

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 SigV²,

dass sein Produkt

Govello, Version 3.1

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

Bremen, den 24.09.2009

gez. Dr. Stephan Klein

Geschäftsführung

Diese Herstellereklärung in der Version 1.0 mit der Dokumentennummer bos2009003 besteht aus 18 Seiten.

¹ Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz – SigG) vom 16.05. Mai 2001 (BGBl. I S. 876)), zuletzt geändert durch Erstes Gesetz zur Änderung Artikel 4 des Signaturgesetzes (1. SigÄndG) Gesetzes vom 04.01.200526. Februar 2007 (BGBl. I S. 2)179)

² Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) vom 16.11. November 2001 (BGBl. I S. 3074)), zuletzt geändert durch 1. SigÄndG Artikel 9 Abs. 18 des Gesetzes vom 23. November 2007 (BGBl. I S. 2631)

Dokumentenhistorie

Version	Datum	Autor	Bemerkung
1.0	24.09.2009	bremen online services Entwicklungs- und Betriebsgesellschaft mbH & Co. KG	Erstellung für Govello, Version 3.1

Beschreibung des Produkts

1. Handelsbezeichnung und Hersteller

Die Handelsbezeichnung lautet: Govello, Version 3.1

Auslieferung: online per Download

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

Handelsregisterauszug: HRA 22041

2. Lieferumfang und Versionsinformationen

Nachstehend ist der Lieferumfang der Software "Govello, Version 3.1" aufgezählt:

Produktbestandteile	Bezeichnung	Version	Übergabeform
Software	Govello, Version 3.1	3.1	online per Download
Benutzerhandbuch	bremen online services GmbH & Co. KG, "Benutzerhandbuch – Govello", Version 3.1, 2009	3.1	online per Download

Tabelle 1: Lieferumfang und Versionsinformation

Die Software "Govello, Version 3.1" besteht aus den in der folgenden Tabelle aufgeführten Dateien:

Datei	Version	Größe	Hersteller	Übergabeform
Govello Bibliotheken				
beistellung_backend.jar	3.1	498 KB	bos	online per Download
beistellung_client.jar	3.1	218 KB	bos	online per Download
help_backend_de.jar	3.1	434 KB	bos	online per Download
help_client_de.jar	3.1	402 KB	bos	online per Download
mandanten.jar	3.1	5 KB	bos	online per Download
log4j.jar	3.1	6 KB	bos	online per Download
govello_framework.jar	3.1.0.0	2093 KB	bos	online per Download
registration_client.jar	3.1.0.0	125 KB	bos	online per Download
service_modules.jar	3.1.0.0	1655 KB	bos	online per Download
ServiceModules Bibliotheken				
mcard.jar	1.10.1	982 KB	bos	online per Download
Bouncy Castle Bibliotheken				
gov_crypto_provider-1.0.jar	1.0	48 KB	bos	online per Download
bcprov-jdk15-143-bos-0.1.jar	1.0	2070 KB	bos	online per Download

bctsp-jdk15-143-bos-0.1.jar	1.0	32 KB	bos	online per Download
bcmail-jdk15-143-bos-0.1.jar	1.0	282 KB	bos	online per Download
bc.extensions-jdk15-143-bos-0.1.jar	1.0	95 KB	bos	online per Download
Governikus Bibliotheken				
certificatechooser.jar	1.0	39 KB	bos	online per Download
CertificateViewer.jar	1.0	34 KB	bos	online per Download
certqualitycheck.jar	1.0	19 KB	bos	online per Download
clientenabler.jar	1.0	520 KB	bos	online per Download
osci-bibliothek.jar	1.0	348 KB	bos	online per Download
streamedpkcs7.jar	1.0	15 KB	bos	online per Download
Thirdparty Bibliotheken				
activation.jar	1.0.2	54 KB	Sun Microsystems	online per Download
commons-codec-1.3.jar	1.3	51 KB	Apache Software	online per Download
commons-httpclient-3.0.1.jar	3.0.1	286 KB	Apache Software	online per Download
commons-logging.jar	1.0.3	35 KB	Apache Software	online per Download
drivers.jar	1.8.0	109 KB	Sun, Open Card, Kobil und SCM Microsystems	online per Download
jdkic.jar (Linux)	20061102	51 KB	Sun Microsystems	online per Download
jdkic.jar (Windows)	20061102	90 KB	Sun Microsystems	online per Download
jdkic_native.jar (Linux)	20061102	339 KB	Sun Microsystems	online per Download
jdkic_native.jar (Windows)	20061102	54 KB	Sun Microsystems	online per Download
jdkic_stub.jar (Linux)	20061102	53 KB	Sun Microsystems	online per Download
jhall.jar	2.0_01	543 KB	Sun Microsystems	online per Download
jRegistryKey.jar	1.2.3	14 KB	bayblade	online per Download
log4j-1.2.15.jar	1.2.15	407 KB	Apache Software	online per Download
mysql-connector-java-5.0.4-bin.jar	5.0.4	501 KB	MySQL	online per Download
natlib.jar	1.8.0	115 KB	Sun Microsystems	online per Download
ojdbc14.jar	10.2.0.3	1552 KB	Oracle	online per Download
truezip-6.jar	6.6	483 KB	Apache Software	online per Download
xerces.jar	2.9.1	1275 KB	Apache Software	online per Download
xmlParserAPIs.jar	1.2.01	137 KB	Apache Software	online per Download
xmlsec-1.4.1.jar	1.4.1	435 KB	Apache Software	online per Download

