Sicherheitsbestätigung

T-Systems.02246.TE.10.2010

Signatur-Modul für die KOBIL Chipkartenterminals KAAN TriB@nk, EMV-TriCAP und SecOVID Reader III

KOBIL Systems GmbH

Bestätigung
von Produkten für qualifizierte elektronische Signaturen

gemäß §§ 15 Abs. 7 und 17 Abs. 4 Gesetz über Rahmenbedingungen für elektronische Signaturen[1] und §§ 11 Abs. 3 und 15 Signaturverordnung[2]

Bestätigung
T-Systems.02246.TE.10.2010

T-Systems GEI GmbH
- Bestätigungsstelle -

Vorgebirgsstr. 49, 53119 Bonn

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

Chipkartenterminals
EMV-TriCAP Reader (Artikel-Nr. HCPNCKS/A04, Firmware-Version 82.23),
SecOVID Reader III (Artikel-Nr. HCPNCKS/B07, Firmware-Version 82.23),
KAAN TriB@nk(Artikel-Nr. HCPNCKS/C08, Firmware-Version 79.23)

der

KOBIL Systems GmbH

den nachstehend genannten Anforderungen des SigG und der SigV entsprechen.

Die Dokumentation zu dieser Bestätigung ist registriert unter:

T-Systems.02246.TE.10.2010

Bonn, den 29.10.2010

(Dr. Igor Furgel)

Die T-Systems GEI GmbH – Bestätigungsstelle - ist 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.

---

[1] Signaturgesetz vom 16. Mai 2001 (BGBl. I S. 876), zuletzt geändert durch Artikel 4 des Gesetzes vom 17. Juli 2009 (BGBl. I S. 2091) (BGBl. Jahrgang 2009, Teil I S. 2091)

[2] Signaturverordnung vom 16. November 2001 (BGBl. I S. 3074), zuletzt geändert durch die Verordnung vom 17. Dezember 2009 (BGBl. I S. 3932) (BGBl. I S. 3932)

Beschreibung des Produktes für qualifizierte elektronische Signaturen:

1. Handelsbezeichnung und Lieferumfang

1.1 Handelsbezeichnung

Chipkartenterminals
EMV-TriCAP Reader (Artikel-Nr. HCPNCKS/A04, Firmware-Version 82.23), SecOVID Reader III (Artikel-Nr. HCPNCKS/B07, Firmware-Version 82.23), KAAN TriB@nk(Artikel-Nr. HCPNCKS/C08, Firmware-Version 79.23)“

Hinweis:
Die o.g. Chipkartenterminals der Firma Kobil Systems GmbH[3] sind, vom Typenschild abgesehen, identisch im Aufbau. Die Produkte können in zwei Betriebsmodi betrieben werden: Ein Offline-Modus, welcher je Variante individuelle Funktionalitäten aufweist und ein Online-Modus, welcher identische Funktionalitäten aufweist. Bestandteil dieser Bestätigung ist ausschließlich der Online-Betriebs-Modus.

1.2 Auslieferung

Es wird zwischen physischer (materieller) und elektronischer Auslieferung unterschieden.

a) Materielle Auslieferung

Die materielle Auslieferung erfolgt in einer der drei o.g. Produktvarianten im Versand durch den Hersteller. Zusätzlich enthält das ausgelieferte Produkt eine Docking Station zur Aufnahme des Chipkartenterminals mit USB-Kabel zum Anschluss an einen PC und eine CD-ROM mit Treibern für die von KOBIL unterstützten Betriebssysteme. Die Geräte sind im Rahmen der Endmontage mit drei Sicherheitssiegeln versehen, welche bei Öffnung des Gerätes beschädigt werden.

b) Elektronische Auslieferung

Die elektronische Auslieferung erfolgt über die Webseite des Herstellers. Es wird je o.g. Produktvariante 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.

---

[3] Im Folgenden Kobil oder Hersteller gemannt

Ergänzend zu den über die materielle oder elektronische Auslieferung bezogenen Bestandteilen liefert der Hersteller auf Anfrage folgende Dokumentation zur Stimulation der Sicherheitsfunktionen des EVG:

KOBIL EMV-TriCAP Reader, SecOVID Reader III, KAAN TriB@nk – Developer Notes, Version 1.2, 24. 02. 2009

Zielgruppe sind Entwickler, die den EVG in ihre Anwendungen integrieren wollen.

