# Bestätigung

## von Produkten für qualifizierte elektronische Signaturen gemäß §§ 15 Abs. 7 und 17 Abs. 4 Gesetz über Rahmenbedingungen für elektronische Signaturen und § 11 Abs. 3 Verordnung zur elektronischen Signatur

**TÜV Informationstechnik GmbH**
**Unternehmensgruppe TÜV NORD**
**Zertifizierungsstelle**
**Langemarckstraße 20**

**45141 Essen**

**bestätigt hiermit gemäß**
**§ 15 Abs. 7 Satz 1 Signaturgesetz[1] sowie § 11 Abs. 3 Signaturverordnung[2],**
**dass das**

**Signatursoftwareprodukt**
**Signier- und Verifikations-Anwendung SVA**
**Version 1.4**

**den nachstehend genannten Anforderungen des SigG und der SigV entspricht.**

**Die Dokumentation zu dieser Bestätigung ist unter**

**TUVIT.93131.TU.04.2006**

**registriert.**

**Essen, 11.04.2006** **gez. Dr. Gruschwitz**
Zertifizierungsstelle

TÜV Informationstechnik GmbH ist, gemäß der Veröffentlichung im Bundesanzeiger Nr. 52 vom 17. März 1999, Seite 4142 und gemäß § 25 Abs. 3 SigG, zur Erteilung von Bestätigungen für Produkte für qualifizierte elektronische Signaturen gemäß § 15 Abs. 7 und § 17 Abs. 4 SigG ermächtigt.

---

[1] Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz – SigG) vom 16.05.2001 (BGBl. I S. 876) geändert durch Erstes Gesetz zur Änderung des Signaturgesetzes (1. SigÄndG) vom 04.01.2005 (BGBl. I S. 2)

[2] Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) vom 16.11.2001 (BGBl. I S. 3074) geändert durch 1. SigÄndG

Die Bestätigung zur Registrierungsnummer TUVIT.93131.TU.04.2006 besteht aus 7 Seiten.

# Beschreibung des Produktes:

## 1 Handelsbezeichnung des Produktes und Lieferumfang:

Signatursoftwareprodukt *Signier- und Verifikations-Anwendung SVA*, Version 1.4[3] bestehend aus den beiden Softwarekomponenten

- *Signaturanwendung* (*SGA*), *Version 1.3.1* und
- *Visualisierung der Ziehungs- und Verifikationsdaten* (*VZV*), *Version 1.4*.

Auslieferung:
Als System an die NKL Nordwestdeutsche Klassenlotterie durch persönliche Übergabe auf einer einmal beschreibbaren CD-ROM, welche die folgenden Komponenten enthält:

- Ziehungsaufsichtsanwendung ZAA Version 1.4:
  - beinhaltet die EVG-Komponente *SGA, Version 1.3.1*
- Verifikationsanwendung VER Version 1.4:
  - beinhaltet die EVG-Komponente *VZV, Version 1.4*
- Microsoft-CryptoAPI: `capicom.dll`, Version 2.1.0.1.
- Laufzeitumgebung Microsoft .NET Framework 1.1.4322 Redistributable Package
- Definitionsdateien:
  - XML-Definitionsdateien zur Interpretation der Ziehungsteuerungs- bzw. Verifikationsdaten: `Verifizierung.xsd`, `xml.xsd`, `Ziehungssteuerung.xsd`, `Ziehungssteuerung.xsl`
  - Definitionsdateien (Textschablonen) zum Parsen des Übergabestrings mit den Ziehungsdaten: `haupt_bogen_2.txt`, `haupt_bogen_2_BEZ.txt`.
- Tools zur Durchführung der Integritätsprüfung:
  - WinZip (Archivierungsprogramm),
  - digestIT 2004 (Bildung bzw. Vergleich von Hash-Werten).
- Programmpaket zum Zugriff auf den Kartenleser und die Signaturerstellungseinheit: SmartTrustPersonal-Software, Version 3.3.2
- Installationsanwendung für den Treiber *SPRx32 PC-SC Treiber V1.42* des Kartenlesers
- Betriebsdokumentation: *Handbuch zur Ziehung mittels ZAS und ZLS, Version 1.22*, 03.04.2006

[3] Im Folgenden kurz mit SVA bezeichnet.