Tabelle 2: Software

Alle Dateien der Software "Govello, Version 3.1" 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.

Die Software "Govello, Version 3.1" ist ein eigenständiges, in Java™ geschriebenes Programm, welche unter Zuhilfenahme von Java™ Web Start von einem Webserver via Hyper Text Transfer Protocol (http) auf den PC des Nutzers geladen werden muss.

Das Produkt "Govello, Version 3.1" 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	Produktzentrum Tele-Sec der Deutschen Telekom AG	Signaturerstellungseinheit TCOS 3.0 Signature Card, Version 1.0	TUVIT.93119.TE.09.2006 TUVIT.93146.TE.12.2006
SSEE	Bundesnotarkammer, Zertifizierungsstelle	Signaturerstellungseinheit STARCOS 3.0	TUVIT.93100.TE.09.2005 Nachträge vom 08.08.2006, 20.10.2006 und 07.12.2006
SSEE	Bundesnotarkammer, Zertifizierungsstelle	Signaturerstellungseinheit STARCOS 3.2	BSI.02114.TE.12.2008
SSEE	DATEV eG Zertifizierungsstelle	Signaturerstellungseinheit STARCOS 3.0	TUVIT.93100.TE.09.2005 Nachträge vom 08.08.2006, 20.10.2006 und 07.12.2006
SSEE	DATEV eG Zertifizierungsstelle	Signaturerstellungseinheit STARCOS 3.2	BSI.02114.TE.12.2008
SSEE	D-Trust GmbH	SEE "Chipkarte mit Prozessor SLE66CX322P, CardOS V4.3B mit Applikation für digitale Signatur"	T-Systems.02122.TE.05. 2005
SSEE	Deutsche Post Com GmbH Geschäftsfeld Signtrust	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	Signaturerstellungseinheit STARCOS 3.2	BSI.02114.TE.12.2008
SSEE	TC TrustCenter TrustCenter GmbH	SEE "Chipkarte mit Prozessor SLE66CX322P, CardOS V4.3B mit Applikation für digitale Signatur"	T-Systems.02122.TE.05. 2005
SSEE	D-Trust GmbH	SEE "Chipkarte mit Prozessor SLE66CX322P, Car-	T-Systems.02122.TE.05. 2005

Produktklasse	Bezeichnung		Beschreibung + Registriernummer der Bestätigung
		dOS V4.3B mit Applikation für digitale Signatur"	
SSEE	S-Trust, Deutscher Sparkassen Verlag GmbH	SEE ZKA-Signaturkarte, Version 5.02 der Gemplu-mids GmbH	TUVIT.09385.TU.09.2004
SSEE	S-Trust, Deutscher Sparkassen Verlag GmbH	SEE ZKA Banking Signature Card, Version 6.2b NP und 6.2f NP, Type 3 der Giesecke & Devrient GmbH	TUVIT.09395.TU.01.2005
SSEE	S-Trust, Deutscher Sparkassen Verlag GmbH	SEE ZKA Banking Signature Card, Version 6.31 NP, Type 3 der Giesecke & Devrient GmbH	TUVIT.09397.TU.03.2005
SSEE	S-Trust, Deutscher Sparkassen Verlag GmbH	SEE ZKA Banking Signature Card, Version 6.32 NP, Type 3 der Giesecke & Devrient GmbH	TUVIT.93125.TU.12.2005
SSEE	S-Trust, Deutscher Sparkassen Verlag GmbH	SEE ZKA Banking Signature Card, Version 6.4 der Giesecke & Devrient GmbH	TUVIT.93123.TU.12.2006
SSEE	S-Trust, Deutscher Sparkassen Verlag GmbH	SEE ZKA-Signaturkarte, Version 5.10 der Gemplu-mids GmbH	TUVIT.93132.TU.06.2006
SSEE	S-Trust, Deutscher Sparkassen Verlag GmbH	SEE ZKA Banking Signature Card, Version 6.6 der Giesecke & Devrient GmbH	TUVIT.93130.TU.05.2006, 1. Nachtrag vom 28.08.2006 und 2. Nachtrag vom 18.10.2006
SSEE	S-Trust, Deutscher Sparkassen Verlag GmbH	Signaturerstellungseinheit ZKA SECCOS Sig v1.5.3 der Sagem Orga GmbH	BSI.02076.TE.12.2006
SSEE	S-Trust, Deutscher Sparkassen Verlag GmbH	ZKA-Signaturkarte, Version 5.11 Gemplu GmbH (Gematto)	TUVIT.93138.TU.11.2006
SSEE	S-Trust, Deutscher Sparkassen Verlag GmbH	Multisignaturerstellungseinheit ZKA Banking	Signature Card Version 5.11M
SSEE	S-Trust, Deutscher Sparkassen Verlag GmbH	Signaturerstellungseinheit ZKA Banking	Signature Card, Version 7.1.2 der Giesecke
SSEE	Deutsche Rentenversicherung Bund	SEE "Chipkarte mit Prozessor SLE66CX322P, CardOS V4.3B mit Appli-	T-Systems.02122.TE.05. 2005

