



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 SICHERE SIGNATUR

hotSign

Version 2.0

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 1.069
Auftraggeber	BDC – EDV Consulting GmbH, 1020 Wien, Gredlerstraße 4/2
Ansprechperson	Dipl. Ing. Helmut Biely Ing. Markus Punz
Auftrag erteilt am	31.05.2007
Typenbezeichnung	hotSign 2.0 (17.07.07)
Gutachten ausgestellt am	31.10.2007
Vertraulichkeit	Kurzfassung zur Veröffentlichung

Inhalt

1. Zusammenfassung	3
2. Beschreibung des Produktes	3
2.1. Lieferumfang	3
2.2. Technische Einsatzumgebung	4
2.3. Funktionsumfang	4
2.4. Funktionsbeschreibung	5
3. Befundaufnahme	8
3.1. Referenzmuster	8
3.2. Unterlagen	8
3.3. Durchführung der Befundaufnahme	8
4. Gutachten	8
4.1. Eignung für die sichere Signatur	8
4.2. Detailgutachten	9
5. Einsatzbedingungen	9
6. Unterschriften	10
Anhang A – Zulässige Zeichen und Character-Encodings bei text/plain	11
Anhang B – Zulässige Zeichen und Character-Encodings bei text/xml und text/html	12
Anhang C – XML-Schema zur Validierung von HTML-Daten (BDC HTML Viewer)	14
Anhang D – Zulässige Farben und unzulässige Farbkombination in HTML-Daten	27
Zulässige Farben	27
Unzulässige Farbkombinationen	27
Anhang E - Tabelle aller JPEG-Marker	28
Anhang F – Sektionen und Parameter der signierten Konfigurationsdatei	29

1. Zusammenfassung

A-SIT wurde von der BDC EDV Consulting GmbH (nachstehend BDC genannt) mit der Erstellung eines Gutachtens über die Eignung des Produktes „hotSign 2.0.0“ (nachstehend Signatur-Client 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 der Signatur-Client 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 „hotSign“, Version 2.0.0 vom 17.07.07¹.

Der Signatur-Client ist eine Software, welche es ermöglicht, dass dem Signator die zu signierenden Daten vor Auslösung des Signaturvorganges dargestellt werden, sowie eine Software zur Bereitstellung der zu signierenden Daten.

Weiters enthält das Produkt Funktionen zur Signaturprüfung von elektronisch signierten Dokumenten, zur Identifikation im Rahmen von E-Government Applikationen und zum Ändern und Entsperren der Authentisierungsdaten (PINs). Diese Funktionen sind nicht Gegenstand dieses Gutachtens.

Hersteller des Signatur-Clients 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
- über einen akkreditierten Zertifizierungsdiensteanbieter oder
- per Download über HTTPS von einem authentifizierten Server des Herstellers mit Benutzerzugriffskontrolle (Download-Portal).

Zum Lieferumfang gehören das Installationsprogramm (selbstauführendes Setupprogramm), ein Benutzerhandbuch für Endbenutzer bzw. ein Entwicklerhandbuch für Entwickler von Anwendungen, die auf dem Signatur-Client basieren.

Der Signatur-Client wird mit einer durch eine elektronische Signatur gesicherten² Konfiguration für die nachfolgend beschriebenen Komponenten ausgeliefert. Jede Erweiterung der zu benutzenden Komponenten erfordert vom Hersteller das Erzeugen einer erweiterten gesicherten Konfiguration³.

Signatur-Clients mit einer geänderten Konfiguration sind nicht Gegenstand dieses Gutachtens.

¹ Version und Datum des installierten Signatur-Clients können im Menü unter dem Punkt „Über BDC hot:Sign“ abgefragt werden.

² Der Hersteller signiert die SHA-1 MACs 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.

³ Eine Übertragung der Aussagen des Gutachtens auf eine erweiterte Konfiguration ist in Einzelfällen möglich, A-SIT gibt hierüber in Abstimmung mit dem Hersteller des Signatur-Clients Auskunft.

2.2. Technische Einsatzumgebung

Der Signatur-Client ist eine unter Win32⁴ lauffähige Applikation, und 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 Versionen des Microsoft Windows Betriebssystems und des Browsers unterstützt (lt. Angabe des Herstellers):

- Windows 2000 professional, Service Pack 4+, Internet Explorer 6.0+
- Windows XP Home/Professional, Service Pack 2+, IE 6.0+
- Windows VISTA (alle Editionen), IE 7.0+

Hardwaremindestanforderungen: siehe Mindestanforderungen des entsprechenden Betriebssystems.

