



**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

DVR: 1035461

ZVR: 948166612

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

MBS Client

Version 2.0 R 1.5.2

Mit der Änderung der Signaturverordnung durch BGBl. II Nr. 527/2004 vom 30. Dezember 2004 ist eine Bescheinigung nach § 18 Abs. 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 qualifizierte Signatur ein.

Projektnummer	A-SIT 1.081
Auftraggeber	STUZZA Studiengesellschaft für Zusammenarbeit im Zahlungsverkehr GmbH
Ansprechperson	DI Helmut Biely
Auftrag erteilt am	16.02.2009
Typenbezeichnung	MBS Modul 2.0 R 1.5.2
Gutachten ausgestellt am	12.10.2009
Vertraulichkeit	Kurzfassung zur Veröffentlichung



Akkreditierte Inspektionsstelle

© A-SIT, Partner für Sicherheitsfragen

Inhalt

Inhalt	2
1. Auftrag	3
2. Zusammenfassung	3
3. Beschreibung des Produkts	3
3.1. Lieferumfang	3
3.2. Technische Einsatzumgebung	4
3.3. Funktionsumfang	4
3.4. Funktionsbeschreibung	5
4. Befunde	5
4.1. Referenzmuster	5
4.2. Unterlagen	5
4.3. Durchführung der Befundaufnahme	6
5. Gutachten	6
5.1. Eignung für die qualifizierte Signatur	6
5.2. Detailgutachten	6
6. Einsatzbedingungen	6
7. Unterschriften	8
Anhang A – Erlaubter Zeichensatz	9

1. Auftrag

Der Auftrag umfasst ein Gutachten des MBS Client V.2.0 R.1.5.2 über die Eignung für die qualifizierte Signatur. Die Schwerpunkte der Begutachtung liegen auf den neu hinzugekommenen Funktionalitäten und Schnittstellen wie z.B. Unterstützung der E-Card, der neuen ACOS Karte oder der Terminalserver-Variante. Bei den bereits früher begutachteten Teilen wird auf allfällige Veränderungen und Auswirkungen der Neuerungen geachtet.

Programm und Dokumentation wurden vom Hersteller BDC direkt bezogen.

2. Zusammenfassung

A-SIT wurde von der BDC.EDV-Consulting GmbH (nachstehend BDC genannt) mit der Erstellung eines Gutachtens über die Eignung des Produktes „MBS Modul, Version 2.0 Release 1.5.2“ (nachstehend das Modul genannt) für die qualifizierte Signatur beauftragt.

Eine ausführliche Beschreibung des Produktes und seiner Funktion wird in Kapitel 3 gegeben und Kapitel 4 beschreibt die durchgeführten Befundaufnahmen.

Zusammenfassung der gutachterlichen Aussagen:

Wie in Kapitel 5 im Detail ausgeführt, ist das Modul unter den in Kapitel 6 genannten Einsatzbedingungen für die Darstellung der zu signierenden Daten in der Systemumgebung der Signaturerstellungseinheit bei qualifizierten Signaturen geeignet. Die gutachterlichen Aussagen sind zum Zeitpunkt des Ausstellens des gegenständlichen Gutachtens gültig.

3. Beschreibung des Produkts

Der Gegenstand des Gutachtens ist das MBS¹ Modul Version 2.0, Release 1.5.2, welches zur Anzeige der zu signierenden Daten vor der Erstellung qualifizierter Signaturen unter Verwendung geeigneter sicherer Signaturerstellungseinheiten dient.

Das Modul besteht aus einer Win32 Programmbibliothek (Dynamic Link Librarys), 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

3.1. Lieferumfang

Die Auslieferung an den Endkunden erfolgt

- direkt vom Hersteller auf einem Read-Only Datenträger (CD-ROM)
- per Datei-Download über HTTP von der Website des Herstellers

Den Lieferumfang bildet das Setupprogramm [1081_16] welches auch das Benutzerhandbuch für Endbenutzer bzw. ein Entwicklerhandbuch für Entwickler von MBS-Applikationen enthält. Das Modul wird mit einer durch eine elektronische Signatur authentifizierten Konfiguration für die nachfolgenden beschriebenen Komponenten ausgeliefert. Eine Erweiterung oder Änderung der zu benutzenden Komponenten erfordert vom Hersteller das Erzeugen einer erweiterten authentifizierten Konfiguration². Module mit einer geänderten Konfiguration sind nicht Gegenstand dieses Gutachtens.