Produktklasse	Bezeichnung		Beschreibung + Registriernummer der Bestätigung
		kation für digitale Signatur"	
SSEE	Hessen-PKI (unter der PKI-1 Verwaltung)	Signaturerstellungseinheit TCOS 3.0	Signature Card, Version 1.0, Version 1.1
Kartenleser	OMNIKEY GmbH	SAK Chipkartenterminal der Familie CardMan Trust CM3621, Firmware-Version 6.00	BSI.02057.TE.12.2005
Kartenleser	Cherry GmbH	Chipkartenterminal der Familie SmartBoard xx44 Firmware-Version 1.04	BSI.02048.TE.12.2004
Kartenleser	Cherry GmbH	Chipkartenterminal der Familie SmartTerminal ST-2xxx, Firmware Version 5.11	BSI.02059.TE.02.2006
Kartenleser	Reiner SCT Kartenlesegeräte GmbH	CyberJack e-com, Version 3.0	TUVIT.93155.TE.09.2008
Kartenleser	Reiner SCT Kartenlesegeräte GmbH	CyberJack e-com plus, Version 3.0	TUVIT.93156.TU.09.2008
Kartenleser	Reiner SCT Kartenlesegeräte GmbH	Chipkartenleser CyberJack secoder Version 3.0	TUVIT.93154.TE.09.2008
Kartenleser	Reiner SCT Kartenlesegeräte GmbH	CyberJack pinpad, Version 2.0	T-Systems. 09362.TE.05.2002
Kartenleser	Reiner SCT Kartenlesegeräte GmbH	Chipkartenleser, cyberJack pinpad, Version 3.0	TUVIT.93107.TU.11.2004
Kartenleser	Kobil Systems GmbH	Chipkartenterminal KAAAN Advanced, Firmware Version 1.02, Hardware Version K104R3, Firmware 1.19 nach bestätigt.	BSI.02050.TE.12.2006 Nachtrag zur Bestätigung vom 07.04.2008: TSystems. 02207.TU.04.2008
Kartenleser	Kobil Systems GmbH	KOBIL Chipkartenterminal KAAAN Professional HW-Version KCT100, FW 2.08 GK 1.04	TUVIT.09331.TE.03.2002
Kartenleser	Kobil Systems GmbH	EMV-TriCAP Reader (Art.-Nr. HCPNCKS/A03, Firmware 69.18)	BSI.02096.TE.12.2008
Kartenleser	Kobil Systems GmbH	SecOVID Reader III (Art.-Nr. HCPNCKS/B05, Firmware 69.18)	BSI.02096.TE.12.2008
Kartenleser	Kobil Systems GmbH	KAAAN TriB@nk (Art.-	BSI.02096.TE.12.2008

Produktklasse	Bezeichnung		Beschreibung + Registriernummer der Bestätigung
		Nr. HCPNCKS/C05, Firmware 68.17)	
Kartenleser	SCM Microsystems GmbH	Chipkartenleser SPR132, SPR332, SPR532, Firmware Version 4.15	TUVIT.09370.TE.03.2003
Kartenleser	Fujitsu Siemens	Chipkartenleser-Tastatur Sachnummer S26381-K329-V2xx Firmware Version 1.06	BSI.02082.TE.01.2007

Tabelle 3: Zusätzliche, nach SiG bestätigte Produkte

3. Funktionsbeschreibung

Die Software "Govello, Version 3.1" ist Teil einer Signaturanwendungskomponente gemäß § 2 Nr. 11 SigG; die auf geeigneter Hardware mit geeigneten Betriebsmitteln – insbesondere mit SigG-konformen Chipkartenlesern und sicheren Signaturerstellungseinheiten (siehe Tabelle 3) in einem "geschützten Einsatzbereich (Regelfall/Standardlösung)" [BNetzA2005]³ betrieben und über eine Oberfläche (Graphical User Interface – GUI) von einem autorisierten Nutzer konfiguriert und genutzt wird.