Eine Farbtiefe und Bildschirmauflösung von mind. 24 Bit und 800 x 600 wird vom Hersteller empfohlen. Die Farbtiefe von 24 Bit ist erforderlich, falls auch Bilder (im GIF bzw. JPEG - Format) angezeigt und signiert werden sollen.

Zur Erstellung elektronischer Signaturen bedient sich der Signatur-Client einer Signaturkarte und eines Chipkartenterminals.

Folgende Chipkartenterminals werden unterstützt (lt. Angabe des Herstellers⁵):

- KOBIL KAAAN Professional
- KOBIL KAAAN Advanced
- REINER SCT cyberJack® e-com
- REINER SCT cyberJack® KB
- REINER SCT cyberJack® pinpad
- SCM SPR532
- Cherry Smartboards (G83-6700LQZ, G81-8015 LQZ, G83-6744 LBZ, G83-6744 LUZ)
- Gemplus USB SL
- Omnikey Cardman 3621
- Omnikey Cardman 3821
- Fujitsu-Siemens SCR Keyboard

Zum Ansprechen des Chipkartenterminals wird sowohl CT-API als auch PC/SC verwendet, ein passender funktionsfähiger Treiber des jeweiligen Herstellers muss installiert sein.

Es handelt sich dabei um Kartenleser die von A-Trust für die Erstellung von sicheren Signaturen empfohlen sind. Darüber hinausgehend werden auch PC/SC-Kartenleser unterstützt, die nicht explizit für die Verwendung von hotSign freigegeben und vom Hersteller getestet wurden. Der Anwender wird im Rahmen der Installation darauf hingewiesen.

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

- a-sign Premium⁶ (STARCOS SPK 2.3, ACOS-EMVA03)
- eCard (STARCOS 3.1 ECC, nur in der eCard – Edition von hotSign)

Die Komponenten der technischen Einsatzumgebung des Signatur-Clients sind nicht Gegenstand dieses Gutachtens.

2.3. Funktionsumfang

Folgende Funktionen des Signatur-Clients sind für dieses Gutachten relevant:

⁴ Microsoft® 32bit Windows™ API

⁵ lt. Benutzerhandbuch f. BDC hotSign 2.0, Version 1.0.1

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

- **Secure Viewer:** Diese Funktion prüft das Format der zu signierenden Daten und stellt diese nach erfolgreicher Prüfung dar.
- **Hashberechnung:** Diese Funktion berechnet den Hashwert über die zu signierenden Daten, als Hashfunktionen werden die folgenden verwendet:
 - **SHA-1**
 - **SHA-224**
 - **SHA-256**
 - **SHA-384**
 - **SHA-512**
 - **RIPEMD-160**

Zusätzlich stellt der Signatur-Client folgende Funktionen zur Verfügung:

- Aktivieren der PINs (eCard)
- Ändern der Signatur-PIN
- Entsperren der PINs

Diese Funktionen sind nicht Gegenstand dieses Gutachtens.

2.4. Funktionsbeschreibung

Die zu signierenden Dateien können dem Signatur-Client entweder mittels Security-Layer⁷ Signatur-Request oder in einer Datei übergeben werden. Im Folgenden werden diese beiden Varianten getrennt beschrieben.

Signieren via Signatur-Request

Der Signatur-Client ist ein einfacher HTTP-Server, der Anfragen auf einem TCP-Port entgegennehmen und bearbeiten kann. Anfragen werden dabei nur vom lokalen Rechner entgegengenommen. Der Signatur-Client unterstützt das Security-Layer Protokoll 1.1.0⁸ und 1.2.0⁹.

Es werden zwei unterschiedliche Kommandos zur Erstellung von Signaturen unterstützt:

- **CreateXMLSignatureRequest:** Erstellung von Signaturen im XMLDSIG Format (nach Internet RFC 3275 bzw. ETSI TS 101.903)
- **CreateCMSSignatureRequest:** Erstellung von Signaturen im CMS Format (nach Internet RFC 3370 bzw. ETSI TS 101 733)

Der Signatur-Client prüft, ob die zu signierenden Daten einem gültigen Format entsprechen und stellt diese nach erfolgreicher Prüfung mittels eines integrierten „Secure Viewers“ dar. Anderenfalls wird der Signaturvorgang mit einer Fehlermeldung abgebrochen. Es werden drei Content-Formate unterstützt:

