durch die berechtigt signierende Person erfolgt [...].“ [§ 15 Abs. 2 Nr. 1b SigV]

| Sicherheitsanforderungen an Signaturanwendungskomponenten [BNetzA2005] | Umsetzung der Anforderungen aus SigG und SigV | |
|---|---|---|
| | in EVG | in der IT-Umgebung |
| ▪ die Identifikationsdaten nicht preisgegeben und nur auf der jeweiligen „sicheren Signaturerstellungseinheit“ gespeichert werden.[31] | - | 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 | OSCI-Client-Enabler und OSCI-Backend-Enabler prüfen qualifizierte elektronische Signaturen.<br>Teilfunktionalitäten der Validierung erfolgen beim OSCI-Manager; Plausibilitätsprüfung bei OSCI-Client-Enabler und OSCI-Backend-Enabler; | |
| ▪ erkennbar wird, auf welche Daten sich die Signatur bezieht,[32] | wird vom OSCI-Client-Enabler angezeigt | - |
| ▪ erkennbar wird, ob die Daten unverändert sind,[33] | die Prüfung, ob Daten unverändert sind, erfolgt bei OSCI-Client-Enabler und -Backend-Enabler;<br>die entsprechende Anzeige wird vom OSCI-Client-Enabler geleistet | - |
| ▪ bei Bedarf der Inhalt der signierten Daten hinreichend zu erkennen ist,[34] | kann vom OSCI-Client-Enabler angezeigt werden | - |

[31] vgl. „Signaturanwendungskomponenten nach § 17 Abs. 2 des Signaturgesetzes müssen gewährleisten, dass [...] bei der Erzeugung einer qualifizierten elektronischen Signatur [...] die Identifikationsdaten nicht preisgegeben und diese nur auf der jeweiligen sicheren Signaturerstellungseinheit gespeichert werden [...].“ [§15 Abs. 2 Nr. 1a SigV]

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

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

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

| Sicherheitsanforderungen an Signaturanwendungskomponenten [BNetzA2005] | Umsetzung der Anforderungen aus SigG und SigV | |
|---|---|---|
| | in EVG | in der IT-Umgebung |
| ▪ erkennbar wird, welchem Signaturschlüssel-Inhaber die Signatur zuzuordnen ist,[35] | wird vom OSCI-Client-Enabler angezeigt | - |
| ▪ erkennbar wird, welche Inhalte das qualifizierte Zertifikat, auf dem die Signatur beruht, und zugehörige qualifizierte Attribut-Zertifikate[26] aufweisen,[36] | wird vom OSCI-Client-Enabler angezeigt, allerdings werden keine Attribut-Zertifikate unterstützt | - |
| ▪ erkennbar wird, ob die nachgeprüften qualifizierten Zertifikate im jeweiligen Zertifikatverzeichnis zum angegebenen Zeitpunkt vorhanden und nicht gesperrt waren,[37] | der OSCI-Manager erzeugt OSCI-Laufzettel mit Validierungsergebnis;<br>Plausibilitätsprüfung (Gehört das validierte Zertifikat zur Signatur?) erfolgt bei OSCI-Client-Enabler und -Backend-Enabler;<br>die entsprechende Anzeige des Validierungsergebnisses erfolgt beim OSCI-Client-Enabler, wobei der im OSCI-Laufzettel angegebene Zeitpunkt der Zeitpunkt ist, zu dem die Nachricht beim OSCI-Manager eingegangen ist[38] | die eigentliche Statusprüfung (Validierung) des Zertifikats erfolgt in der Basiskomponente |

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

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

[37] vgl. „Für die Überprüfung signierter Daten sind Signaturanwendungskomponenten erforderlich, die feststellen lassen, [...] zu welchem Ergebnis die Nachprüfung von Zertifikaten nach § 5 Abs. 1 Satz 3 geführt hat. [...]." [§17 Abs. 2 Nr. 5 SigG] sowie „Signaturanwendungskomponenten nach § 17 Abs. 2 des Signaturgesetzes müssen gewährleisten, dass [...] bei der Prüfung einer qualifizierten elektronischen Signatur [...] eindeutig erkennbar wird, ob die nachgeprüften qualifizierten Zertifikate im jeweiligen Zertifikat-

| Sicherheitsanforderungen an Signaturanwendungskomponenten [BNetzA2005] | Umsetzung der Anforderungen aus SigG und SigV | |
|---|---|---|
| | in EVG | in der IT-Umgebung |
| ▪ die Korrektheit der Signatur zuverlässig geprüft und zutreffend angezeigt wird.[39] | führen OSCI-Client-Enabler und -Backend-Enabler durch | - |
| Schutz vor unbefugter Veränderung: Sicherheitstechnische Veränderungen an der Signaturanwendungskomponente müssen für den Nutzer erkennbar werden.” | Prüftool für den OSCI-Client-Enabler zum Schutz vor unbefugter Veränderung wird zur Verfügung gestellt | für die serverseitigen Komponenten OSCI-Manager und -Backend-Enabler muss der sichere Betrieb in der Umgebung gewährleistet werden;<br>für den OSCI-Client-Enabler ist muss der sichere Betrieb am Arbeitsplatz gewährleistet werden; zusätzliche Absicherung zum Integritätsschutz durch Prüftool |

## 2.6 Produktbestandteile und EVG-Abgrenzung

63 Der Lieferumfang des EVG ist in Tabelle 2 aufgeführt:

Verzeichnis zum angegebenen Zeitpunkt vorhanden und nicht gesperrt waren.“ [§ 15 Abs. 2 Nr. 2b SigV]

[38] Das Ergebnis der Statusprüfung zum Zeitpunkt der Prüfung beim OSCI-Intermediär – die zeitlich vorher erfolgte – bleibt gültig: Ein zum Prüfzeitpunkt gültiges Zertifikat kann nachträglich nicht ungültig geworden sein.

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

**Tabelle 2: Lieferumfang EVG**

| Liefergegenstand | | Typ | Medium |
|---|---|---|---|
| Alle Komponenten | Betriebshandbuch | Dokumentation | CD-ROM oder Archiv-Datei |
| OSCI-Client-Enabler | OSCI-Client-Enabler-Software | Software | CD-ROM oder Archiv-Datei |
| | Entwicklerdokumentation | Dokumentation | |
| OSCI-Manager | OSCI-Manager-Software | Software | CD-ROM oder Archiv-Datei |
| OSCI-Backend-Enabler | OSCI-Backend-Enabler-Software | Software | CD-ROM oder Archiv-Datei |
| | Entwicklerdokumentation | Dokumentation | |
| Prüftool | Prüftool-Software | Software | CD-ROM oder Archiv-Datei |
| | Benutzer- und Betriebshandbuch Prüfwerkzeug | Dokumentation | |

64 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, mit der der EVG betrieben wird;
- geeignete, SigG-konforme sichere Signaturerstellungseinheiten (Signaturkarten[40] mit entsprechendem Zertifikat) samt SigG-konformem Chipkartenleser (mit PIN-Pad);
- qualifizierte Zertifikate;

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

- kryptographische Schlüssel und (System-)Zertifikate zur Gewährleistung der Systemsicherheit;
- Basiskomponente von Governikus (vgl. [bos_Basis_ST]);
- OSCI-Client und -Backend, die auf den EVG – d. h. auf OSCI-Client-Enabler bzw. -Backend-Enabler – zugreifen und welche die Funktionalitäten des EVG nutzen.

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

## 2.7 Absicherung

65 Die Client-Komponenten[41] des EVGs – d. h. der OSCI-Client-Enabler – ist durch ein Prüftool zum Schutz vor unbefugter Veränderung (Integritätsschutz) abgesichert, das im Folgenden näher beschrieben wird.

- Das Prüftool überprüft die elektronische Signatur der JAR-Files des OSCI-Client-Enablers.
- Das Prüftool kennt die Dateinamen aller JAR-Files, die überprüft werden müssen.
- Die JAR-Files sind durch den Hersteller (vgl. Abschnitt 2.8) signiert; die zugehörigen Zertifikate des Herstellers, die die öffentlichen Schlüssel zwecks Verifikation enthalten, sind im Prüftool enthalten.
- Dem Anwender wird zu jedem überprüften JAR-File der Dateiname, der Dateipfad, die Version, das jeweilige Prüfergebnis (Signatur korrekt, Signatur nicht korrekt) sowie das Gesamtergebnis (Produktintegrität bestätigt, Produktintegrität nicht bestätigt) angezeigt. Entsprechende Hinweise und Maßnahmen für den Fall, dass die Produktintegrität nicht bestätigt werden kann, werden im Benutzerhandbuch beschrieben.
- Die Integritätsprüfung erfolgt bei gestartetem OSCI-Client-Enabler, d. h. im laufenden Betrieb.
- Den Dateipfad der JAR-Files ermittelt das Prüftool aus einem Übergabeparameter und dem in Java Web Start eingetragenen Pfad des Caches.
- Werden die JAR-Archive vom Prüftool nicht gefunden, kann der Anwender den/die Speicherort/e über den Java-File-Explorer auswählen.

66 Die technische Realisierung des Prüftools:

- Das Prüftool ist ein Java-Applet, das vom Hersteller signiert ist.
- Der Anwender benötigt die Java Virtual Machine und einen Browser.
- Genutzte Hashfunktion: SHA-256 (Mechanismenstärke „hoch“).

[41] Hinsichtlich der Server-Komponenten (OSCI-Manager und -Backend-Enabler) ist zu berücksichtigen, dass der Schutz vor unbefugter Veränderung durch bauliche und organisatorische Maßnahmen sichergestellt wird (vgl. A.ServerBetrieb).

- Genutzter Verifikationsalgorithmus: RSA mit 1024 bzw. 2048 Bit[42] Schlüssellänge.

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

## 2.8 Auslieferung

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

- Hersteller von Governikus, Version 3.3 (OSCI):

  bremen online services GmbH & Co. KG

  Am Fallturm 9

  28359 Bremen

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

- Vertreiber von Governikus, Version 3.3 (OSCI):

  bremen online services GmbH & Co. KG

  Am Fallturm 9

  28359 Bremen

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

- Betreiber von Governikus, Version 3.3 (OSCI) sind beispielsweise Bundes- oder Landesbehörden.

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

  Der Betreiber konfiguriert, installiert, administriert und betreibt OSCI-Manager und OSCI-Backend-Enabler.

  Der Betreiber liefert den OSCI-Client-Enabler, das Prüftool und die zugehörige Dokumentation an den Benutzer aus. Die Auslieferung kann über ein Onlineverfahren (beispielsweise Java Web Start) oder durch Zustellung einer einmal beschreibbaren CD-ROM auf gesicherte Weise erfolgen.

- Anwendungsentwickler entwickelt auf die EVG-Schnittstellen aufsetzend Signaturanwendungskomponenten[43].

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

- Benutzer sind Anwender des OSCI-Client-Enablers und des Prüftools.

[43] Zur Information: Ein Anwendungsentwickler übergibt Signaturanwendungskomponenten, die die Funktionalitäten von OSCI-Client-Enabler und -Backend-Enabler nutzen, an den Betreiber.

# 3 EVG-Sicherheitsumgebung

## 3.1 Rollen

69 Es gibt im Kontext der OSCI-Komponente folgende Rollen, die hinsichtlich des Standortes differenziert werden:

70 serverseitig:

- **System-Administrator**: Ein System-Administrator ist für die Verwaltung und Organisation der grundlegenden IT-Infrastruktur zuständig, die für den EVG (OSCI-Manager und -Backend-Enabler) benötigt werden.[44] Typische Aktivitäten – mit dedizierter Beschränkung der Rechte 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 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 (OSCI-Manager) benötigte Referenz auf den kryptographischen Schlüssel zur Gewährleistung der Systemsicherheit.[17]
- **Revisor:** Der Revisor prüft beim EVG (OSCI-Manager und -Backend-Enabler) die Sicherheitsparameter, konfiguriert die Protokollierung und

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

wertet sie aus und begleitet den Security-Administrator zur Gewährleistung des Vier-Augen-Prinzips. Typische Aktivitäten des Revisors sind:

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

71 clientseitig:

- **Benutzer:** Der Benutzer in der IT-Umgebung nutzt den OSCI-Client – und damit den OSCI-Client-Enabler. Typischerweise wird der Benutzer der Signaturschlüssel-Inhaber sein (s. u.).
- **Signaturschlüssel-Inhaber:** Der Signaturschlüssel-Inhaber gibt am Chipkartenleser des OSCI-Client-Enablers in der IT-Umgebung seine PIN zur Erstellung einer qualifizierten elektronischen Signatur durch die sichere Signaturerstellungseinheit ein.

72 allgemein:

- **Anwendungsentwickler:** Eine Person, die auf Basis von OSCI-Client-Enabler oder -Backend-Enabler eine Signaturanwendungskomponente entwickelt.
- **nicht autorisierte Person:** Eine nicht autorisierte Person ist jede Person – während des EVG-Betriebs –, die weder System-, Security- oder Schlüssel-Administrator noch Revisor, Benutzer oder Signaturschlüssel-Inhaber ist.

## 3.2 Annahmen

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

74 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;
- private Schlüssel und (System-)Zertifikate (zur Gewährleistung der Systemsicherheit);
- Basiskomponente von Governikus für die Validierung von qualifizierten Zertifikaten (vgl. [bos_Basis_ST]).

Dabei werden geeignete kryptographische Verfahren mit entsprechenden Schlüssellängen eingesetzt.

Eine Verbindung zur Basiskomponente ist vorhanden.

Eine Auflistung findet sich im Anhang in Abschnitt 12.

75 A.SAK OSCI-Client und -Backend, die auf den EVG – d. h. auf OSCI-Client-Enabler bzw. -Backend-Enabler – zugreifen und

die die Funktionalitäten des EVG nutzen, stehen zur Verfügung. Die Anforderungen von Signaturgesetz und -verordnung an eine Signaturanwendungskomponente werden beachtet. Insbesondere gewährleisten sie die Funktionalitäten hinsichtlich Identifikation und Authentisierung zum Management von Sicherheitsattributen, d. h. den kryptographischen Schlüsseln und (System-)Zertifikaten.

Durch den OSCI-Client bzw. -Backend ist gewährleistet, dass auf Anforderung des Benutzers resp. Security-Administrators angezeigt wird, welcher OSCI-Manager angesprochen wird – durch Adresse und (System-) Zertifikat.

76 A.ServerBetrieb Für den Betrieb ist vertrauenswürdiges Personal eingesetzt, das einen Beitrag zur Sicherheit leistet, und die notwendigen räumlichen Gegebenheiten sowie Hard- und Software für den sicheren Betrieb der serverseitigen Komponenten des EVG (OSCI-Manager und -Backend-Enabler) sind vorhanden.

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

Es wird gewährleistet, dass der EVG korrekt aufgebaut ist, inkl. Einhaltung der Vorgaben hinsichtlich der räumlichen Gegebenheiten und für die Realisierung der Netzwerkarchitektur und der internen Verbindungen zwischen den einzelnen Systemkomponenten mit Firewall, Demilitarisierter Zone (DMZ) etc. Vgl. dazu die Vorgaben und Auflagen zum Betrieb von Governikus, die im „Generischen Sicherheitskonzept für die Kern- und Webkomponenten der Virtuellen Poststelle“ beschrieben werden [VPS-SiKo].

OSCI-Manager und Kernsystem der Basiskomponente ([bos_Basis_ST]) werden zusammen innerhalb eines vertrauenswürdigen Netzes betrieben.

Der OSCI-Backend-Enabler als Funktionsbibliothek nutzt kryptographische Schlüssel und (System-)Zertifikate, die vom OSCI-Backend zur Verfügung gestellt werden; eine geeignete Identifikation und Authentisierung zum Management dieser Sicherheitsattribute wird vom OSCI-Backend sichergestellt.

Die Anforderungen aus [BNetzA2005] an einen „geschützten Einsatzbereich (Regelfall/Standardlösung)“ werden umgesetzt, um „potentielle Angriffen über das Internet, ein angeschlossenes Intranet, einen manuellen Zugriff Unbefugter und einen Datenaustausch per Datenträger [...] durch eine

Kombination von Sicherheitsvorkehrungen in der Signaturanwendungskomponente selbst und der Einsatzumgebung mit hoher Sicherheit“ hinsichtlich eines hohen Angriffspotentials abzuwehren:

- Auflagen zur Anbindung an das Internet/Intranet: Es wird angenommen, dass Netzwerkverbindungen so abgesichert sind, dass Angriffe erkannt bzw. unterbunden werden – z. B. durch eine geeignet konfigurierte Firewall, geeignete Absicherung des LAN und durch die Verwendung geeigneter Anti-Viren-Programme;
- Auflagen zur Sicherheit der IT-Plattform und Applikationen: Es wird angenommen, dass gewährleistet wird, dass von der Hardware, auf der der EVG betrieben wird, keine Angriffe ausgehen. Insbesondere ist sicherzustellen, dass die auf dem eingesetzten Computer installierte Software nicht böswillig manipuliert oder verändert werden kann, auf dem Computer keine Viren oder Trojanischen Pferde eingespielt werden können, die Hardware des Computers nicht unzulässig verändert werden kann.
- Auflagen zum Schutz vor manuellem Zugriff Unbefugter und Datenaustausch per Datenträger: Es wird angenommen, dass die folgenden baulichen, personellen und organisatorischen Anforderungen umgesetzt sind:
    - Rechner, Monitor und Tastatur befinden sich in einem Betriebsraum.
    - Für die Administratoren müssen Vertreterregelungen für Krankheit und Urlaub bestehen.
    - Wartungs- bzw. Reinigungspersonal erhält den Zugang zum zugriffssicheren Betriebsraum nur durch einen Administrator, der den Aufenthalt überwacht.

77 A.ClientBetrieb Signaturschlüssel-Inhaber leisten einen Beitrag zur Sicherheit, indem sie sich beispielsweise vergewissern, dass sie bei der Eingabe ihres Identifikationsmerkmals nicht beobachtet werden, oder ihr Identifikationsmerkmal ändern, wenn sie den Verdacht oder die Gewissheit haben, Ihr Merkmal könnte nicht mehr geheim sein.