Die Software "Govello, Version 3.1" erfüllt alle Anforderungen gemäß § 17 Abs. 2 SigG, umfasst allerdings keine Chipkartenleser oder sichere Signaturerstellungseinheiten. Eine Übersicht, welche signaturrechtlichen Anforderungen vom Produkt erfüllt werden, findet sich in Abschnitt 4. Im Nachfolgenden erfolgen zunächst die Funktionsbeschreibung des Produktes und anschließend eine Darstellung der Schnittstellen.

Die Software "Govello, Version 3.1" stellt Funktionen zur Erzeugung qualifizierter elektronischer Signaturen und zur Prüfung qualifizierter elektronischer Signaturen im Rahmen einer OSCI-Kommunikation⁴ zur Verfügung:

- Die Software "Govello, Version 3.1" unterstützt den Nutzer bei der Erzeugung von qualifizierten elektronischen Signaturen, die lokal von einer sicheren Signaturerstellungseinheit – unter Verwendung der Schnittstelle zum Chipkartenleser – erzeugt werden.

Signiert wird insbesondere eine Nachricht (in UTF-8-Codierung), die der Nutzer in einem Nachrichtenfenster eingeben kann, sowie mögliche Dateianhänge, die dem Nutzer unter Zuhilfenahme der Schnittstelle zur GUI angezeigt werden.

³ 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.

⁴ Das Online Services Computer Interface (OSCI)-Protokoll stellt einen Standard im E-Government dar, in dem zwei Kommunikationspartner (OSCI-Client oder -Backend) über einen OSCI-Intermediär kommunizieren (vgl. www.osci.de).

Der Signaturschlüssel-Inhaber hat an seinem Arbeitsplatz unmittelbar zur Signaturerzeugung Zugriff auf seine sichere Signaturerstellungseinheit (SSEE) und den Chipkartenleser.

Zum Signieren steckt der Signaturschlüssel-Inhaber seine SSEE in den Chipkartenleser, betätigt den Signier-Button – woraufhin die zu signierenden Daten der sicheren Signaturerstellungseinheit zugeführt werden, in der sein privater Signaturschlüssel vorgehalten wird – und autorisiert das Signieren durch Eingabe seiner PIN am PIN-Pad des Kartenlesegeräts. Anschließend kann der Nutzer die signierte OSCI-Nachricht weiterverarbeiten – typischerweise über das OSCI-Protokoll an den OSCI-Manager, der nicht Bestandteil der Software "Govello, Version 3.1" ist, des Empfängers senden.

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 "Govello, Version 3.1" ruft OSCI-Nachrichten vom OSCI-Manager ab und zeigt sie dem Nutzer im Posteingangsordner an. Dabei prüft die Software "Govello, Version 3.1" lokal
 - die mathematische Korrektheit der qualifizierten elektronischen Signatur des Absenders sowie
 - die elektronische Signatur des OSCI-Managers des Laufzettels, auf dem u.a. das Ergebnis der Validierung dokumentiert ist, die der OSCI-Manager durchgeführt hat und die die folgenden Prüfungen (Gültigkeitsmodell: Kettenmodell) umfasst:
 - 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?
 - Dem Nutzer wird das Ergebnis der oben spezifizierten Prüfungen angezeigt:
 - Status o.k.: Alle Prüfungen ergaben "gültig".
 - Status nicht eindeutig: Mindestens eine Prüfung konnte nicht abschließend durchgeführt werden
 - Status nicht o.k.: Mindestens eine Prüfung hatte das Ergebnis "ungültig" zur Folge.

Darüber hinaus wird dem Nutzer in einem Nachrichtenfenster insbesondere die signierte Nachricht (in UTF-8-Codierung) sowie die signierten Dateianhänge angezeigt.

Des Weiteren wird eine Online-Validierung eines Zertifikates über einen Verifikationsserver unterstützt (vgl. Schnittstelle zum Verifikationsserver), der die oben angegebenen Prüfungen analog durchführt und dokumentiert.

