Bestätigung
von Produkten für qualifizierte elektronische Signaturen

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

Bundesamt für Sicherheit in der Informationstechnik[3]
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 das

Keyboard with SmartCard Reader SmartCase KB SCR eSIG (S26381-K529-Vxxx HOS:01)

den nachstehend genannten Anforderungen des SigG und der SigV entspricht.

Die Dokumentation zu dieser Bestätigung ist registriert unter:

BSI.02107.TE.03.2010

Bundesamt für Sicherheit in der Informationstechnik

Bonn, den 8. März 2010

Im Auftrag
Bernd Kowalski
Abteilungspräsident

Das Bundesamt für Sicherheit in der Informationstechnik ist auf Grundlage des Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG) vom 14. August 2009, Bundesgesetzblatt I S. 2821 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.

---

1 Gesetz über die Rahmenbedingungen für elektronische Signaturen (Signaturgesetz - SigG) in der Fassung vom 16. Mai 2001 (BGBl. Jahrgang 2001 Teil I Nr. 22) zuletzt geändert durch Artikel 4 des Gesetzes vom 17. Juli 2009 (BGBl. I S. 2091)

2 Verordnung zur elektronischen Signatur (Signaturverordnung - SigV) in der Fassung vom 16. November 2001 (BGBl. Jahrgang 2001 Teil I Nr. 59) zuletzt geändert durch die Verordnung vom 17. Dezember 2009 (BGBl. I S. 3932)

3 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, Web: www.bsi.bund.de

Beschreibung des Produktes für qualifizierte elektronische Signaturen:

1 Handelsbezeichnung des Produktes und Lieferumfang:

Das Chipkartenterminal **SmartCase KB SCR eSIG** (S26381-K529-Vxxx) mit der Hardware-Version HOS:01 sowie der Firmware-Version 1.20 der Fujitsu Technology Solutions GmbH[4] ist eine Computertastatur mit integriertem Chipkartenterminal. Das Gerät kann sowohl in unterschiedlichen Farbvarianten, als auch mit unterschiedlichen Tastaturbeschriftungen angeboten werden. Der Platzhalter „xxx" im dritten Block der Sachnummer wird der Ausprägung entsprechend angepasst:

Hunderterstelle	Gehäusefarbe
1xx	marble grey
2xx	schwarz

Tabelle 1: Gehäusefarben (Beispiele)

Zehner- und Einerstelle	Tastaturbeschriftung (Layout)
x10	US (United States)
x11	H (Hungary)
x20	D (Germany)
x65	GB (Great Britain)

Tabelle 2: Tastaturbeschriftung (Beispiele)

1.1 Auslieferung und Lieferumfang:

Das SmartCase KB SCR eSIG (S26381-K529-Vxxx) Hardware-Version HOS:01, Firmware-Version 1.20 wird wie in Kapitel 1.3 dargestellt ausgeliefert:

Das Gehäuse des Chipkartenterminals ist versiegelt. Die Siegel sind vor der Inbetriebnahme durch den Kunden entsprechend der Betriebsanleitung auf Unversehrtheit zu prüfen. Ebenso ist entsprechend der Betriebsanleitung zu prüfen, dass die richtige Hardware- und Firmware ausgeliefert wird.

Das Gerät ist für ein Firmware-Upgrade vorbereitet. Hierfür prüft es vor dem Laden der neuen Firmware in den Controller deren Signatur. Ist die Firmware nicht authentisch und integer, wird diese nicht akzeptiert. Andere Firmware-Versionen als die oben genannte sind nicht Gegenstand dieser Bestätigung und müssen durch eine Nachtragsbestätigung oder separate Bestätigung erneut betrachtet werden.

1.2 Antragsteller dieser Bestätigung sowie Hersteller und Vertreiber des Produkts:

Fujitsu Technology Solutions GmbH
Bürgermeister-Ulrich-Straße 100
86199 Augsburg
Germany

[4] Im Folgenden auch Fujitsu genannt.

1.3 Lieferumfang des Produktes:

Nr	Typ	Identifier	Version	Auslieferungsart
1	HW/ SW	SmartCase KB SCR eSIG (S26381-K529-Vxxx) Vxxx bezeichnet unterschiedliche Ausführungen des Terminals (s. Tabellen 1 und 2)	Hardware: HOS:01 Firmware: 1.20	Direkter Versand vom Hersteller zum Kunden.
2	DOC	USB-Security-Tastatur KB SCR eSIG Betriebsanleitung	Ausgabe Oktober 2009	
3	DOC	USB-Security-Keyboard KB SCR eSIG Operating Manual	October 2009 edition	
4	SW	FWCheck_KBSCReSIG.exe Programm zur Prüfung der korrekten Firmwareversion des EVG	SHA-256 Hash: 3D82 8D51 59E5 BA52 FA59 D56C ED20 EF30 B0D9 FD75 7F6A 5AAE 8588 0EA0 832B B9B2	

Tabelle 3: Auslieferungsumfang des Produktes

2 Funktionsbeschreibung

2.1 Kurzbeschreibung

Das Chipkartenterminal KB SCR eSIG (S26381-K529-Vxxx HOS:01) stellt eine USB-Tastatur mit einem integrierten Chipkartenleser dar. Ziel des Produktes ist der Einsatz im Zusammenhang mit Anwendungen zur Erzeugung qualifizierter elektronischer Signaturen nach dem deutschen Signaturgesetz (SigG). Die Sicherheitsfunktionen der Chipkartenleser-Tastatur KB SCR eSIG zielen darauf ab, die Anforderungen

- keine Preisgabe oder Speicherung der Identifikationsdaten und
- Erkennbarkeit sicherheitstechnischer Veränderungen

zu erfüllen.

