

## **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 SigG<sup>1</sup>

in Verbindung mit § 15 Abs. 5 SigV<sup>2</sup>,

dass sein Produkt

### **Elektronisches Gerichts- und Verwaltungspostfach (EGVP), Version 2.5.0.0**

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

Bremen, den 17.11.2009

gez. Stephan Klein

---

Geschäftsführung bos KG

Diese Herstellereklärung in der Version 1.0 mit der Dokumentennummer bos2009004 besteht aus 19 Seiten.

---

<sup>1</sup> 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)

<sup>2</sup> 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	17.11.2009	bremen online services Entwicklungs- und Betriebsgesellschaft mbH & Co. KG	Initialversion

## Beschreibung des Produkts

### 1. Handelsbezeichnung und Hersteller

Die Handelsbezeichnung lautet:	Elektronisches Gerichts- und Verwaltungspostfach (EGVP), Version 2.5.0.0
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:

Produktbestandteile	Bezeichnung	Version	Übergabeform
Software	EGVP, Version 2.5.0.0	2.5.0.0	online per Download
Benutzerhandbuch	Anwenderdokumentation „Elektronisches Gerichts- und Verwaltungspostfach – sichere Kommunikation mit Gerichten und Behörden –; Bürgerinnen und Bürger; EGVP Version 2.5.0“	2.5.0	online per Download
	Anwenderdokumentation „Elektronisches Gerichts- und Verwaltungspostfach – sichere Kommunikation mit Gerichten und Behörden –; Bürgerinnen und Bürger; EGVP Version 2.5.0“	2.5.0	online per Download

Tabelle 1: Lieferumfang und Versionsinformation

Der signaturgesetzrelevante Teil der Software „EGVP, Version 2.5.0.0“ besteht aus den in der folgenden Tabelle aufgeführten Dateien:

Datei	Version <sup>3</sup>	Größe	Hersteller/Herausgeber
<b>EGVP-JAR-Dateien</b>			
egvp_backend.jar	2.5.0.0	546 KB	bos KG
egvp_client.jar	2.5.0.0	588 KB	bos KG
<b>Govello-Bibliotheken</b>			
govello_framework.jar	3.1.2.0	2106 KB	bos KG
service_modules.jar	3.1.2.0	1702 KB	bos KG
<b>bos ServiceModules Bibliotheken</b>			

<sup>3</sup> „Version“ bezieht sich in diesem Fall auf die Versionsverwaltung des Servers.

Datei	Version <sup>3</sup>	Größe	Hersteller/Herausgeber
mcard.jar	1.10.1	981 KB	bos KG
<b>Bouncy Castle Bibliotheken</b>			
gov_crypto_provider-1.0.jar	1.0	48 KB	bos KG
bcprov-jdk15-143-bos-0.1.jar	1.0	2070 KB	Bouncy Castle
bctsp-jdk15-143-bos-0.1.jar	1.0	32 KB	Bouncy Castle
bcmail-jdk15-143-bos-0.1.jar	1.0	282 KB	Bouncy Castle
bc.extensions-jdk15-143-bos-0.1.jar	1.0	95 KB	Bouncy Castle
<b>Governikus SDK Bibliotheken</b>			
clientenabler.jar	1.0	520 KB	bos KG
osci-bibliothek.jar	1.0	348 KB	bos KG
streamedpkcs7.jar	1.0	15 KB	bos KG

**Tabelle 2: Software**

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](http://www.bos-bremen.de)) zur Verfügung gestellt.