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

Der OSCI-Client-Enabler als Funktionsbibliothek nutzt kryptographische Schlüssel und (System-)Zertifikate, die vom OSCI-Client zur Verfügung gestellt werden; eine geeignete Identifikation und Authentisierung zum Management dieser Sicherheitsattribute wird vom OSCI-Client sichergestellt. Der OSCI-Client sichert auch die Integrität der kryptographischen Schlüssel und (System-)Zertifikate – denkbar ist, dass diese Sicherheitsattribute Bestandteil der integritätsgeschützten Software sind oder dass diese Konfigurationsdaten – ähnlich wie bei EVG3 – gesondert abgesichert werden.

Die Anforderungen aus [BNetzA2005] an einen „geschützten Einsatzbereich (Regelfall/Standardlösung)“ werden umgesetzt, um „potentielle Angriffen über das Internet, ein angeschlossenes Intranet, einen manuellen Zugriff Unbefugter und einen Datenaustausch per Datenträger [...] durch eine Kombination von Sicherheitsvorkehrungen in der Signaturanwendungskomponente selbst und der Einsatzumgebung mit hoher Sicherheit“ hinsichtlich eines hohen Angriffspotentials abzuwehren:

- Auflagen zur Anbindung an das Internet/Intranet: Es wird angenommen, dass Netzwerkverbindungen so abgesichert sind, dass Angriffe erkannt bzw. unterbunden werden – z. B. durch eine geeignet konfigurierte Firewall, und durch die Verwendung geeigneter Anti-Viren-Programme;
- Auflagen zur Sicherheit der IT-Plattform und Applikationen: Es wird angenommen, dass gewährleistet wird, dass von der Hardware, auf der der EVG betrieben wird, keine Angriffe ausgehen. Insbesondere ist sicherzustellen, dass die auf dem eingesetzten Computer installierte Software nicht böswillig manipuliert oder verändert werden kann, auf dem Computer keine Viren oder Trojanischen Pferde eingespielt werden können, die Hardware des Computers nicht unzulässig verändert werden kann, 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:
    - Aufbewahrung der PIN: Es wird angenommen, dass der Signaturschlüssel-Inhaber die PIN der Signaturkarte nicht weitergibt und die Regelungen zum Umgang mit der sicheren Signaturer-

stellungseinheit, die der Hersteller dem Benutzer mitgeteilt hat, umsetzt.

- Raum des Arbeitsplatzes: Es ist Sorge zu tragen, dass ein Zugriff Unbefugter ausgeschlossen ist oder zumindest mit hoher Sicherheit erkennbar wird – beispielsweise durch ein Sperren des Bildschirmes oder Verschließen des Büros bei Abwesenheit.
- Rechner und Chipkartenleser sind durch einen sicheren Kanal per Kabel verbunden.
- Der Benutzer hat vor Gebrauch mit einem vom Hersteller zur Verfügung gestellten Prüftool die Integrität des OSCI-Client-Enablers zu prüfen – vgl. Abschnitt 2.7.
- Bei der Installation hat der Benutzer die Integrität und Authentizität des OSCI-Client-Enablers mit dem vom Hersteller zur Verfügung gestellten Prüftool zu prüfen – vgl. Abschnitt 2.7.

78 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

79 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.

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

81 Weitere Bedrohungen ergeben sich implizit durch Nennung organisatorischer Sicherheitspolitiken.

## 3.4 Organisatorische Sicherheitspolitiken[45]

82 P.SignaturZuf Der EVG (hier: OSCI-Client-Enabler) muss beim Erzeugen einer Signatur gewährleisten, dass auf die zu signierenden

[45] Die für den EVG relevanten organisatorischen Sicherheitspolitiken ergeben sich aus den Anforderungen von Signaturgesetz und -verordnung (vgl. Abschnitt 2.5).

Daten eine Hashfunktion gemäß OSCI-Transport (vgl. Abschnitt 2.2) angewendet und der Hashwert einer sicheren Signaturerstellungseinheit zugeführt wird.

83 P.Anzeige Der EVG (hier: OSCI-Client-Enabler) muss gewährleisten, dass beim Erzeugen einer Signatur

- das Erzeugen einer Signatur vorher eindeutig angezeigt wird,
- erkennbar ist, auf welche Daten sich die Signatur bezieht, und
- bei Bedarf der Inhalt der zu signierenden Daten hinreichend zu erkennen ist

und beim Prüfen einer Signatur

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

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

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

86 P.Manipulation Der EVG muss zum Schutz vor unbefugter Veränderung am OSCI-Client-Enabler gewährleisten, dass sicherheitstechnische Veränderungen festgestellt werden können.

***Erklärung 1*** *Die organisatorischen Sicherheitspolitiken entstammen den für den EVG relevanten Anforderungen des Signaturgesetzes und der -verordnung, wie in [BNetzA2005] zusammenfassend dargestellt (vgl. Abschnitt 2.5.2 und Tabelle 1).*

# 4 Sicherheitsziele

## 4.1 EVG-Sicherheitsziele

87 O.SignaturZuf Der EVG (hier: OSCI-Client-Enabler) muss zum Erzeugen einer qualifizierten elektronischen Signatur auf die zu signierenden Daten eine Hashfunktion gemäß OSCI-Transport (vgl. Abschnitt 2.2) anwenden, den erzeugten Hashwert einer angeschlossenen sicheren Signaturerstellungseinheit zuführen, wo die qualifizierte elektronische Signatur erzeugt wird, und anschließend durch Verifikation der zuvor erzeugten Signatur mit dem auf der sicheren Signaturerstellungseinheit befindlichen Zertifikat prüfen, ob für die korrekten zu signierenden Daten eine Signatur generiert wurde.

***Erklärung 2*** *Das Sicherheitsziel O.SignaturZuf deckt die organisatorische Sicherheitspolitik P.SignaturZuf zur Erzeugung einer qualifizierten elektronischen Signatur ab und präzisiert, dass der OSCI-Client-Enabler die zu signierenden Daten gemäß OSCI-Transport der Hashfunktion zuführt und den Hashwert einer sicheren Signaturerstellungseinheit in der IT-Umgebung (vgl. OE.PKI) zugeführt. Zusätzlich wird durch die Verifikation der zuvor durch die Signaturkarte generierte qualifizierte elektronische Signatur mit dem auf der Signaturkarte befindlichen Zertifikat gewährleistet, dass für die richtigen Daten eine Signatur erzeugt wurde.*

88 O.Anzeige Der EVG (hier: OSCI-Client-Enabler) muss gewährleisten, dass dem Benutzer folgende Informationen angezeigt werden bzw. bei Bedarf – d. h. optional – angezeigt werden können:

- Erzeugen einer Signatur durch prozedurale Anzeigetexte;
- Bezug zu den Daten, auf die sich die Signatur bezieht – beim Signieren und Verifizieren;
- Ergebnis der Verifikation einer qualifizierten elektronischen Signatur;
- Ergebnis der Validierung eines qualifizierten Zertifikats;
- zu signierende und signierte Daten (optional);
- Signaturschlüssel-Inhaber der Signatur (optional);
- Zertifikatsinhalt (optional).

***Erklärung 3*** *Das Sicherheitsziel O.Anzeige deckt die organisatorische Sicherheitspolitik P.Anzeige zur sicheren und zuverlässigen Anzeige bei der Erzeugung und Prüfung qualifizierter elektronischer Signaturen beim OSCI-Client-Enabler ab. Dabei wird durch die Verifikation festgestellt, ob die Daten unverändert sind. Die Anzeige umfasst nicht nur, was signiert wird und wurde, sondern auch ergänzende Informationen zur Nachricht, wie Zertifikatsin-*

*halt, Signaturschlüssel-Inhaber und Verifikations- und Validierungsergebnisse.*

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

- die Funktionalitäten einer Basiskomponente[46] anfordern (OSCI-Manager) und
- eine Plausibilitätsprüfung (Prüfung, ob das validierte Zertifikat zur Signatur gehört.) sowie Verifikation des OSCI-Laufzettels mit dem Validierungsergebnis des OSCI-Managers beim OSCI-Client-Enabler und -Backend-Enabler vornehmen.

***Erklärung 4*** *Das Sicherheitsziel O.ValidZert deckt die organisatorische Sicherheitspolitik P.ValidZert zur Validierung qualifizierter Zertifikate ab und präzisiert die Aufgabenteilung. Zu berücksichtigen ist, dass die wesentlichen Aufgaben bei der Validierung in der IT-Umgebung durch die Basiskomponente (vgl. Sicherheitsziel für die IT-Umgebung OE.PKI) geleistet wird und dass zur Gewährleistung der Systemsicherheit (innerhalb des verteilten System) die Sicherheitsziele für die IT-Umgebung OE.ServerBetrieb und OE.ClientBetrieb benötigt werden.*

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

- Prüfung der Integrität: Der Hashwert des signierten Dokuments muss mit dem übermittelten Hashwert übereinstimmen, wobei die Hashwertbildung gemäß OSCI-Transport (vgl. Abschnitt 2.2) zu berücksichtigen ist.
- Prüfung der Authentizität: Dieser Hashwert muss gleich dem Ergebnis sein, das durch Anwendung des öffentlichen Signaturschlüssels auf die elektronische Signatur mit einem geeigneten kryptographischen Algorithmus berechnet wird.

***Erklärung 5*** *Das Sicherheitsziel O.VerifySign deckt die organisatorische Sicherheitspolitik P.VerifySign zur Prüfung einer qualifizierten elektronischen Signatur ab und präzisiert, dass die Verifikation durch die Prüfung der Integrität und der Authentizität erfolgt (qualifizierte Zertifikate via Sicherheitsziel für die IT-Umgebung OE.PKI).*

91 O.Manipulation Der EVG muss zum Schutz vor unbefugter Veränderung am OSCI-Client-Enabler gewährleisten, dass durch Integritätsprüfung festgestellt werden kann, ob Veränderungen am OSCI-Client-Enabler vorgenommen wurden.

[46] Wie bereits in Abschnitten 2.3 und 2.4 ausgeführt, wird die eigentliche Validierung von der Basiskomponente durchgeführt.

***Erklärung 6*** *Das Sicherheitsziel O.Manipulation deckt die organisatorische Sicherheitspolitik P.Manipulation zum Schutz vor unbefugter Veränderung des OSCI-Client-Enablers ab.*

## 4.2 Sicherheitsziele für die Umgebung

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

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

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

  Darüber hinaus wird ein unterstützender Sicherheitsmechanismus der Basiskomponente für die Erzeugung einer elektronischen Signatur für einen vom OSCI-

Manager erzeugten und übergebenen Hashwert zum Signieren des OSCI-Laufzettels genutzt.

***Erklärung 7*** *Das Sicherheitsziel für die Umgebung OE.PKI zielt auf die gleichnamige Annahme A.PKI ab, wobei zu berücksichtigen ist, dass OE.PKI auch für die organisatorischen Sicherheitspolitiken P.SignaturZuf (für die Erzeugung einer qualifizierten elektronischen Signatur durch die sichere Signaturerstellungseinheit mittels Chipkartenleser), P.ValidZert (für die Gültigkeitsprüfung durch obige Funktionalitäten der Basiskomponenten, für die Existenz qualifizierter Zertifikate sowie die kryptographischen Schlüssel und (System-)Zertifikate zur Gewährleistung der Systemsicherheit) sowie P.VerifySign (für Existenz qualifizierter Zertifikate) benötigt werden. Zudem wehrt OE.PKI die Bedrohung TE.RatePIN durch Verwendung einer geeigneten Signaturkarte ab.*

94 OE.SAK Die IT-Umgebung muss OSCI-Client und -Backend zur Verfügung stellen, die auf den EVG – d. h. auf OSCI-Client-Enabler bzw. -Backend-Enabler – zugreifen, die die Funktionalitäten des EVG nutzen und welche die Anforderungen von Signaturgesetz und -verordnung an eine Signaturanwendungskomponente beachten. Insbesondere gewährleisten sie die Funktionalitäten hinsichtlich Identifikation und Authentisierung zum Management von Sicherheitsattributen, d. h. den kryptographischen Schlüsseln und den (System-) Zertifikaten.

In der IT-Umgebung muss beim OSCI-Client bzw. -Backend gewährleistet sein, dass auf Anforderung des Benutzers resp. Security-Administrators angezeigt wird, welcher OSCI-Manager angesprochen wird – durch Adresse und (System-) Zertifikat.

***Erklärung 8*** *Das Sicherheitsziel für die Umgebung OE.SAK zielt auf die gleichnamige Annahme A.SAK ab.*

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

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

Es muss gewährleistet sein, dass der EVG korrekt aufgebaut ist, inkl. Einhaltung der Vorgaben hinsichtlich der räumlichen Gegebenheiten und für die Realisierung der Netzwerkarchitektur und der internen Verbindungen zwischen den einzel-

nen 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].

OSCI-Manager und Kernsystem der Basiskomponente ([bos_Basis_ST]) müssen zusammen innerhalb eines vertrauenswürdigen Netzes betrieben werden.

Der OSCI-Backend-Enabler als Funktionsbibliothek nutzt kryptographische Schlüssel und (System-)Zertifikate, die vom OSCI-Backend zur Verfügung gestellt werden; eine geeignete Identifikation und Authentisierung zum Management dieser Sicherheitsattribute muss durch den OSCI-Backend sichergestellt werden.

Die Anforderungen aus [BNetzA2005] an einen „geschützten Einsatzbereich (Regelfall/Standardlösung)“ müssen umgesetzt sein, um „potentielle Angriffen über das Internet, ein angeschlossenes Intranet, einen manuellen Zugriff Unbefugter und einen Datenaustausch per Datenträger [...] durch eine Kombination von Sicherheitsvorkehrungen in der Signaturanwendungskomponente selbst und der Einsatzumgebung mit hoher Sicherheit“ hinsichtlich eines hohen Angriffspotentials abzuwehren:

- Auflagen zur Anbindung an das Internet/Intranet: Netzwerkverbindungen müssen so abgesichert sind, dass Angriffe erkannt bzw. unterbunden werden – z. B. durch eine geeignet konfigurierte Firewall, geeignete Absicherung des LAN und durch die Verwendung geeigneter Anti-Viren-Programme;
- Auflagen zur Sicherheit der IT-Plattform und Applikationen: Es muss gewährleistet sein, dass von der Hardware, auf der der EVG betrieben wird, keine Angriffe ausgehen. Insbesondere muss sichergestellt sein dass die auf dem eingesetzten Computer installierte Software nicht böswillig manipuliert oder verändert werden kann, auf dem Computer keine Viren oder Trojanischen Pferde eingespielt werden können, die Hardware des Computers nicht unzulässig verändert werden kann.
- Auflagen zum Schutz vor manuellem Zugriff Unbefugter und Datenaustausch per Datenträger: Die folgenden baulichen, personellen und organisatorischen Anforderungen müssen umgesetzt sein:
    - Rechner, Monitor und Tastatur befinden sich in einem Betriebsraum.

- Für die Administratoren müssen Vertreterregelungen für Krankheit und Urlaub bestehen.
- Wartungs- bzw. Reinigungspersonal erhält den Zugang zum zugriffssicheren Betriebsraum nur durch einen Administrator, der den Aufenthalt überwacht.

***Erklärung 9*** *Das Sicherheitsziel für die Umgebung OE.ServerBetrieb zielt auf die gleichnamige Annahme A.ServerBetrieb ab und ist zur Realisierung der organisatorischen Sicherheitspolitik P.ValidZert (für die Gewährleistung der Systemsicherheit aufgrund der Realisierung der Validierung innerhalb des verteilten Systems – d. h. dem Management des OSCI-Managers zum Signieren des OSCI-Laufzettels durch das Kernsystem und des (System-) Zertifikats im OSCI-Backend-Enabler zur Verifikation des OSCI-Laufzettels) notwendig.*

96 OE.ClientBetrieb Für den Betrieb des OSCI-Client-Enablers muss der Signaturschlüssel-Inhaber einen Beitrag zur Sicherheit leisten, sich beispielsweise vergewissern, dass er bei der Eingabe seines Identifikationsmerkmals nicht beobachtet wird, oder sein Identifikationsmerkmal ändert, wenn er den Verdacht oder die Gewissheit hat, sein Merkmal könnte nicht mehr geheim sein.

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

Der OSCI-Client-Enabler als Funktionsbibliothek nutzt kryptographische Schlüssel und (System-)Zertifikate, die vom OSCI-Client zur Verfügung gestellt werden; eine geeignete Identifikation und Authentisierung zum Management dieser Sicherheitsattribute muss vom OSCI-Client sichergestellt werden. Der OSCI-Client muss auch die Integrität der kryptographischen Schlüssel und (System-)Zertifikate sichern – denkbar ist, dass diese Sicherheitsattribute Bestandteil der integritätsgeschützten Software sind oder dass diese Konfigurationsdaten – ähnlich wie bei EVG3 – gesondert abgesichert werden.

