



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

<http://www.a-sit.at>
E-Mail: office@a-sit.at

Bescheinigung nach §18(5) SigG: Signatursoftware MBS Modul zur Erstellung sicherer Signaturen Version 2.0, Release 1.2

Antragsteller:
BDC EDV Consulting GmbH
Gredlerstraße 4
1020 Wien

1. Beschreibung der bescheinigten Komponente

Der Gegenstand der Bescheinigung ist das „MBS¹ Modul zur Erstellung sicherer Signaturen“, Version 2.0, Release 1.2, nachstehend das Modul genannt.

Das Modul besteht aus einer Win32² Programmbibliothek, die MBS-Applikationen Funktionen zur vertrauenswürdigen Anzeige und zur Bereitstellung der zu signierenden Daten zur Verfügung stellt. Zusätzlich stellt das Modul ausführbare Programme zum Ändern und zum Entsperren einer Signatur-PIN zur Verfügung (nicht Gegenstand dieser Bescheinigung).

Hersteller des Moduls ist die BDC EDV Consulting GmbH, Gredlerstraße 4, 1020 Wien.

1.1. Lieferumfang

Die Auslieferung an den Endkunden erfolgt

- direkt vom Hersteller auf einem nur lesbaren Datenträger (CD-ROM) oder
- per Datei-Download über HTTPS von einem authentifizierten Server des Herstellers mit Benutzerzugriffskontrolle.

Zum Lieferumfang gehören das Setupprogramm³, ein MSI⁴-Package⁵, ein CAB-Archiv⁶, und ein Benutzerhandbuch für Endbenutzer bzw. ein Entwicklerhandbuch für Entwickler von MBS-Applikationen.

Das Modul wird mit einer durch eine elektronische Signatur authentifizierte⁷ Konfiguration für die nachfolgend beschriebenen Komponenten ausgeliefert. Jede Erweiterung der zu benutzenden Komponenten erfordert vom Hersteller das Erzeugen einer erweiterten authentifizierten Konfiguration⁸.

¹ MBS = Multi Bank Standard

² Microsoft® 32bit Windows™ API

³ setup.exe

⁴ Microsoft® Installer

⁵ MBS Client v2.0 R1.2.msi

⁶ Data1.cab

⁷ Der Hersteller signiert die SHA-1 Hashwerte über die zu benutzenden DLLs und Konfigurationseinträge mit einem 1024 Bit langen DSA Schlüssel. Zur Erstellung und Verwaltung der Schlüsselpaare werden die CDSA Manifest Signing Tools verwendet.

⁸ Eine Übertragung der Bescheinigung auf eine erweiterte Konfiguration ist in Einzelfällen möglich, die Bestätigungsstelle gibt hierüber Auskunft.

1.2. Technische Einsatzumgebung

Das Modul ist für den Einsatz auf Arbeitsplatzrechnern im Heim- oder Bürobereich vorgesehen. Es werden folgende Versionen des Microsoft Windows Betriebssystems und des Browsers unterstützt:

- Microsoft Windows 98 SE, Internet Explorer 6.0
- Microsoft Windows ME, Internet Explorer 6.0
- Microsoft Windows NT 4.0 (SP6+), Internet Explorer 6.0
- Microsoft Windows 2000 professional (SP2+), Internet Explorer 6.0
- Microsoft Windows XP Home bzw. Professional, Internet Explorer 6.0

Das Modul benötigt mindestens folgende Hardware: PC ab Intel Pentium III/AMDK6 500 MHz, 128 MB RAM, 15 MB freier Festplattenspeicher.

Für die Verwendung der Java-Komponenten des Moduls ist eine installierte Java – Laufzeitumgebung (Java™ 2 Runtime Environment ab Version 1.2) erforderlich.

Zur Erstellung elektronischer Signaturen bedient sich das Modul einer Signaturkarte und eines Chipkartenterminals.