Das Produkt „EGVP, Version 2.5.0.0“ 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		Beschreibung + Registriernummer der Bestätigung
SSEE	Produktzentrum Tele-Sec der Deutschen Telekom AG	PKS-Card (NetKey 3.01) Signaturerstellungseinheit TCOS 3.0 Signature Card, Version 1.0, Version 1.1	TUVIT.93119.TE.09.2006
SSEE	Bundesnotarkammer, Zertifizierungsstelle	Signaturkarte der Bundesnotarkammer, qualifizierte elektronische Signatur Signaturerstellungseinheit STARCOS 3.0	TUVIT.93100.TE.09.2005
SSEE	Bundesnotarkammer, Zertifizierungsstelle	Signaturkarte der Bundesnotarkammer, qualifizierte elektronische Signatur Signaturerstellungseinheit STARCOS 3.2	BSI.02114.TE.12.2008
SSEE	DATEV eG Zertifizierungsstelle	zertifizierte Signaturkarte für Berufsträger der DATEV (2048 Bit RSA Schlüssellänge)	TUVIT.93100.TE.09.2005

Produkt- klasse	Bezeichnung		Beschreibung + Registriernummer der Bestätigung
		Signaturerstellungseinheit STARCOS 3.0	
SSEE	D-Trust GmbH	D-Trust-Signaturkarte Version 2.2 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	Signtrust-Identity-Card Signaturerstellungseinheit STARCOS 3.0	TUVIT.93100.TE.09.2005
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	D-Trust GmbH	D-Trust-Card (2.02c qualified), auch Chambersignkarte der teilnehmenden IHKs (mit 2048 Bit RSA Schlüssellänge) SEE „Chipkarte mit Prozessor SLE66CX322P, CardOS V4.3B mit Applikation für digitale Signatur“	T-Systems.02122.TE.05. 2005
SSEE	S-Trust, Deutscher Sparkassen Verlag GmbH	SparkassenCard oder GeldKarte SEE ZKA-Signaturkarte, Version 5.02 der Gemplusmids GmbH	TUVIT.09385.TU.09.2004
SSEE	S-Trust, Deutscher Sparkassen Verlag GmbH	SparkassenCard oder GeldKarte 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	SparkassenCard oder GeldKarte SEE ZKA Banking Signature Card, Version 6.31 NP, Type 3	TUVIT.09397.TU.03.2005

Produkt- klasse	Bezeichnung	Beschreibung + Registriernum- mer der Bestätigung	
		der Giesecke & Dev- rient GmbH	
SSEE	S-Trust, Deutscher Sparkassen Verlag GmbH	SparkassenCard oder GeldKarte SEE ZKA Banking Signature Card, Versi- on 6.32 NP, Type 3 der Giesecke & Dev- rient GmbH	TUVIT.93125.TU.12.2005
SSEE	S-Trust, Deutscher Sparkassen Verlag GmbH	SparkassenCard oder GeldKarte SEE ZKA Banking Signature Card, Versi- on 6.4 der Giesecke & Devrient GmbH	TUVIT.93123.TU.12.2006
SSEE	S-Trust, Deutscher Sparkassen Verlag GmbH	SparkassenCard oder GeldKarte SEE ZKA- Signaturkarte, Version 5.10 der Gemplus- mids GmbH	TUVIT.93132.TU.06.2006
SSEE	S-Trust, Deutscher Sparkassen Verlag GmbH	SparkassenCard oder GeldKarte SEE ZKA Banking Signature Card, Versi- on 6.6 der Giesecke & Devrient GmbH	TUVIT.93130.TU.05.2006
SSEE	S-Trust, Deutscher Sparkassen Verlag GmbH	SparkassenCard oder GeldKarte SEE ZKA Banking Signature Card, Versi- on 6.51 der Giesecke & Devrient GmbH	TUVIT.93129.TU.03.2006
SSEE	S-Trust, Deutscher Sparkassen Verlag GmbH	SparkassenCard oder GeldKarte Signaturerstellung- seinheit ZKA SECCOS Sig v1.5.3 der Sagem Orga GmbH	BSI.02075.TE.08.2006
SSEE	S-Trust, Deutscher Sparkassen Verlag GmbH	SparkassenCard oder GeldKarte ZKA-Signaturkarte, Version 5.11 Gemplus GmbH (Gemalto)	TUVIT.93138.TU.11.2006
SSEE	Deutsche Rentenver- sicherung Bund	Signaturkarte der Deutschen Rente Bund SEE „Chipkarte mit Prozessor SLE66CX322P, Car- dOS V4.3B mit Appli-	T-Systems.02122.TE.05. 2005