Hersteller:
pdv Technische Automation + Systeme GmbH
Dorotheenstraße 64
22083 Hamburg

für

NKL Nordwestdeutsche Klassenlotterie
Überseering 4
22297 Hamburg

# 2 Funktionsbeschreibung

SVA ist ein System, das innerhalb der Räumlichkeiten der NKL Nordwestdeutsche Klassenlotterie[4] zum Einsatz kommt. SVA ist selbst Teil der Software der Ziehungsaufsichtstation der NKL *ZAS, Version 1.4*.

SVA stellt Teile der Funktionen einer Signaturanwendungskomponente gemäß § 2 Nr. 11 SigG bereit. Zu signierende elektronische Ziehungsdaten werden in Form eines speziell formatierten Übergabestrings von SVA entgegengenommen, dem Nutzer angezeigt und nach seiner expliziten Einwilligung einer sicheren Signaturerstellungseinheit gemäß § 2 Nr. 10 SigG zum Signieren zugeführt. Signierte Daten und Signatur werden in einem speziellen XML-Format von SVA zurückgegeben. Ferner können mit SVA erzeugte Signaturen und die zugehörigen qualifizierten Zertifikate auf mathematische Korrektheit überprüft werden. Dabei zeigt SVA die signierten Daten und das Verifikationsergebnis dem Nutzer an.

SVA beinhaltet keine Nachprüfung der Gültigkeit von Zertifikaten im Sinne der §§ 17 Abs. 2 Nr. 5 SigG bzw. 15 Abs. 2 Nr. 2b SigV.

# 3 Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

## 3.1 Erfüllte Anforderungen

SVA erfüllt die Anforderungen nach § 17 Abs. 2 Satz 1 (eindeutige Anzeige und Feststellbarkeit der Daten bei Signaturerzeugung), Satz 2 Nr. 1 (Feststellbarkeit der Daten), Nr. 2 (Feststellbarkeit des Unverändertseins der Daten) und Nr. 3 (Feststellbarkeit der Zuordnung zum Signaturschlüsselinhaber) sowie Satz 3 (bei Bedarf Anzeige des Inhalts der zu signierenden oder signierten Daten) SigG und nach § 15 Abs. 2 Nr. 1 (keine Preisgabe der Identifikationsdaten, Signatur nur durch berechtigt signierende Person, eindeutige Anzeige der Signatur vor Erzeugung) und Nr. 2a) (korrekte Prüfung der Signatur) sowie Abs. 4 (Erkennbarkeit von sicherheitstechnischen Veränderungen) SigV.

[4] Im Folgenden kurz mit NKL bezeichnet.

## 3.2 Einsatzbedingungen

Dies gilt unter der Voraussetzung, dass folgende Einsatzbedingungen gewährleistet sind:

Grundlage dieser Bestätigung ist der Einsatz von SVA in einem ***geschützten Einsatzbereich***. Für den sicheren Einsatz von SVA und zur Verhinderung von erfolgreichen Angriffen mit den Zielen, dass:

- Daten signiert werden, die nicht signiert werden sollen,
- das Prüfergebnis der Signatur- bzw. Zertifikatprüfung falsch angezeigt wird,
- die Geheimhaltung des Identifikationsmerkmals (PIN) nicht gewährleistet ist,

sind die folgenden Auflagen zu beachten:

### 3.2.1 Auflagen zur Anbindung an das Internet

SVA wird ausschließlich in einem lokalen Netz der NKL betrieben. Die Internetanbindung muss so abgesichert sein, z. B. durch eine geeignet konfigurierte Firewall, dass online Angriffe aus dem Internet auf den eingesetzten Personalcomputer erkannt bzw. unterbunden werden.

### 3.2.2 Auflagen zur Anbindung an ein Intranet

Die Netzverbindung muss geeignet abgesichert sein, so dass online Angriffe aus dem Intranet auf den Computer erkannt bzw. unterbunden werden.