Die Software "Govello, Version 3.1" 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 graphischen Bedienungsfläche (Graphical User Interface – GUI):

Die Software "Govello, Version 3.1" nutzt die graphische Oberfläche als Schnittstelle zum Nutzer und visualisiert die Interaktion mit dem Signaturschlüssel-Inhaber durch entsprechende informelle und prozedurale Anzeigen.

- Schnittstelle zum OSCI-Manager und zum Verifikationsserver:

Im Rahmen der OSCI-Kommunikation dient der OSCI-Manager in der Rolle des OSCI-Intermediärs als Mittler zwischen Sender und Empfänger, wobei der OSCI-Intermediär Zertifikate prüft und das Ergebnis in einem Laufzettel dokumentiert. Für die OSCI-Kommunikation wird das OSCI-Transport-Protokoll verwendet. Darüber hinaus ist eine Online-Validierung über einen Verifikationsserver möglich.

Die vorliegende Herstellereklärung bezieht sich ausschließlich auf die Eigenschaft der Software "Govello, Version 3.1" 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 und
- qualifizierte Signaturen zu prüfen oder qualifizierte Zertifikate nachzuprüfen und die Ergebnisse anzuzeigen.

4. Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

Die Software "Govello, Version 3.1" erfüllt die nachfolgenden Anforderungen des SigG:

- § 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,
 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.
- § 17 Abs. 2 Satz 3 SigG Signaturanwendungskomponenten müssen nach Bedarf auch den Inhalt der zu signierenden oder signierten Daten hinreichend erkennen lassen.

Zur Umsetzung dieser gesetzlichen Anforderungen ist in der Software "Govello, Version 3.1" eine entsprechende Anzeige implementiert, die anzeigt

- bevor eine Signatur erzeugt werden soll,
- 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).

Die Software "Govello, Version 3.1" erfüllt die nachfolgenden Anforderungen der SigV:

- § 15 Abs. 2 SigV Signaturanwendungskomponenten nach § 17 Abs. 2 des Signaturgesetzes müssen gewährleisten, dass
 1. bei der Erzeugung einer qualifizierten elektronischen Signatur
 - a) die Identifikationsdaten nicht preisgegeben und diese nur auf der jeweiligen sicheren Signaturerstellungseinheit gespeichert werden,
 - b) eine Signatur nur durch die berechtigt signierende Person erfolgt,
 - c) die Erzeugung einer Signatur vorher eindeutig angezeigt wird und
 2. bei der Prüfung einer qualifizierten elektronischen Signatur
 - a) die Korrektheit der Signatur zuverlässig geprüft und zutreffend angezeigt wird und
 - b) eindeutig erkennbar wird, ob die nachgeprüften qualifizierten Zertifikate im jeweiligen Zertifikat-Verzeichnis zum angegebenen Zeitpunkt vorhanden und nicht gesperrt waren.
- § 15 Abs. 4 SigV Sicherheitstechnische Veränderungen an technischen Komponenten nach den Absätzen 1 bis 3 müssen für den Nutzer erkennbar werden.

Zur Umsetzung dieser Anforderungen ist in der Software "Govello, Version 3.1" implementiert,

- dass die Signaturerzeugung auf einer sicheren Signaturerstellungseinheit erfolgt, die über einen Chipkartenleser angesprochen wird,
- dass die PIN-Eingabe ausschließlich über Chipkartenleser erfolgt – damit werden die Identifikationsdaten nicht in der Software "Govello, Version 3.1" verarbeitet –,

- die Erzeugung einer Signatur vorher eindeutig angezeigt wird,
- dass die Verifikation der Signatur (lokale mathematische Prüfung) und
- die Validierung des Zertifikats (Überprüfung, ob die nachgeprüften qualifizierten Zertifikate im jeweiligen Zertifikatverzeichnis zum angegebenen Zeitpunkt vorhanden und nicht gesperrt waren) korrekt ausgeführt und zutreffend angezeigt werden.
- Die Anforderungen zur Erkennung sicherheitstechnischer Veränderungen werden durch die Signaturen der Software und die Auflagen zum Betrieb realisiert, vgl. Abschnitt 5.

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 Govello, Version 3.1 umsetzbar.

Die Software "Govello, Version 3.1" erfüllt alle Anforderungen gemäß § 17 Abs. 2 SigG, umfasst allerdings keine Chipkartenleser und keine sicheren Signaturerstellungseinheiten.