¹ MBS = Multi Bank Standard

² 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.

3.2. Technische Einsatzumgebung

Das Modul ist für den Gebrauch im privaten Bereich und in normalen Büroumgebungen vorgesehen, wobei die Integrität der verwendeten Hard- und Software durch den Benutzer sichergestellt werden muss. Im Betriebsmodus „Terminal-Server“ muss der jeweilige Systemadministrator die Integrität der genannten Komponenten sicherstellen.

Es werden folgende Versionen des Microsoft Windows Betriebssystem und des Browser unterstützt (lt. Angaben des Herstellers):

- Windows 2000 Professional, Service Pack 2+, Inter Explorer 6.0
- Windows XP Home / Professional, Internet Explorer 6.0
- Windows VISTA (alle Editionen)
- Windows 7 (alle Editionen)
- Windows Terminal Server 2003 bzw. 2008 bzw. 2008 SP2
- Citrix Presentation Server (basierend auf Windows Terminal Server)

Das Modul benötigt mindestens folgende Hardware:

- Intel Pentium III/AMD K6 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 Chipkartenlesers.

Folgende Chipkartenleser werden unterstützt (lt. Angaben des Herstellers):

- KOBIL KAN professional
- KOBIL KAN advanced
- REINER SCT cyberJack e-com
- REINER SCT cyberJack KB
- REINER SCT cyberJack PinPad
- SCM SPR 532
- Cherry Smardboards (G83-6700LQZ, G81-8015LQZ, G83-6744LBZ, G83-6744LUZ)
- Omnikey Cardman 3621 /3821

Im Terminal-Server Betrieb unterstützt das MBS-Modul grundsätzlich alle Kartenlesegeräte, die den PC/SC-Standards 1 und 2 entsprechen. Mit anderen als den obig genannten Geräten wurden jedoch von Seiten des Herstellers keine Tests durchgeführt.

Zum Ansprechen des Chipkartenlesers wird ausschließlich die CT-API bzw. PC/SC verwendet. Die verwendete Schnittstelle ist abhängig von der Einsatzumgebung. Bei der Verwendung des MBS-Moduls am Arbeitsplatzrechner wird CT-API verwendet, während im Terminal-Server Betrieb PC/SC verwendet wird.

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

- a-Trust TrustSign
- a-sign Premium mit Starcos Betriebssystem
- a-sign Premium mit ACOS Betriebssystem
- Bankkarte (Maestro / Mastercard mit Signaturfunktion)
- eCard

3.3. 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:

- Änderung der Signatur-PIN
- Entsperrn der Singatur-PIN und Geheimhaltungs-PIN

Diese beiden Funktionen sind nicht Gegenstand dieses Gutachtens.

3.4. Funktionsbeschreibung

Das Modul prüft das Format der zu signierenden Daten und stellt diese nach erfolgreicher Prüfung mittels eines integrierten „Secure Viewers“ dar. Der erlaute 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 Chipkartenleser. Die Bereitstellung des zu signierenden Dokuments sowie die Anzeige der Information für den Signator über eventuell aufgetretene Fehler während es Signaturvorganges ist von der aufrufenden Applikation durchzuführen.

Die Ausführung des Moduls kann lokal oder in einer Terminal-Server Variante erfolgen. Im Gegensatz zur lokalen Variante liegen bei der Terminal-Server Variante Daten und Modul nicht beim Client, sondern auf einem dafür vorgesehen Terminal-Server. Die zu signierenden Daten werden über eine Terminal-Client Verbindung via PC/SC - Schnittstelle vom Server an den Chipkartenleser des Clients zur Signatur geschickt und danach am Server weiter verarbeitet.