Zum Ansprechen des Chipkartenterminals wird ausschließlich die CT-API verwendet. Folgende CT-API Treiber werden vom Modul unterstützt:

- CT-API Treiber für den KOBIL KAAAN Professional und den KOBIL KAAAN Standard plus, v 2002.11.29.1 vom 29. 11. 2002
- CT-API Treiber für den REINER SCT cyberJack™ e-com und den REINER SCT cyberJack™ und für den REINER SCT cyberJack™ Pinpad v 3.6.10.0 vom 21.10.2002
- CT-API Treiber für den SCM SPR 532, v 2.0.2.0 vom 03.03.2003
- CT-API Treiber für die Cherry Smartboards (G83-6700LQZxx/01 + G81-8015LQZxx/01 + G81-12000LTZxx/01)

Folgende Chipkartenterminals werden unterstützt:

- KOBIL KAAAN Professional, v2.08 GK v1.04
- KOBIL KAAAN Standard Plus
- REINER SCT cyberJack™ e-com, v2.0
- REINER SCT cyberJack™, v3.0
- REINER SCT cyberJack™ Pinpad, v2.0
- SCM SPR 532
- Cherry Smartboards (G83-6700LQZxx/01 + G81-8015LQZxx/01 + G81-12000LTZxx/01)

Folgende Signaturkarten werden unterstützt:

- A-Trust TrustMark, v3.12
- A-Trust TrustSign, v1.2
- a-sign Premium

1.3. Funktionsumfang

Folgende Funktion des Moduls ist für diese Bescheinigung relevant:

- **Secure Viewer:** Diese Funktion prüft das Format der zu signierenden Daten und bringt diese nach erfolgreicher Prüfung sicher zur Anzeige.

Zusätzlich stellt das Modul folgende Funktionen zur Verfügung:

- Ändern der Signatur-PIN
- Entsperren der Signatur-PIN und Geheimhaltungs-PIN

Diese Funktionen sind nicht Gegenstand dieser Bescheinigung.

1.4. Funktionsbeschreibung

Das Modul prüft das Format der zu signierenden Daten und bringt diese nach erfolgreicher Prüfung mittels eines integrierten Secure Viewers zur Anzeige. Der erlaubte Zeichensatz

ist ein eingeschränktes ISO 8859-1 (erlaubte Zeichen siehe Anhang A – Erlaubter Zeichensatz).

Nach einer Bestätigung des Signators werden die zu signierenden Daten an die Hash- bzw. Signaturkomponente weitergeleitet. Das endgültige Auslösen des Signaturvorganges geschieht durch die Eingabe der Signatur-PIN am verwendeten Chipkartenterminal. Die Bereitstellung des zu signierenden Dokuments sowie die Anzeige der Information für den Signator über eventuell aufgetretene Fehler während des Signaturvorganges ist von der aufrufenden Applikation durchzuführen.

Nach erfolgter Signaturberechnung liefert das Modul der aufrufenden Applikation die von der Signaturkomponente erhaltene Signatur im geeigneten Format zurück.

Applikationen, die das Modul nutzen, sind **nicht** Gegenstand dieser Bescheinigung.

2. Erfüllung der Anforderungen des SigG⁹ und der SigV¹⁰

Das Modul erfüllt unter nachstehenden Einsatzbedingungen

- Anforderungen nach §18(1) SigG¹¹
- Anforderungen nach §18(2) SigG¹²
- Anforderungen nach §7(2) SigV¹³

Das Modul ist daher in der folgenden Kategorie bescheinigt:

- Komponenten und Verfahren zur Darstellung der zu signierenden Daten.

3. Gültigkeitsdauer der Bescheinigung

Diese Bescheinigung ist zwei Jahre nach der Ausstellung gültig.

4. Einsatzbedingungen

- (1) Die vorgesehene Einsatzumgebung des Moduls sind Arbeitsplatzrechner im Büro- oder Heimbereich. Der Zugang zum verwendeten Rechner kann vom Signator kontrolliert werden. Manipulationen an der Hardware und Software des Rechners, auf dem das Modul installiert ist, sind zu verhindern. Es ist sicherzustellen, dass die Sicherheit der technischen Einsatzumgebung des Moduls nicht kompromittiert ist. Für einen sicheren Betrieb ist es erforderlich, dass die Empfehlungen der Benutzerdokumentation eingehalten und die Anforderungen an die Einsatzumgebung beachtet werden.
- (2) Zur Erzeugung der sicheren elektronischen Signatur sind ausschließlich sichere Signaturerstellungseinheiten zu verwenden, welche die Anforderungen von SigG und SigV erfüllen.
- (3) Zur Verbindung des Moduls mit der Signaturerstellungseinheit ist ein Chipkartenterminal zu verwenden, das die Anforderungen von SigG und SigV erfüllt. Die Verantwortung für die Integrität der Daten bei der Übertragung zum Chipkartenterminal liegt nicht im Verantwortungsbereich der bescheinigten Komponente. Die Integrität der Daten ist durch geeignete technische und/oder organisatorische Maßnahmen in der Einsatzumgebung

⁹ Bundesgesetz über elektronische Signaturen (Signaturgesetz – SigG, BGBl I Nr. 190/1999 vom 19. August 1999) in der Fassung des Bundesgesetzes BGBl. I Nr. 152/2001 vom 21. Dezember 2001.

