



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

**GUTACHTEN ÜBER DIE EIGNUNG VON PRODUKTEN
FÜR DIE SICHERE SIGNATUR**

MBS Modul zur Erstellung sicherer Signaturen

Version 2.0, Release 1.3 (Linux Edition)

Mit der Änderung der Signaturverordnung durch BGBl. II Nr. 527/2004 vom 30. Dezember 2004 ist eine Bescheinigung nach §18(5) für Signaturprodukte, die der Umgebung der Signaturerstellungseinheit zuzuzählen sind, nicht mehr erforderlich. Dieses Gutachten geht in analoger Weise wie Bescheinigungen für derartige Produkte auf die Eignung für die sichere Signatur ein.

Projektnummer	A-SIT 1.040
Auftraggeber	BDC – EDV Consulting GmbH, 1020 Wien, Gredlerstraße 4/2
Ansprechperson	Dipl. Ing. Helmut Biely Dipl. Ing. Markus Schlatzer
Auftrag erteilt am	05.10.2004
Typenbezeichnung	MBS Modul zu Erstellung sicherer Signaturen, Version 2.0 Release 1.3 (Linux Edition)
Gutachten ausgestellt am	19.05.2005
Vertraulichkeit	Kurzfassung zur Veröffentlichung

Inhalt

1. Zusammenfassung	3
2. Beschreibung des Produktes	3
2.1. Lieferumfang	3
2.2. Technische Einsatzumgebung	3
2.3. Funktionsumfang	4
2.4. Funktionsbeschreibung	4
3. Befundaufnahme	5
3.1. Referenzmuster	5
3.2. Unterlagen	5
3.3. Durchführung der Befundaufnahme	5
4. Gutachten	6
4.1. Eignung für die sichere Signatur	6
4.2. Detailgutachten	6
5. Einsatzbedingungen	7
Anhang A – Erlaubter Zeichensatz	8

1. Zusammenfassung

A-SIT wurde von der BDC EDV Consulting GesmbH (nachstehend BDC genannt) mit der Erstellung eines Gutachtens über die Eignung des Produktes „MBS Modul zur Erstellung sicherer Signaturen, Version 2.0, Release 1.3 (Linux Edition)“ (nachstehend das Modul genannt) für die sichere Signatur beauftragt.

Eine ausführliche Beschreibung des Produktes und seiner Funktion wird in Kapitel 2 gegeben und Kapitel 3 beschreibt die durchgeführten Befundaufnahmen.

Zusammenfassung der gutachterlichen Aussagen:

Wie in Kapitel 4 im Detail ausgeführt, ist das Modul unter den in Kapitel 5 genannten Einsatzbedingungen für die Darstellung der zu signierenden Daten in der Systemumgebung der Signaturerstellungseinheit bei sicheren Signaturen geeignet. Die gutachterlichen Aussagen sind zum Zeitpunkt des Ausstellens des gegenständlichen Gutachtens gültig.

2. Beschreibung des Produktes

Der Gegenstand des Gutachtens ist das „MBS¹ Modul zur Erstellung sicherer Signaturen, Linux Edition“², Version 2.0, Release 1.3.

Das Modul besteht aus einer Programmbibliothek im ELF-Format³, die MBS-Applikationen Funktionen zur Darstellung und zur Bereitstellung der zu signierenden Daten zur Verfügung stellt. Zusätzlich stellt das Modul Funktionen zum Ändern und zum Entsperren einer Signatur-PIN zur Verfügung (diese beiden Funktionen sind nicht Gegenstand dieses Gutachtens).

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

2.1. Lieferumfang

Die Auslieferung an den Endkunden erfolgt

- direkt vom Hersteller auf einem Read-Only Datenträger (CD),
- per Datei-Download über HTTPS von einem authentifizierten Server des Herstellers mit Benutzerzugriffskontrolle (Download-Portal).

Zum Lieferumfang gehören eine Archivdatei⁴ (im Format tar.gz), diese enthält das Setupprogramm und alle anderen benötigten Dateien, ein Benutzerhandbuch und ein Entwicklerhandbuch für Entwickler von MBS-Applikationen.

