



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 (für Windows)

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	1.051
Auftraggeber	BDC EDV Consulting GesmbH, Gredlerstraße 4/2 1020 Wien
Ansprechperson	DI Helmut Biely, helmut.biely@bdc.at , +43 (664) 9012053
Auftrag erteilt am	05.10.2004
Typenbezeichnung	MBS Modul zur Erstellung sicherer Signaturen, Version 2.0, Release 1.3
Gutachten ausgestellt am	25.04.2005

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	6
6.	Unterlagen	7
	Anhang A – Erlaubter Zeichensatz	9
	Anhang B – Sektionen und Parameter der signierten Konfigurationsdatei	10

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“ (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“², Version 2.0, Release 1.3.

Das Modul besteht aus einer Win32³ Programmbibliothek, 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 (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) oder
- per Datei-Download über HTTPS von einem authentifizierten Server des Herstellers mit Benutzerzugriffskontrolle (Download-Portal).

Den Lieferumfang bildet das Setupprogramm [1051_29] bzw. [1051_30] welches auch das Benutzerhandbuch für Endbenutzer bzw. ein Entwicklerhandbuch für Entwickler von MBS-Applikationen enthält.

Das Modul wird mit einer durch eine elektronische Signatur authentifizierten⁴ Konfiguration für die nachfolgend beschriebenen Komponenten ausgeliefert. Eine Erweiterung oder Änderung der zu benutzenden Komponenten erfordert vom Hersteller das Erzeugen einer erweiterten authentifizierten Konfiguration⁵. 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 die Integrität der verwendeten Hard- und Software durch den Benutzer sichergestellt werden muss. Es werden folgende Versionen des Microsoft Windows Betriebssystems und des Browsers unterstützt (lt. Angabe des Herstellers):

- Microsoft Windows 98 SE, Internet Explorer 6.0

¹ MBS = Multi Bank Standard

² Produktbezeichnung des Herstellers

³ Microsoft® 32bit Windows™ API

⁴ 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.

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.

- 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: IBM kompatibler PC, 500 MHz CPU, 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.

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

- KOBIL KAAAN Professional, v2.08 GK v1.04
- KOBIL KAAAN Standard Plus
- REINER SCT cyberJack™ e-com, v2.0
- REINER SCT cyberJack™ KB
- REINER SCT cyberJack™ Pinpad, v2.0, v3.0
- SCM SPR 532
- Cherry Smartboards (G83-6700LQZ, G81-8015LQZ, G83-6744 LBZ, G83-6744 LUZ)

Zum Ansprechen des Chipkartenterminals wird ausschließlich die CT-API verwendet.

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 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 dieses Gutachtens.

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

3. Befundaufnahme

Der Hersteller des Moduls hat das Referenzmuster und die erforderlichen Unterlagen zur Begutachtung eingereicht. Details sind der Referenzliste in Kapitel 6 zu entnehmen.

3.1. Referenzmuster

Der Hersteller hat die

- Benutzerversion [1051_29] sowie die
- Entwicklerversion [1051_30]
- Benutzerversion mit aktiviertem Logging für Testzwecke [1051_29], [1051_27]
- Entwicklerversion mit aktiviertem Logging für Testszwecke [1051_30], [1051_27]
- Testprogramme (in [1051_11] enthalten)

zur Begutachtung bereitgestellt.

3.2. Unterlagen

Der Hersteller hat folgende Dokumente zur Begutachtung bereitgestellt:

- „Deckblatt“ [1051_18]
- „Sicherheitskonzept“ (enthält die Sicherheitsziele, funktionale Spezifikation und den Entwurf auf hoher Ebene und Schwachstellenanalyse des Herstellers) [1051_20]
- „Benutzerhandbuch [1051_28]
- „Entwicklerhandbuch [1051_22]
- „Java-Entwicklerhandbuch [1051_23]
- „Informationen über die Sicherheit der Entwicklungsumgebung“ [1051_03]
- „Sicherheitskonzept / Testfälle der Java Version“ [1051_19]
- „Testbericht“ und Logfiles der Tests [1051_13], [1051_14], [1051_15]
- „MBS V2-R3 Erweiterungen“ [1051_16]

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

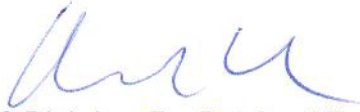
- (1) Die vorgesehene Einsatzumgebung des Moduls sind Arbeitsplatzrechner im Büro- oder Heimbereich. Der Zugang zum verwendeten Rechner kann vom Signator kontrolliert werden. Manipulationen an der Hardware und Software des Rechners, auf dem das Modul installiert ist, sind zu verhindern. Es ist sicherzustellen, 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.

