

Herstellereklärung

Der Hersteller

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

Am Fallturm 9

28359 Bremen

erklärt hiermit gemäß § 17 Abs. 4 Satz 2 SigG¹

in Verbindung mit § 15 Abs. 5 SigV²,

dass sein Produkt

Governikus Signer, Version 2.1.0.0

die nachstehend genannten Anforderungen des Signaturgesetzes¹ bzw. der Signaturverordnung² in Teilen erfüllt.

Bremen, den 03.03.2009

gez. Dr. Stephan Klein

Geschäftsführung

Diese Herstellereklärung mit der Dokumentennummer bos2009001 besteht aus 28 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	Autor	Bemerkung
1.0	03.03.2009	bremen online services Entwicklungs- und Betriebsgesellschaft mbH & Co. KG	Initialversion

Beschreibung des Produkts

1 Handelsbezeichnung

Die Handelsbezeichnung lautet: Governikus Signer, Version 2.1.0.0³

Die Handelsbezeichnung umfasst folgende Varianten der Software:

„Governikus Signer, Version 2.1.0.0 Basic Edition“

„Governikus Signer, Version 2.1.0.0 Professional Edition“

„Governikus Signer, Version 2.1.0.0 Integration Edition“.

Auslieferung: online per Download

Hersteller: bremen online services Entwicklungs- und Betriebsgesellschaft mbH & Co. KG (bos KG), Am Fallturm 9, 28359 Bremen

Handelsregisterauszug: HRA 22041

2 Lieferumfang und Versionsinformationen

Nachfolgend ist der Lieferumfang, einschließlich der Versionsinformationen, aufgezählt:

Produktart	Bezeichnung	Version	Übergabeform
Software	Governikus Signer Basic Edition	2.1.0.0	online per Download
	Governikus Signer Professional Edition	2.1.0.0	online per Download
	Governikus Signer Integration Edition	2.1.0.0	online per Download
Dokumentation	Governikus Signer Benutzerhandbuch	2.1_0	online per Download ⁵
	Governikus Signer Systemanforderungen	2.1.0.0	online per Download ⁵
	bos-Prüfprotokoll	1.5.0	online per Download ⁵
	Governikus Signer Integration Edition Entwicklerhandbuch	2.1_0	online per Download
	Governikus Signer Integration Edition Administratorhandbuch	2.1_0	online per Download

Tabelle 1: Lieferumfang und Versionsinformation

³ Das Produkt „Governikus Signer, Version 2.1.0.0“ ist in drei Varianten verfügbar (vgl. Abschnitt 3). Die vorliegende Herstellereklärung bezieht sich auf alle drei Varianten. Es wird dabei einheitlich die Bezeichnung „Governikus Signer, Version 2.1.0.0“ verwendet.

⁵ Dieses Dokument steht zum einen separat zum Download zur Verfügung und ist zum anderen auch Bestandteil der Softwareinstallation.

Die Software „Governikus Signer, Version 2.1.0.0“ besteht aus den in der folgenden Tabelle aufgeführten Dateien:

Datei	Version	Größe	Hersteller/Herausgeber
Governikus Signer-JAR-Dateien			
bc.gov.server-jdk15-139-bos-0.1.jar	jdk15-139-bos-0.1	2.362.432	bos KG
bos_base64.jar	-	8.373	bos KG
bos_licence.jar	2.1.0.0	2.827 ⁶ 2.823 ⁷ 2.827 ⁸	bos KG
bos_unlimited_strength_jurisdiction_policy_files_installer.jar	1.1.0	49.850	bos KG
CertificateViewer.jar	3.3.0.0	30.958	bos KG
ci.jar	CI_1_6_0	248.668	bos KG
clientenabler.jar	3.3.0.0	505.634	bos KG
commons.jar	1.2.2	137.414	bos KG
commons_http_utils.jar	2_1_0	141.344	bos KG
debug_mode.jar	1.0.0	13.039	bos KG
DIHandler.jar	3.3.0.0	247.199	bos KG
eCardAPI.jar	1.0.25	1.370.996	bos KG
gov2netsignerclient.jar	3.3	54.108	bos KG
gov2server_common.jar	-	107.791	bos KG
gov2server_utils.jar	-	98.466	bos KG
jca_ocf_provider_netsigner_signed.jar	3.3.0.0	109.160	bos KG
libOCFPCSC1.so ⁹	MCARD_1_9_0	33.298	bos KG
mcardStaple.jar	MCARD_1_9_0	878.605	bos KG
OCFPCSC1.dll ¹⁰	MCARD_1_9_0	63.488	bos KG
osci-bibliothek.jar	1.3	342.761	bos KG
plugin_sdk.jar	3.3.0.0	23.787	bos KG
streamedpkcs7.jar	3.3.0.0	10.747	bos KG
vi.jar	1_5_0	128.062	bos KG

⁶ Nur Variante „Governikus Signer, Version 2.1.0.0 Basic Edition“

⁷ Nur Variante „Governikus Signer, Version 2.1.0.0 Professional Edition“

⁸ Nur Variante „Governikus Signer, Version 2.1.0.0 Integration Edition“

⁹ Nur bei einer Installation unter Linux enthalten

¹⁰ Nur bei einer Installation unter Microsoft Windows enthalten

Datei	Version	Größe	Hersteller/Herausgeber
viewer_modules.jar	-	1.197.862	bos KG
viewermodules.jar	3.3.0.0	1.375	bos KG
viewerPKCS7.jar	-	238.025	bos KG
GovernikusSigner.jar	2.1.0.0	1.769.920	bos KG
helpset_de.jar	2.1.0.0	109.838	bos KG
helpset_en.jar	2.1.0.0	81.824	bos KG
Third Party DLL- und JAR-Dateien			
commons-codec-1.3.jar	1.3	46.725	Apache Software Foundation
commons-httpclient-3.0.1.jar	3.0.1	279.781	Apache Software Foundation
commons-logging.jar	1.0.3	31.605	Apache Software Foundation
leEmbed.exe ¹⁰		61.440	JDesktop Integration Components (JDIC) Project
itext-1.4.5.jar	1.4.5	1.841.952	com.lowagie.tools.Toolbox
jai_codec.jar	1.1.2	213.579	Sun Microsystems, Inc.
jai_core.jar	1.1.2	1.576.539	Sun Microsystems, Inc.
jbossall-client.jar	4.2.2.GA	4.945.303	JBoss Inc.
jdic.jar	jdic-20061102	58.761	JDesktop Integration Components (JDIC) Project
jdic.dll ¹⁰	0.9.1.0	110.592	JDesktop Integration Components (JDIC) Project
jdic_stub.jar	jdic-20061102	31.640	JDesktop Integration Components (JDIC) Project
jhall.jar	2.0_01	557.529	Sun Microsystems, Inc
jRegistryKey.jar	1.2.3	9.835	BEQ Technologies / http://sourceforge.net/projects/jregistrykey
jRegistryKey.dll ¹⁰	1.2.3	30.160	BEQ Technologies / http://sourceforge.net/projects/jregistrykey
Libjdic.so ⁹	jdic-20061102	21.447	JDesktop Integration Components (JDIC) Project
Libmozembed-linux-gtk1.2.so ⁹	jdic-20061102	469.368	JDesktop Integration Components (JDIC) Project
Libmozembed-linux-gtk2.so ⁹	jdic-20061102	250.273	JDesktop Integration Components (JDIC) Project
Libtray.so ⁹	jdic-20061102	18.501	JDesktop Integration Components (JDIC) Project
log4j-1.2.15.jar	1.2.15	391.834	Apache Software Foundation
mail.jar	1.3.1	327.603	Sun Microsystems, Inc.
MozEmbed.exe ¹⁰	jdic-20061102	192.512	JDesktop Integration Components (JDIC) Project

Datei	Version	Größe	Hersteller/Herausgeber
Mozembed-linux-gtk2 ⁹	jdic-20061102	9.547	JDesktop Integration Components (JDIC) Project
Mozembed-linux-gtk1.2 ⁹	jdic-20061102	9.511	JDesktop Integration Components (JDIC) Project
serializer.jar	2.7.0	188.993	Apache Software Foundation
tray.dll ¹⁰	0.9.1.0	45.056	JDesktop Integration Components (JDIC) Project
webservices-api.jar	2.1	174.830	Sun Microsystems, Inc.
webservices-rt.jar	1.0	12.167.133	Sun Microsystems, Inc.
webservices-tools.jar	1.0	3.634.260	Sun Microsystems, Inc.
win32com.dll ¹⁰	1.6.1	27.648	Sun Microsystems, Inc
xalan.jar	2.7.0	3.078.601	Apache Software Foundation
xercesImpl-2.9.0.jar	2.9.0	1.223.877	Apache Software Foundation
xml-apis-2.9.0.jar	2.9.0	194.354	Apache Software Foundation
xmlsec-1.4.1.jar	1.4.1	415.492	

Tabelle 2: Enthaltene Dateien

Alle Dateien der Software werden vor der Auslieferung vom Hersteller signiert, um Schutz vor unerkannten nachträglichen Manipulationen zu bieten. Das der Signatur zugrunde liegende Zertifikat wird vom Hersteller auf seiner Web-Seite (www.bos-bremen.de) zur Verfügung gestellt.

