

Herstellereklärung

Der Hersteller

bremen online services Entwicklungs- und Betriebsgesellschaft mbH & Co. KG

Am Fallturm 9

D-28359 Bremen

erklärt hiermit gemäß § 17 Abs. 4 Satz 2 SigG¹

in Verbindung mit § 15 Abs. 5 Satz 1 SigV²,

dass sein Produkt

Governikus, Version 3.2.1.0 (Basis)

die nachstehend genannten Anforderungen des Signaturgesetzes bzw. der Signaturverordnung in Teilen erfüllt.

Bremen, den 27.10.2008

gez. Dr. Stephan Klein

Geschäftsführung

Diese Herstellereklärung in Version 1.2 mit der Dokumentennummer bos2008003 besteht aus 14 Seiten.

¹ Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz – SigG) vom 16. Mai 2001 (BGBl. I S. 876), zuletzt geändert durch Artikel 4 des Gesetzes vom 26. Februar 2007 (BGBl. I S. 179)

² Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) vom 16. November 2001 (BGBl. I S. 3074), zuletzt geändert durch Artikel 9 Abs. 18 des Gesetzes vom 23. November 2007 (BGBl. I S. 2631)

Dokumentenhistorie

Version	Datum	Bemerkung
1.0	21.05.2008	Initialversion
1.1	15.10.2008	Gesamtüberarbeitung
1.2	27.10.2008	eine Referenz korrigiert

Beschreibung des Produkts

1. Handelsbezeichnung

Die Handelsbezeichnung lautet: Governikus, Version 3.2.1.0 (Basis)³

Auslieferung: online per Download

Hersteller: bremen online services Entwicklungs- und Betriebsgesellschaft mbH & Co. KG

Handelsregisterauszug: HRA 22041

2. Lieferumfang und Versionsinformationen

Nachfolgend ist der Lieferumfang, einschließlich der Versionsinformationen, aufgezählt:

Produktbestandteile	Bezeichnung	Version	Übergabeform
Software	Governikus, Version 3.2.1.0 (Basis) mit den Teilkomponenten Kernsystem, Net-Signer und OCSP/CRL-Relay	3.2.1.0	online per Download
Handbuch	Betriebshandbuch „Governikus – Teil der virtuellen Poststelle des Bundes“	3.2.1.0	online per Download
Handbuch	Installation „Governikus – Teil der virtuellen Poststelle des Bundes“	3.2.1.0	online per Download

Tabelle 1: Lieferumfang und Versionsinformationen

Die Software „Governikus, Version 3.2.1.0 (Basis)“ besteht aus den in der folgenden Tabelle aufgeführten Dateien:

Bibliothek	Beschreibung	Version
Gov2Core.ear	Governikus-Kernsystem	3.2.1.0
Gov2CoreTest.ear	Test-Anwendung für Kernsystem	3.2.1.0
Gov2Core_SOAPEntry.ear	SOAP-Zugang zum Kernsystem	3.2.1.0
gov2core_adatimestamp.rar	Adapter für Anbindung des Zeitstempeldienstes von Authentidate	3.2.1.0
gov2core_drvtimestamp.rar	Adapter für Anbindung des Zeitstempeldienstes der DRV	3.2.1.0
Gov2NetSigner.ear	NetSigner Serveranwendung	3.2.1.0

³ Dieses Produkt stellt die Weiterentwicklung eines gemäß Common Criteria evaluierten und zertifizierten sowie gemäß Signaturgesetz bestätigten Produktes dar: Virtuelle Poststelle des Bundes (Basis), Version 2.2.2.6, vgl. Zertifizierungs-ID: BSI-DSZ-CC-0331-2007; Bestätigungs-ID: BSI.02070.TE.11.2007 (Bestätigungsurkunde vom 27.11.2007)

