



Zentrum für sichere Informationstechnologie – Austria Secure Information Technology Center - Austria

A-1040 Wien, Weyringergasse 35
Tel.: ++43 1 – 503 19 63 – 0
Fax: ++43 1 – 503 19 63 – 66

A-8010 Graz, Inffeldgasse 16a
Tel.: ++43 316 – 873 5514
Fax: ++43 316 – 873 5520

Homepage: www.a-sit.at
E-Mail: office@a-sit.at

Bescheinigung nach §18(5) SigG: Chipkartenleser mit Tastatur und Display KOBIL KAAN Professional HW-Version KCT100 FW-Version 2.08 GK 1.04

Antragsteller:
Bull AG
Lemböckgasse 49
1230 Wien

1. Beschreibung der bescheinigten Komponente

Die bescheinigte Komponente ist KOBIL KAAN Professional HW-Version KCT100, FW-Version 2.08 GK 1.04 (nachstehend Chipkartenleser genannt) der Fa. Kobil Systems GmbH¹. Es handelt sich um einen universellen Chipkartenleser der Klasse 3 mit Tastatur, Display, LEDs, einer seriellen Schnittstelle oder einer USB-Schnittstelle.

Der Chipkartenleser wird als fertig konfiguriertes Gerät mit dem zugehörigen Benutzerhandbuch² in Transportverpackung mit versiegeltem Gehäuse ausgeliefert. Updates sind nicht Gegenstand dieser Bescheinigung.

Der Chipkartenleser kann für sichere elektronische Signaturen eingesetzt werden, um

- Identifikationsdaten (d.h. PIN³) zu erfassen und an sichere Signaturerstellungseinheiten (d.h. Signaturkarten) weiterzuleiten,
- Hashwerte der zu signierenden Dokumente von der aufrufenden Signaturanwendung an die Signaturkarte zu übermitteln und
- Signaturen von der Signaturkarte an die aufrufende Signaturanwendung zu übermitteln.

Die Auslieferung der zu bescheinigenden Komponente umfasst folgende Komponenten:

- KOBIL Chipkartenterminal KCT 100 KAAN Professional bzw. B1 Professional Firmware 2.08 GK 1.04,
- serielles Anschlusskabel oder USB-Anschlusskabel,
- CD-ROM mit Treibern, Tools und Handbuch Version 2.3,
- Faltblatt „Anschluss Chipkartenterminal KAAN Pro / B1 Pro“ und
- Karton.

¹ Weinsheimer Str. 71, D-67547 Worms

² KOBIL Chipkartenterminal Handbuch (CD), Version 2.3, KOBIL Systems GmbH, 25.02.2002

³ Personal Identification Number

2. Erfüllung der Anforderungen des SigG und der SigV

Der Chipkartenleser erfüllt unter nachstehenden Einsatzbedingungen

- die Anforderungen nach §7(3) SigV⁴, dass das unbefugte Erfahren der Autorisierungs-codes praktisch ausgeschlossen sein muss,
- die Anforderungen nach §7(3) SigV⁵, dass die eingegebenen Autorisierungs-codes von den verwendeten Systemelementen nicht gespeichert werden dürfen und dass Eingabeerleichterungen bei wiederholter Eingabe von Autorisierungs-codes ausgeschlossen sein müssen,
- die Anforderung nach §18(2) SigG⁶, dass die zu signierenden Daten nicht verändert werden, und
- die Anforderung nach §9(2)⁷ SigV an die Prüfung der übrigen (d.h. weder für die Erzeugung und Speicherung von Signaturerstellungsdaten noch für die Erstellung sicherer elektronischer Signaturen noch für die sichere Signaturprüfung eingesetzten) technischen Komponenten und Verfahren, dass die Evaluationsstufe ITSEC E2 mit der Mindeststärke der Sicherheitsmechanismen "hoch" eingehalten sein muss.

Der Chipkartenleser ist daher in folgenden Kategorien bescheinigt:

- Komponenten und Verfahren zur Sicherstellung des autorisierten Zuganges.

3. Gültigkeitsdauer der Bescheinigung

Diese Bescheinigung ist zwei Jahre nach der Ausstellung gültig.

4. Einsatzbedingungen

Alle Einsatzbedingungen aus der deutschen Bestätigung TUVIT.09331.TE.03.2002⁸ mit Ausnahme der folgenden Einsatzbedingungen:

- Abschnitt 3.2 Buchstabe a) Punkt 3 und
 - Abschnitt 2.3 Buchstabe c) Punkt 4
- sind gültig.