Das Produkt „Governikus Signer, Version 2.1.0.0“ 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):

Produkt-klasse	Bezeichnung (Herausgeber/Hersteller, Handelsbezeichnung, Bezeichnung in der Bestätigung)		Beschreibung + Registrierungsnummer der Bestätigung
SSEE	Produktzentrum TeleSec der Deutschen Telekom AG (T-Systems Enterprise Services GmbH)	Telesec NetKey 3.0 mit PKS Signaturerstellungseinheit TCOS 3.0 Signature Card, Version 1.0	TUVIT.93119.TE.09.2006
SSEE	Produktzentrum TeleSec der Deutschen Telekom AG (T-Systems Enterprise Services GmbH)	Telesec NetKey 3.0 M mit PKS ¹¹ Signaturerstellungseinheit TCOS 3.0 Signature Card, Version 1.0	TUVIT.93119.TE.09.2006
SSEE	Bundesnotarkammer, Zertifizierungsstelle	Signaturkarte der Bundesnotarkammer, qualifizierte elektronische Signatur ¹²	TUVIT.93100.TE.09.2005 Nachträge vom 08.08.2006,

¹¹ Hierbei handelt es sich um eine Multisignaturkarte. Die Anzahl der möglichen Signaturerzeugungen nach einer erfolgreichen Authentifizierung mit der Signatur-PIN ist durch die Software „Governikus Signer, Version 2.1.0.0“ bei lokaler Verwendung auf 1 begrenzt.

Produkt-klasse	Bezeichnung (Herausgeber/Hersteller, Handelsbezeichnung, Bezeichnung in der Bestätigung)	Beschreibung + Registrierungsnummer der Bestätigung	
	(Giesecke & Devrient GmbH)	Signaturerstellungseinheit STARCOS 3.0	20.10.2006 und 07.12.2006
SSEE	DATEV eG Zertifizierungsstelle (Giesecke & Devrient GmbH)	zertifizierte Signaturkarte für Berufsträger der DATEV (2048 Bit RSA Schlüssellänge) Signaturerstellungseinheit STARCOS 3.0	TUVIT.93100.TE.09.2005 Nachträge vom 08.08.2006, 20.10.2006 und 07.12.2006
SSEE	D-Trust GmbH (Siemens AG)	D-TRUST Card 2.02c, 2.2, 2.3, 2.4 SEE „Chipkarte mit Prozessor SLE66CX322P, CardOS V4.3B mit Applikation für digitale Signatur“	T-Systems.02122.TE.05.2005 Nachtrag vom 06.05.2008
SSEE	Deutsche Post Com GmbH Geschäftsfeld Signtrust (Giesecke & Devrient GmbH)	SIGNTRUST CARD Signaturerstellungseinheit STARCOS 3.0	TUVIT.93100.TE.09.2005 Nachträge vom 08.08.2006, 20.10.2006 und 07.12.2006
SSEE	Deutsche Post Com GmbH Geschäftsfeld Signtrust	SIGNTRUST MCARD 100 ¹² Signaturerstellungseinheit STARCOS 3.0	TUVIT.93100.TE.09.2005 Nachträge vom 08.08.2006, 20.10.2006 und 07.12.2006
SSEE	Deutsche Post Com GmbH Geschäftsfeld Signtrust	SIGNTRUST MCARD ¹¹ Signaturerstellungseinheit STARCOS 3.0	TUVIT.93100.TE.09.2005 Nachträge vom 08.08.2006, 20.10.2006 und 07.12.2006
SSEE	TC TrustCenter TrustCenter GmbH	TC-Trustcenter QSign-Card (limited) SEE „Chipkarte mit Prozessor SLE66CX322P, CardOS V4.3B mit Applikation für digitale Signatur“	T-Systems.02122.TE.05. 2005
SSEE	TC TrustCenter TrustCenter GmbH	TC-Trustcenter QSign-Card (unlimited) ¹¹ SEE „Chipkarte mit Prozessor SLE66CX322P, CardOS V4.3B mit Applikation für digitale Signatur“	T-Systems.02122.TE.05. 2005
SSEE	D-Trust GmbH	D-TRUST Card 2.02c 2.2, 2.3, 2.4 SEE „Chipkarte mit Prozessor SLE66CX322P, CardOS V4.3B mit Applikation für digitale Signatur“	T-Systems.02122.TE.05. 2005
SSEE	D-Trust GmbH	D-Trust-Multicard ¹¹	T-Systems.02122.TE.05. 2005

¹² Hierbei handelt es sich um eine Stapelsignaturkarte, die eine Anzahl von maximal 100 Signaturen mit nur einer einmaligen PIN-Eingabe ermöglicht. Die Software „Governikus Signer, Version 2.1.0.0“ unterstützt diese Funktionalität (vgl. Abschnitt 3.1).

Produkt- klasse	Bezeichnung (Herausgeber/Hersteller, Handelsbe- zeichnung, Bezeichnung in der Bestätigung)	Beschreibung + Registrier- nummer der Bestätigung	
		SEE „Chipkarte mit Prozes- sor SLE66CX322P, CardOS V4.3B mit Applikation für digitale Signatur“	
SSEE	S-Trust, Deutscher Sparkassen Verlag GmbH (Gemplus-mids GmbH)	SparkassenCard oder Geld- Karte SEE ZKA-Signaturkarte, Version 5.02	TUVIT.09385.TU.09.2004
SSEE	S-Trust, Deutscher Sparkassen Verlag GmbH (Giesecke & Devrient GmbH)	SparkassenCard oder Geld- Karte SEE ZKA Banking Signature Card, Version 6.2b NP und 6.2f NP, Type 3	TUVIT.09395.TU.01.2005
SSEE	S-Trust, Deutscher Sparkassen Verlag GmbH (Giesecke & Devrient GmbH)	SparkassenCard oder Geld- Karte SEE ZKA Banking Signature Card, Version 6.31 NP, Type 3	TUVIT.09397.TU.03.2005
SSEE	S-Trust, Deutscher Sparkassen Verlag GmbH (Giesecke & Devrient GmbH)	SparkassenCard oder Geld- Karte SEE ZKA Banking Signature Card, Version 6.32 NP, Type 3	TUVIT.93125.TU.12.2005
SSEE	S-Trust, Deutscher Sparkassen Verlag GmbH (Giesecke & Devrient GmbH)	SparkassenCard oder Geld- Karte SEE ZKA Banking Signature Card, Version 6.4	TUVIT.93123.TU.12.2006
SSEE	S-Trust, Deutscher Sparkassen Verlag GmbH (Gemplus GmbH)	SparkassenCard oder Geld- Karte SEE ZKA-Signaturkarte, Version 5.10	TUVIT.93132.TU.06.2006
SSEE	S-Trust, Deutscher Sparkassen Verlag GmbH (Giesecke & Devrient GmbH)	SparkassenCard oder Geld- Karte SEE ZKA Banking Signature Card, Version 6.6	TUVIT.93130.TU.05.2006
SSEE	S-Trust, Deutscher Sparkassen Verlag GmbH (Giesecke & Devrient GmbH)	SparkassenCard oder Geld- Karte SEE ZKA Banking Signature Card, Version 6.51 der Giesecke & Devrient GmbH	TUVIT.93129.TU.03.2006
SSEE	S-Trust, Deutscher Sparkassen Verlag GmbH (Sagem Orga GmbH)	SparkassenCard oder Geld- Karte Signaturerstellungseinheit ZKA SECCOS Sig v1.5.3	BSI.02076.TE.12.2006
SSEE	S-Trust, Deutscher Sparkassen Verlag	SparkassenCard oder Geld- Karte	TUVIT.93138.TU.11.2006

Produkt-klasse	Bezeichnung (Herausgeber/Hersteller, Handelsbezeichnung, Bezeichnung in der Bestätigung)	Beschreibung + Registrierungsnummer der Bestätigung	
	GmbH (Gemplus GmbH)	ZKA-Signaturkarte, Version 5.11	
SSEE	S-Trust, Deutscher Sparkassen Verlag GmbH (Giesecke & Devrient GmbH)	SparkassenCard oder Geld-Karte SEE ZKA Banking Signature Card, Version 6.5	TUVIT.93120.TU.09.2005
SSEE	S-Trust, Deutscher Sparkassen Verlag GmbH (Gematlo GmbH)	SparkassenCard oder Geld-Karte SEE ZKA-Signaturkarte, Version 6	TUVIT.93143.TE.11.2007
SSEE	S-Trust, Deutscher Sparkassen Verlag GmbH (Giesecke & Devrient GmbH)	SparkassenCard oder Geld-Karte SEE ZKA Banking Signature Card, Version 7.1	TUVIT.93149.TE.09.2007
SSEE	S-Trust, Deutscher Sparkassen Verlag GmbH (Giesecke & Devrient GmbH)	SparkassenCard oder Geld-Karte SEE ZKA Banking Signature Card, Version 7.1.1	TUVIT.93159.TE.09.2007
SSEE	S-Trust, Deutscher Sparkassen Verlag GmbH (Giesecke & Devrient GmbH)	SparkassenCard oder Geld-Karte SEE ZKA Banking Signature Card, Version 7.1.2	TUVIT.93166.TU.06.2008
SSEE	S-Trust, Deutscher Sparkassen Verlag GmbH (Giesecke & Devrient GmbH)	SparkassenCard oder Geld-Karte SEE ZKA Banking Signature Card, Version 7.2.1	TUVIT.93157.TE.06.2008
SSEE	S-Trust, Deutscher Sparkassen Verlag GmbH (Gematlo GmbH)	SparkassenCard oder Geld-Karte SEE ZKA Signatur-Karte, Version 6.01	TUVIT.93169.TU.09.2008
SSEE	S-Trust, Deutscher Sparkassen Verlag GmbH (Gemplus GmbH)	S-Trust Multisignaturkarte ¹¹ Multisignaturerstellungseinheit ZKA Banking Signature Card Version 5.11M	TUVIT.93148.TU.06.2007
SSEE	Deutsche Rentenversicherung Bund (Siemens AG)	Signaturkarte der Deutschen Rente Bund SEE „Chipkarte mit Prozessor SLE66CX322P, CardOS V4.3B mit Applikation für digitale Signatur	T-Systems.02122.TE.05. 2005
SSEE	Deutsche Rentenversicherung Bund (Siemens AG)	Signaturkarte der Deutschen Rente Bund ¹¹ SEE „Chipkarte mit Prozessor SLE66CX322P, CardOS	T-Systems.02122.TE.05. 2005