Bibliothek	Beschreibung	Version
Gov2NetSignerTest.ear	Test-Anwendung für NetSigner	3.2.1.0
keystorehost.jar	NetSigner-Kartenanwendung	3.2.1.0
Gov2NetSignerCommon.jar	Gemeinsame Klassen beider NetSigner-Anwendungen	3.2.1.0
commons-logging.jar	Apache Commons Logging	1.0.3
log4j-1.2.8.jar	Log4J	1.2.8
gov2server_common.jar	Governikus-Bibliotheken (komponenten-übergreifend)	3.2.1.0
gov2server_utils.jar	Governikus-Bibliotheken (komponenten-übergreifend)	3.2.1.0
jca_ocf_provider_netsigner_signed.jar jRegistryKey.jar mcard-1.5.1.jar	Kartenansteuerung	3.2.1.0 bzw. 1.5.1
mbeanloader.war Gov2NetSignerManagement.jar Gov2NetSignerServer.jar	Teile der Netsigner Server-Anwendung	3.2.1.0
jbossall-client.jar	Client-Bibliothek für JBoss	4.2.2 GA
javax77.jar jms.jar jta.jar	J2EE-Bibliotheken benötigt von OC4J-Client	
commons-codec.jar	common encoders and decoders wie Base64, Hex, Phonetic und URLs.	1.3
BC134withExtensions_signed.jar	BOS - Bouncycastle	1.3.4
commons-httpclient-3.0.1.jar	Transport	3.0.1
mail.jar	Abbildung von SMIME-Objekten	1.3.1
xmlsec-1.4.1.jar	Abbildung von XML-Signature	1.4.1
activation.jar	JavaBeans Activation Framework	1.0.2
servlet.jar (j2ee.jar)	EJB-Klassen	1.4.0
gov_parser	XKMS-Parser	3.2.1.0
gov2server_tests.jar	Komponentenübergreifende Helfer-Klassen für Tests	3.2.1.0
base64.jar	Helfer für Base64	3.2.1.0
commons_http_utils.jar	Transport	3.2.1.0
jaxb-api.jar	Das javax.xml.bind interfaces und Helfer-Klassen	2.1.3

Bibliothek	Beschreibung	Version
jsr-api.jar		173_1.0
jaxb-impl.jar	Die JAXB RI binding runtime framework Klassen	2.1.3
xsdlib.jar	XML Schema type library	20050516

Tabelle 2: Auflistung der Dateien

Das Produkt „Governikus, Version 3.2.1.0 (Basis)“ nutzt die folgenden nach SigG bestätigten Produkte, die von Dritten hergestellt werden und nicht Bestandteil dieser Erklärung sind (z.B. Kartenleser oder sichere Signaturerstellungseinheit (SSEE)):

Produktklasse	Bezeichnung		Beschreibung + Registriernummer der Bestätigung
SSEE	D-Trust GmbH	D-Trust-Card_MS Version 1.0 Signaturkarte D-TRUST Card_MS Version 1.0	TUVIT.09361.TE.10.2001 Nachtrag vom 24.03.2004
SSEE	D-Trust GmbH	D-Trust-Card_MS Version 2.02c SEE „Chipkarte mit Prozessor SLE66CX322P, CardOS V4.3B mit Applikation für digitale Signatur“	T-Systems.02122.TE.05. 2005
SSEE	Deutsche Rentenversicherung Bund	Multisign-Karte der Deutschen Rente Bund SEE „Chipkarte mit Prozessor SLE66CX322P, CardOS V4.3B mit Applikation für digitale Signatur“	T-Systems.02122.TE.05. 2005
Kartenleser	OMNIKEY GmbH	SAK Chipkartenterminal der Familie CardMan Trust CM3821, Firmware-Version 6.00	BSI.02057.TE.12.2005
Kartenleser	Reiner SCT Kartenlesegeräte GmbH	CyberJack e-com, Version 2.0	T-Systems. 09363.TE.06.2002
Kartenleser	Kobil Systems GmbH	KOBIL Chipkartenterminal KAAN Professional HW-Version KCT100, FW 2.08 GK 1.04	TUVIT.09331.TE.03.2002

Tabelle 3: Zusätzliche Produkte

3. Funktionsbeschreibung

Die Software „Governikus, Version 3.2.1.0 (Basis)“ ist als Funktionsbibliothek Teil einer Signaturanwendungskomponente gemäß § 2 Nr. 11 SigG und stellt damit eine Basis für weitere Signaturanwendungskomponenten dar. Die Software „Governikus, Version 3.2.1.0 (Basis)“ ist keine vollständige Signaturanwendungskomponente.