Die Anforderungen aus [BNetzA2005] an einen „geschützten Einsatzbereich (Regelfall/Standardlösung)“ müssen umgesetzt sein, um „potentielle Angriffen über das Internet, ein angeschlossenes Intranet, einen manuellen Zugriff Unbefugter und einen Datenaustausch per Datenträger [...] durch ei-

ne Kombination von Sicherheitsvorkehrungen in der Signaturanwendungskomponente selbst und der Einsatzumgebung mit hoher Sicherheit“ hinsichtlich eines hohen Angriffspotentials abzuwehren:

- Auflagen zur Anbindung an das Internet/Intranet: Netzwerkverbindungen müssen so abgesichert sein, dass Angriffe erkannt bzw. unterbunden werden – z. B. durch eine geeignet konfigurierte Firewall, und durch die Verwendung geeigneter Anti-Viren-Programme;
- Auflagen zur Sicherheit der IT-Plattform und Applikationen: Es muss gewährleistet sein, dass von der Hardware, auf der der EVG betrieben wird, keine Angriffe ausgehen. Insbesondere muss sichergestellt sein, dass die auf dem eingesetzten Computer installierte Software nicht böswillig manipuliert oder verändert werden kann, auf dem Computer keine Viren oder Trojanischen Pferde eingespielt werden können, die Hardware des Computers nicht unzulässig verändert werden kann, 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:
    - Aufbewahrung der PIN: Es wird angenommen, dass der Signaturschlüssel-Inhaber die PIN der Signaturkarte nicht weitergibt und die Regelungen zum Umgang mit der sicheren Signaturerstellungseinheit, die der Hersteller dem Benutzer mitgeteilt hat, umsetzt.
    - Raum des Arbeitsplatzes: Es muss Sorge getragen werden, dass ein Zugriff Unbefugter ausgeschlossen ist oder zumindest mit hoher Sicherheit erkennbar wird – beispielsweise durch ein Sperren des Bildschirmes oder Verschließen des Büros bei Abwesenheit.
    - Rechner und Chipkartenleser müssen durch einen sicheren Kanal per Kabel verbunden sein.
    - Der Benutzer hat vor Gebrauch mit einem vom Hersteller zur Verfügung gestellten Prüftool die Integrität des OSCI-Client-Enablers zu prüfen – vgl. Abschnitt 2.7.
    - Bei der Installation hat der Benutzer die Integrität und Authentizität des OSCI-Client-Enablers mit

dem vom Hersteller zur Verfügung gestellten Prüftool zu prüfen – vgl. Abschnitt 2.7.

***Erklärung 10*** *Das Sicherheitsziel für die Umgebung OE.ClientBetrieb zielt auf die gleichnamige Annahme A.ClientBetrieb ab und ist zur Realisierung der organisatorischen Sicherheitspolitik P.ValidZert (für die Gewährleistung der Systemsicherheit aufgrund der Realisierung der Validierung innerhalb des verteilten Systems – d. h. dem Management des (System-) Zertifikats im OSCI-Client-Enabler zur Verifikation des OSCI-Laufzettels) notwendig. Zudem wehrt OE.ClientBetrieb die Bedrohung TE.SpähePIN durch geeignete Auflagen und Hinweise an den Signaturschlüssel-Inhaber zur Nutzung seiner Signaturkarte ab.*

97 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.

***Erklärung 11*** *Das Sicherheitsziel für die Umgebung OE.ZufPIN zielt auf die gleichnamige Annahme A.ZufPIN ab.*

# 5 IT-Sicherheitsanforderungen

## 5.1 EVG-Sicherheitsanforderungen

### 5.1.1 Definition der funktionalen Sicherheitspolitik (FSP)

98 Bevor die funktionalen Sicherheitsanforderungen an den EVG aufgeführt werden, wird die funktionale Sicherheitspolitik (FSP) für die Zugriffskontrolle auf die Systemsicherheit (Systemsicherheit-Zugriffskontrollpolitik) definiert, wobei zu berücksichtigen ist, dass diese funktionale Sicherheitspolitik *nicht* für das Erzeugen oder die Prüfung einer qualifizierten elektronischen Signatur relevant ist:[47]

99 Der OSCI-Manager lässt den OSCI-Laufzettel vom Kernsystem der Basiskomponente mit einer elektronischen Signatur versehen[17], welche OSCI-Client-Enabler und -Backend-Enabler verifizieren.

100 Dazu wird die Referenz auf den zu nutzenden privaten Schlüssel im OSCI-Manager verwaltet, während der private Schlüssel selber im Kernsystem der Basiskomponente[17] und die (System-)Zertifikate in OSCI-Client resp. -Backend außerhalb des EVG in der IT-Umgebung abgespeichert sind.

[47] Der Zugriff auf einen privaten Schlüssel zur Erzeugung einer qualifizierten elektronischen Signatur bzw. ein qualifiziertes Zertifikat zur Prüfung einer qualifizierten elektronischen Signatur oder eines qualifizierten Zertifikats wird in der IT-Umgebung (in der sicheren Signaturerstellungseinheit bzw. dem unterliegenden System) kontrolliert.

101 Für das Management der Referenz des privaten Schlüssels sind folgende Subjekte, Objekte und Operationen relevant:[48]

- Subjekte:
  - Schlüssel-Administrator (für OSCI-Manager);
- Objekte:
  - Referenz auf privaten Schlüssel;
- Operationen:
  - Speichern der Referenz des privaten Schlüssels;
  - Löschen der Referenz des privaten Schlüssels.

102 Der Zugriff auf die Operationen Speichern und Löschen erfolgt nur nach erfolgreicher Authentisierung des Schlüssel-Administrators.

### 5.1.2 Funktionale EVG-Sicherheitsanforderungen

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

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

**Tabelle 3: Funktionale Sicherheitsanforderungen an den EVG**

| Funktionale Sicherheitsanforderung an den EVG | Beschreibung |
|---|---|
| FCS_COP.1 (Hash) | Kryptographischer Betrieb (für die kryptographische Operation „Hashen“ im Rahmen der Erzeugung einer qualifizierten elektronischen Signatur durch die Signaturkarte) |
| FCS_COP.1 (Valid) | Kryptographischer Betrieb (für die kryptographische Operation „Verifizieren“ des OSCI-Laufzettels) |
| FCS_COP.1 (OSCI) | Kryptographischer Betrieb (für die kryptographische Operation „Hashen“ im Rahmen der Erzeugung einer elektronischen Signatur des OSCI-Laufzettels) |
| FCS_COP.1 (Verify) | Kryptographischer Betrieb (für die kryptographische Operation „Verifizieren“ einer qualifizierten elektronischen Signatur) |
| FCS_COP.1 (VSign) | Kryptographischer Betrieb (für die kryptographische Operation „Verifizieren“ einer zuvor von der Signaturkarte erzeugten quali- |

[48] Das Management der Sicherheitsattribute in OSCI-Client und -Backend obliegen der IT-Umgebung.

| Funktionale Sicherheits-anforderung an den EVG | Beschreibung |
|---|---|
| | fizierten elektronischen Signatur) |
| FCS_COP.1 (Tool) | Kryptographischer Betrieb (für die kryptographische Operation „Verifikation“ im Rahmen des Prüftools) |
| FDP_SVR.1[49] | Sichere Anzeige |
| FDP_ACC.1 | Teilweise Zugriffskontrolle |
| FDP_ACF.1 | Zugriffskontrolle basierend auf Sicherheitsattributen |
| FDP_ITC.1 | Import von Benutzerdaten ohne Sicherheitsattribute |
| FIA_UID.2 | Benutzeridentifikation vor jeglicher Aktion |
| FIA_UAU.2 | Benutzerauthentisierung vor jeglicher Aktion |
| FMT_MSA.1 | Management der Sicherheitsattribute |
| FMT_MSA.3 | Initialisierung statischer Attribute |
| FMT_SMR.1 | Sicherheitsrollen |
| FTP_ITC.1 | Inter-TSF Vertrauenswürdiger Kanal |

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

**106** **FCS_COP.1 (Hash)** **Kryptographischer Betrieb (für die kryptographische Operation „Hashen“ im Rahmen der Erzeugung einer qualifizierten elektronischen Signatur durch die Signaturkarte)**

107 FCS_COP.1.1/Hash Die TSF müssen **im Zusammenhang mit der Erzeugung einer qualifizierten elektronischen Signatur durch die Signaturkarte die kryptographische Operation „Hashen**“ gemäß eines spezifizierten kryptographischen Algorithmus **SHA-1[50], SHA-256, SHA-512 sowie RIPEMD-160** und kryptographischer Schlüssellängen**, die bei einer Hashfunktion nicht relevant sind**, die der folgenden **Norm [SHA]** entspricht, durchführen.

***Erklärung 12*** *Die in FCS_COP.1.1/Hash spezifizierte Hashfunktion wird gemäß OSCI-Transport genutzt (vgl. Abschnitt 2.2).*

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

[50] Der Algorithmus SHA-1 wird zwecks Kompatibilität mit vorherigen Versionen von Governikus weiter unterstützt. Es liegt in der Verantwortung des Anwenders bzw. Administrators, für den jeweiligen Zweck hinreichend starke kryptographische Algorithmen auszuwählen.

***Erklärung 13*** *Die funktionale Sicherheitsanforderung FCS_COP.1 (Hash) wird für die Umsetzung des Sicherheitsziels O.SignaturZuf benötigt.*

***Erklärung 14*** *Die Abhängigkeiten der funktionalen Sicherheitsanforderung FCS_COP.1 (Hash) sind nicht erfüllt, da keine Schlüssel involviert sind (weder Schlüsselerzeugung gemäß FCS_CKM.1 oder Schlüsselimport gemäß FDP_ITC.1 noch Zerstörung eines Schlüssels gemäß FCS_CKM.4) und daher kein Schlüsselmanagement gemäß FMT_MSA.2 notwendig ist.*

**108** **FCS_COP.1 (Valid) Kryptographischer Betrieb (für die kryptographische Operation „Verifizieren“ des OSCI-Laufzettels)**

109 FCS_COP.1.1/Valid Die TSF müssen **im Rahmen der Gewährleistung der Systemsicherheit die kryptographische Operation „Verifizieren**“ gemäß eines spezifizierten kryptographischen Algorithmus **RSA im Zusammenhang mit den Hashfunktionen SHA-1**[50]**, SHA-256 sowie SHA-512 und RIPEMD 160** und kryptographischer Schlüssellängen**, die entsprechend der X.509-Serverzertifikate derzeit 2048 Bit aufweisen**, die den folgenden **Normen [RSA] und [SHA]** [51] entsprechen, durchführen.

***Erklärung 15*** *Die funktionale Sicherheitsanforderung FCS_COP.1 (Valid) wird für die Umsetzung des Sicherheitsziels O.ValidZert in der Weise benötigt, dass OSCI-Client-Enabler und -Backend-Enabler die Signatur des OSCI-Laufzettels (vom OSCI-Manager mit Hilfe der Basiskomponente erzeugt) mit dem (System-)Zertifikat verifizieren müssen.*

***Erklärung 16*** *Die Abhängigkeiten der funktionalen Sicherheitsanforderung FCS_COP.1 (Valid) – Schlüsselerzeugung gemäß FCS_CKM.1 oder Schlüsselimport gemäß FDP_ITC.1, Zerstörung eines Schlüssels gemäß FCS_CKM.4 und Schlüsselmanagement gemäß FMT_MSA.2) – sind in der IT-Umgebung im OSCI-Client bzw. -Backend, auf dem OSCI-Client-Enabler resp. -Backend-Enabler betrieben werden, zu realisieren.*

**110** **FCS_COP.1 (OSCI) Kryptographischer Betrieb (für die kryptographische Operation „Hashen“ im Rahmen der Erzeugung einer elektronischen Signatur des OSCI-Laufzettels)**

111 FCS_COP.1.1/OSCI Die TSF müssen **im Rahmen der Gewährleistung der Systemsicherheit die kryptographische Operation „Hashen**“ gemäß eines spezifizierten kryptographischen Algorithmus **SHA-1**[50]**, SHA-256, SHA-512 sowie RIPEMD-160** und kryptographischer Schlüssellängen**, die bei einer Hashfunktion nicht relevant sind**, die der folgenden **Norm [SHA]** entspricht, durchführen.

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

***Erklärung 17*** *Die funktionale Sicherheitsanforderung FCS_COP.1 (OSCI) wird für die Umsetzung des Sicherheitsziels O.ValidZert in der Weise benötigt, dass der OSCI-Manager auf den OSCI-Laufzettel die Hashfunktion SHA-1, SHA-256 und SHA-512 sowie RIPEMD 160 anwendet und durch das Kernsystem der Basiskomponente signieren lässt, so dass die elektronische Signatur des OSCI-Laufzettels dann von OSCI-Client-Enabler und -Backend-Enabler mit dem – dem OSCI-Manager zugeordneten – (System-) Zertifikat verifiziert werden kann.*

***Erklärung 18*** *Die Abhängigkeiten der funktionalen Sicherheitsanforderung FCS_COP.1 (OSCI) sind nicht erfüllt, da keine Schlüssel involviert sind (weder Schlüsselerzeugung gemäß FCS_CKM.1 oder Schlüsselimport gemäß FDP_ITC.1 noch Zerstörung eines Schlüssels gemäß FCS_CKM.4) und daher kein Schlüsselmanagement gemäß FMT_MSA.2 notwendig ist wird.*

| | | | |
|---|---|---|---|
| 112 | **FCS_COP.1 (Verify)** | **Kryptographischer Betrieb <u>(für die kryptographische Operation „Verifizieren“ einer qualifizierten elektronischen Signatur)</u>** | |
| 113 | FCS_COP.1.1/Verify | Die TSF müssen **für die Verifikation einer qualifizierten elektronischen Signatur die kryptographische Operation „Verifizieren**“ gemäß eines spezifizierten kryptographischen Algorithmus **RSA im Zusammenhang mit den Hashfunktionen SHA-1**[50]**, SHA-256, SHA-512 sowie RIPEMD-160** und kryptographischer Schlüssellängen**, die entsprechend der X.509-Zertifikate derzeit 1024 oder 2048 Bit aufweisen**, die den folgenden **Normen [RSA] und [SHA]**[51] entsprechen, durchführen. | |

***Erklärung 19*** *Die funktionale Sicherheitsanforderung FCS_COP.1 (Verify) wird für die Umsetzung des Sicherheitsziels O.VerifySign benötigt.*

***Erklärung 20*** *Die Abhängigkeiten der funktionalen Sicherheitsanforderung FCS_COP.1 (Verify) sind nicht erfüllt, da die für die Verifikation genutzten öffentlichen Schlüssel aus den Zertifikaten öffentliche Informationen sind und keine Sicherheitsattribute darstellen (keine Schlüsselerzeugung gemäß FCS_CKM.1, kein Schlüsselimport gemäß FDP_ITC.1 , keine Zerstörung eines Schlüssels gemäß FCS_CKM.4, kein Schlüsselmanagement gemäß FMT_MSA.2).*

| | | | |
|---|---|---|---|
| 114 | **FCS_COP.1 (VSign)** | **Kryptographischer Betrieb <u>(für die kryptographische Operation „Verifizieren“ einer zuvor von der Signaturkarte erzeugten qualifizierten elektronischen Signatur)</u>** | |
| 115 | FCS_COP.1.1/VSign | Die TSF müssen **für die Verifikation einer qualifizierten elektronischen Signatur die kryptographische Operation „Verifizieren**“ gemäß eines spezifizierten | |

kryptographischen Algorithmus **RSA im Zusammenhang mit den Hashfunktionen SHA-1**[50]**, SHA-256, SHA-512 und RIPEMD 160** und kryptographischer Schlüssellängen**, die entsprechend der X.509-Zertifikate derzeit 1024 oder 2048 Bit aufweisen**, die den folgenden **Normen [RSA] und [SHA]**[51] entsprechen, durchführen.

***Erklärung 21*** *Die funktionale Sicherheitsanforderung FCS_COP.1 (VSign) wird für die Umsetzung des Sicherheitsziels O.SignaturZuf in der Weise benötigt, dass eine zuvor erzeugte qualifizierte elektronische Signatur mit Hilfe des zum privaten Schlüssel korrespondierenden Zertifikats, das sich auf der Signaturkarte befindet, verifiziert wird.*

***Erklärung 22*** *Die Abhängigkeiten der funktionalen Sicherheitsanforderung FCS_COP.1 (VSign) – Schlüsselimport gemäß FDP_ITC.1, Zerstörung eines Schlüssels gemäß FCS_CKM.4 und Schlüsselmanagement gemäß FMT_MSA.2) – sind in der IT-Umgebung für die Signaturkarte zu realisieren; eine Schlüsselerzeugung gemäß FCS_CKM.1 ist nicht anwendbar, da Zertifikate auf der Signaturkarte abgespeichert, dort aber nicht erzeugt werden.*

116 **FCS_COP.1 (Tool) Kryptographischer Betrieb <u>(für die kryptographische Operation „Verifizieren“ im Rahmen des Prüftools)</u>**

117 FCS_COP.1.1/Tool Die TSF müssen **im Zusammenhang mit dem Prüftool die kryptographische Operation „Verifizieren**“ gemäß eines spezifizierten kryptographischen Algorithmus SHA-256 oder **RSA im Zusammenhang mit den Hashfunktionen SHA-1**[50] und kryptographischer Schlüssellängen (nur für RSA relevant)**, die 1024 bzw. 2048 Bit aufweisen**, die den folgenden **Normen [RSA] und [SHA]**[51] entsprechen, durchführen.

***Erklärung 23*** *Die funktionale Sicherheitsanforderung FCS_COP.1 (Tool) wird für die Umsetzung des Sicherheitsziels O.Manipulation benötigt.*

***Erklärung 24*** *Die Abhängigkeiten der funktionalen Sicherheitsanforderung FCS_COP.1 (Tool) – Schlüsselimport gemäß FDP_ITC.1 (Schlüsselerzeugung gemäß FCS_CKM.1 ist bei Zertifikaten nicht anwendbar), Zerstörung eines Schlüssels gemäß FCS_CKM.4 und Schlüsselmanagement gemäß FMT_MSA.2) – sind in der IT-Umgebung für das Prüftool zu realisieren, da die für die Prüfung notwendigen Zertifikate vom Hersteller in das Tool eingebracht und mit dem Tool ausgeliefert werden.*

***Erklärung 25*** *Bei jeder JAR-Datei, die nicht über SHA-1 und RSA abgesichert ist, wird zusätzlich ein Hashwertvergleich durchgeführt: Dazu stellt das Prüftool zunächst fest, welcher Signaturalgorithmus und welche Hashfunktion genutzt wurden, und prüft ab, ob RSA und SHA-1 genutzt wurden. Andernfalls erfolgt der zusätzliche Hashwertvergleich, indem mit SHA-256 ein*

*Hashwert über die gesamte JAR-Datei gebildet und mit einem Referenzwert verglichen wird. Der Referenzwert wird analog zu den JNLP-Dateien als Parameter übergeben. Falls kein Referenzwert vorhanden ist oder die Hashwerte nicht gleich sind, lautet das Prüfergebnis insgesamt: Produktintegrität nicht gewährleistet.*

**118** **FDP_SVR.1** **Sichere Anzeige**

119 FDP_SVR.1.1 Die TSF müssen sicherstellen, dass der dem Benutzer angezeigte Inhalt eines Dokumentes (also die zu signierenden oder signierten Daten) entsprechend den folgenden Normen **plain-text (UTF-8-codiert) und tiff** sowie hinsichtlich dem Erzeugen einer Signatur durch prozedurale Anzeigetexte, dem Bezug zu den Daten, auf die sich die Signatur bezieht – beim Signieren und Verifizieren –, dem Ergebnis der Verifikation einer qualifizierten elektronischen Signatur, dem Ergebnis der Validierung eines qualifizierten Zertifikats, dem Signaturschlüssel-Inhaber der Signatur (optional) und dem Zertifikatsinhalt (optional) eindeutig ist.