Produkt-klasse	Bezeichnung (Herausgeber/Hersteller, Handelsbezeichnung, Bezeichnung in der Bestätigung)	Beschreibung + Registrierungsnummer der Bestätigung	
		V4.3B mit Applikation für digitale Signatur“	
Kartenleser	OMNIKEY GmbH	CardMan 3621 SAK Chipkartenterminal der Familie CardMan Trust CM3621, Firmware-Version 6.00	BSI.02057.TE.12.2005
Kartenleser	OMNIKEY GmbH	CardMan 3821 SAK Chipkartenterminal der Familie CardMan Trust CM3821, Firmware-Version 6.00	BSI.02057.TE.12.2005
Kartenleser	Cherry GmbH	Cherry Smartboard G83-6744 Chipkartenterminal der Familie SmartBoard xx44 Firmware-Version 1.04	BSI.02048.TE.12.2004
Kartenleser	Cherry GmbH	Cherry SmartTerminal 2000 U Chipkartenterminal der Familie SmartTerminal ST-2xxx, Firmware Version 5.11	BSI.02095.TE.10.2007
Kartenleser	Reiner Kartengeräte GmbH & Co, KG	CyberJack e-com Chipkartenleser, cyberJack e-com, Version 3.0	TUVIT.93155.TE.09.2008
Kartenleser	Reiner Kartengeräte GmbH & Co, KG	cyberJack secoder Chipkartenleser, cyberJack secoder, Version 3.0	TUVIT.93154.TE.09.2008
Kartenleser	Reiner Kartengeräte GmbH & Co, KG	CyberJack pinpad Chipkartenleser, cyberJack pinpad, Version 2.0	TUVIT. 09362.TE.05.2002
Kartenleser	Reiner Kartengeräte GmbH & Co, KG	CyberJack pinpad Version 3 Chipkartenleser, cyberJack pinpad, Version 3.0	TUVIT.93107.TU.11.2004
Kartenleser	Kobil Systems GmbH	Kobil KAAAN Advanced Chipkartenterminal KAAAN Advanced, Firmware Version 1.02, Hardware Version K104R3	BSI.02050.TE.12.2006
Kartenleser	Kobil Systems GmbH	Kobil KAAAN Prof. seriell KOBIL Chipkartenterminal KAAAN Professional HWVersion KCT100, FW 2.08 GK 1.04	TUVIT.09331.TE.03.2002
Kartenleser	SCM Microsystems	SPR 332	TUVIT.09370.TE.03.2003

Produkt-klasse	Bezeichnung (Herausgeber/Hersteller, Handelsbezeichnung, Bezeichnung in der Bestätigung)		Beschreibung + Registrierungsnummer der Bestätigung
ser	GmbH	Chipkartenleser SPR132, SPR332, SPR532, Firmware Version 4.15	
Kartenleser	SCM Microsystems GmbH	SPR 532 usb (Chipdrive pinpad pro) Chipkartenleser SPR132, SPR332, SPR532, Firmware Version 4.15	TUVIT.09370.TE.03.2003
Kartenleser	Fujitsu Siemens Computers GmbH	Chipkartenleser-Tastatur KB SCR Pro Chipkartenleser-Tastatur Sachnummer S26381-K329-V2xx Firmware Version 1.06	BSI.02082.TE.01.2007

Tabelle 3: Zusätzliche Produkte

Für die Prüffunktionalität sowie die Multisignaturerstellung nutzt das Produkt „Governikus Signer, Version 2.1.0.0“ außerdem das folgende zu Signaturgesetz und -verordnung konforme Produkt, welches ebenfalls von der bremen online services Entwicklungs- und Betriebsgesellschaft mbH & Co. KG hergestellt wird, jedoch nicht Bestandteil dieser Erklärung ist:

Produktklasse	Hersteller	Bezeichnung
Signaturanwendungskomponente	bremen online services Entwicklungs- und Betriebsgesellschaft mbH & Co. KG	Governikus – Teil der virtuellen Poststelle des Bundes ¹³ , Version 3.3.1.0 (Basis)
Signaturanwendungskomponente	bremen online services Entwicklungs- und Betriebsgesellschaft mbH & Co. KG	Virtuelle Poststelle des Bundes ¹⁴ , Version 2.2.2.6 (Verifikationsmodul)
Signaturanwendungskomponente	bremen online services Entwicklungs- und Betriebsgesellschaft mbH & Co. KG	Virtuelle Poststelle des Bundes ¹⁵ , Version 2.2.2.6 (Basis)

Tabelle 4: Zusätzliche SigG- und SigV-konforme Produkte

¹³ Die Software „Governikus, Version 3.3.1.0 (Basis)“ ist als Signaturanwendungskomponente unter der Registriernummer BSI.02113.TE.03.2009 nach SigG bestätigt. Diese Bestätigung umfasst u.a. die Governikus-Komponenten „NetSigner“ sowie das Kernsystem.

¹⁴ Die Software „Virtuelle Poststelle des Bundes (Verifikationsmodul), Version 2.2.2.6“ ist als Signaturanwendungskomponente unter der Registriernummer BSI.02071.TE.11.2007 nach SigG bestätigt. Diese Bestätigung beinhaltet u.a. die Komponente „Verifikationsserver“.

¹⁵ Die Software „Virtuelle Poststelle des Bundes (Basis), Version 2.2.2.6“ ist als Signaturanwendungskomponente unter der Registriernummer BSI.02070.TE.11.2007 nach SigG bestätigt. Diese Bestätigung beinhaltet u.a. die Komponente „OCSP/CRL-Relay“ sowie das „Kernsystem“.

3 Funktionsbeschreibung

Die Software „Governikus Signer, Version 2.1.0.0“ ist Teil einer Signaturanwendungskomponente gemäß § 2 Nr. 11 SigG; die auf geeigneter Hardware mit geeigneten Betriebsmitteln – insbesondere mit SigG-konformen Chipkartenlesern und sicheren Signaturerstellungseinheiten in einem „geschützten Einsatzbereich (Regelfall/Standardlösung)“ [BNetzA2005] betrieben und über eine Oberfläche (Graphical User Interface – GUI) von einem autorisierten Nutzer konfiguriert und genutzt wird.

Die vorliegende Herstellereklärung bezieht sich ausschließlich auf die Eigenschaft der Software „Governikus Signer, Version 2.1.0.0“ als Signaturanwendungskomponente i. S. d. § 2 Nr. 11 SigG, d. h. auf diejenigen Funktionalitäten, die dazu bestimmt sind,

- Daten dem Prozess der Erzeugung oder Prüfung qualifizierter elektronischer Signaturen zuzuführen oder
- qualifizierte elektronische Signaturen zu prüfen oder qualifizierte Zertifikate nachzuprüfen und die Ergebnisse anzuzeigen.

Die Software „Governikus Signer, Version 2.1.0.0“ umfasst keine Chipkartenleser oder sichere Signaturerstellungseinheiten.

Die Software „Governikus Signer, Version 2.1.0.0“ ist in drei Varianten verfügbar:

- **„Governikus Signer, Version 2.1.0.0 Basic Edition“**
Durch einen Benutzer installierbare und startbare Variante mit Basis-Funktionsumfang
- **„Governikus Signer, Version 2.1.0.0 Professional Edition“**
Wie „Basic Edition“, jedoch mit erweitertem Funktionsumfang
- **„Governikus Signer, Version 2.1.0.0 Integration Edition“**
Variante zur Integration in andere (Fach-)Anwendungen. Nur über Schnittstellen startbar. Gegenüber der „Basic Edition“ erweiterter Funktionsumfang.

Alle drei Varianten sind technisch identisch. Die vorliegende Herstellereklärung bezieht sich auf alle drei Varianten. Es wird dabei einheitlich die Bezeichnung „Governikus Signer, Version 2.1.0.0“ verwendet. Sofern nachfolgend Funktionen oder Eigenschaften beschrieben werden, die nicht für alle Varianten gleichermaßen gelten, werden die relevanten Varianten explizit namentlich genannt.

Bei dem nachfolgend beschriebenen Funktionsumfang wird der Benutzer durch visuelle Anzeigen begleitet.