6. Unterlagen

Interne Bez.	Erhalten am	Typ	Titel, Version	Status
1051_00	2005-04-21	elektronisch	Statusblatt	Endgültig
1051_01	2005-10-08	Papier	Antrag	Endgültig
1051_02	2004-11-24	elektronisch	MBS Deckblatt v1.2.pdf	Ungültig (ersetzt durch 1051_18)
1051_03	2004-11-24	elektronisch	MBS Entwicklungsumgebung v0.2.2.pdf	Endgültig
1051_04	2004-11-24	elektronisch	MBS Java Sicherheit, Testfälle v0.3.pdf	Ungültig (ersetzt durch 1051_19)
1051_05	2004-11-24	elektronisch	MBS Sicherheitskonzept v1.4.pdf	Ungültig (ersetzt durch 1051_20)
1051_06	2004-11-24	elektronisch	MBS-Benutzerhandbuch v1.1.pdf	Ungültig (ersetzt durch 1051_21)
1051_07	2004-11-24	elektronisch	MBS-Entwicklungshandbuch v1.4.2.pdf	Ungültig (ersetzt durch 1051_22)
1051_08	2004-11-24	elektronisch	MBS-Java-Entwicklungshandbuch v0.6.pdf	Ungültig (ersetzt durch 1051_23)
1051_09	2004-11-24	elektronisch	Referenzmuster Benutzer (MBS_Setup_2.0_R1.3_Ben.exe)	Ungültig (ersetzt durch 1051_25)
1051_10	2004-11-24	elektronisch	Referenzmuster Benutzer, Logging aktiviert, (MBS_Setup_2.0_R1.3_Ben_Logging.exe)	Ungültig (ersetzt durch 1051_25 und 1051_27)
1051_11	2004-11-24	elektronisch	Referenzmuster Entwickler (MBS_Setup_2.0_R1.3_Ent.exe)	Ungültig (ersetzt durch 1051_26)
1051_12	2004-11-24	elektronisch	Referenzmuster Entwickler, Logging aktiviert, (MBS_Setup_2.0_R1.3_Ent_Logging.exe)	Ungültig (ersetzt durch 1051_26 und 1051_27)
1051_13	2004-11-24	elektronisch	MBS Test v0.5.pdf	Endgültig
1051_14	2004-11-24	elektronisch	Logfile des Tests, KOBIL (mbscsp20_kobil_firmware.log)	Endgültig
1051_15	2004-11-24	elektronisch	Logfile des Tests, Speicherimage (mbscsp20_Module_speicherimage_tampered.log)	Endgültig
1051_16	2004-09-29	elektronisch	Änderungen von V2.0 auf Release 1.3 (MBS V2-R3 Erweiterung.doc)	Endgültig
1051_17	2005-03-15	elektronisch	Antwort zu den Kommentaren von ASit vom 2005-02-24anBDC.doc	Endgültig
1051_18	2005-03-15	elektronisch	MBS Deckblatt v1.3.pdf	Endgültig
1051_19	2005-03-15	elektronisch	MBS Java Sicherheit, Testfälle v0.4.pdf	Endgültig
1051_20	2005-03-15	elektronisch	MBS Sicherheitskonzept v1.5.pdf	Endgültig
1051_21	2005-03-15	elektronisch	MBS-Benutzerhandbuch v1.2.pdf	Ungültig (ersetzt durch 1051_28)
1051_22	2005-03-15	elektronisch	MBS-Entwicklungshandbuch v1.4.3.pdf	Endgültig
1051_23	2005-03-15	elektronisch	MBS-Java-Entwicklungshandbuch v0.7.pdf	Endgültig
1051_24	2005-03-15	elektronisch	Umwandlung in gleichwertiges Gutachten (Fw_Stellungnahme_Bescheinigungen - Gutachten - Information für Hersteller von Komponenten zur sicheren elektronischen Signatur.eml)	Endgültig
1051_25	2005-03-22	elektronisch	Referenzmuster Benutzer (MBS_Setup_2.0_R1.3_Ben.exe)	Ungültig (ersetzt durch 1051_29)
1051_26	2005-03-22	elektronisch	Referenzmuster Entwickler (MBS_Setup_2.0_R1.3_Ent.exe)	Ungültig (ersetzt durch 1051_30)
1051_27	2005-03-22	elektronisch	Konfigurationsdateien (esw-Dateien) mit aktiviertem Logging (logging_esws.zip)	Endgültig
1051_28	2005-03-29	elektronisch	MBS Benutzerhandbuch Version 1.2.1	Endgültig
1051_29	2005-04-07	elektronisch	Referenzmuster Benutzer (MBS_Setup_2.0_R1.3_Ben.exe)	Endgültig
1051_30	2005-04-07	elektronisch	Referenzmuster Entwickler (MBS_Setup_2.0_R1.3_Ent.exe)	Endgültig