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

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

***Erklärung 26*** *Die funktionale Sicherheitsanforderung FDP_SVR.1 wird für die Umsetzung des Sicherheitsziels O.Anzeige benötigt.*

***Erklärung 27*** *FDP_SVR.1 hat keine Abhängigkeiten.*

**122** **FDP_ACC.1** **Teilweise Zugriffskontrolle**

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

- **die betrachteten Subjekte:**
  - **Schlüssel-Administrator;**
- **die betrachteten Objekte:**
  - **Referenz auf privaten Schlüssel;**
- **und die betrachteten Operationen:**
  - **Speichern der Referenz des privaten Schlüssels;**

- **Löschen der Referenz des privaten Schlüssels;**

durchsetzen.

***Erklärung 28*** *Die funktionale Sicherheitsanforderung FDP_ACC.1 ergibt sich aus der Abhängigkeit von FDP_ITC.1 und wird daher implizit für die Umsetzung des Sicherheitsziels O.ValidZert in der Weise benötigt, dass der OSCI-Manager den OSCI-Laufzettel durch das Kernsystem der Basiskomponente signieren lässt und dazu den zu nutzenden Schlüssel referenziert. In dieser Sicherheitsanforderung werden Subjekt, Objekt sowie zulässige Operationen zwischen Subjekten und Objekten hinsichtlich der Systemsicherheit-Zugriffskontrollpolitik definiert.*

***Erklärung 29*** *Die Abhängigkeit von FDP_ACC.1 – FDP_ACF.1 – ist aufgenommen.*

**124** **FDP_ACF.1** **Zugriffskontrolle basierend auf Sicherheitsattributen**

125 FDP_ACF.1.1 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.

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

**Speichern und Löschen der Referenz des privaten Schlüssels erfolgt nur nach erfolgreicher Authentisierung des Schlüssel-Administrators.**

127 FDP_ACF.1.3 Die TSF müssen den Zugriff von Subjekten auf Objekte basierend auf den folgenden zusätzlichen Regeln explizit autorisieren: **Die TSF müssen hierbei keine zusätzlichen Regeln berücksichtigen**.

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

***Erklärung 30*** *Die funktionale Sicherheitsanforderung FDP_ACF.1 ergibt sich aus der Abhängigkeit von FDP_ACC.1 und wird daher implizit für die Umsetzung des Sicherheitsziels O.ValidZert in der Weise benötigt, dass der OSCI-Manager den OSCI-Laufzettel durch das Kernsystem der Basiskomponente signieren lässt und dazu den zu nutzenden Schlüssel referenziert. In dieser Sicherheitsanforderung wird thematisiert, dass eine zulässige Operation (vgl. FDP_ACC.1) erst nach erfolgreicher Authentisierung des Schlüssel-Administrators erfolgen kann.*

***Erklärung 31*** *Die Abhängigkeiten von FDP_ACF.1 – FDP_ACC.1 und FMT_MSA.3 sind aufgenommen.*

**129** **FDP_ITC.1** **Import von Benutzerdaten ohne Sicherheitsattribute**

130 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.

131 FDP_ITC.1.2 Die TSF müssen die mit den Benutzerdaten (hier: Referenz auf privaten Schlüssel) verknüpften Sicherheitsattribute ignorieren, wenn diese von außerhalb des TSC importiert werden.

132 FDP_ITC.1.3 Die TSF müssen die folgenden Regeln beim Import unter Kontrolle der SFP stehender Benutzerdaten von außerhalb des TSC durchsetzen: **Keine zusätzlichen Importkontrollregeln**.

***Erklärung 32*** *Die funktionale Sicherheitsanforderung FDP_ITC.1 wird für die Umsetzung des Sicherheitsziels O.ValidZert in der Weise benötigt, dass der OSCI-Manager den OSCI-Laufzettel durch das Kernsystem der Basiskomponente signieren lässt – und dazu den zu nutzenden Schlüssel referenziert –, so dass die Signatur dann von OSCI-Client-Enabler und -Backend-Enabler mit dem (System-)Zertifikat verifizieren werden kann.*

***Erklärung 33*** *Die Abhängigkeiten von FDP_ITC.1 – FDP_ACC.1 für die Zugriffskontrolle und FMT_MSA.3 zum Management des privaten Schlüssels sind aufgenommen.*

**133** **FIA_UID.2** **Benutzeridentifikation vor jeglicher Aktion**

134 Ist hierarchisch zu: FIA_UID.1

135 FIA_UID.2.1 Die TSF müssen erfordern, dass sich jeder Benutzer (hier: Schlüssel- und Security-Administrator) identifiziert, bevor für diesen jegliche andere TSF-vermittelte Aktionen erlaubt werden.

***Erklärung 34*** *Die funktionale Sicherheitsanforderung FIA_UID.2 ergibt sich aus der Abhängigkeit von FMT_SMR.1, wobei statt FIA_UID.1 die hierarchische Anforderung FIA_UID.2 genutzt wird. FIA_UID.2 wird damit implizit für die Umsetzung des Sicherheitsziels O.ValidZert benötigt.*

***Erklärung 35*** *FIA_UID.2 hat keine Abhängigkeiten.*

**136** **FIA_UAU.2** **Benutzerauthentisierung vor jeglicher Aktion**

137 Ist hierarchisch zu: FIA_UAU.1

138 FIA_UAU.2.1 Die TSF müssen erfordern, daß jeder Benutzer (hier: Schlüssel- und Security-Administrator) erfolgreich authentisiert wurde, bevor diesem jegliche andere TSF-vermittelte Aktionen erlaubt werden.

***Erklärung 36*** *Die funktionale Sicherheitsanforderung FIA_UAU.2 wird – wie FIA_UID.2 auch – für die Umsetzung des Sicherheitsziels O.ValidZert benötigt.*

***Erklärung 37*** *FIA_UAU.2 hat die Abhängigkeit FIA_UID.1, die durch die hierarchische Anforderung FIA_UID.2 realisiert wird.*

**139 FMT_MSA.1 Management der Sicherheitsattribute**

140 FMT_MSA.1.1 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 Security-Administrator** durchsetzen.

***Erklärung 38*** *Die funktionale Sicherheitsanforderung FMT_MSA.1 ergibt sich aus der Abhängigkeit von FMT_MSA.3 und wird implizit für die Umsetzung des Sicherheitsziels O.ValidZert benötigt. Im Fokus der Betrachtung steht hierbei das Management der Rolle des Schlüssel-Administrators durch den Security-Administrator; die zulässigen Operationen mit den privaten Schlüsseln werden in FDP_ACC.1 und FDP_ACF.1 thematisiert.*

***Erklärung 39*** *Die Abhängigkeiten von FMT_MSA.1 – FDP_ACC.1 und FMT_SMR.1 – sind aufgenommen.*

**141 FMT_MSA.3 Initialisierung statischer Attribute**

142 FMT_MSA.3.1 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.

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

***Erklärung 40*** *Die funktionale Sicherheitsanforderung FMT_MSA.3 ergibt sich aus den Abhängigkeiten von FDP_ITC.1 und FDP_ACF.1 und wird daher implizit für die Umsetzung des Sicherheitsziels O.ValidZert benötigt. Im Fokus der Betrachtung steht hierbei das Management der Rolle des Schlüssel-Administrators durch den Security-Administrator; die zulässigen Operationen werden in FDP_ACC.1 und FDP_ACF.1 thematisiert.*

***Erklärung 41*** *Die Abhängigkeiten von FMT_MSA.3 – FMT_MSA.1 und FMT_SMR.1 – sind aufgenommen.*

**144** **FMT_SMR.1** **Sicherheitsrollen**

145 FMT_SMR.1.1 Die TSF müssen die Rollen **Schlüssel-Administrator und Security-Administrator** erhalten.

146 FMT_SMR.1.2 Die TSF müssen Benutzer mit Rollen verknüpfen können.

***Erklärung 42*** *Die funktionale Sicherheitsanforderung FMT_SMR.1 ergibt sich aus den Abhängigkeiten von FMT_MSA.1 (für die Rolle des Security-Administrators für die Konfiguration der Rechte, Rollen und Berechtigungen) und FMT_MSA.3 (für die Rolle des Schlüssel-Administrators zum Management der Referenz der privaten Schlüssel) und wird implizit für die Umsetzung des Sicherheitsziels O.ValidZert benötigt.*

***Erklärung 43*** *Die Abhängigkeit von FMT_SMR.1 – FIA_UID.1 – ist aufgenommen.*

**147** **FTP_ITC.1** **Inter-TSF Vertrauenswürdiger Kanal**

148 FTP_ITC.1.1 Die TSF müssen einen Kommunikationskanal zwischen sich und einem entfernten vertrauenswürdigen IT-Produkt bereitstellen, der logisch von den anderen Kommunikationskanälen getrennt ist und eine gesicherte Identifikation seiner Endpunkte sowie den Schutz der Daten des Kanals vor Modifizierung oder Preisgabe bereitstellt.

149 FTP_ITC.1.2 Die TSF müssen **den TSF** erlauben, eine Kommunikation über den vertrauenswürdigen Kanal einzuleiten.

150 FTP_ITC.1.3 Die TSF müssen für **die Erzeugung einer qualifizierten elektronischen Signatur** eine Kommunikation über den vertrauenswürdigen Kanal einleiten.

***Erklärung 44*** *Die funktionale Sicherheitsanforderung FTP_ITC.1 wird implizit für die Umsetzung des Sicherheitsziels O.SignaturZuf benötigt, wobei ein vertrauenswürdiger Kanal zwischen EVG und Signaturkarte aufgebaut wird.*

***Erklärung 45*** *FTP_ITC.1 hat keine Abhängigkeiten.*

### 5.1.3 Anforderungen an die Vertrauenswürdigkeit des EVG

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

152 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

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

**Tabelle 5: Funktionale Sicherheitsanforderungen an die IT-Umgebung**

| Funktionale Sicherheits-anforderung an die IT-Umgebung | Beschreibung |
|---|---|
| FCS_CKM.1[52] | Kryptographische Schlüsselgenerierung |
| FDP_ITC.1[52] | Import von Benutzerdaten ohne Sicherheitsattribute |
| FCS_CKM.4 | Zerstörung des kryptographischen Schlüssels |
| FMT_MSA.2 | Sichere Sicherheitsattribute |
| FCO_NRO.1 | Selektiver Urheberschaftsbeweis (vgl. [bos_Basis_ST]) |
| FCS_CKM.4 | Zerstörung des kryptographischen Schlüssels (vgl. [bos_Basis_ST]) |
| FCS_COP.1 (Verify) | Kyptographischer Betrieb (für die kryptographische Operation „Verifizieren“ einer qualifizierten elektronischen Signatur) (vgl. [bos_Basis_ST]) |
| FCS_COP.1 (SVVE[53]) | Kyptographischer Betrieb (für die Erzeugung einer elektronischen Signatur für Verifikations- und Validierungsergebnisse) (vgl. [bos_Basis_ST]) |
| FCS_COP.1 (VVE[54]) | Kyptographischer Betrieb (für die Verifikation eines Validierungsergebnisses) (vgl. [bos_Basis_ST]) |
| FDP_ACC.1 (Sys) | Teilweise Zugriffskontrolle (Systemsicherheit-Zugriffskontrollpolitik) (vgl. [bos_Basis_ST]) |
| FDP_ACF.1 (Sys) | Zugriffskontrolle basierend auf Sicherheitsattributen (Systemsicherheit-Zugriffskontrollpolitik) (vgl. [bos_Basis_ST]) |
| FDP_ITC.1 | Import von Benutzerdaten ohne Sicherheitsattribute (vgl. [bos_Basis_ST]) |
| FIA_UID.2 | Benutzeridentifikation vor jeglicher Aktion (vgl. [bos_Basis_ST]) |
| FMT_MSA.1 (Sys) | Management der Sicherheitsattribute (Systemsicherheit-Zugriffskontrollpolitik) (vgl. [bos_Basis_ST]) |
| FMT_MSA.2 | Sichere Sicherheitsattribute (vgl. [bos_Basis_ST]) |
| FMT_MSA.3 (Sys) | Initialisierung statischer Attribute (Systemsicherheit -Zugriffskontrollpolitik) (vgl. [bos_Basis_ST]) |
| FMT_SMR.1 (Sys) | Sicherheitsrollen (Systemsicherheit -Zugriffskontrollpolitik) (vgl. [bos_Basis_ST]) |

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

[53] Signieren von Verifikations- und Validierungs-Ergebnissen

[54] Verifizieren eines Validierungs-Ergebnisses

| Funktionale Sicherheits-anforderung an die IT-Umgebung | Beschreibung |
|---|---|
| funktionale Sicherheitsanforderungen, die an SigG-konforme sichere Signaturerstellungs-einheiten und Chipkartenleser gestellt werden, sind den Sicherheitsvorgaben bestätigter Produkte zu entnehmen (vgl. beispielsweise http://www.bundesnetzagentur.de); weitere Anforderungen werden nicht benötigt | |

**154** **FCS_CKM.1**[52] **Kryptographische Schlüsselgenerierung**

155 FCS_CKM.1.1 Die Sicherheitsfunktionen in der IT-Umgebung müssen die kryptographischen Schlüssel gemäß eines spezifizierten Algorithmus zur kryptographischen Schlüsselgenerierung **mit einem geeigneten Algorithmus zur kryptographischen Schlüsselgenerierung** und spezifizierte kryptographische Schlüssellängen**, die 2048 Bit aufweisen**, die den folgenden **Normen [RSA] und [SHA]**[51] entsprechen, generieren.

**156** **FDP_ITC.1**[52] **Import von Benutzerdaten ohne Sicherheitsattribute**

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

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

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

**160** **FCS_CKM.4** **Zerstörung des kryptographischen Schlüssels**

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

**162** **FMT_MSA.2** **Sichere Sicherheitsattribute**

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

***Erklärung 46*** *Die drei funktionalen Sicherheitsanforderungen an die IT-Umgebung – FCS_CKM.1 oder FDP_ITC.1 sowie FCS_CKM.4 und FMT_MSA.2 – ergeben sich aus den Sicherheitszielen O.ValidZert (bzgl. Schlüsselerzeugung oder -import, Zerstörung und Schlüsselmanagement des (System-) Zertifikats in OSCI-Client bzw. -Backend, auf dem OSCI-Client-Enabler resp. -Backend-Enabler betrieben werden), O.SignaturZuf (bzgl. Schlüsselimport, -zerstörung und -management des zum privaten Schlüssel korrespondierenden Zertifikats, das sich auf der Signaturkarte befindet,) O.Manipulation (bzgl. Schlüsselimport, -zerstörung und -management in Prüftool), OE.PKI (bzgl. Schlüsselerzeugung oder -import, Schlüsselzerstörung und -management für Schlüssel und korrespondierende (System-) Zertifikate in IT-Umgebung) und OE.SAK (bzgl. der Sicherstellung, dass nur sichere Sicherheitsattribute – insbesondere für die (System-) Zertifikate – akzeptiert werden). Die Ausgestaltung der Operationen der funktionalen Sicherheitsanforderungen sowie die Abhängigkeiten dieser Anforderungen sind in der IT-Umgebung zu realisieren, da Schlüsselerzeugung, -import und -löschung sowie Management der Sicherheitsattribute in der IT-Umgebung außerhalb des EVG liegt.*

***Erklärung 47*** *Die in Tabelle 5 referenzierten funktionalen Sicherheitsanforderungen an die IT-Umgebung FCO_NRO.1, FCS_CKM.4, FCS_COP.1 (Verify), FCS_COP.1 (SVVE), FCS_COP.1 (VVE), FDP_ACC.1 (Sys), FDP_ACF.1 (Sys), FDP_ITC.1, FIA_UID.2, FMT_MSA.1 (Sys), FMT_MSA.2, FMT_MSA.3 (Sys) und FMT_SMR.1 (Sys) lassen sich auf das Sicherheitsziel der IT-Umgebung OE.PKI hinsichtlich der Validierung qualifizierter Zertifikate und des unterstützenden Sicherheitsmechanismus' zur Erzeugung einer elektronischen Signatur für einen vom OSCI-Manager erzeugten und übermittelten Hashwert, für die die Basiskomponente von Governikus (vgl. [bos_Basis_ST]) benötigt wird, zurückführen.*

***Erklärung 48*** *Die funktionalen Sicherheitsanforderungen an die IT-Umgebung zu den SigG-konformen sicheren Signaturerstellungseinheiten und Chipkartenlesern, die den Sicherheitsvorgaben bestätigter Produkte zu entnehmen sind (vgl. beispielsweise http://www.bundesnetzagentur.de), lassen sich auf die Sicherheitsziele der IT-Umgebung OE.PKI und OE.ZufPIN hinsichtlich der SigG-konformen sicheren Signaturerstellungseinheiten und Chipkartenleser sowie der qualifizierten Zertifikate zurückführen; weitere Anforderungen werden nicht benötigt.*

## 5.3 Sicherheitsanforderungen an die Nicht-IT-Umgebung

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

# 6 EVG-Übersichtsspezifikation

165 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 Signaturen (Hashen und Zuführen zu signierender Dokumente zu einer sicheren Signaturerstellungseinheit);

SF2 Schutz gegen Hashwertmanipulation;

SF3 Verifikation einer qualifizierten elektronischen Signatur;

SF4 Verifikation eines OSCI-Laufzettels bei der Validierung eines qualifizierten Zertifikats;

SF5 Sichere und zuverlässige Anzeige;

SF6 Unterstützung bei der Validierung qualifizierter Zertifikate;

SF7 Identifikation und Authentisierung;

SF8 Prüftool.