3.1 Erzeugung von Signaturen

Die Software „Governikus Signer, Version 2.1.0.0“ stellt folgende Funktionen zur Erzeugung qualifizierter elektronischer Signaturen zur Verfügung.

- Die Software „Governikus Signer, Version 2.1.0.0“ unterstützt den Signaturschlüssel-Inhaber bei der Erzeugung von qualifizierten elektronischen Signaturen, die lokal von einer sicheren Signaturerstellungseinheit erzeugt werden („Lokalsignatur“).
- Es können beliebige Dokumente signiert werden – beispielsweise
 - Word-Dateien,
 - Excel-Dateien,
 - PDF,
 - XML-Datensätze.

- Darüber hinaus muss sich der Benutzer vergewissern, dass das benutzte Format vom Empfänger zugelassen und akzeptiert ist.
- Der Signaturschlüssel-Inhaber hat an seinem Arbeitsplatz unmittelbar zur Signaturerzeugung Zugriff auf seine sichere Signaturerstellungseinheit (SSEE) und den Chipkartenleser.
- Sobald eine SSEE erkannt bzw. ausgewählt wurde, kann ein Dokument signiert werden. Das ausgewählte Signaturzertifikat und sein Signaturniveau werden dabei angezeigt.
- Zum Signieren sind aus der Software „Governikus Signer, Version 2.1.0.0“ heraus eine oder mehrere Dateien zur Anbringung jeweils einer Signatur über einen Dateiauswahldialog auszuwählen. Alternativ können auch eine oder mehrere zu signierende Dateien direkt mit der Maus auf die Dateiliste der Anwendung gezogen werden. Falls die Software „Governikus Signer, Version 2.1.0.0“ über das Kontextmenü des Explorers des Dateisystems aufgerufen wurde, ist die Dateiliste bereits entsprechend vorbelegt.
- Zu jeder ausgewählten Datei kann der zu signierende Inhalt eingesehen werden. Der „Governikus Signer, Version 2.1.0.0“ bietet eine sichere Anzeige von folgenden Daten:
 - plain-text (UTF-8-codiert).
 - TIFF (Tagged Image File Format)

Für andere Formate obliegt es dem Benutzer, eine geeignete externe Anzeige zu nutzen, die ihm die zu signierenden Inhalte auf geeignete Weise anzeigt.

- Durch Doppelklick auf den Dateinamen oder Anklicken des Visualisierungssymbols innerhalb der Dateiliste wird der Dateiinhalt, je nach Dateiformat, mit der internen sicheren Anzeige oder externen Anzeige dargestellt. Jede angezeigte Datei wird visuell durch ein Symbol in der Dateiliste gekennzeichnet. Zusätzlich wird eine Hashfunktion auf die angezeigte Datei angewendet. Die Software „Governikus Signer, Version 2.1.0.0“ merkt sich den ermittelten Hashwert jeder angezeigten Datei.
- Nach Betätigung des „Signieren“-Buttons startet der Signiervorgang bei der ersten Datei der Dateiliste. Sofern die zu signierende Datei zuvor angezeigt und ein Hashwert ermittelt wurde, wird zunächst erneut die Hashfunktion auf die Datei angewendet und über einen Hashwertvergleich geprüft, ob die zu signierenden Daten zwischenzeitlich verändert wurden.

Liefert der Hashwertvergleich ein positives Ergebnis (unveränderte Daten), wird der Benutzer aufgefordert, seine PIN am PIN-Pad des Chipkartenlesers einzugeben, woraufhin die zu signierenden Daten der sicheren Signaturerstellungseinheit zugeführt werden, in der sein privater Signaturschlüssel vorgehalten wird.

Für jede weitere zu signierende Datei der Dateiliste ist die PIN erneut über das PIN-Pad des Chipkartenlesers einzugeben. Es sei denn, als SSEE wird eine Stapelsignaturkarte (siehe Tabelle 3: „Bundesnotarkammer“ und „SIGNTRUST MCARD 100“) eingesetzt. In diesem Fall ist nach Betätigen des „Signieren“-Buttons nur eine einmalige PIN-Eingabe für die Erstellung von qualifizierten elektronischen Signaturen für die definierte Dateiliste erforderlich. Die Anzahl der mit nur einer einmaligen PIN-Eingabe signierbaren Dateien ist jedoch beschränkt: Zum einen durch die Software „Governikus Signer, Version 2.1.0.0“, mit der nur die vor dem Start des Signiervorgangs in der Dateiliste zusammengestellten Dateien mit nur einer einmaligen PIN-Eingabe signiert werden können. Zum anderen erlaubt die SSEE nur eine beschränkte Anzahl von Signaturen mit nur einer einmaligen PIN-Eingabe. Enthält die Dateiliste eine größere Anzahl Dateien als die erlaubte Anzahl an Signaturen, sind innerhalb des Signiervorgangs weitere PIN-Eingaben notwendig.

Änderungen an der Dateiliste mit den zu signierenden Dateien sind während des laufenden Signaturvorgangs nicht möglich. Ein Abbruch und erneutes Starten des Vorgangs erfordert stets auch eine erneute PIN-Eingabe.

Sowohl die Einzelsignatur als auch die Signierung eines Stapels mit nur einer einmaligen PIN-Eingabe ist mit der Software „Governikus Signer, Version 2.1.0.0“ nur über eine lokal angeschlossene SSEE möglich („Lokalsignatur“).

- 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.
- Es wird eine Ausgabedatei erzeugt; das Signaturformat wird vom Benutzer konfiguriert:
 - PKCS#7 (enveloped): Signatur im Format der Cryptographic Message Syntax (CMS/PKCS#7). Die signierten Daten sind in der Signatur enthalten. Diese hat die Endung ".p7s".
 - PKCS#7 (detached): Signatur im Format der Cryptographic Message Syntax (CMS/PKCS#7), wobei die signierten Daten nicht in der Signatur enthalten sind. Die Signatur-Datei hat die Endung ".p7s".
 - PDF-Dateien im PDF-inline-Format mit eingebetteten PKCS#7-Signaturen. Eine signierte PDF-Datei wird mit der Endung "_signed.pdf" geschrieben.
- Anschließend werden die erzeugten Signaturen in einem Verzeichnis abgelegt; je nach Konfiguration werden
 - die Ausgabedateien in das Verzeichnis geschrieben, in dem die Eingabedatei steht, oder
 - die Ausgabedateien in ein Verzeichnis geschrieben, das der Benutzer zuvor bestimmt hat.
- Nur die Variante „Governikus Signer, Version 2.1.0.0 Professional Edition“ bietet zusätzlich die Möglichkeit, zu einer erstellten Signatur einen Zeitstempel anzufordern. Der Zeitstempel wird über einen externen Zeitstempelservers bei einem Zeitstempeldienstleister angefordert (zur Schnittstellenbeschreibung siehe Punkt 3.3).
- Nur die Varianten „Governikus Signer, Version 2.1.0.0 Professional Edition“ und „Governikus Signer, Version 2.1.0.0 Integration Edition“ bieten zusätzlich die Möglichkeit der Erstellung von Multisignaturen (Massensignaturen).

Die Signaturerstellung erfolgt hierbei über die externe Signatur-Anwendungskomponente Governikus, Version 3.3.1.0 (Basis)¹³ (eine Schnittstellenbeschreibung wird unter Punkt 3.3 wiedergegeben). Auf diesem externen System muss sich der Signaturschlüssel-Inhaber zunächst ein Signaturkontingent (Zeit- oder Mengenkongingent) einrichten und anschließend durch die Eingabe der Signatur-PIN auf dem an dem Governikus-System angeschlossenen Kartenleser die Multisignatur-SSEE freischalten. Ferner muss durch den Governikus Security-Administrator ein Zugang der Software „Governikus Signer, Version 2.1.0.0“ zu der Komponente NetSigner der Software „Governikus, Version 3.3.1.0 (Basis)“ eingerichtet worden sein.

Auf dem Governikus Signer wählt der Signaturschlüssel-Inhaber nun anstelle einer lokal angeschlossenen SSEE den „NetSigner“ aus. Der Ablauf der Signaturerstellung ist identisch mit dem oben beschriebenen Ablauf unter Verwendung einer Stapelsignaturkarte. Mit jedem Start des Signaturvorgangs über einen Dialog ist die Eingabe einer PIN zur Authentisierung gegenüber der Komponente NetSigner der Software „Governikus, Version 3.3.1.0 (Basis)“ erforderlich. Nur wenn die Authentisierung erfolgreich ist, ein Signaturkontingent eingerichtet und noch nicht aus-

geschöpft sowie die korrekte Signatur-PIN der SSEE eingegeben wurde, werden die Signaturen erstellt.

Die Nutzung des Produktes „Governikus Signer, Version 2.1.0.0“ zur Signaturerstellung kann nur nach dem Prinzip der „Individualsignatur“¹⁷ erfolgen, auch im Falle der Erstellung von Multi-signaturen über die externe Software Governikus. Das bedeutet zum einen, dass die Signaturerstellung nur durch den Signaturschlüssel-Inhaber erfolgen darf – dieser also das Signaturkontingent einrichtet, die Signatur-PIN eingibt und dieses Kontingent dann selber über die Variante „Governikus Signer, Version 2.1.0.0 Professional Edition“ oder „Governikus Signer, Version 2.1.0.0 Integration Edition“ nutzt. Zum anderen sind „unterschiedliche Vorgänge“¹⁷ einzeln durch den Signaturschlüssel-Inhaber zu lesen. Intention dieses Szenarios ist die Erstellung großer Mengen von Signaturen, etwa an Scan-Arbeitsplätzen.