Zusätzlich werden folgende Einsatzbedingungen definiert:

- (1) Der Einsatz für sichere elektronische Signaturen gem. §2 Punkt 3 SigG setzt die Nutzung einer sicheren Signaturerstellungseinheit gem. §2 Punkt 5 und §18(5) SigG voraus. Falls die Signaturerstellungseinheit eine Prozessorchipkarte mit dem Protokoll T=0 oder T=1 entsprechend ISO/IEC 7816 ist, ist Folgendes zu beachten: Zur korrekten Ausführung der Sicherheitsfunktion 2 "Sichere PIN-Eingabe" und der Sicherheitsfunktion 3 "Sichere PIN-Änderung" muss das Chipkarten-Betriebssystem mindestens eines der folgenden Kommandos unterstützen:
 - VERIFY (INS-Byte=20h; ISO/IEC 7816-4),
 - CHANGE REFERENCE DATA (INS-Byte=24h; ISO/IEC 7816-8),
 - ENABLE VERIFICATION REQUIREMENT (INS-Byte=28h; ISO/IEC 7816-8),
 - DISABLE VERIFICATION REQUIREMENT (INS-Byte=26h; ISO/IEC 7816-8) oder
 - RESET RETRY COUNTER (INS-Byte=2Ch; ISO/IEC 7816-8).
- (2) Die Komponenten, die dem Prozess der Erzeugung sicherer elektronischer Signaturen gem. §2 Punkt 3 SigG Daten zuführen und die mit dem Chipkartenleser verwendet werden, dürfen eine Signatur-PIN-Eingabe nur auf der Tastatur des Chipkartenlesers zulassen.

⁴ (...) Das unbefugte Erfahren der Autorisierungs-codes muss (...) praktisch ausgeschlossen sein. (...)

⁵ (...) Die eingegebenen Autorisierungs-codes dürfen von den verwendeten Systemelementen nicht gespeichert werden. Eingabeerleichterungen bei wiederholter Eingabe von Autorisierungs-codes müssen ausgeschlossen sein. (...)

⁶ Die bei der Erstellung einer sicheren Signatur verwendeten technischen Komponenten und Verfahren müssen zudem sicherstellen, dass die zu signierenden Daten nicht verändert werden; (...)

⁷ Die Prüfung der technischen Komponenten und Verfahren nach § 7 Abs. 2, § 10 und § 18 SigG kann auch nach den Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC), (...), erfolgen. Bei der Anwendung von ITSEC muss für die Erzeugung und Speicherung von Signaturerstellungsdaten sowie für die Erstellung sicherer elektronischer Signaturen und gegebenenfalls für die sichere Signaturprüfung die Evaluationsstufe E 3 mit der Mindeststärke der Sicherheitsmechanismen "hoch" eingehalten sein; bei den übrigen technischen Komponenten und Verfahren muss die Evaluationsstufe E 2 mit der Mindeststärke der Sicherheitsmechanismen "hoch" eingehalten sein.

⁸ <https://www.secure.trusted-site.de/certuvit/pdf/9331UD.pdf>

5. Algorithmen und zugehörige Parameter

Nicht relevant.

6. Prüfstufe und Mechanismenstärke

Der Chipkartenleser wurde von der TÜV Informationstechnik GmbH⁹ erfolgreich nach der Prüfstufe ITSEC E2 hoch (Mindeststärke der Mechanismen) evaluiert.

Es liegt die deutsche 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 für „KOBIL Chipkartenterminals KAAAN Professional und B1 Professional HW-Version KCT100, FW-Version 2.08 GK 1.04“ (TUVIT.09331.TE.03.2002) vor, ausgestellt durch die TÜV Informationstechnik GmbH⁹ am 15.03.2002. Dieses Dokument bestätigt die Erfüllung der Anforderungen nach § 15 Abs. 2 Nr. 1a) (keine Preisgabe oder Speicherung der Identifikationsdaten) und Abs. 4 (Erkennbarkeit der sicherheitstechnischen Veränderungen) aus der deutschen SigV.

Wien, 24.06.2002

A-SIT Zentrum für sichere Informationstechnologie - Austria



o. Univ.-Prof. Dipl.-Ing. Dr. Reinhard Posch
Wissenschaftlicher Gesamtleiter



Manfred Holzbach
Geschäftsführender Vorstand

⁹ ein Unternehmen der RWTÜV-Gruppe, Zertifizierungsstelle, Am Technologiepark 1, D-45307 Essen