

# Bestätigung

## von Produkten für qualifizierte elektronische Signaturen

gemäß §§ 15 Abs. 7 S. 1, 17 Abs. 4 Gesetz über Rahmenbedingungen für elektronische Signaturen<sup>1</sup> und §§ 11 Abs. 3 und 15 Signaturverordnung<sup>2</sup>

**Bundesamt für Sicherheit in der Informationstechnik<sup>3</sup>**  
**Godesberger Allee 185-189**  
**53175 Bonn**

bestätigt hiermit gemäß  
§§ 15 Abs. 7 S. 1, 17 Abs. 2 SigG sowie §§ 11 Abs.3, 15 Abs. 2 und 4 SigV,  
dass die

**Chipkartenterminals**  
**EMV-TriCAP Reader (Art.-Nr. HCPNCKS/A03, Firmware 69.18),**  
**SecOVID Reader III (Art.-Nr. HCPNCKS/B05, Firmware 69.18) und**  
**KAAN TriB@nk (Art.-Nr. HCPNCKS/C05, Firmware 68.17)**

den nachstehend genannten Anforderungen des SigG und der SigV entspricht.

---

Die Dokumentation zu dieser Bestätigung ist registriert unter:

**BSI.02096.TE.12.2008**



**Bonn, den 19. Dezember 2008**

gez. Bernd Kowalski

Im Auftrag  
Bernd Kowalski  
Abteilungspräsident

Das Bundesamt für Sicherheit in der Informationstechnik ist auf Grundlage des BSI-Errichtungsgesetzes vom 17.12.1990, Bundesgesetzblatt I S. 2834 und gemäß der Veröffentlichung im Bundesanzeiger Nr. 31 vom 14. Februar 1998, Seite 1787, zur Erteilung von Bestätigungen für Produkte gemäß § 15 Abs. 7 S. 1 (oder § 17 Abs. 4) SigG ermächtigt.

<sup>1</sup> Gesetz über die Rahmenbedingungen für elektronische Signaturen (Signaturgesetz - SigG) in der Fassung vom 16. Mai 2001 (BGBl. Jahrgang 2001 Teil I Nr. 22) geändert durch Erstes Gesetz zur Änderung des Signaturgesetzes (1. SigÄndG) vom 04.01.2005 (BGBl. I S. 2)

<sup>2</sup> Verordnung zur elektronischen Signatur (Signaturverordnung - SigV) in der Fassung vom 16. November 2001 (BGBl. Jahrgang 2001 Teil I Nr. 59) geändert durch 1. SigÄndG

<sup>3</sup> Bundesamt für Sicherheit in der Informationstechnik, Godesberger Allee 185-189, 53175 Bonn, Postfach 200363, 53133 Bonn, Tel: +49(0)3018 9582-0, Fax: +49(0)3018 9582-5477, E-Mail: [bsi@bsi.bund.de](mailto:bsi@bsi.bund.de), Web: [www.bsi.bund.de](http://www.bsi.bund.de)

# Beschreibung des Produktes für qualifizierte elektronische Signaturen:

## 1 Handelsbezeichnung des Produktes und Lieferumfang:

Die Chipkartenterminals EMV-TriCAP Reader, SecOVID Reader III und KAAN TriB@nk (aufgeführt in Tabelle 1) der Firma Kobil Systems GmbH<sup>4</sup> sind, vom Typenschild abgesehen, identisch im Aufbau. Die Firmware des Produktes ist in zwei Betriebsmodi unterteilt: Ein Offline-Modus, welcher je Variante individuelle Funktionalitäten aufweist und ein Online-Modus, welcher identische Funktionalitäten aufweist. Bestandteil dieser Bestätigung ist der Online-Betriebs-Modus.

Name	Artikelnummer	Hauptplatine	Firmware Version
EMV TriCAP	HCPNCKS/A03	KCT106r1	69.18 - EMV TriCAP
SecOVID Reader III	HCPNCKS/B05	KCT106r1	69.18 - SecOVID Reader III
KAAN TriB@nk	HCPNCKS/C05	KCT106r1	68.17 - KAAN TriB@nk

Tabelle 1: Produktvarianten

### 1.1 Auslieferung und Lieferumfang:

Die materielle Auslieferung erfolgt in einer der drei Produktvarianten im Versand durch den Hersteller. Zusätzlich enthält das ausgelieferte Produkt eine Docking-Station zur Aufnahme des Chipkartenterminals. Diese wird mit USB-Kabel an einen PC angeschlossen. Auch ist eine CD-ROM mit Treibern und Werkzeugen im Auslieferungsumfang enthalten. Die Geräte sind im Rahmen der Endmontage mit drei Sicherheitssiegeln versehen, welche bei Öffnung des Gerätes beschädigt werden.