1.3 Lieferumfang

a) Die Bestandteile der physischen (materiellen) Auslieferung sind:

Produktname	Artikelnr.	Paketnr.[4]	HW[5]- und FW[6]- Version Dokumentation
EMV-TriCAP Reader	HCPNCKS/A04	PCPPGKS/010	HW: KCT106r1, FW: 82.23 – EMVTriCAP
			KOBIL EMV-TriCAP Reader – Manual Dokumenten-ID DB22.DEEN.3 Version 2.13 vom 21. 09. 2010 **oder** KOBIL EMV-TriCAP Reader – Manual Dokumenten-ID DB22.DEEN.1 Version 2.10 vom 21. 05. 2008 mit Informationsblatt, Version 1.01 vom 21.09.2010
SecOVID Reader III	HCPNCKS/B07	PR5PGKS/012	HW: KCT106r1, FW: 82.23 – SecOVID III
			KOBIL SecOVID Reader III – Manual Dokumenten-ID DB21.DEEN.3 Version 2.19 vom 21. 09. 2010 **oder** KOBIL SecOVID Reader III – Manual Dokumenten-ID DB21.DEEN.1 Version 2.16 vom 21. 05. 2008 mit Informationsblatt, Version 1.01 vom 21.09.2010
KAAN TriB@nk	HCPNCKS/C08	PTB00KS/015	HW: KCT106r1, FW: 79.23 – KAANTriB@nk
			KAAN TriB@nk – Manual Dokumenten-ID DB31.DE.3 Version 1.25 vom 21.09. 2010 **oder** KAAN TriB@nk – Manual Dokumenten-ID DB31.DE.1 Version 1.22 vom 20.01.2009 mit Informationsblatt, Version 1.01 vom 21.09.2010

Die Identifizierung des Produktes erfolgt über das jeweilige Typschild, auf dem der Produktname, die die Artikelnummer und die Hardware-Version angegeben sind.

---

4 Nummer auf der Verpackung

5 Hardware-Versionsnummer der Hauptplatine (identisch für alle Produktversionen)

6 Firmware-Versionsnummer. Diese Versionsnummer wird bei jedem Start am LCD-Display angezeigt.

b) Die Bestandteile der elektronischen Auslieferung sind die nachfolgend angegebenen Dateien, die die in der obigen Tabelle angegebenen Firmware-Versionen enthalten:

- EMV_TriCAP_82.23_40.exe
- SecOVID_Reader_III_82.23_40.exe
- KAAN_TriBank_79.23_40.exe.

c) Für Entwickler, die die Produkte in ihre Anwendungen integrieren wollen, wird auf Anfrage noch folgende aktualisierte Dokumentation bereitgestellt:

- KOBIL EMV-TriCAP Reader, SecOVID Reader III, KAAN TriB@nk – Developer Notes, Version 1.2, 24. 02. 2009.

d) Gerätetreiber

Für die Verwendung der sicheren PIN-Eingabe und der Update-Funktionalität muss der EVG über die Docking Station mit dem Host-PC verbunden werden. Zur Stimulation der Sicherheitsfunktionen werden Gerätetreiber als unterstützende Software auf dem Host-PC benötigt. Der Hersteller stellt Treiber für Microsoft Windows™ zur Verfügung, die die Stimulation der Sicherheitsfunktionen „Sichere PIN-Eingabe“ und „Sicherer Firmwareupdate“ ermöglichen.

Die Gerätetreiber sind nicht Bestandteil dieser Bestätigung (vgl. Abschn. 3.2.3). Da der Hersteller den Benutzer auffordert, bei jedem Systemstart zu prüfen, ob die in der Bestätigungsurkunde angegebene Treiberkonfiguration tatsächlich geladen ist (vgl. Abschn. 3.2.2), werden ihre vom Hersteller als korrekt eingestuften Versionen nachfolgend informativ angegeben:

Bezeichnung	Dateiname(n)	Version
CT-API-Treiber (32 Bit)	ct32.dll	2010.3.17.1
ZKA SigAPI-Treiber (32 Bit)	ZKASigApi.dll	2010.6.14.1
PCSC-Treiber für Windows 2000 (32 Bit)	kobccid.sys / kobccex.sys	2008.7.1.1
PCSC-Treiber für Windows XP (32/64 Bit)	kobccid.sys / kobccex.sys	2009.10.2.1

1.4 Antragsteller dieser Bestätigung und Hersteller der Produkts

KOBIL Systems GmbH
Pfortenring 11
67547 Worms
Deutschland

2. Funktionsbeschreibung

Der EVG stellt Funktionen zur Verfügung als Teil einer Signatur-Anwendungs-komponente gemäß §2 SigG:

- „Im Sinne dieses Gesetzes sind [...] 11. ‚Signaturanwendungskomponenten' Software- und Hardwareprodukte, die dazu bestimmt sind, a) Daten dem Prozess der Erzeugung oder Prüfung qualifizierter elektronischer Signaturen zuzuführen oder b) [...]"