Lokale Variante und Terminal-Server Variante unterscheiden sich bzgl. Architektur oder Sicherheitsfunktionen des Moduls nicht.

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.

4. Befunde

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

4.1. Referenzmuster

Der Hersteller hat die

- Benutzerversion [1081_16]
- Terminal-Server-Version [1081_11] sowie die
- Entwicklerversion [1081_09]

zur Begutachtung bereitgestellt.

4.2. Unterlagen

Der Hersteller hat folgende Dokumente zur Begutachtung bereitgestellt:

- „Deckblatt“ [1081_15]
- „Sicherheitskonzept“ (enthält die Sicherheitsziele, funktionale Spezifikation und den Entwurf auf hoher Ebene und Schwachstellenanalyse des Herstellers) [1081_20]
- „Benutzerhandbuch“ [1081_19]
- „Entwicklerhandbuch“ [1081_12]
- „Java-Entwicklerhandbuch“ [1081_18]
- „Testbericht“ [1081_06]
- Logfiles der Tests [1081_08]

4.3. 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.

5. Gutachten

5.1. Eignung für die qualifizierte 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 qualifizierten 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 alle in Kapitel 6 genannten Einsatzbedingungen gültig.

5.2. Detailgutachten

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


6. 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 Hard- 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 qualifizierten elektronischen Signatur sind ausschließlich sichere Signaturerstellungseinheiten zu verwenden, welche die Anforderungen von SigG und SigV erfüllen.
- (4) Die Verantwortung für die Integrität der Daten bei der Übertragung zum zur Verbindung des Rechners mit der Signaturerstellungseinheit verwendeten Chipkartenlesers liegt nicht im Verantwortungsbereich der begutachteten Komponenten. Die Integrität der Daten ist durch geeignete technische und/oder

organisatorische Maßnahmen in der Einsatzumgebung sicherzustellen. Der Signator muss sich von der unmittelbaren und sicheren Verbindung des Chipkartenlesers mit dem Arbeitsplatzrechner vergewissern können.

7. Unterschriften

A-SIT Zentrum für sichere Informationstechnologie – Austria

Signaturwert	lriVzy5vOrrT5GqFyglOMy+yO/Of0PvaYDlEkSPmTrbYBY38uHNsPXateG8Y0vis	
	Unterzeichner	Manfred Holzbach, geschäftsführender Vorstand
	Datum/Zeit-UTC	2009-10-12T11:35:08Z
	Aussteller-Zertifikat	CN=a-sign-Premium-Sig-02,OU=a-sign-Premium-Sig-02,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Serien-Nr.	261828
	Methode	urn:pdfsigfilter:bka.gv.at:text:v1.1.0
	Parameter	etsi-bka-1.0@1255347308-20458140@14887-31581-0-10997-23945
Prüfhinweis	Prüfservice: https://www.buergerkarte.at/signature-verification/	

Signaturwert	yEDkzFZc7i5CG16hGtFu5KelaPpaavdY98cvLYGgqlBR37iQzNIaInCvjEuIIQ0	
	Unterzeichner	Prof. Dr. Reinhard Posch, Wissenschaftlicher Gesamtleiter
	Datum/Zeit-UTC	2009-10-13T08:44:17Z
	Aussteller-Zertifikat	CN=a-sign-Premium-Sig-02,OU=a-sign-Premium-Sig-02,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Serien-Nr.	221297
	Methode	urn:pdfsigfilter:bka.gv.at:text:v1.1.0
	Parameter	etsi-bka-1.0@1255423457-297487@19-25593-0-32029-8506
Prüfhinweis	Prüfservice: https://www.buergerkarte.at/signature-verification/	

Anhang A – Erlaubter Zeichensatz

(eingeschränktes ISO-8859-1)

Zeichen	Hex-Wert
LF	0x0a
CR	0x0d
CR/LF	0x0d0a
*	0x2a
Ü	0x2b
,	0x2c
SPACE	0x20
Ä	0x23
-	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

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