Die Versionsangaben zur Hauptplatine, die Artikelnummer und der Name des Gerätes sind auf dem Typenschild auf der Geräterückseite ersichtlich. Die Firmwareversion wird im Display des Gerätes angezeigt.

Folgend die drei Produktvarianten und die jeweilige Dokumentation:

#### 1. KOBIL Chipkartenterminal EMV-TriCAP Reader

Artikel-Nr.: HCPNCKS/A03  
Hauptplatine: KCT106r1  
Firmware: 69.18 – EMVTriCAP  
Dokumentation:

- KOBIL EMV-TriCAP Reader – Manual, DB22.DEEN.1, Version 2.10 vom 21.05.2008

#### 2. KOBIL Chipkartenterminal SecOVID Reader III

Artikel-Nr.: HCPNCKS/B05  
Hauptplatine: KCT106r1  
Firmware: 69.18 – SecOVID III  
Dokumentation:

- KOBIL SecOVID Reader III – Manual, DB21.DEEN.1, Version 2.16 vom 21.05.2008

<sup>4</sup> Im Folgenden Kobil oder Hersteller genannt.

### 3. KOBIL Chipkartenterminal KAAN TriB@nk

Artikel-Nr.:	HCPNCKS/C05
Hauptplatine:	KCT106r1
Firmware:	68.17 – KAANTriB@nk
Dokumentation:	

- KAAN TriB@nk – Manual, DB25.DE.1, Version 1.17 vom 21.05.2008
- KAAN TriB@nk Beipackzettel, Version 1.19 vom 10.11.2008

Die elektronische Auslieferung erfolgt über die Webseite des Herstellers. Es wird je Produktvariante (s. Tabelle 1) ein Installationswerkzeug (Software) bereitgestellt, in welches die jeweilige Firmware integriert ist. Die elektronische Auslieferung dient der Aktualisierung ausgelieferter Geräte. Der Update-Prozess ist in der Produktdokumentation beschrieben. Die bei materieller Auslieferung auf der CD-ROM enthaltenen Treiber können auch über die elektronische Auslieferung bezogen werden.

Ergänzend zu den über die materielle oder elektronische Auslieferung bezogenen Bestandteilen liefert der Hersteller auf Anfrage folgende Dokumentation zur Unterstützung bei der Entwicklung von Signaturanwendungskomponenten, die sich der Produktvarianten bedienen:

- KOBIL EMV-TriCAP Reader, SecOVID Reader III, KAAN TriB@nk – Developer Notes, Version 1.0, 23.10.2008

## 1.2 Antragsteller dieser Bestätigung und Hersteller des Produkts:

Kobil Systems GmbH  
Pfortenring 11  
67547 Worms  
DEUTSCHLAND

## 2 Funktionsbeschreibung

### 2.1 Kurzbeschreibung

Das Produkt ist in drei Produktvarianten (EMV-TriCAP Reader, SecOVID Reader III und KAAN TriB@nk) lieferbar. Alle Varianten stellen Funktionen eines Chipkartenterminals über verschiedene Applikations-Schnittstellen bereit. Es werden Prozessorchipkarten gemäß ISO-7816<sup>5</sup>- und EMV<sup>6</sup>-Standards unterstützt. Das Produkt verfügt über ein LCD, eine Tastatur zur sicheren PIN-Eingabe sowie über updatefähige Firmware.

Die drei Varianten unterscheiden sich in der aufgespielten Firmware, speziell dem Anteil, in dem der Offline-Betrieb (s.u.) implementiert ist. Die Hardware ist identisch, abgesehen von dem Typenschild. Die Hardware lässt sich anhand des Typenschildes identifizieren, die Firmware-Version und -Variante wird im Display des Produktes angezeigt. (s. Tabelle 1).

Der Anschluss erfolgt über eine Docking Station an der USB-Schnittstelle des Host-PCs (Online-Betrieb). Das Produkt kann auch ohne Anschluss an den Host-PC

<sup>5</sup> DIN ISO 7816, Teile 1 - 8.

<sup>6</sup> EMV 2000 Book 1 - Application independent ICC to Terminal Interface requirements, Version 4.0, December 2000

betrieben werden (Offline-Betrieb). Hierbei wird die Spannungsversorgung von Batterien übernommen. Der Offline-Betrieb ist Varianten-individuell. Die Verwendung zur Unterstützung bei der Erstellung von qualifizierten elektronischen Signaturen und zum Firmwareupdate erfolgt ausschließlich im Online-Betrieb. Nur auf letzteren Modus bezieht sich diese Bestätigung. Die Abgrenzung der Betriebsmodi ist Bestandteil der durchgeführten Prüfungen.