Ein automatisches Zuführen von Dokumenten zur Signaturerstellung ermöglichen weder die Variante „Governikus Signer, Version 2.1.0.0 Professional Edition“ noch die Variante „Governikus Signer, Version 2.1.0.0 Integration Edition“.

- Nur die Variante „Governikus Signer, Version 2.1.0.0 Integration Edition“ ermöglicht es der aufrufenden Anwendungen, Vorgaben zu machen, sodass die interaktive Auswahl durch den Benutzer hier entfällt. Folgende Vorgaben sind möglich:
 - Zu signierende Datei(en)
 - Zielverzeichnis
 - Signaturformat
 - Zur Signaturerstellung zu verwendender Schlüssel

Nicht unterbunden werden kann das Einsehen der zu signierenden Dateien sowie das Einsehen des zur Signaturerstellung verwendeten Zertifikats. Das Starten des Signaturvorgangs sowie die Eingabe der Signatur-PIN ist nur interaktiv durch den Benutzer möglich.

- Nur die Variante „Governikus Signer, Version 2.1.0.0 Integration Edition“ ermöglicht es dem Benutzer, ein oder mehrere Attributzertifikate in die Signatur miteinzubeziehen. Die Attributzertifikate können als Datei oder auf der zur Signatur verwendeten Signaturkarte vorliegen. Jedes ausgewählte Zertifikat kann durch den Benutzer eingesehen werden.
- Die Varianten „Governikus Signer, Version 2.1.0.0 Basic Edition“ und „Governikus Signer, Version 2.1.0.0 Professional Edition“ bieten weiterhin eine Bedienoberfläche für folgende Funktionalität: Nur für die PKS-Signaturkarte Netkey 3.0 ist unter Benutzung einer der beiden Kartenleser Reiner SCT CyberJack e-com oder Reiner SCT CyberJack pinpad Version 3 die Funktionalität der PIN-Freischaltung und -Änderung möglich.

3.2 Verifizierung von Signaturen

Die Software „Governikus Signer, Version 2.1.0.0“ stellt folgende Funktionen zur Verifizierung qualifizierter elektronischer Signaturen zur Verfügung:

- Die Software „Governikus Signer, Version 2.1.0.0“ unterstützt den Benutzer bei der Prüfung von qualifizierten elektronischen Signaturen hinsichtlich der Integrität des signierten Dokuments sowie der Authentizität des Signierenden.

¹⁷ Vgl. www.bundesnetzagentur.de, Sachgebiet qualifizierte elektronisch Signatur, FAQ Nr. 18 und Nr. 18a

- Der Benutzer wählt eine oder mehrere zu verifizierende Dateien über einen Dateidialog aus. Alternativ können auch eine oder mehrere zu verifizierende Dateien direkt mit der Maus auf die Dateiauswahlliste der Anwendung gezogen werden. Falls die Software „Governikus Signer, Version 2.1.0.0“ über das Kontextmenü des Explorers des Dateisystems aufgerufen wurde, ist die Dateiauswahlliste bereits entsprechend vorbelegt.
- Das Signaturformat wird automatisch erkannt: Folgende Signaturformate werden unterstützt:
 - PKCS#7 (enveloped): Signatur im Format der Cryptographic Message Syntax (CMS/PKCS#7). Die signierten Daten sind in der Signatur enthalten.
 - PKCS#7 (detached): Signatur im Format der Cryptographic Message Syntax (CMS/PKCS#7), wobei die signierten Daten nicht in der Signatur enthalten sind.
 - PDF-Dateien im PDF-inline-Format mit eingebetteten PKCS#7-Signaturen.
- Zu jeder ausgewählten Datei kann das enthaltene Signaturzertifikat über eine anwendungsinterne Ansicht eingesehen werden.
- Zu jeder ausgewählten Datei kann der signierte Inhalt eingesehen werden. Die Software „Governikus Signer, Version 2.1.0.0“ bietet eine sichere Anzeige von folgenden signierten Daten:
 - plain-text (UTF-8-codiert),
 - TIFF (Tagged Image File Format).

Für andere Formate obliegt es dem Benutzer, eine geeignete Anzeige zu nutzen, die ihm die zu signierenden Inhalte auf geeignete Weise angezeigt.

- Zu jeder ausgewählten Datei im Format PKCS#7 (enveloped) kann der signierte Inhalt aus der Signaturdatei extrahiert und gespeichert werden.
- Nach Betätigen der Schaltfläche "Verifizieren" werden die Signaturen aller ausgewählten Dateien geprüft.
 - Verifizieren: Die Software „Governikus Signer, Version 2.1.0.0“ verifiziert qualifizierte elektronische Signaturen und legt das Verifikationsergebnis (gültige oder ungültige Signatur oder Fehlermeldung) in Form einer Prüfprotokoll-Datei ab.

Zusätzlich wird bei jedem Verifizieren eine Validierung (Statusprüfung) durchgeführt (siehe nächster Spiegelstrich).

- Validieren: Die Software „Governikus Signer, Version 2.1.0.0“ führt die Statusprüfung eines qualifizierten Zertifikats durch. Als Prüfzeitpunkt wird der in der Nachricht enthaltene Zeitpunkt verwendet. Ist dieser nicht vorhanden, wird der aktuelle Zeitpunkt genutzt.

Die Software „Governikus Signer, Version 2.1.0.0“ validiert nicht selber, sondern nutzt dazu einen Verifikationsserver sowie ein nachgelagertes OCSP/CRL-Relay (vgl. Tabelle 4), von dem die Software „Governikus Signer, Version 2.1.0.0“ anschließend das Ergebnis der Validierung erhält, das mit einer elektronischen Signatur versehen ist. Das Ergebnis der Validierung umfasst neben den Verzeichnisdienst-Ergebnissen eine Interpretation (gültig und nicht gesperrt, unbekannt oder gesperrt).

Die Software „Governikus Signer, Version 2.1.0.0“ verifiziert die elektronische Signatur des Validierungsergebnisses mit dem (System-)Zertifikat des OCSP/CRL-Relay und prüft, ob das validierte Zertifikat dasjenige Zertifikat ist, das der Signatur entspricht, und ob der Zertifikatsstatus zum angefragten Prüfzeitpunkt ermittelt wurde (Plausibilitätscheck). Die Soft-

ware „Governikus Signer, Version 2.1.0.0“ visualisiert das Ergebnis der Validierung (Statusprüfung).

- Zu jeder verifizierten Datei erstellt die Software „Governikus Signer, Version 2.1.0.0“ ein ausführliches Prüfprotokoll und speichert dieses im HTML-Format. Die Ablage des Prüfprotokolls erfolgt je nach Konfiguration
 - in dem Verzeichnis, in dem die jeweilige Eingabedatei steht, oder
 - in einem festen Verzeichnis, das der Benutzer zuvor bestimmt hat.
- Das erstellte Prüfprotokoll kann über eine in der Software „Governikus Signer, Version 2.1.0.0“ enthaltene Anzeige eingesehen werden. Mithilfe eines intern vorgehaltenen Hashwerts über das Prüfprotokoll wird sichergestellt, dass kein manipuliertes Prüfprotokoll angezeigt wird.
- Der für die Validierung von Zertifikaten benötigte Verifikationsserver ist nicht Bestandteil des „Governikus Signer, Version 2.1.0.0“ (vgl. Tabelle 4).
- Bei dem oben beschriebenen Funktionsumfang wird der Benutzer durch visuelle Anzeigen begleitet. Neben dem Prüfprotokoll wird dem Nutzer das Ergebnis der oben spezifizierten Prüfungen als zusammengefasstes Gesamtergebnis mit drei möglichen Zuständen angezeigt:
 - „Sämtliche durchgeführten Prüfungen lieferten ein positives Ergebnis.“
 - „Mindestens eine der Prüfungen konnte nicht durchgeführt werden.“
 - „Mindestens eine der durchgeführten Prüfungen lieferte ein negatives Ergebnis.“
- Die Validierung (Gültigkeitsmodell: Kettenmodell) umfasst folgende Prüfungen:
 - Ist das Herausgeberzertifikat gültig (vorhanden und nicht gesperrt)?
 - Hat die unterzeichnende Person innerhalb des Gültigkeitszeitraumes ihres qualifizierten Zertifikats signiert (Kettenmodell)?
 - Ist dem Zertifizierungsdiensteanbieter (ZDA) das verwendete qualifizierte Zertifikat bekannt und ist es nicht gesperrt?
- Die Variante „Governikus Signer, Version 2.1.0.0 Integration Edition“ ermöglicht es der aufrufenden Anwendungen, Vorgaben zu machen, sodass die interaktive Auswahl durch den Benutzer hier entfällt. Folgende Vorgaben sind möglich:
 - Zu verifizierende Datei(en)
 - Zielverzeichnis

Nicht unterbunden werden kann das Einsehen des zur Signatur gehörenden Zertifikats und der signierten Inhalte sowie das Einsehen des Verifikationsergebnisses (Prüfprotokoll).