Produkt- klasse	Bezeichnung	Beschreibung + Registriernum- mer der Bestätigung	
		kation für digitale Signatur“	
SSEE	Deutsche Post Com GmbH Geschäftsfeld Signtrust (Giesecke & Devrient GmbH)	SIGNTRUST CARD 3.2 Signaturerstellungseinheit STARCOS 3.2	BSI.02114.TE.12.2008
SSEE	DATEV eG Zertifizierungsstelle <sup>4</sup> (Giesecke & Devrient GmbH)	zertifizierte Signaturkarte für Berufsträger der DATEV Signaturerstellungseinheit STARCOS 3.2	BSI.02114.TE.12.2008
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 5.08	BSI.02059.TE.02.2006
Kartenleser	Reiner SCT Kartenlesegeräte GmbH	CyberJack e-com CyberJack e-com, Version 2.0	TUVIT.09363.TE.06.2002
Kartenleser	Reiner SCT Kartenlesegeräte GmbH	CyberJack pinpad Version 3 Chipkartenleser, cyberJack pinpad, Version 3.0	TUVIT.93107.TU.11.2004
Kartenleser	Reiner SCT Kartenlesegeräte GmbH	CyberJack pinpad	T-Systems. 09362.TE.05.2002

<sup>4</sup> Das Produkt „zertifizierte Signaturkarte für Berufsträger“ wird von der DATEV eG in Kooperation mit der Deutsche Post Com GmbH herausgegeben, die diese produziert und technisch betreut.

Produkt-klasse	Bezeichnung		Beschreibung + Registriernummer der Bestätigung
		Version 2.0	
Kartenleser	Kobil Systems GmbH	Kobil KAAN Advanced Chipkartenterminal KAAN Advanced, Firmware Version 1.02, Hardware Version K104R3	BSI.02050.TE.12.2006
Kartenleser	Kobil Systems GmbH	Kobil KAAN Prof. seriell KOBIL Chipkartenterminal KAAN Professional HWVersion KCT100, FW 2.08 GK 1.04	TUVIT.09331.TE.03.2002
Kartenleser	SCM Microsystems GmbH	SPR 332 Chipkartenleser SPR132, SPR332, SPR532, Firmware Version 4.15	TUVIT.09370.TE.03.2003

**Tabelle 3: Zusätzliche Produkte**

Für die Prüffunktionalität nutzt das Produkt „EGVP, Version 2.5.0.0“ 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
Signaturanwendungs-komponente	bremen online services Entwicklungs- und Betriebsgesellschaft mbH & Co. KG	Governikus – Teil der Virtuellen Poststelle des Bundes, Verifikationsmodul, Version 2.2.2.6 (BSI.02071.TE.11.2007) <sup>5</sup>

**Tabelle 3: Zusätzliche SigG- und SigV-konforme Produkte**

### 3. Funktionsbeschreibung

Die Software „EGVP, Version 2.5.0.0“ 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.

<sup>5</sup> Die Nachfolge-Versionen 3.3.1.0 und 3.3.1.3 befinden sich im Bestätigungsprozess, vgl. BSI.02111.TE.xx.200x resp. BSI.02122.TE.xx.200x.

Die Software „EGVP, Version 2.5.0.0“ 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 erfolgt zunächst die Funktionsbeschreibung des Produktes und anschließend eine Darstellung der Schnittstellen.

Die Software „EGVP, Version 2.5.0.0“ stellt Funktionen zur Erzeugung qualifizierter elektronischer Signaturen und zur Prüfung qualifizierter elektronischer Signaturen im Rahmen einer OSCI-Kommunikation (vgl. [OSCI-Transport]) zur Verfügung:

- Die Software „EGVP, Version 2.5.0.0“ 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.