Das Produkt besteht aus den folgenden Teilsystemen:

- Kernsystem mit NetSigner;
- OCSP/CRL-Relay.

Die Software „Governikus, Version 3.2.1.0 (Basis)“ wird auf geeigneter Hardware mit geeigneten Betriebsmitteln betrieben – insbesondere mit SigG-konformen Chipkartenlesern, sicheren Signaturerstellungseinheiten (in diesen Fall Signaturkarten).

Governikus, Version 3.2.1.0 (Basis) wird auf Servern in einem „geschützten Einsatzbereich (Regelfall/Standardlösung)“ [BNetzA2005]⁴ betrieben und über jeweilige Web-Oberflächen (Graphical User Interface – GUI) von Administratoren konfiguriert.

Nachdem eine Signaturkarte für die Erzeugung von Batchsignaturen⁵ vom Signaturschlüssel-Inhaber freigeschaltet wurde, arbeitet Governikus, Version 3.2.1.0 (Basis) im Produktivbetrieb automatisiert und ohne menschliche Interaktionen.

Die Software „Governikus, Version 3.2.1.0 (Basis)“ stellt folgende Funktionalitäten zur Verfügung:

- Das **Kernsystem** erhält von außen über eine Schnittstelle die Anforderung⁶, Daten serverbasiert mit einer Batchsignatur zu versehen.

⁴ Quelle: 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. Juli 2005.

⁵ Eine Batchsignatur ist eine serverbasiert erzeugte SigG-konforme qualifizierte elektronische Signatur gemäß [BNetzA_FAQ18], bei der „eine große Anzahl praktisch gleicher Vorgänge – z. B. Rechnungen, die sich ‚nur‘ im Betrag und der Zustelladresse unterscheiden – [...] in einer besonders gesicherten Umgebung automatisiert abgearbeitet“ werden.

⁶ Das Produkt wird unter der Annahme betrieben, dass ein anforderndes System, das auf dieses Produkt zugreift – etwa „Governikus (OSCI)“, „Virtuelle Poststelle des Bundes (OSCI)“ oder „Virtuelle Poststelle des Bundes (Verifikationsmodul)“ –, die Anforderungen von SigG und SigV an Signaturanwendungskomponente erfüllt. In der Bestätigungsurkunde wird dazu ausgeführt: „Die Basiskomponente stellt selbst nur einen Teil der Funktionalität zur Verfügung, die vom Signaturgesetz bzw. der Signaturverordnung gefordert wird. So obliegt z.B. die Funktionalität, dass „die Erzeugung einer Signatur vorher eindeutig angezeigt wird“ (§ 15 Abs. 2 SigV), dem anfordernden System in der IT-Umgebung, welches einen Auftrag an die Basiskomponente absendet. Die Basiskomponente erlaubt lediglich einem Inhaber eines Signaturschlüssels, bestimmte Vorgaben zu machen. Dazu gehört die maximale Zeit oder Anzahl für die Erstellung von Signaturen sowie die Festlegung der autorisiert anfordernden Systeme, die auf die Karte des Signaturschlüssel-Inhabers zugreifen dürfen. Ähnliches gilt auch für die Anteile von § 17 Abs. 2 SigG. Der Bezug von Daten zur Signatur („...auf welche Daten sich die Signatur bezieht...“) und das

In diesem Kontext führt der **NetSigner** die zu signierenden Daten einer angeschlossenen sicheren Signaturerstellungseinheit zu. Das Kernsystem liefert das Ergebnis (Signatur oder Fehlermeldung) zurück.

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

Es findet kein automatisierter Prozess statt, der nach Eingabe der PIN diese für das System vorhält, zum Signieren automatisch abrufen und an die SSEE sendet.