3.3 Schnittstellen

Die Software „Governikus Signer, Version 2.1.0.0“ enthält folgende Schnittstellen:

- Schnittstelle zum Chipkartenleser:

Über die Verbindung zum Chipkartenleser sendet die Software zu signierende Daten an die Signaturkarten und empfängt über diese Schnittstelle die von den Signaturkarten signierten Daten.
- Schnittstelle zur grafischen Bedienungsoberfläche (Graphical User Interface – GUI):

Die Software „Governikus Signer, Version 2.1.0.0“ nutzt die grafische Oberfläche als Schnittstelle zum Nutzer und visualisiert die Interaktion mit dem Signaturschlüssel-Inhaber durch entsprechende informelle und prozedurale Anzeigen.

- Schnittstelle zu Governikus¹⁴ (Ansprechen der Komponente Verifikationsserver):

Für die Online-Validierung existiert eine Schnittstelle zu einem Verifikationsserver.

Nur die Varianten „Governikus Signer, Version 2.1.0.0 Professional Edition“ und „Governikus Signer, Version 2.1.0.0 Integration Edition“ enthalten zusätzlich folgende Schnittstelle:

- Schnittstelle zu Governikus¹³ (Ansprechen der Komponente NetSigner):

Zur Erstellung von Multisignaturen existiert eine Schnittstelle zu Governikus. Über diese Verbindung sendet die Software die zu signieren Daten an das Governikus-System und empfängt die durch Governikus erstellte Signatur.

Nur die Variante „Governikus Signer, Version 2.1.0.0 Professional Edition“ enthält zusätzlich folgende Schnittstelle:

- Schnittstelle zu Governikus (Ansprechen der Komponente Zeitstempelservers):

Zur Erstellung von Zeitstempeln existiert eine Schnittstelle zum Anfordern von Zeitstempeln über die Governikus-Komponente Zeitstempelservers. Über diese Verbindung sendet die Software die Zeitstempelanfrage an das Governikus-System und empfängt die durch Governikus erstellte.

Nur die Variante „Governikus Signer, Version 2.1.0.0 Integration Edition“ enthält zusätzlich folgende Schnittstelle:

- Schnittstelle zur aufrufenden Anwendung:

Über diese Schnittstelle kann die Variante „Governikus Signer, Version 2.1.0.0 Integration Edition“ in eine beliebige Anwendung integriert werden. Über diese Schnittstelle kann die Software gestartet und Einstellungen vorgegeben werden sowie der Bearbeitungsstand abgefragt werden.

4 Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

Das Produkt „Governikus Signer, Version 2.1.0.0“ erfüllt die nachfolgenden Anforderungen des SigG:

Referenz	Gesetzestext	Beschreibung
§ 17 Abs. 2 Satz 1	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.	Zur Umsetzung dieser gesetzlichen Anforderungen ist eine entsprechende Anzeige implementiert, die, bevor eine Signatur erzeugt wird, anzeigt <ul style="list-style-type: none"> ▪ auf welche Daten sich die zu erstellende Signatur bezieht und ▪ welchem Signaturschlüssel-Inhaber die zu erstellende Signatur zuzuordnen¹⁸ ist.
§ 17 Abs. 2 Satz 2	Für die Überprüfung signierter Daten sind Signaturanwendungskomponenten erforderlich, die feststellen lassen, <ol style="list-style-type: none"> 1. auf welche Daten sich die Signatur bezieht, 2. ob die signierten Daten unverändert sind, 3. welchem Signaturschlüssel-Inhaber die Signatur zuzuordnen ist, 4. welche Inhalte das qualifizierte Zertifikat, auf dem die Signatur beruht, und zugehörige qualifizierte Attribut-Zertifikate aufweisen und 5. zu welchem Ergebnis die Nachprüfung von Zertifikaten nach § 5 Abs. 1 Satz 3 geführt hat. 	Zu 1., 3., 4. und 5.: Zur Umsetzung dieser gesetzlichen Anforderungen ist eine entsprechende Anzeige implementiert, die anzeigt <ul style="list-style-type: none"> ▪ auf welche Daten sich die Signatur bezieht, ▪ welchen Inhalt die signierten oder zu signierenden Daten aufweisen, ▪ welchem Signaturschlüssel-Inhaber die Signatur zuzuordnen ist, ▪ welche Inhalte das zugehörige qualifizierte (Attribut)-Zertifikat aufweist sowie ▪ das Ergebnis der Verifikation und Validierung (siehe oben), was insbesondere beinhaltet, ob die signierten Daten unverändert sind und das Zertifikat gültig ist (vorhanden und nicht gesperrt). Zu 2.: Über eine kryptografische Signaturprüfung (Integritätsprüfung) wird festgestellt, ob die Signatur bzw. die Daten, auf die sich die Signatur bezieht, unverändert sind.
§ 17 Abs. 2 Satz 3	Signaturanwendungskomponenten müssen nach Bedarf auch den Inhalt der zu signierenden oder signierten Daten hinreichend erkennen lassen.	Zur Umsetzung dieser gesetzlichen Anforderungen ist eine entsprechende Funktion implementiert, die bei Bedarf <ul style="list-style-type: none"> ▪ den Inhalt von zu signierenden Daten in den Formaten Plain-Text (UTF-8) und

¹⁸ Trifft für die Varianten „Governikus Signer, Version 2.1.0.0 Professional Edition“ und „Governikus Signer, Version 2.1.0.0 Integration Edition“ nicht bei der Erstellung von Multisignaturen zu. In diesem Fall erfolgt die Anzeige, welchem Signaturschlüssel-Inhaber die zu erstellenden Signaturen zuzuordnen sind, innerhalb der verwendeten externen Signatur-Anwendungskomponente „Governikus, Version 3.3.1.0 (Basis)“

Referenz	Gesetzestext	Beschreibung
		<p>TIFF sicher anzeigt,</p> <ul style="list-style-type: none"> den signierten Inhalt von CMS/PKCS#7 Signaturdateien (detached oder enveloped) in den Formaten Plain-Text (UTF-8) und TIFF sicher anzeigt.

Tabelle 5: Erfüllung der Anforderungen des SigG

Das Produkt „Governikus Signer, Version 2.1.0.0“ erfüllt die nachfolgenden Anforderungen der SigV bei Verwendung einer lokalen Signaturinfrastruktur:

Referenz	Gesetzestext	Beschreibung
§ 15 Abs. 2 Nr. 1	<p>Signaturanwendungskomponenten nach § 17 Abs. 2 des Signaturgesetzes müssen gewährleisten, dass [...] bei der Erzeugung einer qualifizierten elektronischen Signatur</p> <p>a) die Identifikationsdaten nicht preisgegeben und diese nur auf der jeweiligen sicheren Signaturerstellungseinheit gespeichert werden,</p> <p>b) eine Signatur nur durch die berechtigt signierende Person erfolgt,</p> <p>c) die Erzeugung einer Signatur vorher eindeutig angezeigt wird [...].</p>	<p>Zu a)</p> <p>Die Erzeugung einer qualifizierten elektronischen Signatur erfolgt ausschließlich in einer SSEE.</p> <p>Zu b)</p> <p>Zur Umsetzung der gesetzlichen Anforderungen bei der Verwendung einer lokal angeschlossenen SSEE sind in allen Varianten entsprechende Funktionen implementiert, die sicherstellen, dass</p> <ul style="list-style-type: none"> sich der Signaturschlüssel-Inhaber zur Erstellung von qualifizierten elektronischen Signaturen immer durch die Eingabe der Signatur-PIN über das PIN-Pad des Chipkartenlesers authentisiert, die Authentisierung nur eine einzige Signatur ermöglicht bzw. bei Verwendung einer Stapelsignaturkarte nur die Signaturerstellung für den zuvor bestimmten Stapel zulässt, eine Veränderung der Dateiliste (Stapel) nach Beginn des Signaturvorgangs und der Authentisierung nicht möglich ist, nach der Visualisierung durchgeführte Veränderungen an den zu signierenden Dateien angezeigt werden. <p>Zur Umsetzung der gesetzlichen Anforderungen bei der Erstellung von Multisignaturen über die externe Signatur-Anwendungskomponente „Governikus, Version 3.3.1.0 (Basic)“ sind in den Varianten</p>

Referenz	Gesetzestext	Beschreibung
		<p>„Governikus Signer, Version 2.1.0.0 Professional Edition“ und „Governikus Signer, Version 2.1.0.0 Integration Edition“ entsprechende Funktionen implementiert, die sicherstellen, dass</p> <ul style="list-style-type: none"> ▪ zur Nutzung eines auf der externe Signatur-Anwendungskomponente „Governikus, Version 3.3.1.0 (Basic)“ eingerichteten und freigegebenen Kontingents von Signaturen eine Authentisierung des Benutzers durch eine PIN-Eingabe erforderlich ist. ▪ die Authentisierung nur die Signaturerstellung für den zuvor bestimmten Stapel zulässt, ▪ eine Veränderung der Dateiliste (Stapel) nach Beginn des Signaturvorgangs und der Authentisierung nicht möglich ist, ▪ nach der Visualisierung durchgeführte Veränderungen an den zu signierenden Dateien angezeigt werden. <p>Zu c)</p> <p>Der Benutzer muss zum Erstellen der Signatur explizit eine mit der Bezeichnung "Signieren" versehene Schaltfläche betätigen, wodurch die Erzeugung einer Signatur vorher eindeutig angezeigt wird.</p> <p>Bei der Verwendung einer Stapelsignaturkarte wird dem Benutzer ein zusätzlicher Hinweis angezeigt, dass die Signaturerstellung für alle ausgewählten Dateien mit nur einer PIN-Eingabe erfolgt.</p> <p>Bei der Erstellung von Multisignaturen über die externe Signatur-Anwendungskomponente „Governikus, Version 3.3.1.0 (Basic)“ werden in den Varianten „Governikus Signer, Version 2.1.0.0 Professional Edition“ und „Governikus Signer, Version 2.1.0.0 Integration Edition“ ein zusätzlicher Hinweis angezeigt, dass die Governikus-Komponente NetSigner zur Signaturerstellung verwendet wird.</p>