Das Modul wird mit einer Konfiguration für die nachfolgend beschriebenen Komponenten ausgeliefert. Eine Erweiterung oder Änderung der zu benutzenden Komponenten kann durch eine Konfigurationsänderung⁵ durch den Hersteller durchgeführt werden. Module mit einer geänderten Konfiguration sind nicht Gegenstand dieses Gutachtens.

2.2. Technische Einsatzumgebung

Das Modul ist für den Gebrauch im privaten Bereich und in normalen Büroumgebungen vorgesehen, wobei der Benutzer die Integrität der verwendeten Hard- und Software sicherstellen muss. Es werden folgende Betriebssysteme unterstützt (lt. Angabe des Herstellers):

¹ MBS = Multi Bank Standard

² Produktbezeichnung des Herstellers

³ Standard Format für Binär-Code auf Unix-Betriebssystemen

⁴ mbsinstall_ben_v203.tar.gz bzw. mbsinstall_ent_v203.tar.gz

⁵ Eine Übertragung der Aussagen des Gutachtens auf eine erweiterte Konfiguration ist in Einzelfällen möglich, A-SIT gibt hierüber in Abstimmung mit dem Hersteller des Moduls Auskunft.

- Fedora Core #2
(linux kernel 2.6.5, XFree86-4.3, KDE-3.1, GNOME-2.4, gtk-1.2.10),
- Suse Linux Version 9.1
(linux kernel 2.6.4, XFree86-4.3, KDE-3.2, GNOME-2.4, gtk-1.2.10),
- Suse Linux Version 9.2
(linux kernel 2.6.8, KDE-3.3, GNOME-2.6, gtk-1.2.10)

Das Modul benötigt zumindest folgende Hardware: PC ab Intel Pentium III/AMDK6 500 MHz, 128 MB RAM, 20 MB freier Festplattenspeicher mit einer Bildschirmauflösung zwischen 800x600 und 1280x1024.

Für die Installation der MBS-Java Komponenten 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.

Folgende Chipkartenterminals werden unterstützt (lt. Angabe des Herstellers):

- KOBIL KAAAN professional, v2.08 GK v1.04, für die serielle Schnittstelle
- REINER SCT cyberJack® e-com 2.0, USB-Version
- REINER SCT cyberJack® pinpad (Product-ID 0x100 und Product-ID 0x300), jeweils USB-Version

Zum Ansprechen des Chipkartenterminals wird ausschließlich CT-API verwendet, ein passender funktionsfähiger Treiber des Herstellers muss installiert sein.

Folgende Signaturkarten werden unterstützt (lt. Angabe des Herstellers):

- A-Trust trust|mark
- A-Trust trust|sign
- a-sign Premium⁶
- Bankkarte - Österreichische Maestro-Karte mit Signaturfunktion (mit 192bit ECC Schlüsselpaar)⁷

2.3. Funktionsumfang

Folgende Funktion des Moduls ist für dieses Gutachten relevant:

- **Secure Viewer:** Diese Funktion prüft das Format der zu signierenden Daten und stellt diese nach erfolgreicher Prüfung dar.

Zusätzlich stellt das Modul folgende Funktionen zur Verfügung:

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

Diese beiden Funktionen sind nicht Gegenstand dieses Gutachtens.

2.4. Funktionsbeschreibung

Das Modul prüft das Format der zu signierenden Daten und stellt diese nach erfolgreicher Prüfung mittels eines integrierten „Secure Viewers“ dar. 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

⁶ "a.sign Premium Variante 2" lt. "a.trust Empfehlungen für die Erstellung sicherer Signaturen", abgerufen unter http://www.a-trust.at/docs/verfahren/a-sign-premium/sec_Verfahren.pdf am 07.02.2005

⁷ "a.sign Premium Variante 1" lt. "a.trust Empfehlungen für die Erstellung sicherer Signaturen", abgerufen unter http://www.a-trust.at/docs/verfahren/a-sign-premium/sec_Verfahren.pdf am 07.02.2005

eventuell aufgetretene Fehler während des Signaturvorganges sind von der aufrufenden Applikation durchzuführen.