Im Online-Betrieb erkennt der EVG die von der Host-Software übermittelten (und von der USB Docking Station umgesetzten) Kommandos zur PIN-Eingabe gemäß CCID<sup>7</sup> bzw. CT-BCS<sup>8</sup> und fügt die vom Benutzer über das Keypad eingegebenen Ziffern als PIN an die entsprechenden Stellen des Kommandos an die Chipkarte ein. In keinem Fall wird die Eingabe des Benutzers (und somit auch die PIN) an den Host-PC übertragen. Der Modus der sicheren PIN-Eingabe wird eindeutig am LC-Display des EVG angezeigt, die eingegebenen Ziffern werden als Sternchen (\*) am LC-Display des EVG angezeigt.

Das Produkt ist für den Einsatz im nichtöffentlichen Bereich mit geregelten Zugriffsmöglichkeiten vorgesehen (siehe auch Kapitel 3.2).

## 2.2 Funktionsbeschreibung des Produkts

Das Produkt bietet im Online-Betrieb vier Sicherheitsfunktionen, die nachfolgend erläutert werden:

### 1. Sichere PIN-Eingabe

Wird das Gerät über entsprechende Befehle (gem. CCID oder CT-BCS) von einer Software in den Modus zur sicheren PIN-Eingabe versetzt, wird dies im Display durch ein Schloss-Symbol dargestellt. Die an der Tastatur des Gerätes eingegebene PIN wird gemäß den Vorgaben des Gerätebefehls in den Befehl für die Smartcard eingesetzt und an diese übermittelt. Eine Übermittlung der PIN über andere Schnittstellen, speziell an den PC, findet bei der sicheren PIN-Eingabe nicht statt.

Voraussetzung für den Modus zur sicheren Eingabe der PIN ist die Nutzung einer der folgenden Befehle für die Smartcard (INS steht für Instruction Byte, welches den jeweiligen Befehl repräsentiert):

VERIFY (ISO/IEC 7816-4)	INS=0x20
CHANGE REFERENCE DATA (ISO/IEC 7816-8)	INS=0x24
ENABLE VERIFICATION REQUIREMENT(ISO/IEC 7816-8)	INS=0x28
DISABLE VERIFICATION REQUIREMENT(ISO/IEC 7816-8)	INS=0x26
RESET RETRY COUNTER (ISO/IEC 7816-8)	INS=0x2C
UNBLOCK APPLICATION (EMV2000)	INS=0x18

### 2. Speicheraufbereitung

Nach jeder PIN-Eingabe werden die Speicherbereiche des Lesegerätes aufbereitet, so dass ein nachträgliches Auslesen der Identifikationsmerkmale oder Fragmente dieser ausgeschlossen werden kann. Diese Aufbereitung wird nach Abbruch der PIN-Eingabe (Betätigung der Abbruch-Taste oder Timeout) oder Bestätigung der PIN-Eingabe (PIN-Länge erreicht oder Betätigung der Bestätigungs-Taste) ausgelöst.

<sup>7</sup> USB Implementors Forum, Inc. - Device Working Group (DWG) - Universal Serial Bus Device Class Specification for USB Chip/Smart Card Interface Devices, Revision 1.00, March 20, 2001

<sup>8</sup> TeleTrusT Deutschland e.V. - Multifunktionale KartenTerminals (MKT) - Spezifikation, Teil 4: Anwendungsunabhängiger CardTerminal Basic Command Set (CT-BCS) - Version 1.0, 15. 04. 1999.

### 3. Sicherer Firmwareupdate

Das Gerät kann unter Verwendung einer hierfür vom Hersteller zur Verfügung gestellten Software die Firmware des Gerätes aktualisieren. Hierbei wird die Authentizität und Integrität der Firmware durch eine elektronische Signatur gesichert und vom Gerät geprüft.

Die Verifikation einer Signatur der Firmware mit dem asymmetrischen ECDSA-Algorithmus und einer Bitlänge von 192 garantiert die Integrität und Authentizität der Firmware beim Laden einer neuen Firmware in den Chipkartenleser. Der Hash-Wert über die neu zu ladende Firmware wird basierend auf dem Algorithmus SHA-1 mit einer Länge von 160 Bit ermittelt.

Die PC-Software zur Installation der Firmware ist nicht Gegenstand dieser Bestätigung.

### 4. Gehäuseversiegelung

Zum Schutz vor unbemerkten Manipulationen ist das Gerät durch zwei seitliche Sicherheitssiegel und ein Sicherheitssiegel am unteren Rand neben der Schnittstelle geschützt, welche die Ober- und Unterschale des Gehäuses verbinden. Ein eventuelles Öffnen des Gerätes wird somit durch die Siegel oder das Gehäuse selbst erkennbar.