Referenz	Gesetzestext	Beschreibung
§ 15 Abs. 2 Nr. 2	<p>Signaturanwendungskomponenten nach § 17 Abs. 2 des Signaturgesetzes müssen gewährleisten, dass [...] bei der Prüfung einer qualifizierten elektronischen Signatur</p> <p>a) die Korrektheit der Signatur zuverlässig geprüft und zutreffend angezeigt wird und</p> <p>b) eindeutig erkennbar wird, ob die nachgeprüften qualifizierten Zertifikate im jeweiligen Zertifikat-Verzeichnis zum angegebenen Zeitpunkt vorhanden und nicht gesperrt waren.</p>	<p>Zu a)</p> <p>Zur Umsetzung der gesetzlichen Anforderungen ist eine entsprechende Anzeige implementiert, die anzeigt</p> <ul style="list-style-type: none"> ▪ welchen Inhalt die signierten Daten aufweisen, ▪ welchem Signaturschlüssel-Inhaber die Signatur zuzuordnen ist, ▪ welches Ergebnis die Verifikation und Validierung liefert, insbesondere <ul style="list-style-type: none"> ▪ ob die signierten Daten unverändert sind und ▪ ob das zugehörige qualifizierte Zertifikat gültig ist. <p>Zu b)</p> <p>Zur Umsetzung der gesetzlichen Anforderungen ist eine entsprechende Anzeige implementiert, die das Ergebnis einer Anfrage der zuständigen Verzeichnisdienste, ob ein qualifiziertes Zertifikat zum angegebenen Zeitpunkt gültig war, anzeigt.</p>
§ 15 Abs. 4	<p>Sicherheitstechnische Veränderungen an technischen Komponenten nach den Absätzen 1 bis 3 müssen für den Nutzer erkennbar werden.</p>	<p>Die Anforderungen zur Erkennung sicherheitstechnischer Veränderungen werden durch die Signaturen der Software und die Auflagen zum Betrieb realisiert, vgl. Abschnitt 5.</p>

Tabelle 6: Erfüllung der Anforderungen der SigV

Darüber hinaus ist § 17 Abs. 2 Satz 4 SigG („Die Signaturschlüssel-Inhaber sollen solche Signaturanwendungskomponenten einsetzen oder andere geeignete Maßnahmen zur Sicherheit qualifizierter elektronischer Signaturen treffen.“) nicht direkt durch das Produkt „Governikus Signer, Version 2.1.0.0“ umsetzbar.

5 Maßnahmen in der Einsatzumgebung

5.1 Einrichtung der IT-Komponenten

Für den Betrieb der Software „Governikus Signer, Version 2.1.0.0“ wird folgende Einsatzumgebung vorausgesetzt:

- AMD/Intel-PC mit mindestens
 - 512 MB Hauptspeicher (RAM) und
 - 260 MB Plattenplatz;
- Betriebssystem:

- Microsoft Windows Vista, Windows XP oder Windows Server 2003 (jeweils mit aktuellem Service Pack), oder
- openSUSE 10.3;
- 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;
- Produkt „Virtuelle Poststelle des Bundes (Verifikationsmodul)“ (gemäß Tabelle 4) mit Komponente Verifikationsserver und Produkt „Virtuelle Poststelle des Bundes (Basis)“ (gemäß Tabelle 4) mit Komponente OCSP/CRL-Relay: Für die Verifikation (Online-Prüfung) ist ein Zugriff auf den Verifikationsserver und dem nachgelagertem OCSP/CRL-Relay im Sinne von SigG (vgl. Tabelle 5) und SigV (vgl. Tabelle 6) zwingend erforderlich.
- Nur für die PKS-Signaturkarte Netkey 3.0 unter Benutzung einer der beiden Kartenleser Reiner SCT CyberJack e-com oder Reiner SCT CyberJack pinpad Version 3 ist beim „Governikus Signer, Version 2.1.0.0“ die Funktionalität der PIN-Freischaltung und -Änderung möglich.

Zum anbringen von Zeitstempeln mit der Variante „Governikus Signer, Version 2.1.0.0 Professional Edition“ wird darüber hinaus für den Betrieb der folgende Einsatzumgebung vorausgesetzt:

- Produkt „Governikus, Version 3.3.1.0 (Basis)“.

Zur Erstellung von Multisignaturen mit den Varianten „Governikus Signer, Version 2.1.0.0 Professional Edition“ oder „Governikus Signer, Version 2.1.0.0 Integration Edition“ wird darüber hinaus für den Betrieb der folgende Einsatzumgebung vorausgesetzt:

- Produkt „Governikus, Version 3.3.1.0 (Basis)“ (gemäß Tabelle 4) mit Komponente NetSinger.

Für den Betrieb der Software „Governikus Signer, Version 2.1.0.0“ auf einem Terminalserver wird eine der folgenden Umgebungen vorausgesetzt

- Citrix Metaframe Presentation Server 4.5
- Windows Terminal Server 2003

Das Produkt „Governikus Signer, Version 2.1.0.0“ darf ausschließlich innerhalb der oben beschriebenen Hard- und Softwareausstattung eingesetzt werden.

5.2 Anbindung an ein Netzwerk

Für den Betrieb des Produktes „Governikus Signer, Version 2.1.0.0“ ist, je nach genutztem Funktionsumfang, ein Netzwerk notwendig.

Bei Anbindung des Produktes 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.

Für den Betrieb der Software „Governikus Signer, Version 2.1.0.0“ in einer Terminalserver-Umgebung ist die Verbindung zwischen Client und Server über SSL bzw. TLS zu realisieren. Der Verbindungsaufbau ist durch gegenseitige Authentisierung über ausgetauschte Zertifikate zu schützen. Der Betrieb in einer Terminalserver-Umgebung ist nur innerhalb eines Intranets erlaubt.

Zur Erstellung von Multisignaturen mit den Varianten „Governikus Signer, Version 2.1.0.0 Professional Edition“ oder „Governikus Signer, Version 2.1.0.0 Integration Edition“ ist die Verbindung zu der Software „Governikus, Version 3.3.1.0 (Basis)“ über das Protokoll HTTPS zu realisieren. Der Nutzung der Software „Governikus, Version 3.3.1.0 (Basis)“ zur Erstellung von Multisignaturen ist nur innerhalb eines Intranets erlaubt.

Die in diesem Abschnitt gemachten Auflagen müssen eingehalten werden.

5.3 Auslieferung und Installation

Die Auslieferung erfolgt online per Download von einem Webserver.

Alle Dateien der Software „Governikus Signer, Version 2.1.0.0“ 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 Signer, Version 2.1.0.0“ von der Gültigkeit der Signatur überzeugen. Die Verifikation der Signatur erfolgt über Standard-Java-Mechanismen.

Die Software „Governikus Signer, Version 2.1.0.0“ lässt sich über eine Installationsroutine einfach installieren. In der Installationsroutine werden einige Parameter zur Installation (Ort des Installationsverzeichnisses, Anlegen einer Desktopverknüpfung etc.) abgefragt. Mit dem Produkt „Governikus Signer, Version 2.1.0.0“ wird stets eine Java Runtime Environment (JRE) mitinstalliert. Diese wird ebenfalls im Installationsverzeichnis abgelegt und beeinflusst somit andere Java-Installationen nicht.

Die Variante „Governikus Signer, Version 2.1.0.0 Integration Edition“ bietet darüber hinaus die Möglichkeit, die für die Installation benötigten Parameter über eine Konfigurationsdatei vorzugeben.

5.4 Auflagen für den Betrieb des Produktes

Die Software „Governikus Signer, Version 2.1.0.0“ wird in einem „geschützten Einsatzbereich (Regelfall/Standardlösung)“ (vgl. das Dokument der Bundesnetzagentur, „Einheitliche Spezifizierung der Einsatzkomponenten für Signaturanwendungskomponenten – Arbeitsgrundlage für Entwickler/Hersteller und Prüf-/Bestätigungsstellen“, Version 1.4, 19.07.2005) betrieben.

Für den Betrieb der Software „Governikus Signer, Version 2.1.0.0“ in einer Terminalserver-Umgebung gelten die nachfolgenden Auflagen sowohl für den Terminalserver als auch für den Client-PC des Benutzers.

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 Signer, Version 2.1.0.0“ betrieben wird, keine Angriffe ausgehen. Insbesondere ist sicherzustellen, dass

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

Auflagen zum Schutz vor manuellem Zugriff Unbefugter

Der eingesetzte Personalcomputer muss 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.