Wien, 25.04.2005

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.

Anhang B – Sektionen und Parameter der signierten Konfigurationsdatei

- Beschreibung KOBIL KAAN professional. Diese Sektion enthält folgende Parameter, die zur Authentifizierung des KOBIL KAAN professional Chipkartenterminals benötigt werden:
 - Name: file:beschreibung kobil kaan professional
 - SectionName: KOBIL KAAN professional
 - Digest-Algorithms: SHA-1
 - SHA-1-Digest: 2jmj7I5rSw0yVb/vIWAYkK/YBwk=
 - MAGIC: UsesMetadata
 - Port0: 1
 - isSecure: Yes
 - ctapi: CT-API KOBIL Systems
 - UseGUI: Yes
 - Status0: 4445787878435433393956322e3038

Hinweis: Im Installationspaket ist jeweils eine Datei für Port 1 und 2 enthalten

- Beschreibung KOBIL KAAN Standard plus. Diese Sektion enthält folgende Parameter, die zur Authentifizierung des KOBIL KAAN Standard plus Chipkartenterminals benötigt werden:
 - Name: file:beschreibung kobil kaan standard plus
 - SectionName: KOBIL KAAN Standard plus
 - Digest-Algorithms: SHA-1
 - SHA-1-Digest: 2jmj7I5rSw0yVb/vIWAYkK/YBwk=
 - MAGIC: UsesMetadata
 - Port0: 1
 - isSecure: Yes
 - ctapi: CT-API KOBIL Systems
 - UseGUI: Yes
 - Status0: 4445787878435431393856312e3631
 - Status1: 4445787878435431303156312e3730

Im Installationspaket ist jeweils eine Datei für Port 1 und 2 enthalten.

- Beschreibung Reiner SCT cyberJack e-com. Diese Sektion enthält folgende Parameter, die zur Authentifizierung des Reiner SCT cyberJack e-com Chipkartenterminals benötigt werden:
 - Name: file:beschreibung cyberjack e-com
 - SectionName: cyberJack e-com
 - Digest-Algorithms: SHA-1
 - SHA-1-Digest: 2jmj7I5rSw0yVb/vIWAYkK/YBwk=
 - MAGIC: UsesMetadata
 - Port0: 1
 - isSecure: Yes
 - UseGUI: No
 - Status0: 444553435445435553422056322e30
 - Status1: 444553435445434c50542056322e30
 - ctapi: CT-API REINER SCT

Im Installationspaket ist jeweils eine Datei für Port 1 und 2 enthalten.

- Beschreibung Reiner SCT cyberJack PinPad. Diese Sektion enthält folgende Parameter, die zur Authentifizierung des Reiner SCT cyberJack PinPad Chipkartenterminals benötigt werden:
 - Name: file:beschreibung cyberjack pinpad
 - SectionName: cyberJack PinPad
 - Digest-Algorithms: SHA-1
 - SHA-1-Digest: 2jmj7I5rSw0yVb/vIWAYkK/YBwk=
 - MAGIC: UsesMetadata
 - Port0: 1
 - isSecure: Yes
 - Deckblatt – MBS Modul zur Erstellung

- ctapi: CT-API REINER SCT
- UseGUI: No
- Status0: 444553435450505553422056322e30
- Status1: 444553435450504c50542056322e30
- Status2: 4445534354434a5050412056332e30

Im Installationspaket ist jeweils eine Datei für Port 1 und 2 enthalten.