### 3.2.3 Auflagen zur Sicherheit der IT-Plattform und Applikationen

Die NKL als Benutzer von SVA muss sich davon überzeugen, dass keine Angriffe von dem Personalcomputer und den dort vorhandenen Applikationen durchgeführt werden. Insbesondere muss gewährleistet sein, dass:

1. die auf dem Personalcomputer installierte Software weder böswillig manipuliert noch in irgendeiner anderen Form verändert werden kann,
2. auf dem Personalcomputer keine Viren oder Trojanischen Pferde eingespielt werden können,
3. die Hardware des Personalcomputers nicht unzulässig verändert werden kann und
4. der verwendete Chipkartenleser weder böswillig manipuliert noch in irgendeiner anderen Form verändert wurde, um dadurch Daten (z. B. PIN, zu signierende Daten, Hashwerte, etc.) auszuforschen, zu verändern oder die Funktion anderer Programme unzulässig zu verändern. Dieses kann die in Abschnitt 3.2 angegebenen Folgen haben.

### 3.2.4 Auflagen zur Auslieferung und Installation des Produktes

SVA wird vom Hersteller als System auf einer CD persönlich übergeben und bei NKL installiert. SVA darf ausschließlich in der vorgesehenen Umgebung bei NKL betrieben werden. Nach der Installation von SVA ist mittels des mitgelieferten Programms „*digestIT 2004*“ der Hashwert der Erstinstallation aufzunehmen und sicher zu verwahren. Zur Prüfung von sicherheitsrelevanten Veränderungen ist das Programm erneut aufzurufen und der angezeigte Hashwert mit dem sicher aufbewahrten Hashwert der Erstinstallation zu vergleichen. Beide Hashwerte müssen übereinstimmen.

Das Signatursoftwareprodukt SVA ist für die folgende technische Einsatzumgebung vorgesehen:

- IBM-kompatibler PC (mind.: Pentium III, 500 MHz, 256 MByte Hauptspeicher, 10 MByte verfügbarer Festplattenspeicherplatz) lauffähig mit dem unten genannten Windows Betriebssystem, mit Bildschirm (1024x768 Punkten, 16 Bit Farbtiefe, große Schriftarten) und CD-ROM-Laufwerk sowie Anschlussmöglichkeit für den Chipkartenleser (USB 1.1)

- Betriebssystem Windows 2000 SP4 mit Gebietsschema Deutsch (für den Zeichensatz, Währung und Datum)

- Laufzeitumgebung Microsoft .NET Framework 1.1.4322 Redistributable Package

- Microsoft Crypto-API: `capicom.dll`, Version 2.1.0.1 (gespeichert im Verzeichnis c:\WINNT\system32\

- Klasse 2 Chipkartenleser mit PIN-Pad SPR532, Firmware Version 4.15 (Bestätigung: TUVIT.09370.TE.03.2003 vom 11.03.2003)

- Sichere Signaturerstellungseinheit D-TRUST-CARD, Version 1.0 (oder Variante D-TRUST Card, Version 1.1) (Bestätigung TUVIT.09361.TE.10.2001 vom 23.10.2001 mit Nachtrag vom 24.03.2004)

Eine Übertragung der Evaluationsergebnisse auf andere Plattformen ist nicht möglich, sondern erfordert ggf. eine Reevaluation. Das Signatursoftwareprodukt SVA darf deshalb ausschließlich in der oben beschriebenen Hard- und Softwareumgebung eingesetzt werden.

### 3.2.5 Auflagen zum Schutz vor manuellem Zugriff Unbefugter

Der Personalcomputer, auf dem SVA eingesetzt wird, sowie der verwendete Chipkartenleser müssen gegen eine unberechtigte Benutzung gesichert sein, damit:

1. die auf dem Personalcomputer installierte Software weder böswillig manipuliert noch in irgendeiner anderen Form verändert werden kann,

2. auf dem Personalcomputer keine Viren oder Trojanischen Pferde eingespielt werden können,

3. die Hardware des Personalcomputers nicht unzulässig verändert werden kann oder

4. der verwendete Chipkartenleser weder böswillig manipuliert noch in irgendeiner anderen Form verändert wird, um dadurch Daten (z. B. PIN, zu signierende Daten, Hashwerte, etc.) auszuforschen, zu verändern oder die Funktion anderer Programme unzulässig zu verändern (siehe auch Abschnitt 3.2.3).