Der Signaturschlüssel-Inhaber hat an seinem Arbeitsplatz unmittelbar zur Signaturerzeugung Zugriff auf seine Signaturkarte und den Chipkartenleser.

Zum Signieren steckt der Signaturschlüssel-Inhaber seine Signaturkarte 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 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 „EGVP“ ruft OSCI-Nachrichten vom OSCI-Manager (siehe Schnittstelle zum OSCI-Manager) ab und zeigt sie dem Nutzer im Posteingangsordner an. Dabei prüft die Software „EGVP“ 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 Signaturzertifikats signiert?
    - Ist dem Trustcenter das verwendete Signaturzertifikat 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 nichtabschließend durchgeführt werden; weitere Informationen finden sich in der Anwenderdokumentation im Abschnitt "Prüfergebnisse im Detail".

- Status nicht o.k.: Mindestens eine Prüfung hatte das Ergebnis "ungültig" zur Folge.

Darüber hinaus werden 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 „EGVP, Version 2.5.0.0“ 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 graphischen Bedienungsoberfläche (Graphical User Interface – GUI):  
Die Software „EGVP, Version 2.5.0.0“ 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<sup>6</sup> verwendet. Darüber hinaus ist eine Online-Validierung über einen Verifikationsserver möglich.

Die vorliegende Herstellereklärung bezieht sich ausschließlich auf die Eigenschaft der Software „EGVP, Version 2.5.0.0“ als Signaturanwendungskomponente i.S.d. § 2 Nr. 11 SigG, d.h. auf diejenigen Funktionalitäten, die dazu bestimmt sind,

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

#### 4. Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

Das Produkt „EGVP, Version 2.5.0.0“ 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 be-	Zur Umsetzung dieser gesetzlichen Anforderungen ist eine entsprechende Anzeige implementiert, die – bevor eine Signatur erzeugt werden soll – anzeigt, <ul style="list-style-type: none"> <li>▪ auf welche Daten sich die zu erstellende</li> </ul>

<sup>6</sup>Vgl. OSCI-Leitstelle, "OSCI-Transport 1.2", 6. Juni 2003

Referenz	Gesetzestext	Beschreibung
	zieht.	<p>Signatur bezieht,</p> <ul style="list-style-type: none"> <li>▪ welchen Inhalt die zu signierenden Daten aufweisen und</li> <li>▪ welchem Signaturschlüssel-Inhaber die zu erstellende Signatur zuzuordnen ist.</li> </ul>
§ 17 Abs. 2 Satz 2	<p>Für die Überprüfung signierter Daten sind Signaturanwendungskomponenten erforderlich, die feststellen lassen,</p> <ol style="list-style-type: none"> <li>1. auf welche Daten sich die Signatur bezieht,</li> <li>2. ob die signierten Daten unverändert sind,</li> <li>3. welchem Signaturschlüssel-Inhaber die Signatur zuzuordnen ist,</li> <li>4. welche Inhalte das qualifizierte Zertifikat, auf dem die Signatur beruht, und zugehörige qualifizierte Attribut-Zertifikate aufweisen und</li> <li>5. zu welchem Ergebnis die Nachprüfung von Zertifikaten nach § 5 Abs. 1 Satz 3 geführt hat.</li> </ol>	<p>zu 1., 3., 4. und 5.: Zur Umsetzung dieser gesetzlichen Anforderungen ist eine entsprechende Anzeige implementiert, die anzeigt,</p> <ul style="list-style-type: none"> <li>▪ auf welche Daten sich die Signatur bezieht,</li> <li>▪ welchen Inhalt die signierten Daten aufweisen,</li> <li>▪ welchem Signaturschlüssel-Inhaber die Signatur zuzuordnen ist,</li> <li>▪ welche Inhalte das zugehörige qualifizierte (Attribut)-Zertifikat aufweist sowie</li> <li>▪ 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).</li> </ul> <p>zu 2.: Über eine kryptographische Signaturprüfung (Integritätsprüfung) wird festgestellt, ob die Signatur bzw. die Daten, auf die sich die Signatur bezieht, unverändert sind.</p>
§ 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 den Inhalt von zu signierenden und signierten Daten im Format Plain-Text (UTF-8) sicher anzeigt.