## 6.1 SF1 – Unterstützung bei der Erzeugung qualifizierter elektronischer Signaturen

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

- Der OSCI-Client-Enabler wendet auf Initiative des Benutzers des OSCI-Client-Enablers auf die zu signierende Daten gemäß OSCI-Transport (vgl. Abschnitt 2.2) die Hashfunktionen SHA-1[50], SHA-256, SHA-512 sowie RIPEMD 160 an und führt den erzeugten Hashwert einer angeschlossenen sicheren Signaturerstellungseinheit zu, die eine qualifizierte elektronische Signatur erzeugt und an den OSCI-Client-Enabler zurückliefert.[55]
- Vor jeder Signaturerzeugung erfolgt der EVG die Eingabe einer PIN.
- Signierte Daten werden im inneren Umschlag des OSCI-Protokolls transportiert. Daten, die dem OSCI-Client-Enabler vom OSCI-Client zum Signieren übergeben werden, sind in einer XML-Struktur codiert.

## 6.2 SF2 – Schutz gegen Hashwertmanipulation

167 Die Sicherheitsfunktion SF2 „Schutz gegen Hashwertmanipulation“ ist wie folgt definiert:

- Der OSCI-Client-Enabler vergleicht den von der sicheren Signaturerstellungseinheit signierten Hashwert (vgl. SF1), den er von der Signaturkarte erhält, mit dem Hashwert, den er an die Signaturkarte gesendet hatte.

[55] Dazu ist am Arbeitsplatz-PC in der IT-Umgebung ein Chipkartenleser installiert.

- Dazu werden folgende Schritte ausgeführt:
  - Zuerst wird die Signatur mit dem zum privaten Signaturschlüssel korrespondierenden öffentlichen Schlüssel verifiziert. Kann die Signatur nicht verifiziert werden, erfolgt eine Fehlermeldung und der Signaturvorgang wird abgebrochen.
  - Kann die Signatur verifiziert werden, erfolgt ein Vergleich der beiden Hashwerte. Sind die beiden Hashwerte nicht identisch, erfolgt eine Fehlermeldung und der Signaturvorgang wird abgebrochen, da der Hashwert zwischen EVG und Signaturkarte manipuliert wurde.
- Das für die Verifikation benötigte Zertifikat lädt der OSCI-Client-Enabler von der Signaturkarte.

## 6.3 SF3 – Verifikation einer qualifizierten elektronischen Signatur

168 Die Sicherheitsfunktion SF3 „Verifikation einer qualifizierten elektronischen Signatur“ ist wie folgt definiert:

- OSCI-Client-Enabler und -Backend-Enabler verifizieren eine qualifizierte elektronische Signaturen aus dem inneren Umschlag des OSCI-Protokolls. Initiator ist beim OSCI-Client-Enabler der Benutzer und beim OSCI-Backend-Enabler das OSCI-Backend in der IT-Umgebung.
- Die Verifikation nutzt neben der qualifizierten elektronischen Signatur das mitgelieferte zugehörige Zertifikat mit dem Prüfschlüssel sowie den Verifikationsalgorithmus RSA und die Hashfunktionen SHA-1[50], SHA-256, SHA-512 sowie RIPEMD 160. Benutzte Schlüssellängen sind entsprechend der X.509-Zertifikate derzeit 1024 oder 2048 Bit.
- Während beim OSCI-Client-Enabler das Verifikationsergebnis via SF5 angezeigt wird, übergibt der OSCI-Backend-Enabler das Verifikationsergebnis an das angeschlossene OSCI-Backend in der IT-Umgebung.

## 6.4 SF4 – Verifikation eines OSCI-Laufzettels bei der Validierung eines qualifizierten Zertifikats

169 Die Sicherheitsfunktion SF4 „Verifikation eines OSCI-Laufzettels bei der Validierung eines qualifizierten Zertifikats“ ist wie folgt definiert:[56]

- OSCI-Client-Enabler und -Backend-Enabler verifizieren die elektronische Signatur des OSCI-Laufzettels mit dem (System-)Zertifikat des OSCI-Managers. Initiator ist beim OSCI-Client-Enabler der Benutzer und beim OSCI-Backend-Enabler das OSCI-Backend in der IT-Umgebung.

[56] OSCI-Client-Enabler und -Backend-Enabler validieren nicht selber, sondern nutzen das Ergebnis der Validierung vom OSCI-Manager, welches im OSCI-Laufzettel – mit einer elektronischen Signatur versehen – enthalten ist.

- OSCI-Client-Enabler und -Backend-Enabler führen einen Plausibilitätscheck durch, in der OSCI-Client-Enabler bzw. -Backend-Enabler prüfen, ob das im OSCI-Laufzettel enthaltene Ergebnis der Zertifikats-Statusprüfung zum Zertifikat der OSCI-Nachricht passt.
- Während beim OSCI-Client-Enabler das Verifikationsergebnis via SF5 angezeigt wird, übergibt der OSCI-Backend-Enabler das Verifikationsergebnis an das angeschlossene OSCI-Backend in der IT-Umgebung.

## 6.5 SF5 – Sichere und zuverlässige Anzeige

170 Die Sicherheitsfunktion SF5 „Sichere und zuverlässige Anzeige“ ist wie folgt definiert:

- Der OSCI-Client-Enabler bietet eine sichere Anzeige von folgenden zu signierenden und signierten Daten:
  - plain-text (UTF-8-codiert);
  - tiff-Daten.
- Darüber hinaus bietet der OSCI-Client-Enabler eine sichere Anzeige weiterer signatur-relevanten Informationen;
  - Verweis, auf welche Daten sich eine Signatur bezieht;
  - der Signatur zugeordnete Signaturschlüssel-Inhaber;
  - Inhalte des zugehörigen qualifizierten Zertifikats.
- Der OSCI-Client-Enabler bietet des Weiteren hinreichende Anzeigen für folgende Prozesse:
  - Signierprozess:
    - Das Erzeugen einer Signatur wird vorher eindeutig angezeigt.
    - Das zur Signatur korrespondierende Zertifikat wird angezeigt.
    - Das Verifikationsergebnis zum Schutz vor Hashwertmanipulation (vgl. SF2) wird angezeigt.
  - Verifikationsprozess: Das Ergebnis der Verifikation wird angezeigt, d. h. es wird angezeigt, ob Daten unverändert sind.
  - Validierungsprozess: Das Ergebnis der Validierung wird angezeigt, d. h. es wird angezeigt, ob die nachgeprüften qualifizierten Zertifikate im jeweiligen Zertifikatverzeichnis zum angegebenen Zeitpunkt vorhanden und nicht gesperrt waren.

## 6.6 SF6 – Unterstützung bei der Validierung qualifizierter Zertifikate

171 Die Sicherheitsfunktion SF6 „Unterstützung bei der Validierung qualifizierter Zertifikate“ ist wie folgt definiert:

- Der OSCI-Manager führt in der OSCI-Rolle des OSCI-Intermediärs die Statusprüfung eines qualifizierten Zertifikats durch. Dazu greift der OSCI-Manager auf eine Basiskomponente in der IT-Umgebung zu, wobei der OSCI-Manager zusammen mit dem Kernsystem der Basiskomponente innerhalb eines vertrauenswürdigen Netzes betrieben wird: Der OSCI-Manager sendet einen Request an das Kernsystem – das Request umfasst neben dem nachzuprüfenden Zertifikat die SystemID (Identifier des anfragenden Systems) des OSCI-Managers sowie die OperationID (Identifier der auszuführenden Operation) für das Validieren – und empfängt das Response mit dem Validierungsergebnis.
- Der OSCI-Manager interpretiert die Antwort der Basiskomponente und generiert ein eigenes Ergebnis, das der OSCI-Manager im OSCI-Laufzettel ablegt.
- Den OSCI-Laufzettel versieht der OSCI-Manager mit einer elektronischen Signatur: Dazu
  - führt der OSCI-Manager die zu signierenden Daten den Hashfunktionen SHA-1[50], SHA-256, SHA-512 sowie RIPEMD 160 zu,
  - übergibt den erzeugten Hashwert dem Kernsystem der Basiskomponente, welches die elektronische Signatur für den OSCI-Manager erzeugt und an den OSCI-Manager zurückliefert.[17]
- Daraufhin übergibt der OSCI-Manager im Rahmen des OSCI-Protokolls diesen OSCI-Laufzettel an den OSCI-Client-Enabler bzw. an den OSCI-Backend-Enabler.

## 6.7 SF7 – Identifikation und Authentisierung

172 Die Sicherheitsfunktion SF7 „Identifikation und Authentisierung“ zur Realisierung der Zugriffskontrollpolitik (vgl. Abschnitt 5.1.1) sowie zur Administration des OSCI-Managers (vgl. Abschnitt 3.1) ist wie folgt definiert:[57]

- Bevor ein Schlüssel-Administrator im OSCI-Manager die Referenz des privaten Schlüssel zur Absicherung der Systemsicherheit, mit dem der OSCI-Laufzettel signiert wird, speichern oder löschen kann, muss er sich gegenüber dem OSCI-Manager identifizieren und authentisieren.
- Bevor ein Security-Administrator den OSCI-Manager – in Zusammenarbeit mit dem Revisor – konfiguriert (Rechte der Rollen setzen, ändern und löschen, Administratoren-Rollen konfigurieren), muss er sich gegenüber OSCI-Manager identifizieren und authentisieren.
- Zur Güte des Passwortes realisiert der EVG:
  - keine Trivialpasswörter (z. B. „BBBBBBBB“ oder „12345678“);

[57] Der OSCI-Manager versieht den OSCI-Laufzettel mit einer elektronischen Signatur, dessen privater Schlüssel durch die in Abschnitt 5.1.1 definierte Zugriffskontrollpolitik abgesichert wird.

- o mindestens ein Zeichen pro Passwort, das kein Buchstabe ist (Sonderzeichen oder Zahl);
- o mindestens 8 Zeichen lang.

## 6.8 SF8 – Prüftool

173 Die Sicherheitsfunktion SF8 „Prüftool“ zur Gewährleistung der Integrität des OSCI-Client-Enablers ist wie folgt definiert:

- Das Prüftool überprüft die elektronische Signatur der JAR-Files des OSCI-Client-Enablers.[58]
- Die zugehörigen Zertifikate des Herstellers, die die öffentlichen Schlüssel zwecks Verifikation enthalten, sind im Prüftool enthalten.
- Das Prüftool kennt die Dateinamen aller JAR-Files, die überprüft werden müssen.
- Dem Anwender wird zu jedem überprüften JAR-File der Dateiname, der Dateipfad, die Version, das jeweilige Prüfergebnis (Signatur korrekt, Signatur nicht korrekt) sowie das Gesamtergebnis (Produktintegrität bestätigt, Produktintegrität nicht bestätigt) angezeigt.
- Den Dateipfad der JAR-Files ermittelt das Prüftool aus einem Übergabeparameter und dem in Java Web Start eingetragenen Pfad des Caches.
- Werden die JAR-Archive vom Prüftool nicht gefunden, kann der Anwender den/die Speicherort/e über den Java-File-Explorer auswählen.

174 Das Prüftool ist ein Java-Applet, das vom Hersteller signiert ist. Genutzte Hashfunktion ist SHA-256 (Mechanismenstärke „hoch“), genutzter Verifikationsalgorithmus ist RSA mit 1024 bzw. 2048 Bit[42] Schlüssellänge.

## 6.9 Maßnahmen zur Vertrauenswürdigkeit

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

**Tabelle 6: Maßnahmen zur Erfüllung von EAL3+**

| Anforderungen gemäß EAL3+ | | Maßnahmen der Entwickler |
|---|---|---|
| Konfigurations-management | ACM_CAP.3 | Einsatz eines QM-Systems inklusive Konfigurationskontrolle |
| | ACM_SCP.1 | |
| Auslieferung | ADO_DEL.2 | Dokumentation der zum Schutz des EVG bei |

[58] Dazu wird der OSCI-Client-Enabler als signiertes JAR-Archiv ausgeliefert, vgl. Abschnitt 2.7.

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

# 7 PP-Postulate

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

# 8 Erklärungen

## 8.1 Erklärung der organisatorischen Sicherheitspolitiken

177 Der OSCI-Client-Enabler ist eine Funktionsbibliothek zum Erzeugen und Prüfen qualifizierter elektronischer Signaturen samt Anzeige. Der OSCI-

Backend-Enabler ist eine Funktionsbibliothek zum Prüfen qualifizierter elektronischer Signaturen ohne Anzeige.

178 In Abschnitt 2.5 ist beschrieben, in welchem Umfang die Sicherheitsanforderungen des SigG und der SigV an Signaturanwendungskomponenten vom EVG erfüllt werden und welcher Anteil von der IT-Umgebung umgesetzt werden muss.

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

- Erzeugung von Signaturen:
  - Der OSCI-Client-Enabler muss beim Erzeugen einer Signatur auf die zu signierenden Daten eine Hashfunktion gemäß OSCI-Transport (vgl. Abschnitt 2.2) anwenden und den erzeugten Hashwert der angeschlossenen sicheren Signaturerstellungseinheit zuführen.
  - Der OSCI-Client-Enabler muss beim Erzeugen einer Signatur gewährleisten, dass das Erzeugen einer Signatur vorher eindeutig angezeigt wird.
  - Der OSCI-Client-Enabler muss beim Erzeugen einer Signatur gewährleisten, dass erkennbar ist, auf welche Daten sich die Signatur bezieht.
  - Der OSCI-Client-Enabler muss beim Erzeugen einer Signatur gewährleisten, dass bei Bedarf der Inhalt der zu signierenden Daten hinreichend zu erkennen ist.
- Prüfung von Signaturen:
  - OSCI-Client-Enabler und OSCI-Backend-Enabler müssen qualifizierte elektronische Signaturen prüfen.
  - OSCI-Client-Enabler und OSCI-Backend-Enabler müssen hinsichtlich der Validierung eine Plausibilitätsprüfung durchführen.
  - Der OSCI-Manager führt die Validierung mittels der Basiskomponente durch.
  - Der OSCI-Client-Enabler muss beim Prüfen einer Signatur gewährleisten, dass erkennbar wird, auf welche Daten sich die Signatur bezieht.
  - Der OSCI-Client-Enabler muss beim Prüfen einer Signatur gewährleisten, dass erkennbar wird, ob die Daten unverändert sind.
  - Der OSCI-Client-Enabler muss beim Prüfen einer Signatur gewährleisten, dass bei Bedarf der Inhalt der signierten Daten hinreichend zu erkennen ist.
  - Der OSCI-Client-Enabler muss beim Prüfen einer Signatur gewährleisten, dass erkennbar wird, welchem Signaturschlüssel-Inhaber die Signatur zuzuordnen ist.

- Der OSCI-Client-Enabler muss beim Prüfen einer Signatur gewährleisten, dass erkennbar wird, welche Inhalte das qualifizierte Zertifikat, auf dem die Signatur beruht, aufweisen.
- Der OSCI-Client-Enabler 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.
- OSCI-Client-Enabler und -Backend-Enabler müssen beim Prüfen einer Signatur gewährleisten, dass die Korrektheit der Signatur zuverlässig geprüft wird.

▪ Schutz vor unbefugter Veränderung:

- Für den OSCI-Client-Enabler wird ein Prüftool zur Verfügung gestellt (EVG-Umfang), um die Integrität zu gewährleisten.

180 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 Signaturen:

- Die sichere Signaturerstellungseinheit muss gewährleisten, dass eine Signatur nur durch die berechtigt signierende Person erfolgt.
- Sichere Signaturerstellungseinheit und Chipkartenleser müssen gewährleisten, dass die Identifikationsdaten nicht preisgegeben und nur auf der jeweiligen sicheren Signaturerstellungseinheit gespeichert werden.

▪ Prüfung von Signaturen:

- Die Basiskomponente in der IT-Umgebung muss beim Prüfen einer Signatur gewährleisten, dass festgestellt wird, ob die nachgeprüften qualifizierten Zertifikate im jeweiligen Zertifikatverzeichnis zum angegebenen Zeitpunkt vorhanden und nicht gesperrt waren.

▪ Schutz vor unbefugter Veränderung:

- Sicherheitstechnische Veränderungen an OSCI-Manager sowie OSCI-Client-Enabler und -Backend-Enabler müssen für den Administrator bei den Serverkomponenten und den Benutzer bei den Clientkomponenten erkennbar werden (vgl. Annahmen A.ServerBetrieb und A.ClientBetrieb).