Das Produkt ist für den Einsatz im nichtöffentlichen Bereich wie der privaten Umgebung oder der normalen Büroumgebung mit geregelten Zugriffsmöglichkeiten vorgesehen.

Beim Einsatz wird zwischen zwei verschiedenen Modi unterschieden, dem normalen Tastaturmodus und dem Modus der sicheren PIN-Eingabe. Die sichere PIN-Eingabe wird dem Benutzer durch rotes Blinken der entsprechenden PIN-LED angezeigt.

Das Umschalten des Nummernblocks im Kartenterminal in den sicheren PIN-Eingabemodus wird durch eine Signaturanwendungskomponente im Sinne des Signaturgesetzes durchgeführt. Dies wird optisch durch ein rotes Blinken der PIN-LED angezeigt bis die Vollständigkeit der PIN erreicht beziehungsweise der Vorgang abgebrochen wird. Zum Abbruch des Vorgangs zählen das Ziehen der Karte, das Betätigen der Abbruchtaste und das Überschreiten der vorgegebenen Eingabezeit. Der Eingabefortschritt wird mittels der Übertragung von Dummycodes „*“ dem System mitgeteilt. Während des sicheren PIN-Eingabemodus wird das Betätigen anderer als der für die PIN-Eingabe relevanter Tasten ignoriert.

Der Austausch der PIN erfolgt nur zwischen Chipkarte und der Chipkartenleser-Tastatur KB SCR eSIG (S26381-K529-Vxxx HOS:01) über die Kartenleserschnittstelle. Diese befindet sich in der Tastatur und wird gegen Manipulation durch die Sicherheitssiegel geschützt.

2.2 Funktionsbeschreibung des Produktes

Die folgenden Tabellen beschreiben die Sicherheitsfunktionen und –maßnahmen ausführlich.

<table>
<tr><th>Sicherheitsfunktion</th><th>Beschreibung</th></tr>
<tr><td>SF.1
PIN Command
(Sichere PIN- Eingabe)</td><td>Das Umschalten des Kartenterminals in den sicheren PIN- Eingabemodus wird durch ein explizites CT-Kommando nach CCID durchgeführt. Dieses CT-Kommando enthält die PIN-Handlings-Vereinbarungen und das Chipkartenkommando, in welches die PIN an die spezifizierte Stelle integriert wird.
Anhand des Instructionbytes des Chipkartenkommandos wird überprüft, ob es sich um ein PIN- Kommando handelt, welches explizit eine PIN- Eingabe erwartet.
In der folgenden Tabelle sind die zugelassenen Instructionbytes nach den jeweiligen Normen aufgeführt:
<table>
<tr><th>INS-Byte</th><th>Bezeichnung</th><th>Bedeutung</th><th>Norm</th></tr>
<tr><td>0x20</td><td>VERIFY</td><td>PIN eingeben</td><td>ISO/IEC 7816-4</td></tr>
<tr><td>0x24</td><td>CHANGE REFERENCE DATA</td><td>PIN ändern</td><td>ISO/IEC 7816-8</td></tr>
<tr><td>0x26</td><td>DISABLE VERIFICATION REQUIREMENT</td><td>PIN aktivieren</td><td>ISO/IEC 7816-8</td></tr>
<tr><td>0x28</td><td>ENABLE VERIFICATION REQUIREMENT</td><td>PIN deaktivieren</td><td>ISO/IEC 7816-8</td></tr>
<tr><td>0x18</td><td>APPLICATION</td><td>Applikation entblocken</td><td>EMV 2000</td></tr>
<tr><td>0x2C</td><td>RESET RETRY COUNTER</td><td>PIN entsperren</td><td>ISO/IEC 7816-8</td></tr>
</table>
Die Eingabe der persönlichen Identifikationsdaten wird im RAM zwischengespeichert, um sie nach Beendigung der Eingabe direkt mit dem PIN-Kommando zur Chipkarte zu senden.
Der sichere PIN- Eingabemodus wird optisch durch eine rot blinkende PIN-LED angezeigt, bis die Vollständigkeit der PIN erreicht, beziehungsweise der Vorgang abgebrochen wird. Zum Abbruch des Vorgangs zählen das Ziehen der Karte, das Betätigen der Abbruchtaste und das Überschreiten der vorgegebenen Eingabezeit.
Dem Benutzer wird der Fortschritt seiner Eingabe mit dem Dummycode „*“ für jede eingegebene Ziffer angezeigt. Die Ausgabe der Dummycodes erfolgt über die USB-Schnittstelle, die dann von der entsprechenden PC-Anwendung angezeigt wird. Innerhalb des EVG wird aber mit der korrekten PIN gearbeitet. Das Betätigen für den Modus nicht relevanter Tasten wird ignoriert.</td></tr>
<tr><td>SF.2
PIN Memory
(Speicherwiederauf-bereitung)</td><td>Die Kommunikation zwischen PC-System und Chipkarte basiert gemäß CCID auf den sogenannten APDUs. Wird eine APDU über die USB- Schnittstelle im Kartenterminal empfangen, so wird sie zuerst zwischengespeichert, um anschließend zur Chipkarte gesendet zu werden.
Nach dem Einschalten, dem Weiterleiten eines PIN- Kommandos bzw. dem Ziehen der Chipkarte oder dem Abbruch wird der PIN-Speicherbereich wiederaufbereitet, um sicherzustellen, dass keine persönlichen Identifikationsdaten bzw. Datenfragmente im Kartenterminal erhalten bleiben.
Der Speicherbereich beinhaltet sowohl die PIN als auch die APDU.
Außerdem wird die LED zur Anzeige der sicheren PIN- Eingabe ausgeschaltet.</td></tr>
<tr><td>SF.3
Secure Firmware Download
(Sicherer Firmware-Update)</td><td>Die Verifikation einer Signatur der Firmware mit dem asymmetrischen RSA-Algorithmus und einer Bitlänge von 2048 garantiert die Integrität und Authentizität der Firmware beim Laden einer neuen Firmware in den</td></tr>
</table>