### 3.2.6 Auflagen zum Schutz vor Angriffen über Datenaustausch per Datenträger

Bei Einspielung von Daten über Datenträger muss gewährleistet werden, dass

1. die installierte Software weder böswillig manipuliert noch in irgendeiner anderen Form verändert werden kann und

2. keine Viren oder Trojanischen Pferde eingespielt werden können,

um dadurch Daten (z. B. PIN, zu signierende Daten, Hashwerte, etc.) auszuforschen, zu verändern oder die Funktion anderer Programme unzulässig zu verändern (siehe auch Abschnitt 3.2.3).

### 3.2.7 Auflagen zur Sicherheitsadministration des Betriebes

Eine Sicherheitsadministration des Betriebes von SVA ist nicht vorgesehen. Eine vertrauenswürdige Administration des Personalcomputers sowie der Internet- bzw. Intranetanbindung muss jedoch sichergestellt werden.

### 3.2.8 Auflagen zum Schutz vor Fehlern bei Betrieb/Nutzung

Folgende Auflagen sind für den sachgemäßen Einsatz von SVA zu beachten:

- Die authentischen CA-Zertifikate und qualifizierten (Signaturschlüssel-) Zertifikate müssen durch den Anwender bereitgestellt sein.

- Es wird eine vertrauenswürdige Eingabe der PIN vorausgesetzt. Der Benutzer hat dafür Sorge zu tragen, dass die Eingabe der PIN weder beobachtet wird noch dass die PIN anderen Personen bekannt gemacht wird.

- Die Einstellung der Systemzeit des Personalcomputers muss korrekt sein.

- Die Integritätsprüfung mit dem Programm „*digestIT 2004*“ ist regelmäßig vorzunehmen. Der angezeigte Hashwert muss mit dem sicher aufbewahrten Hashwert der Erstinstallation übereinstimmen.

- Die Unterrichtung durch den Zertifizierungsdiensteanbieter zur Handhabung der Signaturerstellungseinheit ist zu beachten.

### 3.2.9 Anforderungen an das Wartungs-/Reparaturpersonal

Eine Wartung bzw. Reparatur von SVA ist nicht vorgesehen. Eine Wartung bzw. Reparatur des Personalcomputers ist nur von vertrauenswürdigen Personen durchzuführen. Nach den durchgeführten Arbeiten ist die Integrität des Personalcomputers und aller Applikationen einschließlich der Integrität von SVA zu überprüfen.

### 3.2.10 Authentisierung des Wartungs-/Reparaturpersonals

Eine Wartung bzw. Reparatur von SVA ist nicht vorgesehen. Eine Authentisierung des Personals für die Wartung bzw. Reparatur des Personalcomputers muss geeignet erfolgen.

### 3.2.11 Aufbewahrung/Transport der Produkte

SVA wird vom Hersteller auf einer einmal beschreibbaren CD-ROM persönlich übergeben. Es ist darauf zu achten, dass die CD-ROM und der Hashwert der Erstinstallation (siehe 3.2.4) geschützt aufbewahrt werden.

## 3.3 Algorithmen und zugehörige Parameter

Zur Erzeugung elektronischer Signaturen und zur Überprüfung der mathematischen Korrektheit werden die Algorithmen SHA-1 und RSA mit 1024 Bit verwendet.

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung reicht für SHA-1 mindestens bis Ende des Jahres 2009 (siehe BAnz. Nr. 58 vom 23.06.2006, Seite 1.913).

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung reicht für RSA mit 1024 Bit bis mindestens Ende des Jahres 2007 (siehe BAnz. Nr. 58 vom 23.06.2006, Seite 1.913).

Die festgestellte Eignung der Algorithmen reicht somit mindestens bis Ende des Jahres 2007.