**Tabelle 4: Erfüllung der Anforderungen des SigG**

Das Produkt „EGVP, Version 2.5.0.0“ erfüllt die nachfolgenden Anforderungen der SigV:

Referenz	Gesetzestext	Beschreibung
§ 15 Abs. 2 Nr. 1	Signaturanwendungskomponenten nach § 17 Abs. 2 des Signaturgesetzes müssen gewährleisten, dass [...] bei der Erzeugung einer qualifizierten elektronischen Signatur	<p>zu a) und b) Die Erzeugung einer qualifizierten elektronischen Signatur erfolgt ausschließlich in einer SSEE, die über einen Chipkartenleser angesprochen wird.</p> <p>Die PIN-Eingabe erfolgt ausschließlich über</p>

Referenz	Gesetzestext	Beschreibung
	<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>Chipkartenleser – damit werden die Identifikationsdaten nicht in der Software „EGVP, Version 2.5.0.0“ verarbeitet. Der Signaturschlüssel-Inhaber hat an seinem Arbeitsplatz unmittelbar zur Signaturerzeugung Zugriff auf seine Signaturkarte und den Chipkartenleser.</p> <p>zu c) 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>§ 15 Abs. 2 Nr. 2</p>	<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) Zur Umsetzung der gesetzlichen Anforderungen ist eine entsprechende Anzeige implementiert, die anzeigt</p> <ul style="list-style-type: none"> <li>▪ welchen Inhalt die signierten Daten aufweisen,</li> <li>▪ welchem Signaturschlüssel-Inhaber die Signatur zuzuordnen ist,</li> <li>▪ welches Ergebnis die Verifikation und Validierung liefert, insbesondere             <ul style="list-style-type: none"> <li>▪ ob die signierten Daten unverändert sind und</li> <li>▪ ob das zugehörige qualifizierte Zertifikat gültig ist.</li> </ul> </li> </ul> <p>zu b) 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 vorhanden und nicht gesperrt war, anzeigt.</p>
<p>§ 15 Abs. 4</p>	<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 5: 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 „EGVP, Version 2.5.0.0“ umsetzbar.

Die Software „EGVP, Version 2.5.0.0“ 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 gewährleisten<sup>7</sup>, 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 „EGVP, Version 2.5.0.0“ aktuell wie folgt erfüllt:

Anforderung	Erfüllung und Verhalten der Software „EGVP, Version 2.5.0.0“
<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 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>Bei der Prüfung einer Signatur prüft das Produkt „EGVP, Version 2.5.0.0“, ob die verwendeten kryptographischen Algorithmen – sowohl zum Zeitpunkt der Prüfung (Prüfzeitpunkt) als auch zum Signierzeitpunkt als – als geeignet anzusehen sind. Bzgl. der Eignung kryptographischer Algorithmen werden die Angaben des offiziellen Algorithmenkatalogs der Bundesnetzagentur genutzt.<sup>8</sup></p> <p>Das Prüfprotokoll, in dem die Ergebnisse der Prüfung zusammenfassend dem Benutzer dargestellt werden, hebt Signaturen, deren zugehörige kryptographische Algorithmen zum Prüf- oder zum Signierzeitpunkt als nicht mehr geeignet anzusehen sind, entsprechend farblich hervor und weist den Benutzer darauf hin, dass ein verwendeter Algorithmus zum Zeitpunkt der Prüfung oder zum Signierzeitpunkt gemäß Algorithmenkatalog nicht mehr für eine qualifizierte elektronische Signatur geeignet ist oder war.<sup>9</sup> Außerdem zeigt das Prüfprotokoll an, bis zu welchem Zeitpunkt die verwendeten Algo-</p>

<sup>7</sup> 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

<sup>8</sup> Detaillierte Erläuterungen finden sich im Informationspapier zur Umsetzung des bos-Prüfprotokolls gemäß FAQ 28 der BNetzA. (Vgl. Ausgliederte Zusatzdokumentation)