Die Software „Governikus, Version 3.2.1.0 (Basis)“ gewährleistet, dass nach Freischaltung der sicheren Signaturerstellungseinheit je nach Konfiguration entweder

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

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

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

Anzeigen signierter Daten („...nach Bedarf auch den Inhalt der zu signierenden Daten hinreichend erkennen lassen...“) muss ebenfalls durch das anfordernde System in der IT-Umgebung der Basiskomponente gewährleistet werden. Die autorisiert anfordernden Systeme müssen auch sicherstellen, dass einer Batchsignatur ausschließlich praktisch gleiche Vorgänge zugeführt werden, da die Basiskomponente keine Analyse der Inhalte vornimmt. Daher müssen anfordernde Systeme bestätigt werden, bevor sie zusammen mit der Basiskomponente zur Erstellung von qualifizierten elektronischen Signaturen genutzt werden können. Die anfordernden Systeme sind nicht Bestandteil dieser Bestätigung.

Die Kommunikation mit den anfordernden Systemen sichert die Basiskomponente durch den Einsatz von elektronischen Signaturen ab. Anforderungen zum Erzeugen qualifizierter elektronischer Batchsignaturen werden durch eine elektronische Signatur gegen eine Integritätsverletzung geschützt, die ein autorisiert anforderndes System erstellt. [...] Für die Anforderung von qualifizierten elektronischen Batchsignaturen wird auf jedem autorisiert anfordernden System ein eigenes Serverzertifikat mit dem geheimen Signaturschlüssel hinterlegt, wobei der Schutz des geheimen Signaturschlüssels dem anfordernden System oder seiner Umgebung obliegt. Das Serverzertifikat mit dem dazugehörigen öffentlichen Schlüssel ist der Basiskomponente zugänglich und zur vereinfachten Verwaltung einer sog. Rolle zugeordnet. Durch Anzeige einer solchen Rolle kann z.B. dem Signaturschlüssel-Inhaber das zugeordnete Serverzertifikat und damit das anfordernde System, das auf seine Signaturkarte zugreifen kann, übersichtlich angezeigt werden. [...] Da Serverzertifikate nicht öffentlich abprüfbar sind, verfügen sie über keine zeitliche Begrenzung und werden nicht gesperrt. Liegt der Verdacht der Kompromittierung vor, so müssen sie ausgetauscht werden. Für die Beschaffung, sichere Verteilung und ggf. den Austausch der Serverzertifikate von Basiskomponente oder anforderndem System mit den öffentlichen und geheimen Schlüsseln sind die Schlüsseladministratoren [...] zuständig. Die eingesetzten Algorithmen zur Signatur von Daten mit Hilfe der Serverzertifikate sind durch die Bundesnetzagentur als geeignet für die Verwendung bei der qualifizierten elektronischen Signatur eingestuft.“

sehene Ergebnis der Verifikation (korrekte oder nicht korrekte Signatur oder Fehlermeldung) an das anfordernde System zurück.

- Das Kernsystem erhält von außen über eine Schnittstelle die Anforderung, die Gültigkeit eines qualifizierten Zertifikats zu einem übermittelten Zeitpunkt bzw. – sofern kein expliziter Zeitpunkt übermittelt wurde – zum Prüfzeitpunkt festzustellen. Das Kernsystem stellt fest, ob das qualifizierte Zertifikat zum angegebenen Zeitpunkt bzw. zum Prüfzeitpunkt
 - vorhanden und nicht gesperrt war und
 - der Gültigkeitszeitraum des qualifizierten Zertifikats zum angegebenen Zeitpunkt bzw. Prüfzeitpunkt bereits begonnen und noch nicht abgelaufen war,

und liefert das mit einer elektronischen Signatur versehene Ergebnis der Validierung in Form des Verzeichnisdienst-Ergebnisses sowie einer Interpretation (gültig und nicht gesperrt, unbekannt oder gesperrt) zurück.

In diesem Kontext prüft das **OCSP/CRL-Relay** die mathematische Korrektheit der qualifizierten elektronischen Signaturen von Antworten auf Zertifikatsstatus-Anfragen (Online Certificate Status Protocol – OCSP) und Sperrlisten (Certificate Revocation Lists – CRLs), holt Zertifikate via Lightweight Directory Access Protocol (LDAP) ein und validiert Zertifikate der Zertifikatskette. Als Gültigkeitsmodell wird das Kettenmodell genutzt.