## 3.4 Prüfstufe und Mechanismenstärke

Das Signatursoftwareprodukt SVA, Version 1.4 wurde erfolgreich nach der Prüfstufe E2 der ITSEC evaluiert. Die eingesetzten Sicherheitsmechanismen erreichen die Stärke **hoch**.

## Ende der Bestätigung

# Bestätigung

## von Produkten für qualifizierte elektronische Signaturen gemäß §§ 15 Abs. 7 und 17 Abs. 4 Gesetz über Rahmenbedingungen für elektronische Signaturen und § 11 Abs. 3 Verordnung zur elektronischen Signatur

## Nachtrag 1 zur Bestätigung TUVIT.93131.TU.04.2006 vom 11.04.2006

**TÜV Informationstechnik GmbH**
**Unternehmensgruppe TÜV NORD**
**Zertifizierungsstelle**
**Langemarckstraße 20**

**45141 Essen**

**bestätigt hiermit gemäß**
**§ 15 Abs. 7 Satz 1 Signaturgesetz[1] sowie § 11 Abs. 3 Signaturverordnung[2], dass für das**

## Signatursoftwareprodukt Signier- und Verifikations-Anwendung SVA Version 1.4

**das Kapitel 1 sowie die Abschnitte 3.2.4 und 3.3 der o. g. Bestätigung aufgrund der Unterstützung einer zusätzlichen SSEE mit 2048 Bit Schlüssellänge, der Aktualisierung des Kartenlesertreibers und der Betriebsdokumentation sowie der aktuellen Bekanntmachung zur elektronischen Signatur im Bundesanzeiger durch diesen Nachtrag ersetzt wurden.**

**Die Dokumentation zu dieser Nachtrags-Bestätigung ist im zugehörigen Bestätigungsbericht vom 29.11.2007 festgehalten.**

**Essen, 29.11.2007**

**gez. Dr. Sutter**
Zertifizierungsstelle

TÜV Informationstechnik GmbH ist, gemäß der Veröffentlichung im Bundesanzeiger Nr. 52 vom 17. März 1999, Seite 4142 und gemäß § 25 Abs. 3 SigG, zur Erteilung von Bestätigungen für Produkte für qualifizierte elektronische Signaturen gemäß § 15 Abs. 7 und § 17 Abs. 4 SigG ermächtigt.

---

[1] Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz – SigG) vom 16.05.2001 (BGBl. I S. 876) zuletzt geändert durch Artikel 4 des Gesetzes vom 26.02.2007 (BGBl. I S. 179)

[2] Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) vom 16.11.2001 (BGBl. I S. 3074) geändert durch Artikel 2 des Gesetzes vom 04.01.2005 (BGBl. I S. 2)

Der Nachtrag 1 der Bestätigung zur Registrierungsnummer TUVIT.93131.TU.04.2006 besteht aus 5 Seiten.

# 1 Handelsbezeichnung des Produktes und Lieferumfang

*Dieses Kapitel „1 Handelsbezeichnung des Produktes und Lieferumfang“ ersetzt das Kapitel 1 der Bestätigung TUVIT.93131.TU.04.2006 vom 11.04.2006 aufgrund des aktualisierten Kartenlesertreibers und der zusätzlichen Betriebsdokumentation mit Hinweisen für die Unterstützung der SSEE „D-TRUST c-card, Version 2.0“ mit einer Schlüssellänge von 2048 Bit.*

Signatursoftwareprodukt *Signier- und Verifikations-Anwendung SVA*, Version 1.4[3] bestehend aus den beiden Softwarekomponenten

- *Signaturanwendung* (*SGA*), *Version 1.3.1* und
- *Visualisierung der Ziehungs- und Verifikationsdaten* (*VZV*), *Version 1.4*.