¹⁰ Verordnung des Bundeskanzlers über elektronische Signaturen (Signaturverordnung – SigV), BGBl. II Nr. 30/2000 vom 2. Februar 2000.

¹¹ Für die Erzeugung und Speicherung von Signaturerstellungsdaten sowie für die Erstellung sicherer Signaturen sind solche technische Komponenten und Verfahren einzusetzen, die die Fälschung von Signaturen sowie die Verfälschung signierter Daten zuverlässig erkennbar machen (...).

¹² Die bei der Erstellung einer sicheren Signatur verwendeten technischen Komponenten und Verfahren müssen zudem sicherstellen, dass die zu signierenden Daten nicht verändert werden; sie müssen es weiters ermöglichen, dass dem Signator die zu signierenden Daten vor Auslösung des Signaturvorgangs dargestellt werden. (...)

¹³ Die von den Signatoren eingesetzten technischen Komponenten und Verfahren zur Erstellung sicherer elektronischer Signaturen müssen die vollständige Anzeige der zu signierenden Daten ermöglichen. Für die zu signierenden Daten dürfen nur die vom Zertifizierungsdiensteanbieter empfohlenen Formate verwendet werden. Die Spezifikation dieser Formate muss allgemein verfügbar sein. Können in einem Format auch dynamische Veränderungen oder unsichtbare Daten codiert werden, so dürfen die betreffenden Codierungen nicht verwendet werden. Der Zertifizierungsdiensteanbieter hat die Anwender anzuweisen oder ihnen Methoden bereitzustellen, um dynamische Veränderungen oder unsichtbare Daten auszuschließen.

sicherzustellen. Das Chipkartenterminal muss direkt am Arbeitsplatzrechner angeschlossen sein. Der Signator muss sich von der unmittelbaren und sicheren Verbindung des Chipkartenterminals mit dem Arbeitsplatzrechner vergewissern können.

- (4) Die Authentifizierung des Signators gegenüber der Signaturerstellungseinheit muss durch Eingabe der Signatur-PIN über das verwendete Chipkartenterminal erfolgen.

5. Algorithmen und zugehörige Parameter

Die zur Erstellung einer sicheren elektronischen Signatur erforderlichen Algorithmen werden nicht von der bescheinigten Komponente ausgeführt.

6. Prüfstufe und Mechanismenstärke

Das Modul wurde im Rahmen des Bescheinigungsverfahrens von der Bestätigungsstelle A-SIT begutachtet. Als Leitlinie für die Begutachtung der Vertrauenswürdigkeit wurden die Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Criteria – ISO/IEC 15408) - Teil 3: Anforderungen an die Vertrauenswürdigkeit (Vertrauenswürdigkeitsstufe EAL3) herangezogen. Folgende Bereiche wurden als ausreichend begutachtet:

- Sicherheitsziele
- Konfigurationsmanagement
- Auslieferung und Betrieb der bescheinigten Komponente
- Entwicklung der bescheinigten Komponente
- Handbücher
- Lebenszyklus-Unterstützung
- Tests
- Schwachstellenbewertung

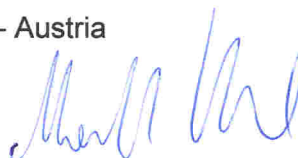
Eine Bewertung der Mechanismenstärke durch die Bestätigungsstelle wurde nicht durchgeführt.

Wien, 3.11.2003

A-SIT Zentrum für sichere Informationstechnologie - Austria



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



Manfred Holzbach
Geschäftsführender Vorstand

Anhang A – Erlaubter Zeichensatz

(eingeschränktes ISO-8859-1)

Zeichen	Hex-Wert
LF	0x0a
CR	0x0d
CR/LF	0x0d0a
Space	0x20
#	0x23
*	0x2a
+	0x2b
,	0x2c
-	0x2d
.	0x2e
/	0x2f
0-9	0x30-0x39
:	0x3a
;	0x3b
A-Z	0x41-0x5a
a-z	0x61-0x7a
Ä	0xc4
Ö	0xd6
Ü	0xdc
ß	0xdf
ä	0xe4
ö	0xf6
ü	0xfc

Hinweis: Die erlaubten Zeichen LF, CR und CR/LF erzeugen im Viewer immer einen einzelnen Zeilenvorschub.