Anzeigeeinschränkungen:

- Die Länge der im zu signierenden Dokument enthaltenen Textzeilen darf 1024 Zeichen nicht überschreiten. Andernfalls wird das Dokument nicht angezeigt und kann nicht signiert werden.

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 dieses Gutachtens.

3. Befundaufnahme

Der Hersteller des Moduls hat das Referenzmuster und die erforderlichen Unterlagen zur Begutachtung eingereicht.

3.1. Referenzmuster

Der Hersteller hat die

- Benutzerversion
- Entwicklerversion
- Testprogramme

zur Begutachtung bereitgestellt.

3.2. Unterlagen

Der Hersteller hat folgende Dokumente zur Begutachtung bereitgestellt:

- „Deckblatt“
- „Sicherheitskonzept“ (enthält die Sicherheitsziele, funktionale Spezifikation, den Entwurf auf hoher Ebene und Schwachstellenanalyse des Herstellers)
- „Benutzerhandbuch“
- „Entwicklerhandbuch“
- „Java-Entwicklerhandbuch“
- „Informationen über die Sicherheit der Entwicklungsumgebung“
- „Testdokumentation“
- „MBS Erweiterungen - Änderungen“

3.3. Durchführung der Befundaufnahme

Die Befundaufnahme wurde im Rahmen des Gutachtens von A-SIT durchgeführt. 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 begutachtet:

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

Eine Bewertung der Mechanismenstärke wurde nicht durchgeführt.

4. Gutachten

4.1. Eignung für die sichere Signatur

Das Modul überprüft, ob die zu signierenden Daten dem in „Anhang A – Erlaubter Zeichensatz“ spezifizierten Format entsprechen und ermöglicht, dass dem Signator die zu signierenden Daten vor Auslösung des Signaturvorganges dargestellt werden. Im verwendeten Format können keine dynamischen Veränderungen codiert werden.

Das Modul ist damit unter nachstehenden Einsatzbedingungen für die Darstellung der zu signierenden Daten in der Systemumgebung der Signaturerstellungseinheit bei sicheren Signaturen geeignet.

Das gegenständliche Gutachten stellt eine Momentaufnahme unter Berücksichtigung des aktuellen Standes der Technik zum Zeitpunkt der Ausstellung dar. Die Aussagen sind daher zum Zeitpunkt der Ausstellung bei Berücksichtigung aller in Kapitel 5 genannten Einsatzbedingungen gültig.

4.2. Detailgutachten


Hinweis: Dieses Kapitel ist in der ggf. auf der A-SIT-Website veröffentlichten Fassung nicht enthalten.

5. 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.
- (2) Für einen sicheren Betrieb ist es erforderlich, dass die Empfehlungen der Benutzerdokumentation eingehalten und die Anforderungen an die Einsatzumgebung beachtet werden.
- (3) Zur Erzeugung der sicheren elektronischen Signatur sind ausschließlich sichere Signaturerstellungseinheiten zu verwenden, welche die Anforderungen von SigG und SigV erfüllen.
- (4) Zur Verbindung des Moduls mit der Signaturerstellungseinheit ist ein Chipkartenterminal zu verwenden, das die Anforderungen von SigG und SigV erfüllt und vom Modul unterstützt wird. Die Verantwortung für die Integrität der Daten bei der Übertragung zum Chipkartenterminal liegt nicht im Verantwortungsbereich der begutachteten Komponente. Die Integrität der Daten ist durch geeignete technische und/oder organisatorische Maßnahmen in der Einsatzumgebung 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.
- (5) Das verwendete Format zur Darstellung des Inhaltes der zu signierenden Daten (siehe Anhang A – Erlaubter Zeichensatz) muss vom Zertifizierungsdiensteanbieter empfohlen sein.

Wien, 19.05.2005

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. Die Sequenz LFCRCRLF erzeugt beispielsweise drei leere Zeilen