- Die Kommunikation zum anfordernden System⁷ – beispielsweise zu einem Verifikationsserver, OSCI-Manager oder OSCI-Backend-Enabler, die von außen über eine Schnittstelle auf das Kernsystem zugreifen können – erfolgt jeweils abgesichert, so dass die tatsächliche Anforderung bearbeitet und zutreffende Ergebnisse zurückliefert werden.

Die vorliegende Herstellererklärung bezieht sich ausschließlich auf die Eigenschaft der Software „Governikus, Version 3.2.1.0 (Basis)“ als Signaturanwendungskomponente i. S. d. § 2 Nr. 11 SigG, d.h. auf diejenigen Funktionalitäten, die dazu bestimmt sind,

- Daten dem Prozess der Prüfung qualifizierter elektronischer Signaturen zuzuführen und
- qualifizierte Signaturen zu prüfen oder qualifizierte Zertifikate nachzuprüfen.

Die Software „Governikus, Version 3.2.1.0 (Basis)“ erfüllt die Anforderungen gemäß § 17 Abs. 2 SigG sowie § 15 Abs. 2 und 4 SigV, allerdings obliegt jegliche Anzeige dem anfordernden System.

4. Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

Das Produkt „Governikus, Version 3.2.1.0 (Basis)“ erfüllt die nachfolgenden Anforderungen des SigG:

- § 17 Abs. 2 Satz 2 SigG: „Für die Überprüfung signierter Daten sind Signaturanwendungskomponenten erforderlich, die feststellen lassen, [...]
 2. ob die signierten Daten unverändert sind, [...]
 5. zu welchem Ergebnis die Nachprüfung von Zertifikaten nach § 5 Abs. 1 Satz 3 geführt hat.“

⁷ etwa die Produkte „Governikus (OSCI)“, „Virtuelle Postelle des Bundes (OSCI)“ oder „Virtuelle Postelle des Bundes (Verifikationsmodul)“

Zur Umsetzung dieser Anforderungen ist in der Software „Governikus, Version 3.2.1.0 (Basis)“ implementiert:

- Verifikation von Signaturen (lokale mathematische Prüfung) sowie
- Validierung von Zertifikaten (Überprüfung, ob die nachgeprüften qualifizierten Zertifikate im jeweiligen Zertifikatverzeichnis zum angegebenen Zeitpunkt vorhanden und nicht gesperrt waren).

Das Produkt „Governikus, Version 3.2.1.0 (Basis)“ erfüllt die nachfolgenden Anforderungen der SigV, wie in der Bestätigungsurkunde wie folgt dargestellt wird:

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

Hinweis: Die Software „Governikus, Version 3.2.1.0 (Basis)“ stellt eine serverbasierte Basiskomponente für weitere anfordernde Systeme dar, die insgesamt die Anforderungen von Signaturgesetz und -verordnung erfüllen. Die folgenden Anforderungen – insbesondere zur Interaktion mit einem Benutzer – müssen zusätzlich die anfordernden Systeme erfüllen:

- Auslösen und Autorisierung der Erzeugung einer Batchsignatur;
- Visualisierung für den Benutzer mit der in SigG/SigV normierten Anzeige.

Deshalb erfüllt dieses serverseitige Produkt „Governikus, Version 3.2.1.0 (Basis)“ die folgenden Anforderungen explizit **nicht**:

- § 17 Abs. 2 Satz 1 SigG: „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.“
- § 17 Abs. 2 Satz 2 SigG: „Für die Überprüfung signierter Daten sind Signaturanwendungskomponenten erforderlich, die feststellen lassen,

1. auf welche Daten sich die Signatur bezieht, [...]

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 [...]