## 8.2 Erklärung der Sicherheitsziele

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

- Das Sicherheitsziel für die Umgebung OE.PKI zielt auf die gleichnamige Annahme A.PKI ab, wobei zu berücksichtigen ist, dass OE.PKI auch für die organisatorischen Sicherheitspolitiken P.SignaturZuf (für die Erzeugung einer qualifizierten elektronischen Signatur durch die sichere Signaturerstellungseinheit mittels Chipkartenleser), P.ValidZert (für die Gültigkeitsprüfung durch obige Funktionalitäten der Basiskomponenten, für die Existenz qualifizierter Zertifikate sowie die kryptographischen Schlüssel und (System-)Zertifikate zur Gewährleistung der Systemsicherheit) sowie P.VerifySign (für Existenz qualifizierter Zertifikate) benötigt werden. Zudem wehrt OE.PKI die Bedrohung TE.RatePIN durch Verwendung einer geeigneten Signaturkarte ab.
- Das Sicherheitsziel für die Umgebung OE.SAK zielt auf die gleichnamige Annahme A.SAK ab.
- Das Sicherheitsziel für die Umgebung OE.ServerBetrieb zielt auf die gleichnamige Annahme A.ServerBetrieb ab und ist zur Realisierung der organisatorischen Sicherheitspolitik P.ValidZert (für die Gewährleistung der Systemsicherheit aufgrund der Realisierung der Validierung innerhalb des verteilten Systems – d. h. dem Management des OSCI-Managers zum Signieren des OSCI-Laufzettels durch das Kernsystem und des (System-) Zertifikats im OSCI-Backend-Enabler zur Verifikation des OSCI-Laufzettels) notwendig.
- Das Sicherheitsziel für die Umgebung OE.ClientBetrieb zielt auf die gleichnamige Annahme A.ClientBetrieb ab und ist zur Realisierung der organisatorischen Sicherheitspolitik P.ValidZert (für die Gewährleistung der Systemsicherheit aufgrund der Realisierung der Validierung innerhalb des verteilten Systems – d. h. dem Management des (System-) Zertifikats im OSCI-Client-Enabler zur Verifikation des OSCI-Laufzettels) notwendig. Zudem wehrt OE.ClientBetrieb die Bedrohung TE.SpähePIN durch geeignete Auflagen und Hinweise an den Signaturschlüssel-Inhaber zur Nutzung seiner Signaturkarte ab
- Das Sicherheitsziel für die Umgebung OE.ZufPIN zielt auf die gleichnamige Annahme A.ZufPIN ab.
- Das Sicherheitsziel O.SignaturZuf deckt die organisatorische Sicherheitspolitik P.SignaturZuf zur Erzeugung einer qualifizierten elektronischen Signatur ab und präzisiert, dass der OSCI-Client-Enabler die zu signierenden Daten gemäß OSCI-Transport der Hashfunktion zuführt und den Hashwert einer sicheren Signaturerstellungseinheit in der IT-Umgebung (vgl. OE.PKI) zugeführt. Zusätzlich wird durch die Verifikation der zuvor durch die Signaturkarte generierte qualifizierte elektronische Signatur mit dem auf der Signaturkarte befindlichen Zertifikat gewährleistet, dass für die richtigen Daten eine Signatur erzeugt wurde.
- Das Sicherheitsziel O.Anzeige deckt die organisatorische Sicherheitspolitik P.Anzeige zur sicheren und zuverlässigen Anzeige bei der Erzeugung und Prüfung qualifizierter elektronischer Signaturen beim OSCI-Client-Enabler ab. Dabei wird durch die Verifikation festgestellt, ob die Daten unverändert sind. Die Anzeige umfasst nicht nur, was signiert wird und

wurde, sondern auch ergänzende Informationen zur Nachricht, wie Zertifikatsinhalt, Signaturschlüssel-Inhaber und Verifikations- und Validierungsergebnisse.

- Das Sicherheitsziel O.ValidZert deckt die organisatorische Sicherheitspolitik P.ValidZert zur Validierung qualifizierter Zertifikate ab und präzisiert die Aufgabenteilung. Zu berücksichtigen ist, dass die wesentlichen Aufgaben bei der Validierung in der IT-Umgebung durch die Basiskomponente (vgl. Sicherheitsziel für die IT-Umgebung OE.PKI) geleistet wird und dass zur Gewährleistung der Systemsicherheit (innerhalb des verteilten System) die Sicherheitsziele für die IT-Umgebung OE.ServerBetrieb und OE.ClientBetrieb benötigt werden.
- Das Sicherheitsziel O.VerifySign deckt die organisatorische Sicherheitspolitik P.VerifySign zur Prüfung einer qualifizierten elektronischen Signatur ab und präzisiert, dass die Verifikation durch die Prüfung der Integrität und der Authentizität erfolgt (qualifizierte Zertifikate via Sicherheitsziel für die IT-Umgebung OE.PKI).
- Das Sicherheitsziel O.Manipulation deckt die organisatorische Sicherheitspolitik P.Manipulation zum Schutz vor unbefugter Veränderung des OSCI-Client-Enablers ab.

**Tabelle 7: Zuordnung Sicherheitsproblemdefinition zu -zielen**

| Sicherheitsproblemdefinition | zugehörige Sicherheitsziele |
|---|---|
| A.PKI | OE.PKI |
| A.SAK | OE.SAK |
| A.ServerBetrieb | OE.ServerBetrieb |
| A.ClientBetrieb | OE.ClientBetrieb |
| A.ZufPIN | OE.ZufPIN |
| TE.RatePIN | OE.PKI |
| TE.SpähePIN | OE.ClientBetrieb |
| P.SignaturZuf | O.SignaturZuf, OE.PKI |
| P.Anzeige | O.Anzeige |
| P.ValidZert | O.ValidZert, OE.PKI, OE.ServerBetrieb, OE.ClientBetrieb |
| P.VerifySign | O.VerifySign, OE.PKI |
| P.Manipulation | O.Manipulation |

## 8.3 Erklärung der Sicherheitsanforderungen

### 8.3.1 Erklärung zu den funktionalen Sicherheitsanforderungen

182 Wie die Sicherheitsziele, die sich auf IT beziehen, durch die funktionalen Sicherheitsanforderungen erfüllt werden, ist im Folgenden dargestellt und in Tabelle 8 und Tabelle 9 hinsichtlich des EVG und in Tabelle 10 und Tabelle 11 hinsichtlich der IT-Umgebung zusammengefasst:

- Die in FCS_COP.1.1/Hash spezifizierte Hashfunktion wird gemäß OSCI-Transport genutzt (vgl. Abschnitt 2.2).
- Die funktionale Sicherheitsanforderung FCS_COP.1 (Hash) wird für die Umsetzung des Sicherheitsziels O.SignaturZuf benötigt.
- Die funktionale Sicherheitsanforderung FCS_COP.1 (VSign) wird für die Umsetzung des Sicherheitsziels O.SignaturZuf in der Weise benötigt, dass eine zuvor erzeugte qualifizierte elektronische Signatur mit Hilfe des zum privaten Schlüssel korrespondierenden Zertifikats, das sich auf der Signaturkarte befindet, verifiziert wird.
- Die funktionale Sicherheitsanforderung FDP_SVR.1 wird für die Umsetzung des Sicherheitsziels O.Anzeige benötigt.
- Die funktionale Sicherheitsanforderung FCS_COP.1 (Valid) wird für die Umsetzung des Sicherheitsziels O.ValidZert in der Weise benötigt, dass OSCI-Client-Enabler und -Backend-Enabler die Signatur des OSCI-Laufzettels (vom OSCI-Manager mit Hilfe der Basiskomponente erzeugt) mit dem (System-)Zertifikat verifizieren müssen.
- Die funktionale Sicherheitsanforderung FCS_COP.1 (OSCI) wird für die Umsetzung des Sicherheitsziels O.ValidZert in der Weise benötigt, dass der OSCI-Manager auf den OSCI-Laufzettel die Hashfunktion SHA-1, SHA-256 und SHA-512 sowie RIPEMD 160 anwendet und durch das Kernsystem der Basiskomponente signieren lässt, so dass die elektronische Signatur des OSCI-Laufzettels dann von OSCI-Client-Enabler und -Backend-Enabler mit dem – dem OSCI-Manager zugeordneten – (System-) Zertifikat verifiziert werden kann.
- Die funktionale Sicherheitsanforderung FDP_ACC.1 ergibt sich aus der Abhängigkeit von FDP_ITC.1 und wird daher implizit für die Umsetzung des Sicherheitsziels O.ValidZert in der Weise benötigt, dass der OSCI-Manager den OSCI-Laufzettel durch das Kernsystem der Basiskomponente signieren lässt und dazu den zu nutzenden Schlüssel referenziert. In dieser Sicherheitsanforderung werden Subjekt, Objekt sowie zulässige Operationen zwischen Subjekten und Objekten hinsichtlich der Systemsicherheit-Zugriffskontrollpolitik definiert.
- Die funktionale Sicherheitsanforderung FDP_ACF.1 ergibt sich aus der Abhängigkeit von FDP_ACC.1 und wird daher implizit für die Umsetzung des Sicherheitsziels O.ValidZert in der Weise benötigt, dass der OSCI-Manager den OSCI-Laufzettel durch das Kernsystem der Basiskomponente signieren lässt und dazu den zu nutzenden Schlüssel referenziert.

In dieser Sicherheitsanforderung wird thematisiert, dass eine zulässige Operation (vgl. FDP_ACC.1) erst nach erfolgreicher Authentisierung des Schlüssel-Administrators erfolgen kann.

- Die funktionale Sicherheitsanforderung FDP_ITC.1 wird für die Umsetzung des Sicherheitsziels O.ValidZert in der Weise benötigt, dass der OSCI-Manager den OSCI-Laufzettel durch das Kernsystem der Basiskomponente signieren lässt – und dazu den zu nutzenden Schlüssel referenziert –, so dass die Signatur dann von OSCI-Client-Enabler und -Backend-Enabler mit dem (System-)Zertifikat verifizieren werden kann.
- Die funktionale Sicherheitsanforderung FIA_UID.2 ergibt sich aus der Abhängigkeit von FMT_SMR.1, wobei statt FIA_UID.1 die hierarchische Anforderung FIA_UID.2 genutzt wird. FIA_UID.2 wird damit implizit für die Umsetzung des Sicherheitsziels O.ValidZert benötigt.
- Die funktionale Sicherheitsanforderung FIA_UAU.2 wird – wie FIA_UID.2 auch – für die Umsetzung des Sicherheitsziels O.ValidZert benötigt.
- Die funktionale Sicherheitsanforderung FMT_MSA.1 ergibt sich aus der Abhängigkeit von FMT_MSA.3 und wird implizit für die Umsetzung des Sicherheitsziels O.ValidZert benötigt. Im Fokus der Betrachtung steht hierbei das Management der Rolle des Schlüssel-Administrators durch den Security-Administrator; die zulässigen Operationen mit den privaten Schlüsseln werden in FDP_ACC.1 und FDP_ACF.1 thematisiert.
- Die funktionale Sicherheitsanforderung FMT_MSA.3 ergibt sich aus den Abhängigkeiten von FDP_ITC.1 und FDP_ACF.1 und wird daher implizit für die Umsetzung des Sicherheitsziels O.ValidZert benötigt. Im Fokus der Betrachtung steht hierbei das Management der Rolle des Schlüssel-Administrators durch den Security-Administrator; die zulässigen Operationen werden in FDP_ACC.1 und FDP_ACF.1 thematisiert.
- Die funktionale Sicherheitsanforderung FMT_SMR.1 ergibt sich aus den Abhängigkeiten von FMT_MSA.1 (für die Rolle des Security-Administrators für die Konfiguration der Rechte, Rollen und Berechtigungen) und FMT_MSA.3 (für die Rolle des Schlüssel-Administrators zum Management der Referenz der privaten Schlüssel) und wird implizit für die Umsetzung des Sicherheitsziels O.ValidZert benötigt.
- Die funktionale Sicherheitsanforderung FCS_COP.1 (Verify) wird für die Umsetzung des Sicherheitsziels O.VerifySign benötigt.
- Die funktionale Sicherheitsanforderung FCS_COP.1 (Tool) wird für die Umsetzung des Sicherheitsziels O.Manipulation benötigt.
- Die funktionale Sicherheitsanforderung FTP_ITC.1 wird implizit für die Umsetzung des Sicherheitsziels O.SignaturZuf benötigt, wobei ein vertrauenswürdiger Kanal zwischen EVG und Signaturkarte aufgebaut wird.
- Die drei funktionalen Sicherheitsanforderungen an die IT-Umgebung – FCS_CKM.1 oder FDP_ITC.1 sowie FCS_CKM.4 und FMT_MSA.2 – ergeben sich aus den Sicherheitszielen O.ValidZert (bzgl. Schlüsselerzeugung oder -import, Zerstörung und Schlüsselmanagement des (System-)

Zertifikats in OSCI-Client bzw. -Backend, auf dem OSCI-Client-Enabler resp. -Backend-Enabler betrieben werden), O.SignaturZuf (bzgl. Schlüsselimport, -zerstörung und -management des zum privaten Schlüssel korrespondierenden Zertifikats, das sich auf der Signaturkarte befindet,) O.Manipulation (bzgl. Schlüsselimport, -zerstörung und -management in Prüftool), OE.PKI (bzgl. Schlüsselerzeugung oder -import, Schlüsselzerstörung und -management für Schlüssel und korrespondierende (System-) Zertifikate in IT-Umgebung) und OE.SAK (bzgl. der Sicherstellung, dass nur sichere Sicherheitsattribute – insbesondere für die (System-) Zertifikate – akzeptiert werden). Die Ausgestaltung der Operationen der funktionalen Sicherheitsanforderungen sowie die Abhängigkeiten dieser Anforderungen sind in der IT-Umgebung zu realisieren, da Schlüsselerzeugung, -import und -löschung sowie Management der Sicherheitsattribute in der IT-Umgebung außerhalb des EVG liegt.

- Die in Tabelle 5 referenzierten funktionalen Sicherheitsanforderungen an die IT-Umgebung FCO_NRO.1, FCS_CKM.4, FCS_COP.1 (Verify), FCS_COP.1 (SVVE), FCS_COP.1 (VVE), FDP_ACC.1 (Sys), FDP_ACF.1 (Sys), FDP_ITC.1, FIA_UID.2, FMT_MSA.1 (Sys), FMT_MSA.2, FMT_MSA.3 (Sys) und FMT_SMR.1 (Sys) lassen sich auf das Sicherheitsziel der IT-Umgebung OE.PKI hinsichtlich der Validierung qualifizierter Zertifikate und des unterstützenden Sicherheitsmechanismus' zur Erzeugung einer elektronischen Signatur für einen vom OSCI-Manager erzeugten und übermittelten Hashwert, für die die Basiskomponente von Governikus (vgl. [bos_Basis_ST]) benötigt wird, zurückführen.
- Die funktionalen Sicherheitsanforderungen an die IT-Umgebung zu den SigG-konformen sicheren Signaturerstellungseinheiten und Chipkartenlesern, die den Sicherheitsvorgaben bestätigter Produkte zu entnehmen sind (vgl. beispielsweise http://www.bundesnetzagentur.de), lassen sich auf die Sicherheitsziele der IT-Umgebung OE.PKI und OE.ZufPIN hinsichtlich der SigG-konformen sicheren Signaturerstellungseinheiten und Chipkartenleser sowie der qualifizierten Zertifikate zurückführen; weitere Anforderungen werden nicht benötigt.

**Tabelle 8: Zuordnung Sicherheitsziele zu Sicherheitsanforderungen an den EVG**

| Sicherheitsziele | funktionale Sicherheitsanforderungen an den EVG |
|---|---|
| O.SignaturZuf | FCS_COP.1 (Hash), FCS_COP.1 (VSign), FTP_ITC.1 |
| O.Anzeige | FDP_SVR.1 |
| O.ValidZert | FCS_COP.1 (Valid), FCS_COP.1 (OSCI), FDP_ACC.1, FDP_ACF.1, FDP_ITC.1, FIA_UID.2, FIA_UAU.2, FMT_MSA.1, FMT_MSA.3, FMT_SMR.1 |
| O.VerifySign | FCS_COP.1 (Verify) |
| O.Manipulation | FCS_COP.1 (Tool) |

**Tabelle 9: Zuordnung fkt. Sicherheitsanforderungen zu Sicherheitszielen**

| funktionale Sicherheitsanforderungen an den EVG | Sicherheitsziele |
|---|---|
| FCS_COP.1 (Hash) | O.SignaturZuf |
| FCS_COP.1 (Valid) | O.ValidZert |
| FCS_COP.1 (OSCI) | O.ValidZert |
| FCS_COP.1 (Verify) | O.VerifySign |
| FCS_COP.1 (VSign) | O.SignaturZuf |
| FCS_COP.1 (Tool) | O.Manipulation |
| FDP_SVR.1 | O.Anzeige |
| FDP_ACC.1 | O.ValidZert |
| FDP_ACF.1 | O.ValidZert |
| FDP_ITC.1 | O.ValidZert |
| FIA_UID.2 | O.ValidZert |
| FIA_UAU.2 | O.ValidZert |
| FMT_MSA.1 | O.ValidZert |
| FMT_MSA.3 | O.ValidZert |
| FMT_SMR.1 | O.ValidZert |
| FTP_ITC.1 | O.SignaturZuf |

**Tabelle 10: Zuordnung Sicherheitsziele zu Sicherheitsanforderungen an die IT-Umgebung**

| Sicherheitsziele | funktionale Sicherheitsanforderungen an die IT-Umgebung |
|---|---|
| O.SignaturZuf | FDP_ITC.1, FCS_CKM.4, FMT_MSA.2 |
| O.Anzeige | - |
| O.ValidZert | FCS_CKM.1 oder FDP_ITC.1, FCS_CKM.4, FMT_MSA.2 |
| O.VerifySign | - |
| O.Manipulation | FCS_CKM.1 oder FDP_ITC.1, FCS_CKM.4, FMT_MSA.2 |

| | |
|---|---|
| OE.PKI | zu sicheren Signaturerstellungseinheiten, zu Chipkartenlesern, zu qualifizierten Zertifikaten: vgl. Sicherheitsvorgaben bestätigter Produkte<br>zu privaten Schlüsseln und (System-)Zertifikaten: FCS_CKM.1 oder FDP_ITC.1, FCS_CKM.4, FMT_MSA.2<br>zur Validierung eines qualifizierten Zertifikats und zur Erzeugung einer elektronischen Signatur: FCO_NRO.1, FCS_CKM.4, FCS_COP.1 (Verify), FCS_COP.1 (SVVE), FCS_COP.1 (VVE), FDP_ACC.1 (Sys), FDP_ACF.1 (Sys), FDP_ITC.1, FIA_UID.2, FMT_MSA.1 (Sys), FMT_MSA.2, FMT_MSA.3 (Sys) und FMT_SMR.1 (Sys) |
| OE.SAK | FMT_MSA.2 |
| OE.ZufPIN | vgl. Sicherheitsvorgaben bestätigter Produkte |