<sup>9</sup> 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 „EGVP, Version 2.5.0.0“
	rithmen gemäß Algorithmenkatalog als geeignet anzusehen sind, bzw. es waren.
<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>Sofern die Software "EGVP, Version 2.5.0.0" eine Prüfung einer Signatur nicht (vollständig) durchführen kann, da ein benötigter kryptographischer Algorithmus nicht implementiert ist, wird dies dem Benutzer entsprechend angezeigt: Das Prüfprotokoll, in dem die Ergebnisse der Prüfung zusammenfassend dem Benutzer dargestellt werden, hebt Signaturen, deren zugehörige kryptographische Algorithmen nicht implementiert sind, entsprechend hervor und weist den Benutzer darauf hin, dass die Signatur nicht geprüft werden konnte, da ein Algorithmus nicht implementiert ist.</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>Die Software "EGVP, Version 2.5.0.0" bringt keine Zeitstempel an.</p> <p>Mangels standardisiertem Verfahren für die Einbindung von qualifizierten Zeitstempeln, werden qualifizierte Zeitstempel aus Fremdprodukten nicht interpretiert. Gleichwohl ergibt sich ein qualifizierter Zeitstempel aus dem zugehörigen, angezeigten Zertifikat.</p>

## 5. Maßnahmen in der Einsatzumgebung

### 5.1 Einrichtung der IT-Komponenten

Für den Betrieb der Software „EGVP, Version 2.5.0.0“ 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, 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), Derzeit werden mit dem EGVP die JRE-Versionslinien 1.5\_x (mindestens 1.5.0\_06, von bos getestet mit Version 1.5.0\_18) und 1.6\_x (mindestens 1.6.0\_05, von bos getestet mit Version 1.6.0\_17) unterstützt.

Des Weiteren ist für einen reibungslosen und signaturgesetzkonformen Einsatz der Software „EGVP, Version 2.5.0.0“ notwendig, ausschließlich durch den Hersteller geprüfte Kombinationen aus Betriebssystemen, Chipkartenlesegeräten und Signaturkarten zu verwenden.<sup>10</sup>

Für den Betrieb der Software „EGVP, Version 2.5.0.0“ auf einem Terminalserver wird eine der folgenden Umgebungen vorausgesetzt

- Citrix Metaframe Presentation Server 4.5
- Windows Terminal Server 2003

Das Produkt „EGVP, Version 2.5.0.0“ darf ausschließlich innerhalb der oben beschriebenen Hard- und Softwareausstattung eingesetzt werden.

## 5.2 Anbindung an ein Netzwerk

Für den Betrieb des Produktes „EGVP, Version 2.5.0.0“ ist 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 „EGVP, Version 2.5.0.0“ 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.

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 „EGVP, Version 2.5.0.0“ 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 „EGVP, Version 2.5.0.0“ von der Gültigkeit der Signatur überzeugen. Die Verifikation der Signatur erfolgt über Standard-Java-Mechanismen.

---

<sup>10</sup> Eine Übersicht unterstützter Kombinationen ist unter <http://www.egvp.de/technik/index.php> verfügbar.

Die Software „EGVP, Version 2.5.0.0“ lässt sich über eine Installationsroutine einfach installieren: Mit dem Produkt „EGVP, Version 2.5.0.0“ wird immer ein Java Runtime Environment (JRE) 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 „EGVP, Version 2.5.0.0“ 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.

Für den Betrieb der Software „EGVP, Version 2.5.0.0“ 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 „EGVP, Version 2.5.0.0“ 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 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.

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 Trojanischen Pferde eingespielt werden können.