Sicherheitsfunktion	Beschreibung
	Chipkartenleser. Der Hash- Wert über die neu zu ladende Firmware wird basierend auf dem Algorithmus SHA-256 mit einer Länge von 256 Bit ermittelt. Die Verifikation der Integrität und Authentizität erfolgt im EVG durch Vergleich des ermittelten Hash-Wertes und des Hash-Wertes als Bestandteil der Signatur. Der öffentliche Schlüssel zur Authentizitätsprüfung der Firmware ist im Gerät gespeichert.

Tabelle 4: Sicherheitsfunktionen

Sicherheitsmaßnahme	Beschreibung
Versiegelung (SM.1)	Anhand drei authentischer und fälschungssicherer Sicherheitssiegel, welche über die Trennkante zwischen Gehäuseunterteil und -oberteil geklebt werden, kann die Manipulationsfreiheit der Hardware sicher erkannt werden. Dies wird dadurch sichergestellt, dass ein Öffnen nicht ohne Beschädigung des Siegels möglich ist. Die Beschaffenheit (Zerstöreigenschaften) des Siegels gewährleistet, dass es nicht unbeschädigt entfernt und wieder aufgeklebt werden kann. Eine 7-stellige fortlaufende Nummer auf dem Siegel erlaubt eine eindeutige Identifizierung.

Tabelle 5: Sicherheitsmaßnahmen

Der Tastatur-Modus, sowie die Treiber-Software für den PC, sind nicht Gegenstand dieser 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

- Es wird ein PC mit USB-Anschluss und USB-Geräte unterstützendem Betriebssystem gemäß Bedienungsanleitung vorausgesetzt.
- 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 Herstellerangaben korrekt ansteuern.

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. Auch hat er die Authentizität anhand der sieben stelligen Siegelnummern zu prüfen, die bei Inbetriebnahme zum Vergleich notiert werden.
- Es ist regelmäßig mit dem Softwaretool FWCheck_KBSCReSIG.exe die Firmware des Kartenterminals zu prüfen. Die Integrität des Tools ist mittels Hashwertvergleich (siehe Nutzeranleitung) sicher zu stellen.

- Die Eingabe der PIN ist vom Benutzer ausschließlich über den Nummernblock der Tastatur vorzunehmen. Vor der Eingabe hat sich der Benutzer mit Hilfe der Überprüfung der rot blinkenden PIN-LED davon zu überzeugen, dass der sichere PIN-Eingabemodus 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 Chipkartenleser-Tastatur KB SCR eSIG 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 Fujitsu 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

- Der Endanwender wird über seine Verantwortung während der Nutzung durch die mitgelieferte Betriebsdokumentation informiert. Die USB-Schnittstelle stellt die logische und physische Grenze des Produktes dar, Bestandteile außerhalb dieser Grenzen, etwa Treibersoftware, Tools zum Firmware-Update und Anwendungen, die das Produkt nutzen, sind **nicht** Gegenstand dieser Bestätigung.
- Andere Betriebsmodi als die sichere PIN-Eingabe, etwa der reguläre Tastatur-Betrieb, sind ebenfalls **nicht** Gegenstand dieser Bestätigung.

3.3 Algorithmen und zugehörige Parameter

Keine.

3.4 Prüfstufe und Mechanismenstärke

Das Produkt Keyboard with SmartCard Reader SmartCase KB SCR eSIG (S26381-K529-Vxxx HOS:01) wurde 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