- Beschreibung Reiner SCT cyberJack KB. Diese Sektion enthält folgende Parameter, die zur Authentifizierung des Reiner SCT cyberJack KB Chipkartenterminals benötigt werden:
 - Name: file:beschreibung cyberjack kb
 - SectionName: cyberJack KB
 - Digest-Algorithms: SHA-1
 - SHA-1-Digest: 2jmj7I5rSw0yVb/vIWAYkK/YBwk=
 - MAGIC: UsesMetadata
 - Port0: 1
 - ctapi: CT-API REINER SCT
 - UseGUI: No
 - Status0: 4445534354202020202056332e3520
 - isSecure: Yes

Im Installationspaket ist jeweils eine Datei für Port 1 und 2 enthalten.

- Beschreibung SCM SPR 532. Diese Sektion enthält folgende Parameter, die zur Authentifizierung des SCM SPR 532 Chipkartenterminals benötigt werden:
 - Name: file:beschreibung scm spr 532
 - SectionName: SCM SPR 532
 - Digest-Algorithms: SHA-1
 - SHA-1-Digest: 2jmj7I5rSw0yVb/vIWAYkK/YBwk=
 - MAGIC: UsesMetadata
 - Port0: 1
 - isSecure: Yes
 - ctapi: CT-API SCM
 - UseGUI: No
 - Status0: 444553434d535052783346342e3135

Im Installationspaket ist jeweils eine Datei für Port 1 und 2 enthalten.

- Beschreibung Cherry Smartboards. Diese Sektion enthält folgende Parameter, die zur Authentifizierung der Cherry Smartboards benötigt werden:
 - Name: file:beschreibung cherry g83-6700lqzde-0
 - SectionName: Cherry G83 6700LQZDE-0
 - Digest-Algorithms: SHA-1
 - SHA-1-Digest: 2jmj7I5rSw0yVb/vIWAYkK/YBwk=
 - MAGIC: UsesMetadata
 - Port0: 1
 - isSecure: Yes
 - Status0: 444543594d50432f53430000000000
 - UseGUI: No
 - ctapi: CT-API Cherry

Im Installationspaket ist jeweils eine Datei für Port 1 und 2 enthalten.

- Beschreibung MBS-Modul für Kobil KAAAN professional. Diese Sektion enthält folgende Parameter, die zur Authentifizierung und zur Konfigurierung des Moduls benötigt werden:
 - Name: executable:mbscsp20.dll
 - SectionName: mbscsp20
 - Digest-Algorithms: SHA-1
 - SHA-1-Digest: 47aXnX0BKuvJcWMGyUb3mERZ3mY=
 - MAGIC: UsesMetadata
 - Reader0: KOBIL KAAAN professional
 - AllowedOS: Win9x;2000;ME;XP;NT