Auslieferung:
Als System an die NKL Nordwestdeutsche Klassenlotterie durch persönliche Übergabe auf einer einmal beschreibbaren CD-ROM, welche die folgenden Komponenten enthält:

- Ziehungsaufsichtsanwendung ZAA Version 1.4:
  - beinhaltet die EVG-Komponente *SGA, Version 1.3.1*
- Verifikationsanwendung VER Version 1.4:
  - beinhaltet die EVG-Komponente *VZV, Version 1.4*
- Microsoft-CryptoAPI: `capicom.dll`, Version 2.1.0.1.
- Laufzeitumgebung Microsoft .NET Framework 1.1.4322 Redistributable Package
- Definitionsdateien:
  - XML-Definitionsdateien zur Interpretation der Ziehungsteuerungs- bzw. Verifikationsdaten: `Verifizierung.xsd, xml.xsd, Ziehungssteuerung.xsd, Ziehungssteuerung.xsl`
  - Definitionsdateien (Textschablonen) zum Parsen des Übergabestrings mit den Ziehungsdaten: `haupt_bogen_2.txt, haupt_bogen_2_BEZ.txt.`
- Tools zur Durchführung der Integritätsprüfung:
  - WinZip (Archivierungsprogramm),
  - digestIT 2004 (Bildung bzw. Vergleich von Hash-Werten).
- Programmpaket zum Zugriff auf den Kartenleser und die Signaturerstellungseinheit:
  - SmartTrustPersonal-Software, Version 3.3.2 (für den Einsatz mit der SSEE D-TRUST-CARD, Version 1.0 & 1.1 mit 1024 Bit) oder
  - Nexus Personal-Software, Version 4.5.2 (für den Einsatz mit der SSEE D-TRUST c-card, Version 2.0 mit 2048 Bit)

[3] Im Folgenden kurz mit SVA bezeichnet.

- Installationsanwendung für den Treiber *SPRx32 PC-SC Treiber*
  - *V1.42* (für den Einsatz mit der SSEE D-TRUST-CARD, Version 1.0 & 1.1 mit 1024 Bit) oder
  - *V1.81.0001* (für den Einsatz mit der SSEE D-TRUST c-card, Version 2.0 mit 2048 Bit)

  des Kartenlesers
- Betriebsdokumentation *Handbuch zur Ziehung mittels ZAS und ZLS*:
  - Version 1.22, 03.04.2006 (für den Einsatz mit der SSEE D-TRUST-CARD, Version 1.0 & 1.1 mit 1024 Bit) oder
  - Version 1.33, 24.10.2007 (für den Einsatz mit der SSEE D-TRUST c-card, Version 2.0 mit 2048 Bit)

Hersteller:
pdv Technische Automation + Systeme GmbH
Dorotheenstraße 64
22083 Hamburg

für

NKL Nordwestdeutsche Klassenlotterie
Überseering 4
22297 Hamburg

### 3.2.4 Auflagen zur Auslieferung und Installation des Produktes

*Dieser Abschnitt „3.2.4 Auflagen zur Auslieferung und Installation des Produktes“ ersetzt den Abschnitt 3.2.4 der Bestätigung TUVIT.93131.TU.04.2006 vom 11.04.2006 aufgrund der zusätzlichen Unterstützung der SSEE „D-TRUST c-card, Version 2.0“ mit einer Schlüssellänge von 2048 Bit (bestätigt am 27.05.2005 mit der Nummer T-Systems.02122.TE.05.2005 als „Chipkarte mit Prozessor SLE66CX322P, Betriebssystem CardOS V4.3B mit Applikation für digitale Signatur“.*

SVA wird vom Hersteller als System auf einer CD persönlich übergeben und bei NKL installiert. SVA darf ausschließlich in der vorgesehenen Umgebung bei NKL betrieben werden. Nach der Installation von SVA ist mittels des mitgelieferten Programms „*digestIT 2004*“ der Hashwert der Erstinstallation aufzunehmen und sicher zu verwahren. Zur Prüfung von sicherheitsrelevanten Veränderungen ist das Programm erneut aufzurufen und der angezeigte Hashwert mit dem sicher aufbewahrten Hashwert der Erstinstallation zu vergleichen. Beide Hashwerte müssen übereinstimmen.