#### Auflagen zur Sicherheitsadministration des Betriebs

Hinsichtlich der Software „EGVP, Version 2.5.0.0“ 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 „EGVP, Version 2.5.0.0“ in einer Terminalserver-Umgebung ist durch ein geeignetes Berechtigungssystem sicherzustellen, dass die Dateien innerhalb des persönlichen Verzeichnisses des Benutzers der Software „EGVP, Version 2.5.0.0“ 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 „EGVP, Version 2.5.0.0“ zu beachten:

- Sofern eine Visualisierung einer zu signierenden oder signierten 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 OSCI-Manager – gegeben sind.

Bei dem Einsatz der Software „EGVP, Version 2.5.0.0“ in einer Terminalserver-Umgebung muss eine gesicherte und verschlüsselte Verbindung zwischen Terminalserver und Client-PC sichergestellt werden.

#### Auflagen für Wartung/Reparatur

Die Pflege und Wartung der Software „EGVP, Version 2.5.0.0“ 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 „EGVP, Version 2.5.0.0“ die Hashfunktionen SHA-256 und RIPEMD-160 bereitgestellt.<sup>11</sup>

---

<sup>11</sup> Hinweis: Das Produkt unterstützt ferner die Hashfunktion SHA-1, die allerdings zum 30.6.2008 ausgelaufen ist, so dass aufgrund der abgelaufenen oder gesperrten Zertifikate keine qualifizierten elektronischen Signaturen mehr erzeugt werden können.

Zur Prüfung qualifizierter elektronischer Signaturen werden vom Produkt „EGVP, Version 2.5.0.0“ die Hashfunktionen SHA-256, RIPEMD-160 und SHA-1<sup>12</sup> sowie die Signaturalgorithmen RSA und DSA<sup>13</sup> 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. 343) wie folgt als geeignet eingestuft:

- RIPEMD-160: gültig bis 31.12.2010
- SHA-2 Familie (SHA-224, SHA-256, SHA-384, SHA-512): gültig bis 31.12.2015
- RSA mit Schlüssellänge 2048 Bit: gültig bis 31.12.2015
- DSA mit Schlüssellänge 2048 Bit (Parameter  $p$ ) und 224 Bit (Parameter  $q$ ): 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:

- „Unterlagen zur Herstellereklärung gemäß § 17 Abs. 4 SigG für die Software „EGVP, Version 2.5.0.0“ – Sicherheitstechnische Produktbeschreibung und Spezifikation“, 17.11.2009, 89 Seiten.
- „Unterlagen zur Herstellereklärung gemäß § 17 Abs. 4 SigG für die Software „EGVP, Version 2.5.0.0“ – Testdokumentation“, 17.11.2009, 14 Seiten.
- Anwenderdokumentation „Elektronisches Gerichts- und Verwaltungspostfach – sichere Kommunikation mit Gerichten und Behörden –; Bürgerinnen und Bürger; EGVP Version 2.5.0.“, 85 Seiten.
- Anwenderdokumentation „Elektronisches Gerichts- und Verwaltungspostfach – sichere Kommunikation mit Gerichten und Behörden –; Behörden; EGVP Version 2.5.0.“, 102 Seiten.

---

<sup>12</sup> Dem Benutzer wird bei der Prüfung alter Signaturen, die mit SHA-1 erzeugt wurden, die abgelaufene Gültigkeit von SHA-1 mit einem Warnhinweis angezeigt.

<sup>13</sup> Die Schlüssellänge richtet sich nach den zu verifizierenden Signaturen; das Produkt „EGVP, Version 2.5.0.0“ unterstützt die gängigen Schlüssellängen von 2048 Bit

- Anwenderdokumentation „bos-Prüfprotokoll mit Zertifikatsanzeige“, (Verification Interpreter Version 2.1.1), 09.11.2009, 51 Seiten.
- Testkonzept „Elektronisches Gerichts- und Verwaltungspostfach (EGVP)“, Release 2.5.0, Dokumentversion 1.0, 03.08.2008, 181 Seiten.
- Testkonzept „Testhandbuch Verification Interpreter“, Release VI\_2\_1\_1\_CI\_1\_8\_2, 29.9.2009, 29 Seiten.

**Ende der Herstellereklärung**