- Logging: Disabled
- TrustSign0: 07+UAIEx/mVFTFUgQXVzdHJpYSAxLjI4
- TrustMark0: 07+UAIEx/mVFTFUgQXVzdHJpYSAxLjE7
- BankCard0: 078RAIEx/kVFUEE=
- Beschreibung MBS-Modul für Kobil KAA Standard plus. Diese Sektion enthält folgende Parameter, die zur Authentifizierung und zur Konfigurierung des Moduls benötigt werden:
 - Name: executable:mbscsp20.dll
 - SectionName: mbscsp20
 - Digest-Algorithms: SHA-1
 - SHA-1-Digest: 47aXnX0BKuvJcWMGyUb3mERZ3mY=
 - MAGIC: UsesMetadata
 - Reader0: KOBIL KAA Standard plus
 - AllowedOS: Win9x;2000;ME;XP;NT
 - Logging: Disabled
 - TrustSign0: 07+UAIEx/mVFTFUgQXVzdHJpYSAxLjI4
 - TrustMark0: 07+UAIEx/mVFTFUgQXVzdHJpYSAxLjE7
 - BankCard0: 078RAIEx/kVFUEE=
- Beschreibung MBS-Modul für Reiner SCT cyberJack e-com. Diese Sektion enthält folgende Parameter, die zur Authentifizierung und zur Konfigurierung des Moduls benötigt werden:
 - Name: executable:mbscsp20.dll
 - SectionName: mbscsp20
 - Digest-Algorithms: SHA-1
 - SHA-1-Digest: 47aXnX0BKuvJcWMGyUb3mERZ3mY=
 - MAGIC: UsesMetadata
 - Reader0: cyberJack e-com
 - AllowedOS: Win9x;2000;ME;XP;NT
 - Logging: Disabled
 - TrustSign0: 07+UAIEx/mVFTFUgQXVzdHJpYSAxLjI4
 - TrustMark0: 07+UAIEx/mVFTFUgQXVzdHJpYSAxLjE7
 - BankCard: 078RAIEx/kVFUEE=
- Beschreibung MBS-Modul für Reiner SCT cyberJack PinPad. Diese Sektion enthält folgende Parameter, die zur Authentifizierung und zur Konfigurierung des Moduls benötigt werden:
 - Name: executable:mbscsp20.dll
 - SectionName: mbscsp20
 - Digest-Algorithms: SHA-1
 - SHA-1-Digest: 47aXnX0BKuvJcWMGyUb3mERZ3mY=
 - MAGIC: UsesMetadata
 - Reader0: cyberJack PinPad
 - AllowedOS: Win9x;2000;ME;XP;NT
 - Logging: Disabled
 - TrustSign0: 07+UAIEx/mVFTFUgQXVzdHJpYSAxLjI4
 - TrustMark0: 07+UAIEx/mVFTFUgQXVzdHJpYSAxLjE7
 - BankCard: 078RAIEx/kVFUEE=
- Beschreibung MBS-Modul für Reiner SCT cyberJack KB. Diese Sektion enthält folgende Parameter, die zur Authentifizierung und zur Konfigurierung des Moduls benötigt werden:
 - Name: executable:mbscsp20.dll
 - SectionName: mbscsp20
 - Digest-Algorithms: SHA-1
 - SHA-1-Digest: 47aXnX0BKuvJcWMGyUb3mERZ3mY=
 - MAGIC: UsesMetadata
 - Reader0: cyberJack KB
 - AllowedOS: Win9x;2000;ME;XP;NT
 - Logging: Disabled
 - TrustSign0: 07+UAIEx/mVFTFUgQXVzdHJpYSAxLjI4
 - TrustMark0: 07+UAIEx/mVFTFUgQXVzdHJpYSAxLjE7

- BankCard: O78RAIEx/kVFUEE=
- Beschreibung MBS-Modul für SCM SPR 532. Diese Sektion enthält folgende Parameter, die zur Authentifizierung und zur Konfigurierung des Moduls benötigt werden:
 - Name: executable:mbscsp20.dll
 - SectionName: mbscsp20
 - Digest-Algorithms: SHA-1
 - SHA-1-Digest: 47aXnX0BKuvJcWMGyUb3mERZ3mY=
 - MAGIC: UsesMetadata
 - Reader0: SCM SPR 532
 - AllowedOS: Win9x;2000;ME;XP;NT
 - Logging: Disabled
 - TrustSign0: O7+UAIEx/mVFTFUgQXVzdHJpYSAxLjI4
 - TrustMark0: O7+UAIEx/mVFTFUgQXVzdHJpYSAxLjE7
 - BankCard: O78RAIEx/kVFUEE=
- Beschreibung MBS-Modul für Cherry Smartboards. Diese Sektion enthält folgende Parameter, die zur Authentifizierung und zur Konfigurierung des Moduls benötigt werden:
 - Name: executable:mbscsp20.dll
 - SectionName: mbscsp20
 - Digest-Algorithms: SHA-1
 - SHA-1-Digest: 47aXnX0BKuvJcWMGyUb3mERZ3mY=
 - MAGIC: UsesMetadata
 - Reader0: Cherry G83 6700LQZDE-0
 - AllowedOS: Win9x;2000;ME;XP;NT
 - Logging: Disabled
 - TrustSign0: O7+UAIEx/mVFTFUgQXVzdHJpYSAxLjI4
 - TrustMark0: O7+UAIEx/mVFTFUgQXVzdHJpYSAxLjE7
 - BankCard: O78RAIEx/kVFUEE=