- § 17 Abs. 2 Satz 3 SigG: „Signaturanwendungskomponenten müssen nach Bedarf auch den Inhalt der zu signierenden oder signierten Daten hinreichend erkennen lassen.“
- § 15 Abs. 2 Nr. 1a) und c) SigV: „Signaturanwendungskomponenten nach § 17 Abs. 2 des Signaturgesetzes müssen gewährleisten, dass bei der Erzeugung einer qualifizierten elektronischen Signatur
 - a) die Identifikationsdaten nicht preisgegeben und diese nur auf der jeweiligen sicheren Signaturerstellungseinheit gespeichert werden,
 - c) die Erzeugung einer Signatur vorher eindeutig angezeigt wird und
- § 15 Abs. 2 Nr. 2 a) und b) SigV: „Signaturanwendungskomponenten nach § 17 Abs. 2 des Signaturgesetzes müssen gewährleisten, dass bei der Prüfung einer qualifizierten elektronischen Signatur
 - a) die Korrektheit der Signatur [...] zutreffend angezeigt wird und
 - b) eindeutig [angezeigt] wird, ob die nachgeprüften qualifizierten Zertifikate im jeweiligen Zertifikat-Verzeichnis zum angegebenen Zeitpunkt vorhanden und nicht gesperrt waren.“

5. Maßnahmen in der Einsatzumgebung

5.1 Einrichtung der IT-Komponenten

Für den Betrieb der Software „Governikus, Version 3.2.1.0 (Basis)“ wird folgende Einsatzumgebung vorausgesetzt:

- AMD/Intel-PC mit 2 GB Hauptspeicher (RAM);
- Betriebssystem:
 - Microsoft Windows 2003 Server;
 - SUSE Linux Enterprise Server 10;
 - RedHat Enterprise 5
 - Solaris 9;
 - Solaris 10;
 - HP UX 11.11.
- Signaturkarte gemäß Tabelle 3, wobei die Auflagen aus der Bestätigung zu dem Produkt (siehe Registriernummer in Tabelle 3) einzuhalten sind;

- Chipkarten-Lesegerät gemäß Tabelle 3, wobei die Auflagen aus der Bestätigung zu dem Produkt (siehe Registriernummer in Tabelle 3) einzuhalten sind;
- Java Runtime Environment (JRE), Version 1.5.0 und Version 1.6.
- Anfordernde Systeme, die von außen über eine Schnittstelle auf das Produkt zugreifen und Funktionalitäten des Produktes nutzen, stehen zur Verfügung und erfüllen die Anforderungen von Signaturgesetz und -verordnung an eine Signaturanwendungskomponente. Insbesondere gewährleisten sie die SigG-relevanten Funktionalitäten hinsichtlich Autorisierung zur Erzeugung von Batchsignaturen und Visualisierung.⁶

Das Produkt „Governikus, Version 3.2.1.0 (Basis)“ darf ausschließlich innerhalb der oben beschriebenen Hard- und Softwareausstattung eingesetzt werden.

5.2 Anbindung an ein Netzwerk

Zur Anbindung des Produktes „Governikus, Version 3.2.1.0 (Basis)“ an ein Netzwerk müssen die folgenden Maßnahmen zum Schutz beachtet werden: 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.

Die in diesem Abschnitt gemachten Auflagen müssen eingehalten werden.

5.3 Auslieferung und Installation

Die Auslieferung erfolgt online per Download von einem Webserver.⁸

Alle Dateien der Software „Governikus, Version 3.2.1.0 (Basis)“ werden vor der Auslieferung vom Hersteller signiert, um Schutz vor unerkannten nachträglichen Manipulationen und Veränderungen zu bieten. Der Nutzer sollte sich vor der Installation der Software „Governikus, Version 3.2.1.0 (Basis)“ von der Gültigkeit der Signatur überzeugen. Die Verifikation der Signatur erfolgt über Standard-Java-Mechanismen.

Die Installation des „Governikus, Version 3.2.1.0 (Basis)“ wird ausführlich im Handbuch erläutert.

5.4 Auflagen für den Betrieb des Produktes

Während des Betriebs sind die folgenden Bedingungen für den sachgemäßen Einsatz zu beachten:

Auflagen zur Sicherheit der IT-Plattform und Applikationen

Es muss gewährleistet sein, dass von der Hardware, auf der die Software „Governikus, Version 3.2.1.0 (Basis)“ betrieben wird, keine Angriffe ausgehen. Insbesondere ist sicherzustellen, dass

- die auf dem eingesetzten Personalcomputer installierte Software – insbesondere die Java Virtual Maschine – nicht böswillig manipuliert oder verändert werden kann,
- auf dem Personalcomputer keine Viren oder Trojanischen Pferde eingeschleppt werden können,
- die Hardware des Personalcomputers nicht unzulässig verändert werden kann,

⁸ Abweichend von der bestätigten Version dieses Produktes wird für diese Version ausschließlich die Online-Auslieferung via Download angeboten.