Im Fall der Verwendung der Variante „Governikus Signer, Version 2.1.0.0 Professional Edition“ zur Erstellung von Multisignaturen sind der Betrieb und die Aufbewahrung in einem zugriffssicheren Betriebsraum oder Stahlschrank erforderlich, so dass ein Zugriff Unbefugter ausgeschlossen ist oder zumindest mit hoher Sicherheit erkennbar wird.

Der Authentisierungsschlüssel für den Zugriff auf die Komponente NetSigner der Software „Governikus, Version 3.3.1.0 (Basis)“ muss durch den Schlüssel-Administrator des Governikus Systems bereit gestellt werden¹⁹.

Für das Passwort und insbesondere für das Zugangspasswort zu einer Terminalserver-Sitzung sind folgende Auflagen einzuhalten:

- Es dürfen keine Trivialpasswörter (z. B. "BBBBBBBB" oder "12345678") verwendet werden.
- Das Passwort enthält mindestens ein Zeichen, das kein Buchstabe ist (Sonderzeichen oder Zahl),
- Das Passwort muss mindestens 8 Zeichen lang sein

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 Trojanische Pferde eingespielt werden können.

Auflagen zur Sicherheitsadministration des Betriebs

Hinsichtlich der Software „Governikus Signer, Version 2.1.0.0“ ist keine spezielle Sicherheitsadministration für den Betrieb vorgesehen. Der eingesetzte Personalcomputer und der eingesetzte Chipkartenleser sind aber in jedem Fall gegen eine unberechtigte Benutzung zu sichern.

Für den Betrieb der Software „Governikus Signer, Version 2.1.0.0“ in einer Terminalserver-Umgebung ist durch ein geeignetes Berechtigungssystem sicherzustellen, dass die Dateien innerhalb des persönlichen Verzeichnisses des Benutzers der Software „Governikus Signer, Version 2.1.0.0“ nicht durch Unbefugte gelesen oder verändert werden können.

Auflagen zum Schutz vor Fehlern bei Betrieb/Nutzung

Folgende Auflagen sind für den sachgemäßen Einsatz der Software „Governikus Signer, Version 2.1.0.0“ zu beachten:

- Sofern eine Visualisierung einer zu signierenden Datei erfolgen soll, ist eine geeignete Anwendung zu nutzen, d. h. eine Anwendung, die Dateien des entsprechenden Dateityps öffnen und die zu signierenden oder signierten Daten zuverlässig darstellen kann.

¹⁹ Vgl. Dokument „Governikus Betriebshandbuch“, Kapitel „Auflagen für den Betrieb gemäß Signaturgesetz“

- 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. Er muss seine PIN ändern, wenn er den Verdacht oder die Gewissheit hat, die PIN könnte nicht mehr geheim sein.
- Nur beim Betrieb mit einem bestätigten Chipkartenleser mit PIN-Pad ist sicher gestellt, dass die PIN nur zur SSEE übertragen wird.
- Zum Signieren darf die PIN nur am PIN-Pad des Chipkartenlesers eingegeben werden.
- Nur für die PKS-Signaturkarte Netkey 3.0 unter Benutzung einer der beiden Kartenleser Reiner SCT CyberJack e-com oder Reiner SCT CyberJack pinpad Version 3 ist beim „Governikus Signer, Version 2.1.0.0“ die Funktionalität der PIN-Freischaltung und -Änderung möglich. Aus technischen Gründen erfolgt die Freischaltung in zwei Stufen, sodass die folgenden Schritte zu beachten sind: Zunächst ist eine vorläufige PIN zur Freischaltung am Rechner einzugeben. Direkt im Anschluss ist diese vorläufige PIN am PIN-Pad des Chipkartenlesers in die Signatur-PIN zu ändern.
- Zum Ändern der Signatur-PIN darf diese nur am PIN-Pad des Chipkartenlesers eingegeben werden.
- Hinweise von Zertifizierungsdiensteanbietern zum Umgang mit persönlichen, geheimen Signatur-PIN sind zu beachten.
- Eine Signaturgesetz-konforme Nachprüfung qualifizierter Zertifikate kann nur erfolgen, soweit dafür die technischen Voraussetzungen – insbesondere durch die Verbindung zum Verifikationsserver – gegeben sind.

Ergänzend zu den oben genannten Auflagen müssen zur sachgemäßen Erstellung von Multisignaturen mit den Varianten „Governikus Signer, Version 2.1.0.0 Professional Edition“ und „Governikus Signer, Version 2.1.0.0 Integration Edition“ folgende Auflagen beachtet werden.

- Die Erstellung von Multisignaturen über die Varianten „Governikus Signer, Version 2.1.0.0 Professional Edition“ oder „Governikus Signer, Version 2.1.0.0 Integration Edition“ unter Verwendung der Software „Governikus, Version 3.3.1.0 (Basis)“ ist ausschließlich durch den Signaturschlüssel-Inhaber durchzuführen. Für das Signieren eines Dokumentenstapels ist nach dem Prinzip der Individualsignatur²⁰ zu verfahren, wobei der Signaturschlüssel-Inhaber „unterschiedliche Vorgänge“²⁰ vor der Signaturerstellung einzeln lesen muss.
- Für die Erstellung von Multisignaturen über die Variante „Governikus Signer, Version 2.1.0.0 Integration Edition“ muss durch die aufrufende Fachanwendung sicherstellt werden, dass nur „praktisch gleiche Vorgänge“²⁰ (z.B. Rechnungen, die sich nur in Betrag und Zustelladresse unterscheiden) signiert werden.
- Alle Auflagen aus dem Governikus Betriebshandbuch an den Signaturschlüssel-Inhaber hinsichtlich der Nutzung der Software „Governikus, Version 3.3.1.0 (Basis)“ zur Erstellung von Multisignaturen sind einzuhalten¹⁹.
- Es wird eine vertrauenswürdige Eingabe der Authentisierungs-PIN vorausgesetzt. Der Nutzer hat dafür Sorge zu tragen, dass die Eingabe der Authentisierungs-PIN weder beobachtet noch die Authentisierungs-PIN anderen Personen bekannt gemacht wird.

²⁰ Vgl. www.bundesnetzagentur.de, Sachgebiet qualifizierte elektronische Signatur, FAQ Nr. 18 und Nr. 18a

Bei dem Einsatz der Software „Governikus Signer, Version 2.1.0.0“ in einer Terminalserver-Umgebung muss eine gesicherte und verschlüsselte Verbindung zwischen Terminalserver und Client-PC sichergestellt werden.

Auflagen für Wartung/Reparatur

Eine Pflege und Wartung der Software „Governikus Signer, Version 2.1.0.0“ 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 Signer, Version 2.1.0.0“ die Hashfunktionen SHA-256 und RIPEMD-160 bereitgestellt.²¹

Zur Prüfung qualifizierter elektronischer Signaturen werden vom Produkt „Governikus Signer, Version 2.1.0.0“ die Hashfunktionen SHA-256, RIPEMD-160 und SHA-1 sowie der Signaturalgorithmus RSA²² bereitgestellt. Die jeweils verwendete Hashfunktion wird im Prüfprotokoll dargestellt.

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. November 2008) wie folgt als geeignete eingestuft:

- RIPEMD-160: gültig bis 31.12.2010
- SHA-2 Familie (SHA-224, SHA-256, SHA-384, SHA-512): gültig bis 31.12.2015
- RSA mit Schlüssellänge 2048 Bit: gültig bis 31.12.2015.

7 Gültigkeit der Herstellereklärung

Diese Erklärung ist bis zu ihrem Widerruf, längstens jedoch bis zum 31.12.2010 gültig. Die Gültigkeit der Herstellereklärung 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 Herstellereklärung wurden aus dem Veröffentlichungstext ausgegliedert und bei der zuständigen Behörde hinterlegt:

²¹ Hinweis: Das Produkt unterstützt ferner die Hashfunktion SHA-1, die allerdings zum 30.6.2008 ausgelaufen ist, sodass aufgrund der abgelaufenen oder gesperrten Zertifikate keine qualifizierten elektronischen Signaturen mehr erzeugt werden können. Bei der Verwendung einer Signaturkarte, die nur SHA-1 unterstützt, wird ein entsprechender Warnhinweis angezeigt.

²² Die Schlüssellänge richtet sich nach den zu verifizierenden Signaturen; das Produkt „Governikus Signer, Version 2.1.0.0“ unterstützt die gängigen Schlüssellängen von 2048 Bit.

- „Unterlagen zur Herstellereklärung gemäß § 17 Abs. 4 SigG für die Software ‚Governikus Signer, Version 2.1.0.0‘ – Sicherheitstechnische Produktbeschreibung und Spezifikation“, 03.03.2009, 89 Seiten.
- „Unterlagen zur Herstellereklärung gemäß § 17 Abs. 4 SigG für die Software ‚Governikus Signer, Version 2.1.0.0‘ – Testdokumentation“, 03.03.2009, 23 Seiten.
- „Governikus Signer – Benutzerhandbuch“, Dokument-Version 2.1_0, 80 Seiten.
- „Governikus Signer – Testhandbuch“, Version 2.4, 59 Seiten.
- „Governikus Signer Integration Edition – Testhandbuch“, Version 1.2, 23 Seiten.

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

Ende der Herstellereklärung