Das Signatursoftwareprodukt SVA ist für die folgende technische Einsatzumgebung vorgesehen:

- IBM-kompatibler PC (mind.: Pentium III, 500 MHz, 256 MByte Hauptspeicher, 10 MByte verfügbarer Festplattenspeicherplatz) lauffähig mit dem unten genannten Windows Betriebssystem, mit Bildschirm (1024x768 Punkten, 16 Bit Farbtiefe, große Schriftarten) und CD-ROM-Laufwerk sowie Anschlussmöglichkeit für den Chipkartenleser (USB 1.1)

- Betriebssystem Windows 2000 SP4 mit Gebietsschema Deutsch (für den Zeichensatz, Währung und Datum)

- Laufzeitumgebung Microsoft .NET Framework 1.1.4322 Redistributable Package

- Microsoft Crypto-API: `capicom.dll`, Version 2.1.0.1 (gespeichert im Verzeichnis c:\WINNT\system32\

- Klasse 2 Chipkartenleser mit PIN-Pad SPR532, Firmware Version 4.15 (Bestätigung: TUVIT.09370.TE.03.2003 vom 11.03.2003)

- personalisierte sichere Signaturerstellungseinheit gemäß § 2 Nr. 10 SigG:

  – D-TRUST-CARD, Version 1.0 (oder Variante D-TRUST Card, Version 1.1) (Bestätigung TUVIT.09361.TE.10.2001 vom 23.10.2001 mit Nachtrag vom 24.03.2004) oder

  – D-TRUST c-card, Version 2.0, bestätigt als Chipkarte mit Prozessor SLE66CX322P, Betriebssystem CardOS V4.3B mit Applikation für digitale Signatur[4] (Bestätigung: T-Systems.02122.TE.05.2005 vom 27.05.2005).

Eine Übertragung der Evaluationsergebnisse auf andere Plattformen ist nicht möglich, sondern erfordert ggf. eine Reevaluation. Das Signatursoftwareprodukt SVA darf deshalb ausschließlich in der oben beschriebenen Hard- und Softwareumgebung eingesetzt werden.

## 3.3 Algorithmen und zugehörige Parameter

*Dieser Abschnitt „3.3 Algorithmen und zugehörige Parameter“ ersetzt den Abschnitt 3.3 der Bestätigung TUVIT.93131.TU.04.2006 vom 11.04.2006 aufgrund der neuen Bekanntmachung zur elektronischen Signatur im Bundesanzeiger Nr. 69 vom 12.04.2007, Seite 3.759.*

Bei der Erzeugung elektronischer Signaturen und zur Überprüfung der mathematischen Korrektheit werden die Algorithmen SHA-1 und RSA mit 1024 Bit (D-TRUST-CARD, Version 1.0 sowie Version 1.1) und 2048 Bit (D-TRUST c-card, Version 2.0) verwendet.

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung reicht für Hash-Algorithmus SHA-1 bis Ende des Jahres 2009 (siehe BAnz. Nr. 69 vom 12.04.2007, Seite 3.759).

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung für den Signatur-Algorithmus RSA reicht für die Schlüssellänge von 2048 Bit bis Ende des Jahres 2012 und für die Schlüssellänge von 1024 Bit bis Ende des Jahres 2007 (siehe BAnz. Nr. 69 vom 12.04.2007, Seite 3.759).

[4] Auch kurz als *CardOS V4.3B* bezeichnet.

Die Gültigkeit der Bestätigung des Signatursoftwareproduktes SVA, Version 1.4 in Abhängigkeit von Hash-Algorithmus und RSA-Schlüssellänge kann der folgenden Tabelle entnommen werden:

| **Hash-Algorithmus**<br>**Schlüssellänge** | **SHA-1** |
|---|---|
| **1024** | 2007 |
| **2048** | 2009 |

Diese Bestätigung des Signatursoftwareproduktes SVA, Version 1.4 ist somit, abhängig vom Hash-Verfahren und der Mindestschlüssellänge, maximal gültig bis 31.12.2009; die Gültigkeit kann jedoch verlängert werden, wenn zu diesem Zeitpunkt keine Hinderungsgründe hinsichtlich der Sicherheit der Produkte oder der Algorithmen vorliegen, oder verkürzt werden, wenn neue Feststellungen hinsichtlich der Eignung der Algorithmen im Bundesanzeiger veröffentlicht werden.

## Ende der Bestätigung