**Tabelle 11: Zuordnung fkt. Sicherheitsanforderungen an die IT-Umgebung zu Sicherheitszielen**

| funktionale Sicherheitsanforderungen an die IT-Umgebung | Sicherheitsziele |
|---|---|
| FCS_CKM.1 oder FDP_ITC.1 | O.ValidZert, O.SignaturZuf, O.Manipulation, OE.PKI (bzgl. privater Schlüssel und (System-)Zertifikate) |
| FCS_CKM.4 | O.ValidZert, O.SignaturZuf, O.Manipulation, OE.PKI (bzgl. privater Schlüssel und (System-)Zertifikate) |
| FMT_MSA.2 | O.ValidZert, O.SignaturZuf, O.Manipulation, OE.PKI (bzgl. privater Schlüssel und (System-)Zertifikate), OE.SAK |
| FCO_NRO.1, FCS_CKM.4, FCS_COP.1 (Verify), FCS_COP.1 (SVVE), FCS_COP.1 (VVE), FDP_ACC.1 (Sys), FDP_ACF.1 (Sys), FDP_ITC.1, FIA_UID.2, FMT_MSA.1 (Sys), FMT_MSA.2, FMT_MSA.3 (Sys) und FMT_SMR.1 (Sys) | OE.PKI |
| funktionale Sicherheitsanforderungen, die an SigG-konforme sichere Signaturerstellungseinheiten und Chipkartenleser gestellt werden, sind den Sicherheitsvorgaben bestätigter Produkte zu entnehmen | OE.PKI (sichere Signaturerstellungseinheiten und Chipkartenleser)<br>OE.ZufPIN |

### 8.3.2 Erfüllung der Abhängigkeiten

183 Die EVG-Abhängigkeiten sind berücksichtigt, wie im Folgenden ausgeführt und in Tabelle 12 zusammenfassend dargestellt:

- Die Abhängigkeiten der funktionalen Sicherheitsanforderung FCS_COP.1 (Hash) sind nicht erfüllt, da keine Schlüssel involviert sind (weder Schlüsselerzeugung gemäß FCS_CKM.1 oder Schlüsselimport gemäß FDP_ITC.1 noch Zerstörung eines Schlüssels gemäß FCS_CKM.4) und daher kein Schlüsselmanagement gemäß FMT_MSA.2 notwendig ist.
- Die Abhängigkeiten der funktionalen Sicherheitsanforderung FCS_COP.1 (VSign) – Schlüsselimport gemäß FDP_ITC.1, Zerstörung eines Schlüssels gemäß FCS_CKM.4 und Schlüsselmanagement gemäß FMT_MSA.2) – sind in der IT-Umgebung für die Signaturkarte zu realisieren; eine Schlüsselerzeugung gemäß FCS_CKM.1 ist nicht anwendbar, da Zertifikate auf der Signaturkarte abgespeichert, dort aber nicht erzeugt werden.
- FDP_SVR.1 hat keine Abhängigkeiten.
- Die Abhängigkeiten der funktionalen Sicherheitsanforderung FCS_COP.1 (Valid) – Schlüsselerzeugung gemäß FCS_CKM.1 oder Schlüsselimport gemäß FDP_ITC.1, Zerstörung eines Schlüssels gemäß FCS_CKM.4 und Schlüsselmanagement gemäß FMT_MSA.2) – sind in der IT-Umgebung im OSCI-Client bzw. -Backend, auf dem OSCI-Client-Enabler resp. -Backend-Enabler betrieben werden, zu realisieren.
- Die Abhängigkeiten der funktionalen Sicherheitsanforderung FCS_COP.1 (OSCI) sind nicht erfüllt,
- Die Abhängigkeit von FDP_ACC.1 – FDP_ACF.1 – ist aufgenommen.
- Die Abhängigkeiten von FDP_ACF.1 – FDP_ACC.1 und FMT_MSA.3 sind aufgenommen.
- Die Abhängigkeiten von FDP_ITC.1 – FDP_ACC.1 für die Zugriffskontrolle und FMT_MSA.3 zum Management des privaten Schlüssels sind aufgenommen.
- FIA_UID.2 hat keine Abhängigkeiten.
- FIA_UAU.2 hat die Abhängigkeit FIA_UID.1, die durch die hierarchische Anforderung FIA_UID.2 realisiert wird.
- Die Abhängigkeiten von FMT_MSA.1 – FDP_ACC.1 und FMT_SMR.1 – sind aufgenommen. Die Abhängigkeit FMT_MSA.1 - FMT_SMF.1 ist nicht aufgenommen, da die geforderte Managementfunktionalität bereits in FMT_MSA.1 angegeben ist (Modifizieren und Löschen der Sicherheitsattribute Rolle, Benutzerkennung und Rechte) und eine redundante Spezifizierung vermieden werden sollte.
- Die Abhängigkeiten von FMT_MSA.3 – FMT_MSA.1 und FMT_SMR.1 – sind aufgenommen.
- Die Abhängigkeit von FMT_SMR.1 – FIA_UID.1 – ist aufgenommen.

- Die Abhängigkeiten der funktionalen Sicherheitsanforderung FCS_COP.1 (Verify) sind nicht erfüllt, da die für die Verifikation genutzten öffentlichen Schlüssel aus den Zertifikaten öffentliche Informationen sind und keine Sicherheitsattribute darstellen (keine Schlüsselerzeugung gemäß FCS_CKM.1, kein Schlüsselimport gemäß FDP_ITC.1 , keine Zerstörung eines Schlüssels gemäß FCS_CKM.4, kein Schlüsselmanagement gemäß FMT_MSA.2).
- Die Abhängigkeiten der funktionalen Sicherheitsanforderung FCS_COP.1 (Tool) – Schlüsselimport gemäß FDP_ITC.1 (Schlüsselerzeugung gemäß FCS_CKM.1 ist bei Zertifikaten nicht anwendbar), Zerstörung eines Schlüssels gemäß FCS_CKM.4 und Schlüsselmanagement gemäß FMT_MSA.2) – sind in der IT-Umgebung für das Prüftool zu realisieren, da die für die Prüfung notwendigen Zertifikate vom Hersteller in das Tool eingebracht und mit dem Tool ausgeliefert werden.
- FTP_ITC.1 hat keine Abhängigkeiten.
- Zu den funktionalen Sicherheitsanforderungen in der IT-Umgebung:
    - Die Abhängigkeiten der drei funktionalen Sicherheitsanforderungen FCS_CKM.1 oder FDP_ITC.1, FCS_CKM.4 und FMT_MSA.2 sind in der IT-Umgebung zu realisieren, da Schlüsselerzeugung, -import und -löschung sowie Management der Sicherheitsattribute in der IT-Umgebung außerhalb des EVG liegt.
    - Die funktionalen Sicherheitsanforderungen in der IT-Umgebung, die sich aus der Nutzung der Basiskomponente zur Validierung eines qualifizierten Zertifikats und Erzeugung einer elektronischen Signatur – FCO_NRO.1, FCS_CKM.4, FCS_COP.1 (Verify), FCS_COP.1 (SVVE), FCS_COP.1 (VVE), FDP_ACC.1 (Sys), FDP_ACF.1 (Sys), FDP_ITC.1, FIA_UID.2, FMT_MSA.1 (Sys), FMT_MSA.2, FMT_MSA.3 (Sys) und FMT_SMR.1 (Sys) ergeben –, sind in der IT-Umgebung zu realisieren; wie [bos_Basis_ST] zu entnehmen ist, sind diese hinsichtlich der Abhängigkeiten in sich abgeschlossen.

**Tabelle 12: Erfüllung der EVG-Abhängigkeiten**

| funktionale Sicherheitsanforderungen an den EVG | Abhängigkeiten | Bemerkung |
|---|---|---|
| FCS_COP.1 (Hash) | FDP_ITC.1 oder FCS_CKM.1<br>FCS_CKM.4<br>FMT_MSA.2 | formal nicht erfüllt wg. Hashfunktion |
| FCS_COP.1 (Valid) | FDP_ITC.1 oder FCS_CKM.1<br>FCS_CKM.4<br>FMT_MSA.2 | sind in der IT-Umgebung zu realisieren |

| funktionale Sicherheitsanforderungen an den EVG | Abhängigkeiten | Bemerkung |
|---|---|---|
| FCS_COP.1 (OSCI) | FDP_ITC.1 oder FCS_CKM.1<br>FCS_CKM.4<br>FMT_MSA.2 | formal nicht erfüllt wg. Hashfunktion |
| FCS_COP.1 (Verify) | FDP_ITC.1 oder FCS_CKM.1<br>FCS_CKM.4<br>FMT_MSA.2 | formal nicht erfüllt wg. Nutzung öffentlicher Zertifikate |
| FCS_COP.1 (VSign) | FDP_ITC.1 oder FCS_CKM.1<br>FCS_CKM.4<br>FMT_MSA.2 | sind in der IT-Umgebung zu realisieren |
| FCS_COP.1 (Tool) | FDP_ITC.1 oder FCS_CKM.1<br>FCS_CKM.4<br>FMT_MSA.2 | sind in der IT-Umgebung zu realisieren |
| FDP_SVR.1 | - | formal erfüllt |
| FDP_ACC.1 | FDP_ACF.1 | erfüllt |
| FDP_ACF.1 | FDP_ACC.1<br>FMT_MSA.3 | erfüllt<br>erfüllt |
| FDP_ITC.1 | FDP_ACC.1 oder FDP_IFC.1<br>FMT_MSA.3 | erfüllt für FDP_ACC.1<br>erfüllt |
| FIA_UID.2 | - | formal erfüllt |
| FIA_UAU.2 | FIA_UID.1 | erfüllt durch FIA_UID.2, das hierarchisch zu FIA_UID.1 ist |
| FMT_MSA.1 | FDP_ACC.1 oder FDP_IFC.1<br>FMT_SMR.1<br>FMT_SMF.1 | erfüllt für FDP_ACC.1<br>erfüllt<br>nicht erfüllt, weil bereits in FMT_MSA.1 enthalten |
| FMT_MSA.3 | FMT_MSA.1<br>FMT_SMR.1 | erfüllt<br>erfüllt |
| FMT_SMR.1 | FIA_UID.1 | erfüllt durch FIA_UID.2, das hierarchisch zu |

| funktionale Sicherheitsanforderungen an den EVG | Abhängigkeiten | Bemerkung |
|---|---|---|
| | | FIA_UID.1 ist |
| FTP_ITC.1 | - | formal erfüllt |

### 8.3.3 Analyse des Zusammenwirkens der funktionalen Anforderungen

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

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

### 8.3.4 Analyse der Mindest-Stärkestufe

186 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".

187 Die Prüfung gegen ein hohes Angriffspotential (SOF-hoch) korrespondiert gemäß CC-Teil 3, Abschnitt 19.4, [CC-Teil3], und CEM, Abschnitt A.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.

188 Die angestrebten SOF-Stufen der einzelnen Sicherheitsfunktionen sind in Tabelle 13 aufgeführt.

**Tabelle 13: Angestrebten SOF-Stufen für die Sicherheitsfunktionen**

| Sicherheitsfunktion | Mechanismentyp | Angestrebte Stärke |
|---|---|---|
| SF1 | Wahrscheinlichkeits- oder Permutationsmechanismen (Hashfunktion) | SOF-hoch |

| Sicherheits-funktion | Mechanismentyp | Angestrebte Stärke |
|---|---|---|
| SF2 | Wahrscheinlichkeits- oder Permutationsmechanismen (Verifikationsalgorithmus, Hashfunktion) | SOF-hoch |
| SF3 | Wahrscheinlichkeits- oder Permutationsmechanismen (Verifikationsalgorithmus, Hashfunktion) | SOF-hoch |
| SF4 | Wahrscheinlichkeits- oder Permutationsmechanismen (Verifikationsalgorithmus, Hashfunktion) | SOF-hoch |
| SF5 | deterministisch | nicht anwendbar |
| SF6 | Wahrscheinlichkeits- oder Permutationsmechanismen (Hashfunktion) | SOF-hoch |
| SF7 | Wahrscheinlichkeits- oder Permutationsmechanismen (Passwort) | SOF-hoch |
| SF8 | Wahrscheinlichkeits- oder Permutationsmechanismen (Verifikationsalgorithmus, Hashfunktion) | SOF-hoch |

### 8.3.5 Erklärung zu den Anforderungen an die Vertrauenswürdigkeit

189 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

190 Die Sicherheitsfunktionen wirken mit den funktionalen Sicherheitsanforderungen wie folgt (vgl. Tabelle 14, wobei ein „X“ eine für die jeweilige Sicherheitsfunktion zutreffende funktionale Sicherheitsanforderung signalisiert):

- Für die Sicherheitsfunktion SF1 „Unterstützung bei der Erzeugung qualifizierter elektronischer Signaturen (Hashen und Zuführen zu signierender Dokumente zu einer sicheren Signaturerstellungseinheit)“ werden folgende Komponenten benötigt:
  - Komponente FCS_COP.1 (Hash) zum Hashen zu signierender Daten.
- Für die Sicherheitsfunktion SF2 „Schutz gegen Hashwertmanipulation“ werden folgende Komponenten benötigt:
  - Komponente FCS_COP.1 (VSign) zum Verifizieren einer zuvor erzeugten qualifizierten elektronischen Signatur.
  - Komponente FTP_ITC.1 für den vertrauenswürdigen Kanal zwischen EVG und Signaturkarte.

  - In der IT-Umgebung ist FCS_CKM.1 oder FDP_ITC.1, FCS_CKM.4 und FMT_MSA.2 umzusetzen.

- Für die Sicherheitsfunktion SF3 „Verifikation einer qualifizierten elektronischen Signatur“ werden folgende Komponenten benötigt:
  - Komponente FCS_COP.1 (Verify) zur Verifikation einer qualifizierten elektronischen Signatur.
- Für die Sicherheitsfunktion SF4 „Verifikation eines OSCI-Laufzettels bei der Validierung eines qualifizierten Zertifikats“ werden folgende Komponenten benötigt:
  - Komponente FCS_COP.1 (Valid) für die Verifikation des signierten OSCI-Laufzettels, auf dem die Validierungsergebnisse vorhanden sind.
  - In der IT-Umgebung – im OSCI-Client bzw. OSCI-Backend – ist FCS_CKM.1 oder FDP_ITC.1, FCS_CKM.4 und FMT_MSA.2 umzusetzen.
- Für die Sicherheitsfunktion SF5 „Sichere und zuverlässige Anzeige“ werden folgende Komponenten benötigt:
  - Komponente FDP_SVR.1 für die sichere Anzeige.
- Für die Sicherheitsfunktion SF6 „Unterstützung bei der Validierung qualifizierter Zertifikate“ werden folgende Komponenten benötigt:
  - Komponente FCS_COP.1 (OSCI) für das Hashen des OSCI-Laufzettels.
  - In der IT-Umgebung wird die Basiskomponente zur Validierung eines qualifizierten Zertifikats und zur Erzeugung einer elektronischen Signatur benötigt; FCO_NRO.1, FCS_CKM.4, FCS_COP.1 (Verify), FCS_COP.1 (SVVE), FCS_COP.1 (VVE), FDP_ACC.1 (Sys), FDP_ACF.1 (Sys), FDP_ITC.1, FIA_UID.2, FMT_MSA.1 (Sys), FMT_MSA.2, FMT_MSA.3 (Sys) und FMT_SMR.1 (Sys) sind umzusetzen.
  - Diverse weitere Komponenten sind aufgenommen: FDP_ITC.1, FDP_ACC.1, FDP_ACF.1, FMT_MSA.3, FMT_MSA.1, FMT_SMR.1, FIA_UID.2, FIA_UAU.2.
- Für die Sicherheitsfunktion SF7 „Identifikation und Authentisierung“ werden folgende Komponenten benötigt:
  - Komponenten FDP_ACC.1, FDP_ACF.1, FMT_MSA.3, FMT_MSA.1, FTM_SMR.1, FIA_UID.2, FIA_UAU.2 zur Zugriffskontrolle für das Management im OSCI-Manager.
- Für die Sicherheitsfunktion SF8 „Prüftool“ werden folgende Komponenten benötigt:
  - Komponente FCS_COP.1 (Tool) zum Verifizieren von Daten.

- o Über die Abhängigkeiten ist in der IT-Umgebung – im Prüftool – FCS_CKM.1 oder FDP_ITC.1, FCS_CKM.4 und FMT_MSA.2 umzusetzen.

191 Darüber hinaus werden funktionale Sicherheitsanforderungen in der IT-Umgebung für SigG-konforme sichere Signaturerstellungseinheiten und Chipkartenleser referenziert, die den Sicherheitsvorgaben bestätigter Produkte zu entnehmen sind (vgl. beispielsweise http://www.bundesnetzagentur.de/).