Hinweis zu schwachwerdenden Algorithmen und qualifizierten Zeitstempeln

Signaturanwendungskomponenten i. S. v. § 2 Nr. 11 b SigG müssen auch dann eine zuverlässige Prüfung und zutreffende Anzeige des Ergebnisses gem. § 15 Abs. 2 Nr. 2a SigV gewährleisten⁵, wenn die geprüfte Signatur auf einem Algorithmus oder Parameter beruht, der als nicht mehr geeignet und damit als nicht mehr hinreichend zuverlässig eingestuft ist, oder wenn ein qualifizierter Zeitstempel vorliegt.

Seitens der Bundesnetzagentur wurden die Anforderungen an Signaturanwendungskomponenten weiter präzisiert, die das Produkt „Govello, Version 3.1“ aktuell wie folgt erfüllt:

Anforderung	Erfüllung und Verhalten der Software „Govello, Version 3.1“
<p>a) Abgelaufene Algorithmen:</p> <p>Die Prüfung einer Signatur durch eine Signaturanwendungskomponente (SAK) für qualifizierte elektronische Signaturen i.S.v. § 2 Nr. 11b SigG muss bei abgelaufenen Algorithmen für den Nutzer deutlich anzeigen, dass die geprüfte Signatur mit einem Algorithmus erzeugt wurde, der nicht mehr dem Stand der Wissenschaft und Technik entspricht, und sie somit</p>	<p>Zur Verifikation von Signaturen, prüft das Produkt „Govello, Version 3.1“ die Gültigkeit sowohl zum Signaturzeitpunkt als auch zum Zeitpunkt der Prüfung.⁶</p> <p>Das Prüfprotokoll hebt Signaturen, die mit schwachgewordenen Algorithmen erzeugt wurden - farblich gelb markiert - hervor und weist darauf hin, dass der verwendete Algorithmus</p>

⁵ Schreiben der Bundesnetzagentur „Hinweis im Zusammenhang mit der Prüfung von qualifizierten elektronischen Signaturen, die auf ungeeigneten Algorithmen beruhen, und von qualifizierten Zeitstempeln“ vom 06.03.2009

⁶ Detaillierte Erläuterungen finden sich im Informationspapier zur Umsetzung des bos-Prüfprotokolls gemäß FAQ 28 der BNetzA. (Vgl. Ausgliederte Zusatzdokumentation)

⁷ Informationen zur graduellen und sukzessiven Einbuße des Beweiswertes der Signatur, sind dem beiliegenden Dokument „bos-Prüfprotokoll mit Zertifikatsanzeige“ zu entnehmen.

Anforderung	Erfüllung und Verhalten der Software „Govello, Version 3.1“
<p>einen verminderten Beweiswert hinsichtlich der Authentizität und Integrität des verbundenen Dokuments gegenüber dem Signaturzeitpunkt besitzt. Weiter sollte der Zeitpunkt, zu dem der Algorithmus seine Eignung verloren hat, zutreffend angezeigt werden.</p> <p>Unspezifische Aussagen zu abgelaufene Algorithmen sind nicht zulässig.</p>	<p>zum Zeitpunkt der Prüfung gemäß aktuellem Algorithmenkatalog nicht mehr für eine QES geeignet war.⁷</p> <p>Außerdem zeigt das Prüfprotokoll an, bis zu welchem Zeitpunkt die verwendeten Algorithmen gemäß Algorithmenkatalog als geeignet anzusehen sind, bzw. es waren.</p>
<p>b) Nicht implementierte Algorithmen:</p> <p>Ist bei der Prüfung einer Signatur ein Algorithmus zu verwenden, der in der Verifikationskomponente der SAK nicht implementiert ist, so muss dies dem Nutzer zutreffend angezeigt werden.</p> <p>Unspezifische Aussagen zu nicht implementierten Algorithmen sind nicht zulässig</p>	<p>Aktuell wird diese Anforderung nicht vollumfänglich erfüllt.</p> <p>Die Software "Govello, Version 3.1" weist lediglich aus, dass die Signatur nicht geprüft werden konnte.</p> <p>Die Begründung, dass die Verifikation jedoch aufgrund eines nicht implementierten Algorithmus scheiterte, wird im kommenden Release, spätestens jedoch bis zum Ende das Jahres 2009, hinzugefügt.</p>
<p>c) Qualifizierte Zeitstempel:</p> <p>Tragen Daten einer qualifizierten Signatur, bei deren Verifikation zu erkennen ist, dass der Signaturprüf-schlüssel zu einem Zeitstempel-Zertifikat gehört, so ist dies dem Nutzer zutreffend anzuzeigen. Der Zeitpunkt, der im qualifizierten Zeitstempel enthalten ist, ist dem Nutzer ebenfalls darzulegen.</p> <p>Solange kein standardisiertes Verfahren für die Einbindung von qualifizierten Zeitstempeln existiert, ist es ausreichend, wenn das Produkt seine selbst integrierten qualifizierten Zeitstempel auswerten kann. Qualifizierte Zeitstempel, die aus Fremdprodukten und damit in einer ev. proprietären Datenstruktur vorliegen, müssen nicht zwingend durch das Produkt ausgewertet werden.</p> <p>Unspezifische Aussagen zu qualifizierten Zeitstempeln sind nicht zulässig</p>	<p>Das Produkt „Govello, Version 3.1“ selbst bringt keine Zeitstempel an.</p> <p>Mangels standardisiertem Verfahren für die Einbindung von qualifizierten Zeitstempeln, werden qualifizierte Zeitstempel aus Fremdprodukten nicht interpretiert.</p>