Das Siegel trägt hierfür Echtheits- und Integritätsmerkmale. Entsprechende Hinweise in Form von Abbildungen sind der Dokumentation zu entnehmen.

Der Offline-Betrieb ist nicht Gegenstand der Bestätigung.

### **3 Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung**

#### **3.1 Erfüllte Anforderungen**

Das Produkt erfüllt die Anforderungen nach:

##### **SigV**

#### **§ 15 Anforderungen an Produkte für qualifizierte elektronische Signaturen**

##### **§ 15 (2)**

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,

##### **§ 15 (4)**

Sicherheitstechnische Veränderungen an technischen Komponenten nach den Absätzen 1 bis 3 müssen für den Nutzer erkennbar werden.

#### **3.2 Einsatzbedingungen**

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

##### **3.2.1 Anforderungen an die technische Einsatzumgebung**

- Der Anwender benutzt zur Erstellung qualifizierter elektronischer Signaturen ausschließlich bestätigte sichere Signaturerstellungseinheiten nach § 2 Nr. 10 SigG, die der Spezifikation ISO 7816 bzw. EMV genügen.
- Es dürfen für die PIN-Eingabe im Rahmen der Erstellung qualifizierter elektronischer Signaturen ausschließlich nach § 2 Nr. 13 SigG bestätigte bzw. herstellere erklärte Signaturanwendungskomponenten verwendet werden, welche die Sicherheitsfunktion zur sicheren PIN-Eingabe gemäß Herstellerangaben korrekt stimulieren.

##### **3.2.2 Anforderungen an die organisatorische und administrative Einsatzumgebung**

- Der Benutzer hat sich vor der Eingabe der PIN am Chipkartenterminal von der Unversehrtheit der Sicherheitssiegel zu überzeugen. Das Aussehen und der Befestigungsort der Siegel kann der Benutzer aus der Dokumentation entnehmen.
- Die Eingabe der PIN ist vom Benutzer ausschließlich über die Tastatur des Gerätes vorzunehmen. Während der PIN-Eingabe muss der Endanwender die Anzeige im LC-Display dahingehend überprüfen, dass der Modus der sicheren PIN-Eingabe aktiv ist.

- Die Regeln zur sicheren Handhabung und Nichtweitergabe der PIN müssen dem Endanwender vom Herausgeber der Chipkarte mitgeteilt werden, insbesondere die unbeobachtete Eingabe der PIN. Der Nutzer hat bei Eingabe der PIN sicher zu stellen, dass er nicht beobachtet wird.
- Der Einsatz der Produktvarianten ist für nichtöffentliche oder private Umgebungen vorgesehen. Das Gerät ist also so aufzustellen, dass nur autorisierte Personen Zugang haben, eine gegen Manipulationsversuche geschützte Arbeitsumgebung gewährleistet und eine sichere (unbeobachtete) PIN-Eingabe möglich ist.
- Zertifizierte bzw. bestätigte Firmware, die von KOBIL zum Download angeboten wird, muss durch Angabe der Zertifizierungs- bzw. Bestätigungs-IDs gekennzeichnet sein. Der Endanwender muss sich vor der Installation einer neuen Firmware davon überzeugen, dass diese nach SigG/SigV bestätigt und nach Common Criteria zertifiziert ist.

### 3.2.3 Nutzung und Abgrenzung des Chipkartenterminals

- Die Schnittstelle zwischen Gerät und der USB-Docking-Station stellt die logische und physische Grenze des Produktes dar. Bestandteile außerhalb dieser Grenzen wie die Docking-Station, Treibersoftware, Tools zum Firmware-Update und Anwendungen, die das Produkt nutzen, sind **nicht** Gegenstand dieser Bestätigung.
- Für den Online-Betrieb ist eine sichere PIN-Eingabe mit Speicheraufbereitung und das Firmwareupdate implementiert. Der Offline-Betrieb ist **nicht** Gegenstand dieser Bestätigung.

### 3.3 Algorithmen und zugehörige Parameter

Keine

### 3.4 Prüfstufe und Mechanismenstärke

Die Chipkartenterminal-Produktvarianten EMV-TriCAP Reader, SecOVID Reader III und KAAAN TriB@nk wurden erfolgreich nach den Common Criteria (CC) mit der Prüfstufe EAL3+ (EAL3 mit Zusatz AVA\_VLA.4 (gegen ein hohes Angriffspotential), AVA\_MSU.3 (eine vollständige Missbrauchsanalyse), ADV\_IMP.1, ADV\_LLD.1 und ALC\_TAT.1, ADO\_DEL.2 (Erkennung von Manipulation)) evaluiert.

Die eingesetzten Sicherheitsfunktionen erreichen die Stärke hoch.

Ende der Bestätigung