**Tabelle 14: Zuordnung fkt. Sicherheitsanforderungen durch Sicherheitsfunktionen**

| Fkt. Sicherheitsanforderungen an EVG bzw. IT-Umgebung | SF1 | SF2 | SF3 | SF4 | SF5 | SF6 | SF7 | SF8 |
|---|---|---|---|---|---|---|---|---|
| FCS_COP.1 (Hash) | X | | | | | | | |
| FCS_COP.1 (Valid) | | | | X | | | | |
| FCS_COP.1 (OSCI) | | | | | | X | | |
| FCS_COP.1 (Verify) | | | X | | | | | |
| FCS_COP.1 (VSign) | | X | | | | | | |
| FCS_COP.1 (Tool) | | | | | | | | X |
| FDP_SVR.1 | | | | | X | | | |
| FDP_ACC.1 | | | | | | X | X | |
| FDP_ACF.1 | | | | | | X | X | |
| FDP_ITC.1 | | | | | | X | | |
| FIA_UID.2 | | | | | | X | X | |
| FIA_UAU.2 | | | | | | X | X | |
| FMT_MSA.1 | | | | | | X | X | |
| FMT_MSA.3 | | | | | | X | X | |
| FMT_SMR.1 | | | | | | X | X | |
| FTP_ITC.1 | | X | | | | | | |
| FCS_CKM.1 oder FDP_ITC.1 | | X | | X | | | | X |
| FCS_CKM.4 | | X | | X | | | | X |
| FMT_MSA.2 | | X | | X | | | | X |

| Fkt. Sicherheitsanforderungen an EVG bzw. IT-Umgebung | SF1 | SF2 | SF3 | SF4 | SF5 | SF6 | SF7 | SF8 |
|---|---|---|---|---|---|---|---|---|
| FCO_NRO.1, FCS_CKM.4, FCS_COP.1 (Verify), FCS_COP.1 (SVVE), FCS_COP.1 (VVE), FDP_ACC.1 (Sys), FDP_ACF.1 (Sys), FDP_ITC.1, FIA_UID.2, FMT_MSA.1 (Sys), FMT_MSA.2, FMT_MSA.3 (Sys) und FMT_SMR.1 (Sys) | | | | | | X | | |

192 Die Sicherheitsfunktionen wirken in den drei Teilsystemen OSCI-Client-Enabler, -Manager und -Backend-Enabler wie folgt (Tabelle 15):

**Tabelle 15: Zuordnung von Sicherheitsfunktionen zu Teilsystemen**

| | OSCI-Client-Enabler | OSCI-Manager | OSCI-Backend-Enabler |
|---|---|---|---|
| SF1 – Unterstützung bei der Erzeugung qualifizierter elektronischer Signaturen | X | | |
| SF2 – Schutz gegen Hashwertmanipulation | X | | |
| SF3 – Verifikation einer qualifizierten elektronischen Signatur | X | | X |
| SF4 – Verifikation eines OSCI-Laufzettels bei der Validierung eines qualifizierten Zertifikats | X | | X |
| SF5 – Sichere und zuverlässige Anzeige | X | | |
| SF6 – Unterstützung bei der Validierung qualifizierter Zertifikate | | X | |
| SF7 – Identifikation und Authentisierung | | X | |
| SF8 – Prüftool | X | | |

### 8.4.2 Konsistenz der Mechanismenstärke-Postulate

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

### 8.4.3 Analyse des Zusammenwirkens der Sicherheitsfunktionen

194 Im Folgenden ist ausgeführt und in Tabelle 16 zusammengefasst, wie die Sicherheitsfunktionen

- SF1 – Unterstützung bei der Erzeugung qualifizierter elektronischer Signaturen (Hashen und Zuführen zu signierender Dokumente zu einer sicheren Signaturerstellungseinheit),
- SF2 – Schutz gegen Hashwertmanipulation,
- SF3 – Verifikation einer qualifizierten elektronischen Signatur,
- SF4 – Verifikation eines OSCI-Laufzettels bei der Validierung eines qualifizierten Zertifikats,
- SF5 – Sichere und zuverlässige Anzeige,
- SF6 – Unterstützung bei der Validierung qualifizierter Zertifikate,
- SF7 – Identifikation und Authentisierung,
- SF8 – Prüftool

zusammenwirken, wobei ein „X“ in Tabelle 16 ein Zusammenwirken signalisiert. Tabelle 16 ist nicht symmetrisch.

195 Da bei der Unterstützung der Erzeugung einer qualifizierten elektronischen Signatur sowie der Verifikation einer qualifizierten elektronischen Signatur und der Validierung beim OSCI-Client-Enabler der Benutzer bzw. Signaturschlüssel-Inhaber durch geeignete Anzeigen unterstützt wird, wirkt SF5 stets bei SF1, SF2, SF3 und SF4.

196 Da im Rahmen der Erzeugung einer qualifizierten elektronischen Signatur der zuvor erzeugte Hashwert geprüft wird, wirken SF1 und SF2 stets zusammen.

197 Da die Validierung durch den OSCI-Manager ausgeführt wird, der wiederum das Validierungsergebnis OSCI-Client-Enabler und -Backend-Enabler auf dem OSCI-Laufzettel zur Verfügung stellt, setzt SF4 voraus, dass zuvor SF6 ausgeführt wurde.

198 Da der OSCI-Manager den OSCI-Laufzettel signiert und entsprechende private Schlüssel in den OSCI-Manager eingebracht werden müssen, setzt SF6 voraus, dass SF7 für die Identifikation und Authentisierung des Schlüssel-Administrator ausgeführt wurde.

**Tabelle 16: Zusammenwirken der Sicherheitsfunktionen**

| | SF1 | SF2 | SF3 | SF4 | SF5 | SF6 | SF7 | SF8 |
|---|---|---|---|---|---|---|---|---|
| SF1 | X | X | | | | | | |
| SF2 | X | X | | | | | | |
| SF3 | | | X | | | | | |
| SF4 | | | | X | | | | |
| SF5 | X | X | X | X | X | | | |
| SF6 | | | | X | | X | | |
| SF7 | | | | | | X | X | |
| SF8 | | | | | | | | X |

### 8.4.4 Zuordnung der Sicherheitsfunktionen zur Umsetzung der SigG-Anforderungen

199 In Abschnitt 2.5.2 wurde beschrieben, in welchem Umfang die Sicherheitsanforderungen des SigG und der SigV an Signaturanwendungskomponenten vom EVG erfüllt werden und welcher Anteil von der IT-Umgebung umgesetzt werden muss (vgl. Tabelle 1). Im Folgenden wird angegeben, durch welche Sicherheitsfunktion die SigG/SigV-Anforderungen umgesetzt wurden. Zu diesem Zweck wird Tabelle 1 wiederholt und erweitert (vgl. Tabelle 17), wobei zu berücksichtigen ist,

- dass bei der Erzeugung einer qualifizierten elektronischen Signatur SF1 für die Bildung des Hashwertes und SF5 für die Anzeige,
- dass bei der Prüfung einer qualifizierten elektronischen Signatur SF3 für die Verifikation und SF5 für die entsprechende Anzeige,
- dass bei der Statusprüfung eines qualifizierten Zertifikats SF6 für die eigentliche Validierung, SF4 für die Verifikation des OSCI-Laufzettels, SF7 für das Management des OSCI-Managers und SF5 für die entsprechende Anzeige und
- dass zum Schutz vor unbefugter Veränderung SF8

benötigt werden.

**Tabelle 17: Umsetzung der SigG/SigV-Anforderungen durch Sicherheitsfunktionen**

| Sicherheitsanforderungen an Signaturanwendungskomponenten [BNetzA2005] | Umsetzung der Anforderungen aus SigG und SigV | |
|---|---|---|
| | in EVG | Sicherheits-funktion |
| „Erzeugung von Signaturen: Die Signaturanwendungskomponente muss beim Erzeugen einer Signatur gewährleisten, dass | zum Erzeugen wendet der OSCI-Client-Enabler auf die zu signierenden Daten eine Hashfunktion gemäß OSCI-Transport an und führt den erzeugten Hashwert der angeschlossenen sicheren Signaturerstellungseinheit zu; eine erzeugte Signatur wird anschließend verifiziert | SF1<br>SF2 |
| ▪ das Erzeugen einer Signatur vorher eindeutig angezeigt wird, | der OSCI-Client-Enabler unterstützt den Benutzer durch entsprechende Anzeigen | SF5 |
| ▪ erkennbar ist, auf welche Daten sich die Signatur bezieht, | wird im OSCI-Client-Enabler angezeigt | SF5 |
| ▪ bei Bedarf der Inhalt der zu signierenden Daten hinreichend zu erkennen ist, | kann im OSCI-Client-Enabler angezeigt werden | SF5 |
| ▪ eine Signatur nur durch die berechtigt signierende Person erfolgt, | - | |
| ▪ die Identifikationsdaten nicht preisgegeben und nur auf der jeweiligen „sicheren Signaturerstellungseinheit“ gespeichert werden. | - | |
| Prüfung einer Signatur: Die Signaturanwendungskomponente muss beim Prüfen einer Signatur gewährleisten, dass | OSCI-Client-Enabler und OSCI-Backend-Enabler prüfen qualifizierte elektronische Signaturen.<br>Teilfunktionalitäten der Validierung erfolgen beim OSCI-Manager; Plausibilitätsprüfung bei OSCI-Client-Enabler und OSCI-Backend-Enabler; | SF3<br>SF6, SF4, SF7 |
| ▪ erkennbar wird, auf welche Daten sich die Signatur bezieht, | wird vom OSCI-Client-Enabler angezeigt | SF5 |
| ▪ erkennbar wird, ob die Daten unverändert sind, | wird vom OSCI-Client-Enabler geleistet | SF5 |

| Sicherheitsanforderungen an Signaturanwendungskomponenten [BNetzA2005] | Umsetzung der Anforderungen aus SigG und SigV | |
|---|---|---|
| | in EVG | Sicherheits-funktion |
| ▪ bei Bedarf der Inhalt der signierten Daten hinreichend zu erkennen ist, | kann vom OSCI-Client-Enabler angezeigt werden | SF5 |
| ▪ erkennbar wird, welchem Signaturschlüssel-Inhaber die Signatur zuzuordnen ist, | wird vom OSCI-Client-Enabler angezeigt | SF5 |
| ▪ erkennbar wird, welche Inhalte das qualifizierte Zertifikat, auf dem die Signatur beruht, und zugehörige qualifizierte Attribut-Zertifikate aufweisen, | wird vom OSCI-Client-Enabler angezeigt, allerdings werden keine Attribut-Zertifikate unterstützt | SF5 |
| ▪ erkennbar wird, ob die nachgeprüften qualifizierten Zertifikate im jeweiligen Zertifikatverzeichnis zum angegebenen Zeitpunkt vorhanden und nicht gesperrt waren, | wird vom OSCI-Client-Enabler angezeigt, wobei der im OSCI-Laufzettel angegebene Zeitpunkt der Zeitpunkt ist, zu dem die Nachricht beim OSCI-Manager angekommen ist | SF5 |
| ▪ die Korrektheit der Signatur zuverlässig geprüft und zutreffend angezeigt wird. | führen OSCI-Client-Enabler und -Backend-Enabler durch | SF3<br>SF5 |
| Schutz vor unbefugter Veränderung: Sicherheitstechnische Veränderungen an der Signaturanwendungskomponente müssen für den Nutzer erkennbar werden.” | Prüftool für den OSCI-Client-Enabler zum Schutz vor unbefugter Veränderung wird zur Verfügung gestellt | SF8 |

### 8.4.5 Erklärung zu den Maßnahmen der Vertrauenswürdigkeit

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

**Tabelle 18: Erklärung der Maßnahmen zur Erfüllung von EAL3+**

| Anforderungen gemäß EAL3+ | Maßnahmen der Entwickler |
|---|---|
| Konfigurations-management :<br>▪ ACM_CAP.3<br>▪ ACM_SCP.1 | Ein Qualitätssicherungssystem mit Konfigurationskontrolle unterstützt den Entwickler bei der Entwicklung des EVG.<br>Alle der Konfigurationskontrolle unterliegenden Objekte werden eindeutig identifiziert. Es stellt sicher, dass Unbefugte keine Modifikationen vornehmen.<br>Das Konfigurationskontrollsystem ermöglicht eine Historie von Implementierung, Design, Tests und Dokumentation. |
| Auslieferung und Betrieb:<br>▪ ADO_DEL.2<br>▪ ADO_IGS.1 | Es werden Maßnahmen zur Umsetzung der Anforderungen hinsichtlich der Auslieferungsprozeduren sowie Installations-, Generierungs- und Anlaufprozeduren dokumentiert. |
| Entwicklung:<br>▪ ADV_FSP.1<br>▪ ADV_HLD.2<br>▪ ADV_IMP.1<br>▪ ADV_LLD.1<br>▪ ADV_RCR.1 | Entwicklungsprozeduren und Dokumentation erfolgen in einer Weise, so dass sie den Anforderungen der CC genügen. |
| Handbücher:<br>▪ AGD_ADM.1<br>▪ AGD_USR.1 | Systemverwalter- und Benutzerhandbuch werden erstellt und mit dem EVG ausgeliefert. |
| Lebenszyklus-Unterstützung:<br>▪ ALC_DVS.1<br>▪ ALC_TAT.1 | Der Entwicklungsprozess ist durch physikalische, personelle und organisatorische Sicherheitsmaßnahmen gewährleistet.<br>Für die Entwicklung des EVG werden festgelegte Entwicklungswerkzeuge genutzt. |
| Testen:<br>▪ ATE_COV.2<br>▪ ATE_DPT.1<br>▪ ATE_FUN.1<br>▪ ATE_IND.2 | Der Entwickler verwendet ein werkzeugbasiertes und automatisiertes Testsystem. Damit können<br>▪ Tests der Sicherheitsfunktionen,<br>▪ Tests auf Subsystem-Ebene und<br>▪ Tests der funktionalen Spezifikation<br>durchgeführt und die Ergebnisse dokumentiert werden. |

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

# 9 Definition der Familie FDP_SVR[59]

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

**202 FDP_SVR Sichere Anzeige**

203 Familienverhalten

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

204 Komponentenabstufung

FDP_SVR Sichere Anzeige---1

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

205 Management: FDP_SVR.1

Für diese Komponente sind keine Management-Aktivitäten vorgesehen.

206 Protokollierung: FDP_SVR.1

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

207 FDP_SVR.1 Sichere Anzeige

208 Ist hierarchisch zu: Keinen anderen Komponenten

[59] aus [SignCubes]

| | | |
|---|---|---|
| 209 | FDP_SVR.1.1 | Die TSF müssen sicherstellen, dass der dem Benutzer angezeigte Inhalt eines Dokumentes entsprechend den folgenden Normen [Zuweisung: Normen für die Darstellung eines Inhalts] eindeutig ist. |
| 210 | FDP_SVR.1.2 | Die TSF müssen sicherstellen, dass der dem Benutzer anzuzeigende Inhalt eines Dokumentes frei von aktiven oder verdeckten Inhalten ist. Die TSF müssen sicherstellen, dass der Benutzer darüber informiert wird. |
| 211 | FDP_SVR.1.3 | Die TSF müssen sicherstellen, dass der Benutzer über einen nicht darstellbaren Inhalt eines anzuzeigenden Dokumentes informiert wird. |
| 212 | Abhängigkeiten: | Keine Abhängigkeiten |

# 10 Glossar

| | |
|---|---|
| Basiskomponente | Basiskomponente von Governikus mit Kernsystem, OCSP/CRL-Relay und NetSigner (vgl. [bos_Basis_ST]).[11] |
| Chipkarte | gemeint ist stets eine SigG-konforme Chipkarte |
| CRL | Certificate Revocation List (Sperrliste) [CRL] |
| GUI | Graphical User Interface |
| LDAP | Lightweight Directory Access Protocol [LDAP] |
| Objekt | „Eine Einheit im TSC, die Informationen enthält oder empfängt und auf der Subjekte Operationen ausführen.“ [CC-Teil1] |
| OCSP | Online Certificate Status Protocol (Protokoll zur Zertifikatsstatus-Anfrage) [OCSP] |
| OperationId | Identifier für auszuführende Operationen |
| Prüfzeitpunkt | Als Prüfzeitpunkt wird der Zeitpunkt bezeichnet, an dem die aktuelle Prüfung durchgeführt wird. Die Unterscheidung zum Signaturzeitpunkt ist insbesondere von Bedeutung, weil im Laufe der Zeit die Sicherheit mathematischer Verfahren als unzureichend bewertet werden kann. Wenn der Prüfende sich über den Signaturzeitpunkt nicht sicher sein kann, kann er hilfsweise den Prüfzeitpunkt [...] als Signaturzeitpunkt annehmen. ([BSI_SigI_A6]) |
| SAK | Signaturanwendungskomponente |
| SFP | funktionale Sicherheitspolitik |
| Sicherheitsattribut | „Informationen, die mit Subjekten, Benutzern und/oder Objekten verknüpft sind und die zur Durchsetzung der TSP benötigt werden.“ [CC-Teil1] |
| Signaturkarte | sichere Signaturerstellungseinheit (Die sichere Signaturerstellungseinheit gemäß SigG/SigV wird in diesem Kontext aus- |

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

# 11 Literatur


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

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

[BNetzA_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.

[bos_Basis_ST] bremen online services GmbH & Co. KG, „Governikus, Version 3.3 (Basis), Sicherheitsvorgaben (ST)“, Version 1.13, 02.02.2009.

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

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

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

[CC-Teil2] „Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements“, Version 2.3, August 2005.

[CC-Teil3] „Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements“, Version 2.3, August 2005.

[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 3.3.1.0, 05.12.2008.

[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 1.10.1, 25.08.2009.

[Karten_NetSigner] bremen online services GmbH & Co. KG, „Unterstützte Signaturkarten und Chipkartenlesegeräte Governikus NetSigner“, Karten-Leser-Ansteuerung MCARD) Version 1.10.0, 25.06.2009.

[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 1.10.1, 25.08.2009.

[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), http://www.osci.de.

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

[OSCI-Transport_Korr] OSCI Leitstelle, „OSCI-Transport 1.2 – Korrigenda", 10.04.2008.

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

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

[SHA] 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).

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

[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.[60]

# 12 Anhang: Technische Einsatzumgebung

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

## 12.1 Hard- und Software

214 Hinsichtlich der Serverkomponenten für OSCI-Manager und -Backend-Enabler werden folgende Systemumgebungen unterstützt:

[60] 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.

- 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 1.5.0 ab Version 1.5.0_10
- Application Server:
  - JBoss 4.x ;
  - JBoss Enterprise Application Platform 4.2 ;
- Datenbanken:
  - MySQL 5;
  - Oracle 10gR2;

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

216 Hinsichtlich der Clientkomponenten für OSCI-Client-Enabler werden folgende Systemumgebungen unterstützt:

- Hardware:
  - 1 GHz i386 Prozessor mit 256 MB RAM und 20 GB Harddisk;
- Betriebssysteme:
  - Linux (openSUSE 10.x);
  - Windows XP;
  - Windows 2000;
- Java: SUN 1.5.0 ab Version 1.5.0_10.

## 12.2 Sichere Signaturerstellungseinheiten und Chipkartenleser

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

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

## 12.3 Zertifikate und private Schlüssel

219 Folgende X.509v3-Zertifikate werden unterstützt:

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

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

## 12.4 Anfordernde Systeme

221 OSCI-Client und -Backend, die auf den EVG – d. h. auf OSCI-Client-Enabler bzw. -Backend-Enabler – zugreifen, welche die Funktionalitäten des EVG nutzen und die Anforderungen des Signaturgesetzes an eine Signaturanwendungskomponente erfüllen.