5. Maßnahmen in der Einsatzumgebung

5.1 Einrichtung der IT-Komponenten

Für den Betrieb der Software "Govello, Version 3.1" wird folgende Einsatzumgebung vorausgesetzt:

- Personal Computer (PC) mit Internetanschluss;
- Betriebssystem:
 - Microsoft Windows 2000, XP oder Vista (jeweils mit aktuellem Service Pack);
 - openSUSE 10.x;
- Internet-Browser;
- 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 1.6.0; mindestens 1.5.0_06; empfohlen 1.5.0_18 bzw. mindestens 1.6.0_05; empfohlen 1.6.0_13.

Die Software "Govello, Version 3.1" darf ausschließlich innerhalb der oben beschriebenen Hard- und Softwareausstattung eingesetzt werden.

5.2 Anbindung an ein Netzwerk

Für den Betrieb der Software "Govello, Version 3.1" ist ein Netzwerk notwendig.

Bei Anbindung der Software 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.

Alle Dateien der Software "Govello, Version 3.1" 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 "Govello, Version 3.1" von der Gültigkeit der Signatur überzeugen. Die Verifikation der Signatur erfolgt über Standard-Java-Mechanismen.

Die Software "Govello, Version 3.1" lässt sich über eine Installationsroutine einfach installieren, ein Java Runtime Environment (JRE) wird immer mitinstalliert. In der Installationsroutine werden einige Parameter zur Installation (Ort des Installationsverzeichnis, Anlegen einer Desktopverknüpfung etc.) abgefragt.

5.4 Auflagen für den Betrieb des Produktes

Die Software "Govello, Version 3.1" wird in einem "geschützten Einsatzbereich (Regelfall/ Standardlösung)" (vgl. "Einheitliche Spezifizierung der Einsatzkomponenten für Signaturanwendungskomponenten – Arbeitsgrundlage für Entwickler/Hersteller und Prüf-/Bestätigungsstellen", Version 1.4, 19.07.2005) betrieben.

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 "Govello, Version 3.1" 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 Trojanischen 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.

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 zur Sicherheitsadministration des Betriebs

Hinsichtlich der Software "Govello, Version 3.1" 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.

Auflagen zum Schutz vor Fehlern bei Betrieb/Nutzung

Folgende Auflagen sind für den sachgemäßen Einsatz der Software "Govello, Version 3.1" 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.
- 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 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.
- Hinweise von Zertifizierungsdiensteanbietern zum Umgang mit persönlichen sowie 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 OSCl-Manager – gegeben sind.

Auflagen für Wartung/Reparatur

Die Pflege und Wartung der Software "Govello, Version 3.1" erfolgt mittels Bereitstellung aktualisierter Java Archive die vom Benutzer über einen Download von einem Webserver bezogen werden können.

6. Algorithmen und zugehörige Parameter

Zur Erzeugung qualifizierter elektronischer Signaturen werden vom Produkt "Govello, Version 3.1" signaturkartenspezifisch die Hashfunktionen SHA-256 (default), SHA-512 und RIPEMD-160 gemäß aktueller OSCl-Spezifikation bereitgestellt. Die Signatur selbst (Verschlüsselung des Hashwertes) wird durch die unterstützten sicheren Signaturerstellungseinheiten vorgenommen. In diesem Kontext kommen die auf den Signaturkarten (SSEE) implementierten RSA-Algorithmen zum Einsatz.

Zur Prüfung qualifizierter elektronischer Signaturen werden vom Produkt "Govello, Version 3.1" die Hashfunktionen RIPEMD-160, SHA-224, SHA-256, SHA-512 und SHA-1⁸ sowie der Signaturalgorithmus RSA-768, RSA-1024, RSA-1280, RSA-1536, RSA-1728, RSA-1976, RSA-2048 Bit sowie DSA-1024, DSA-1280, DSA-1536, DSA-2048 Bit (Parameter p) jeweils mit 160 oder 224 Bit (Parameter q). bereitgestellt.

