



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: MBS-Sign, MBS Modul zur Erstellung sicherer Signaturen, Version 1.0, Release 2.2

Antragsteller:
BDC EDV Consulting GmbH
Gredlerstraße 4
1020 Wien

1. Beschreibung der bescheinigten Komponente

Der Gegenstand der Bescheinigung ist MBS-Sign – MBS Modul zur Erstellung sicherer Signaturen, Version 1.0, Release 2.2, nachstehend auch das Modul genannt. Hersteller des Moduls ist die BDC EDV Consulting GmbH, Gredlerstraße 4, 1020 Wien.

Das Modul ist eine unter Win32 lauffähige Bibliothek. Es werden folgende Betriebssystemversionen 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 professional, Internet Explorer 6.0

Als Anwendungen des Moduls sind MBS-Applikationen vorgesehen. Diese Applikationen benutzen das Modul, um sichere Signaturen über elektronische Abbildungen des banküblichen Datenträger-Begleitzettels zu erstellen.

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 sind:

Zeichen	Hex-Wert
Linefeed	0x0a,0x0c
Space	0x20
#	0x23
-	0x2d
.	0x2e
:	0x3a
0-9	0x30-0x39
A-Z	0x41-0x5a
a-z	0x61-0x7a

Ä	0xc4
Ö	0xd6
Ü	0xdc
ß	0xdf
ä	0xe4
ö	0xf6
ü	0xfc

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

Gegenstand der Bescheinigung sind die Funktionen des Moduls zur Prüfung des Formats und zur sicheren Anzeige der zu signierenden Daten.

Zusätzlich stellt das Modul folgende Chipkarten-Managementfunktionen zur Verfügung:

- Ändern der Signatur-PIN
- Entsperrn von PINs

Diese Funktionen sind nicht Gegenstand der Bescheinigung.

Es wird folgender CT-API Treiber zum Ansprechen des Chipkartenterminals unterstützt:

- CT-API Treiber für Kobil KAAAN professional, v2001.4.3.1

Es wird folgendes Chipkartenterminal unterstützt:

- Kobil KAAAN professional v2.08 GK v.1.04

Das Chipkartenterminal verfügt über ein integriertes PIN-Pad und ein integriertes Display. Eine Signaturerstellung ist nur möglich, wenn die PIN-Eingabe am PIN-Pad des Terminals durchgeführt wird.

Es werden folgende Signaturkarten unterstützt:

- A-Trust TrustSign v1.2 für sichere Signaturen nach dem Signaturgesetz.
- A-Trust TrustMark v3.12 für einfache Signaturen.

Das Modul wird mit einer gesicherten Konfiguration für die beschriebenen Komponenten ausgeliefert. Jede Erweiterung der zu benutzenden Komponenten erfordert vom Hersteller das Erzeugen einer erweiterten gesicherten Konfiguration.

2. Erfüllung der Anforderungen des SigG und der SigV

MBS-Sign – MBS Modul zur Erstellung sicherer Signaturen, Version 1.0, Release 2.2 erfüllt

- die Anforderung nach §18(2) SigG an technische Komponenten und Verfahren, dass die zu signierenden Daten nicht verändert werden,
- die Anforderung nach §18(2) SigG an technische Komponenten und Verfahren, dass dem Signator die zu signierenden Daten vor Auslösung des Signaturvorgangs dargestellt werden,
- die Anforderung nach §7(2) SigV an technische Komponenten und Verfahren, dass sie die vollständige Anzeige der zu signierenden Daten ermöglichen müssen,
- die Anforderung nach §7(2) SigV, dass für die zu signierenden Daten nur die vom Zertifizierungsdiensteanbieter empfohlenen Formate verwendet werden,
- die Anforderung nach §7(2) SigV, dass die Spezifikation dieser Formate allgemein verfügbar ist,
- die Anforderung nach §7(2) SigV, dass in den zu signierenden Daten dynamische Veränderungen oder unsichtbare Daten ausgeschlossen sind.

Die genannten Anforderungen werden unter den unten genannten Einsatzbedingungen erfüllt.

MBS-Sign – MBS Modul zur Erstellung sicherer Signaturen, Version 1.0, Release 2.2 ist daher in folgender Kategorie bescheinigt:

- Komponenten und Verfahren zur Darstellung der zu signierenden Daten.

3. Gültigkeitsdauer der Bescheinigung

Diese Bescheinigung ist bis 30.6.2004 gültig.

4. Einsatzbedingungen

(1) Chipkartenterminal

Zum Zeitpunkt der Ausstellung der Bescheinigung ist der Betrieb mit folgendem Chipkartenterminal vorgesehen:

- Kobil KAAN professional v2.08 GK v1.04

Das Chipkartenterminal muss direkt am benutzten PC angeschlossen sein und muss sich bei der Signaturerstellung im selben Raum wie der benutzte PC befinden. Der Signator muss sich von der unmittelbaren Verbindung des Chipkartenterminals und des PC vergewissern können, da diese sicherheitsrelevant ist.

(2) Signaturkarte

Zum Zeitpunkt der Ausstellung der Bescheinigung ist der Betrieb mit folgender Signaturkarte vorgesehen:

- A-Trust TrustSign Karte v1.2
(Smart Card mit Chip - Philips Smart Card Controller P8WE5032V0G und Betriebssystem STARCOS SPK 2.3 und Digital Signature Application TrustSign, von A-SIT am 22-10-2001 nach §18(5) SigG bescheinigt)

(3) Einsatzumgebung

Die Verantwortung für die Integrität der Daten bei der Übertragung von der sicheren Anzeige zum Chipkartenterminal liegt nicht im Verantwortungsbereich der bescheinigten Komponente. Die Integrität der Daten ist durch geeignete technische und/oder organisatorische Maßnahmen in der Einsatzumgebung sicherzustellen.

5. Algorithmen und zugehörige Parameter

Die zur Erstellung einer sicheren elektronischen Signatur erforderlichen Algorithmen werden nicht von der bescheinigten Komponente ausgeführt, es werden die Algorithmen der unterstützten Signaturkarte verwendet.

6. Prüfstufe und Mechanismenstärke

MBS-Sign – MBS Modul zur Erstellung sicherer Signaturen, Version 1.0, Release 2.2 wurde im Rahmen der Bescheinigung von 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 herangezogen.

Folgende Bereiche wurden positiv begutachtet:

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


Eine Beurteilung der Mechanismenstärke ist nicht anwendbar.

Wien, 12.4.2002

A-SIT Zentrum für sichere Informationstechnologie - Austria



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



Manfred Holzbach
Geschäftsführender Vorstand