- der verwendete Chipkartenleser nicht böswillig manipuliert wurde, um Daten (z. B. PIN, Hashwerte etc.) auszuforschen oder zu verändern.

Das Ausforschen der PIN auf dem Personalcomputer kann nur dann mit Sicherheit ausgeschlossen werden, wenn ein Chipkartenleser mit sicherer PIN-Eingabe eingesetzt wird.

Rechner und Chipkartenleser sind durch einen sicheren Kanal per Kabel verbunden.

Auflagen zum Schutz vor manuellem Zugriff Unbefugter

Die eingesetzten Server müssen gegen einen manuellen Zugriff Unbefugter geschützt werden – insbesondere, um Manipulation von Dateien auf Dateisystemebene, die die Software zur Darstellung der Nachrichten benötigt, zu unterbinden. Dies kann z. B. durch Aufstellung in einem abschließbaren Raum geschehen.

Für die Aufbewahrung der "Signatur-Arbeitsstation", bestehend aus Software, Chipkartenleser, Signaturkarten, Monitor, Tastatur und Rechner, ist ein zugriffssicherer Betriebsraum erforderlich, so dass ein Zugriff Unbefugter ausgeschlossen ist oder zumindest mit hoher Sicherheit erkennbar wird. Rechner, Chipkartenleser, Signaturkarten, Monitor und Tastatur befinden sich in einem Betriebsraum. Ein Signaturschlüssel-Inhaber erhält den Zugang zum zugriffssicheren Betriebsraum nur durch den Schlüssel-Administrator, der den Aufenthalt überwacht.

Die Unterrichtung des Zertifizierungsdiensteanbieters zur Handhabung der SSEE ist zu beachten.

Auflagen zum Schutz vor Angriffen über Datenaustausch per Datenträger

Bei Einspielen von Daten über Datenträger muss – z. B. durch die Verwendung geeigneter Anti-Viren-Programme – sichergestellt werden, dass keine Viren oder Trojanischen Pferde eingespielt werden können.

Auflagen zum Schutz vor Fehlern bei Betrieb/Nutzung

Folgende Auflagen sind für den sachgemäßen Einsatz der Software „Governikus, Version 3.2.1.0 (Basis)“ zu beachten:

- Es wird eine vertrauenswürdige Eingabe der PIN vorausgesetzt. Der Nutzer hat dafür Sorge zu tragen, dass die Eingabe der PIN weder beobachtet noch die PIN anderen Personen bekannt gemacht wird.
- Nur bei dem Betrieb eines bestätigten Chipkartenlesers mit PIN-Pad ist sicher gestellt, dass die PIN nur zur SSEE übertragen wird.
- Eine signaturgesetz-konforme Nachprüfung qualifizierter Zertifikate kann nur erfolgen, soweit dafür die technischen Voraussetzungen – etwa über die Verbindung zu Verzeichnisdiensten – gegeben sind.

Auflagen für Wartung/Reparatur

Eine Pflege und Wartung der Software „Governikus, Version 3.2.1.0 (Basis)“ ist nicht vorgesehen. Ggf. erfolgt eine Aktualisierung über einen Download von einem Webserver.

6. Algorithmen und zugehörige Parameter

Zur Erzeugung qualifizierter elektronischer Signaturen werden vom Produkt Governikus, Version 3.2.1.0 (Basis) die Hashfunktionen SHA-256 und RIPEMD-160 bereitgestellt.⁹

Zur Prüfung qualifizierter elektronischer Signaturen werden vom Produkt Governikus, Version 3.2.1.0 (Basis) die Hashfunktionen SHA-256, RIPEMD-160 und SHA-1 sowie der Signaturalgorithmus RSA bereitgestellt.