Die gemäß Anlage I Abs. 1 Nr. 2 SigV festgelegte Eignung für die verwendeten kryptographischen Algorithmen 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, veröffentlicht am 27. Januar 2009 im Bundesanzeiger Nr. 13, S. 3746) wie folgt als geeignete eingestuft:

Algorithmus	Parameter		Für die Anbringung		Zur Durchführung der Prüfung	
			Ablauf der Eignung bei Inhaltsdaten	Ablauf der Eignung bei Zertifikaten	Ablauf der Eignung bei Inhaltsdaten	Ablauf der Eignung bei Zertifikaten
RIPEMD-160			31.12.2010	31.12.2010	31.12.2010	31.12.2015
SHA-1			30.06.2008	31.12.2010	30.06.2008	31.12.2015
SHA-2	224		31.12.2015	31.12.2015	31.12.2015	31.12.2015
SHA-2	256		31.12.2015	31.12.2015	31.12.2015	31.12.2015
SHA-2	384		31.12.2015	31.12.2015	31.12.2015	31.12.2015
SHA-2	512		31.12.2015	31.12.2015	31.12.2015	31.12.2015

⁸ Dem Benutzer wird bei der Prüfung alter Signaturen, die mit SHA-1 erzeugt wurden, die abgelaufene Gültigkeit von SHA-1 mit einem Warnhinweis angezeigt.

Algorithmus	Parameter		Für die Anbringung		Zur Durchführung der Prüfung	
			Ablauf der Eignung bei Inhaltsdaten	Ablauf der Eignung bei Zertifikaten	Ablauf der Eignung bei Inhaltsdaten	Ablauf der Eignung bei Zertifikaten
	Parameter n ⁹					
RSA ¹⁰	768		31.12.2000	31.12.2000	31.12.2000	31.12.2000
RSA	1024		31.03.2008	31.03.2008	31.03.2008	31.03.2008
RSA	1280		31.12.2008	31.12.2008	31.12.2008	31.12.2008
RSA	1536		31.12.2009	31.12.2009	31.12.2009	31.12.2009
RSA	1728		31.12.2010	31.12.2010	31.12.2010	31.12.2010
RSA	1976		31.12.2015	31.12.2015	31.12.2015	31.12.2015
RSA	2048		31.12.2015	31.12.2015	31.12.2015	31.12.2015
	Parameter p	Parameter q				
DSA ¹¹	1024	160	31.12.2007	31.12.2007	31.12.2007	31.12.2007
DSA	1280	160	31.12.2008	31.12.2008	31.12.2008	31.12.2008
DAS	1536	160	31.12.2009	31.12.2009	31.12.2009	31.12.2009
DAS	2048	160	31.12.2009	31.12.2009	31.12.2009	31.12.2009
DSA	1024	224	31.12.2007	31.12.2007	31.12.2007	31.12.2007
DSA	1280	224	31.12.2008	31.12.2008	31.12.2008	31.12.2008
DSA	1536	224	31.12.2009	31.12.2009	31.12.2009	31.12.2009
DSA	2048	224	31.12.2015	31.12.2015	31.12.2015	31.12.2015

Tabelle 4: Eignung der Algorithmen für qualifizierte elektronische Signaturen (QES)

7. Gültigkeitsdauer 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.

⁹ "n, p und q" bezeichnen die verschiedenen Parameter der angegebenen kryptographischen Verfahren und deren Bitlängen gemäß Algorithmenkatalog.

¹⁰ Dem Benutzer wird bei der Prüfung alter Signaturen, die mit RSA erzeugt wurden, die abgelaufene Gültigkeit von RSA mit einem Warnhinweis angezeigt.

¹¹ Dem Benutzer wird bei der Prüfung alter Signaturen, die mit DSA erzeugt wurden, die abgelaufene Gültigkeit von DSA mit einem Warnhinweis angezeigt.

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:

- "Unterlagen zur Herstellereklärung gemäß § 17 Abs. 4 SigG für die Software "Govello, Version 3.1" – Sicherheitstechnische Produktbeschreibung und Spezifikation, 24.09.2009, 76 Seiten.
- Unterlagen zur Herstellereklärung gemäß § 17 Abs. 4 SigG für die Software "Govello, Version 3.1" – Testdokumentation, 24.09.2009, 14 Seiten.
- Benutzerhandbuch "Govello", Version 3.1.0, 92 Seiten.
- Testkonzept "Govello Deutsche Version Release 3.1.0", Version 1.0, 03.08.2009, 168 Seiten.
- "bos-Prüfprotokoll mit Zertifikatsanzeige", 25.09.2009, 51 Seiten.

Ende der Herstellereklärung