2.1 Kurzbeschreibung

Das Produkt ist in drei o.g. Produktvarianten lieferbar, s. Kapitel 1. Alle Varianten stellen Funktionen eines Chipkartenterminals über verschiedene Applikationsschnittstellen bereit. Es werden Prozessorchipkarten gemäß ISO-7816- und EMV 2000[7]-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.

Der Anschluss erfolgt über eine Docking Station an der USB-Schnittstelle des Host-PCs (Online-Betrieb).

Das Produkt kann auch ohne Anschluss an einen Host-PC 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, die u.a. ergaben, dass der Offline-Betrieb die bestätigte Sicherheit des Online-Betriebs nicht stören kann.

---

[7] EMVCo LLC *EMV™* Integrated *Circuit Card Specifications for Payment Systems* Version 4.0, 2000. http://www.emvco.org

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[8] bzw. CT-BCS[9] und fügt die vom Benutzer über das Keypad des EVG 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).

2.1 Beschreibung der evaluierten Sicherheitsfunktionalität

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

1. Sichere PIN-Eingabe

Wird das Gerät über entsprechende Befehle (gem. CCID oder CT-BCS) von einer Applikationssoftware 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 Host-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 REQUIR EMENT (ISO/IEC 7816-8): INS=0x28
- DISABLE VERIFICATION REQUIREMENT (ISO/IEC 7816-8): INS=0x26
- RESET RETRY COUNTER (ISO/IEC 7816-8): INS=0x2C

---

[8] 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, http://www.usb.org

[9] TeleTrusT Deutschland e.V., Multifunktionale Karten Terminals (MKT) – Spezifikation, Teil 4: Anwendungsunabhängiger CardTerminal Basic Command Set (CT-BCS), Version 1.0, 15. 04. 1999.

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.

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 der Signatur über die 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.

Aus dem Firmwareupdate- (Bootloader-) Modus kann nur eine neu entgegengenommene, korrekt signierte Firmware wieder aktiviert werden, eine Rückkehr zur vormals installierten Firmware ist nicht mehr möglich. Eine entgegengenommene Firmware mit fehlerhafter Signatur wird nicht aktiviert, sondern es wird wieder in den Bootloader-Modus verzweigt, der wiederum auf eine neue Firmware wartet.

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. herstellererklärte Signaturanwendungskomponenten verwendet werden, welche die Sicherheitsfunktion zur sicheren PIN-Eingabe gemäß Herstellerangeben korrekt stimulieren.

3.2.2 Anforderungen an die organisatorische und administrative Einsatzumgebung

- Der Benutzer hat sich vor jeder 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 (das Schloss-Symbol wird angezeigt).

- 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 ausschließlich 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.

- Bestätigte Firmware, die von KOBIL zum Download angeboten wird, muss durch Angabe der Bestätigungs-ID gekennzeichnet sein. Der Endanwender muss sich vor der Installation einer neuen Firmware davon überzeugen, dass diese nach SigG/SigV bestätigt ist. Er überzeugt sich nach der Installation der neuen Firmware davon, dass diese auch im Gerät aktiv ist.

- Der Benutzer hat bei jedem Systemstart zu prüfen, ob die in der Bestätigungsurkunde angegebene Treiberkonfiguration tatsächlich geladen ist (gilt nur für Microsoft Windows™).

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 im Sinne der SigV, Anlage 1, Abschnitt I, Nr. 2

Produkte, die im Rahmen des aktuellen Bestätigungsverfahrens behandelt werden, implementieren keine Algorithmen im Sinne der SigV, Anlage 1, Abschnitt I, Nr. 2.

3.4 Prüfstufe und Mindeststärke der Sicherheitsfunktionen

Die Chipkartenterminals EMV-TriCAP Reader, SecOVID Reader III, KAAN TriB@nk“ gemäß Abschnitt 1.1 wurden erfolgreich nach der Common Criteria (Version 2.3) Prüfstufe EAL3 (mit Zusatz in Übereinstimmung mit Anlage 1, Abschnitt I, Nr. 1.2 SigV) re-evaluiert.

Die evaluierten Sicherheitsfunktionen[10] erreichen die Mindeststärke "SOF-hoch".

In Bezug auf Verwendung des asymmetrischen ECDSA-Algorithmus mit einer Bitlänge von 192 für die Verifikation der Signatur über die zu ladende Firmware (Sicherer Firmwareupdate) ist **die Gültigkeit dieser Bestätigung zeitlich beschränkt, und zwar bis 31.12.2013**.

Ende der Bestätigung.

[10] In Common Criteria: Strength of Functions (SOF)

Bestätigung
T-Systems.02246.TE.10.2010

Hrsg.: T-Systems GEI GmbH
Adresse: Vorgebirgsstr. 49, 53119 Bonn
Telefon: +49-(0)228-9841-00
Fax: +49-(0)228-9841-6000
Web: www.t-systems.de/ict-security
www.t-systems-zert.com