Die gemäß Anlage I Abs. 1 Nr. 2 SigV festgelegte Eignung für die verwendeten kryptographischen Algorithmen SHA-256, RIPEMD-160 und SHA-1 sind gemäß den Angaben der Bundesnetzagentur (vgl. „Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen)“ der Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahn vom 17. Dezember 2007, veröffentlicht am 05. Februar 2008 im Bundesanzeiger Nr. 19, S. 376) wie folgt als geeignet eingestuft:

- RIPEMD-160: gültig bis 31.12.2010;
- SHA-2 Familie (SHA-224, SHA-256, SHA-384, SHA-512): gültig bis 31.12.2014;
- SHA-1: ungültig; war gültig bis 31.7.2008 (Der Benutzer kann über das anfordernde System die Prüfung eines Zertifikates zu einem zurückliegenden Prüfzeitpunkt anfordern, zu dem SHA-1 noch gültig gewesen sein kann.)
- RSA mit Schlüssellänge 2048 Bit: gültig bis 31.12.2014.

7. Gültigkeit der Herstellererklärung

Diese Erklärung ist bis zu ihrem Widerruf, längstens jedoch bis zum 31.12.2010 gültig. Die Gültigkeit der Herstellererklärung ist weiter beschränkt durch die in Kapitel 6 aufgeführten Gültigkeiten der Algorithmen; die Gültigkeit kann sich verkürzen, wenn z.B. neue Feststellungen hinsichtlich der Sicherheit des Produktes oder der Eignung der Algorithmen im Bundesanzeiger veröffentlicht werden.

Der aktuelle Status der Gültigkeit der Erklärung ist bei der zuständigen Behörde (Bundesnetzagentur, Referat Qualifizierte Elektronische Signatur – Technischer Betrieb) zu erfragen.

8. Zusatzdokumentation

Folgende Bestandteile der Herstellererklärung wurden aus dem Veröffentlichungstext ausgegliedert und bei der zuständigen Behörde hinterlegt:

- „Unterlagen zur Herstellererklärung gemäß § 17 Abs. 4 SigG für die Software ‚Governikus, Version 3.2.1.0 (Basis)‘ – Sicherheitstechnische Produktbeschreibung, Spezifikation und Tests“, 21.05.2008, 15 Seiten.
- „Betriebshandbuch ‚Governikus – Teil der virtuellen Poststelle des Bundes““, Dokument-Version 3.2.1.0_0, 10.04.2008, 217 Seiten.

⁹ Hinweis: Das Produkt Governikus, Version 3.2.1.0 (Basis) unterstützt ferner die Hashfunktion SHA-1, die allerdings zum 31.7.2008 ausgelaufen ist, so dass aufgrund der abgelaufenen oder gesperrten Zertifikate keine qualifizierten elektronischen Signaturen mehr erzeugt werden können.

- „Entwicklerhandbuch ‚Governikus – Teil der virtuellen Poststelle des Bundes‘“, Dokument-Version 3.2.1.0_0, 10.04.2008, 70 Seiten.
- „Installation ‚Governikus – Teil der virtuellen Poststelle des Bundes‘“, Dokument-Version 3.2.1.0_0, 10.04.2008, 103 Seiten.
- Testhandbuch „Kernsystem“, Dokument-Version 1.4, 19.04.2007, 35 Seiten
- Testhandbuch „OCSP/CRL-Relay“, Dokument-Version 1.1, 16.06.2006, 21 Seiten
- Testdokumentation CORE_NS_Testprotokoll.xls
- Testdokumentation OCSP_CRL_RELAY_Testprotokoll_Linux_3_2_1.xls
- „Sicherheitsvorgaben (ST), ‚Virtuelle Poststelle des Bundes 2.2.x.x (Basis)‘“, Dokument-Version 1.0, 21.11.2007, 83 Seiten
- „Funktionale Spezifikation (ADV_FSP) ‚Virtuelle Poststelle des Bundes 2.2.x.x (Basis)‘“, Dokument-Version 0.91, 16.03.2006, 73 Seiten
- „Entwurf auf hoher Ebene (ADV_HLD) ‚Virtuelle Poststelle des Bundes 2.2.x.x (Basis)‘“, Dokument-Version 0.91, 21.03.2006, 50 Seiten

Die Dokumente wurden von der bremen online services Entwicklungs- und Betriebsgesellschaft mbH & Co. KG erstellt.

Ende der Herstellererklärung