- **text/plain:** Die Daten werden ohne Interpretation der Formatierung angezeigt. Eine Liste der zulässigen Zeichen und Character-Encodings¹⁰ ist in „Anhang A – Zulässige Zeichen und Character-Encodings bei text/plain“ angeführt.
- **text/xml:** Die Daten werden als XML-Daten interpretiert und die XML-Elemente werden hierarchisch dargestellt. Eine Liste der zulässigen Zeichen und Character-Encodings ist in „Anhang B – Zulässige Zeichen und Character-Encodings bei text/xml und text/html“ angeführt.
- **text/html:** Für die Interpretation von HTML-Daten gibt es in hotSign 2.0.0 zwei unterschiedliche Implementierungen. Den Viewer von BDC, welcher bereits seit der

⁷ Siehe <http://www.buergerkarte.at/de/technik/index.html>

⁸ <http://www.buergerkarte.at/konzept/securitylayer/spezifikation/20020831/>

⁹ <http://www.buergerkarte.at/konzept/securitylayer/spezifikation/20040514/>

¹⁰ Wird kein Character-Encoding angegeben, werden die Daten gemäß ISO-8859-1 interpretiert

ersten Version von hotSign verwendet wird, und zusätzlich einen Viewer der das Standard Anzeigeformat von Security-Layer 1.2 implementiert.

- **BDC HTML Viewer** (bei Anfragen nach dem Security-Layer Protokoll 1.1.0)
Die Daten werden nach dem HTML-Standard interpretiert und angezeigt, die zulässigen Zeichen und Character-Encodings entsprechen jenen für „text/xml“. Um sicherzustellen, dass alle HTML-Elemente vom „Secure Viewer“ interpretiert und richtig angezeigt werden können, ist der HTML-Sprachumfang eingeschränkt. Die zulässigen HTML-Elemente sind in einem XML-Schema festgelegt (siehe Anhang C – XML-Schema zur Validierung von HTML-Daten (**BDC HTML Viewer**)). Zusätzlich werden die verwendbaren Text- und Hintergrundfarben eingeschränkt und bestimmte Farbkombinationen für Text und Hintergrund ausgeschlossen (siehe Anhang D).
- **Security-Layer 1.2 HTML Viewer** (bei Anfragen nach dem Security-Layer Protokoll 1.2.0)
Bevor die HTML-Daten angezeigt werden, müssen einige Prüfungen durchlaufen werden. Nur falls alle Prüfungen positiv abgeschlossen wurden erfolgt eine Anzeige der HTML-Daten. Die Prüfungen haben den Zweck jegliche dynamischen Elemente aufzudecken, die die Anzeige der Daten beeinflussen könnten, allerdings die Signatur nicht beeinträchtigen. In diesem Fall wäre nach der Signatur nicht mehr nachvollziehbar, welche Daten dem Signator zum Zeitpunkt der Signaturerstellung angezeigt wurden. Enthalten die anzuzeigenden Daten entsprechende Anzeigeelemente wird die Signaturerstellung durch Abbruch des Viewerprogramms verhindert.

Die Formate XML und HTML sehen Kommentar-Tags vor, die üblicherweise nicht angezeigt werden. Aus diesem Grund ist sowohl beim Content-Format text/xml als auch beim Content-Format text/html die Verwendung von Kommentaren ausgeschlossen (Gilt nur für den BDC XML und HTML Viewer, nicht für den Security-Layer 1.2 HTML Viewer).

Um zuverlässig nachvollziehen zu können, wie die signierten Daten dem Signator im Fenster des Viewers dargestellt wurden, werden das Content-Format und auch das Character-Encoding, die für die Darstellung verwendet wurden, in die resultierende Signatur miteinbezogen.

Bei der Verwendung von XMLDSIG-Signaturen unterstützt der Signatur-Client XSLT (Stylesheet) – Transformationen. Zur Berechnung des Hashwertes für die elektronische Signatur wird das Endergebnis der Transformationskette herangezogen.

Anzeigeeinschränkungen:

- Der Umfang der Request-Daten (Textdaten in text/plain, text/html oder text/xml) die verarbeitet werden können ist auf zwei MByte beschränkt. Wird text/html verwendet und werden innerhalb des HTML-Codes zusätzlich Bilddaten eingebunden, muss auch diese Datenmenge berücksichtigt werden.
- Die Anzahl der Zeichen bei Textdaten (text/plain oder text/xml) ist auf maximal 4096 Zeichen pro Zeile beschränkt, um bei der Anzeige zu langer Zeilen den Secure-Viewer nicht zu kompromittieren.
- Die Menge der anzeigbaren Bilddaten ist beschränkt.
- Entsprechen die text/plain-Daten in einem XMLDSIG-Request wellformed XML-Daten, ist eine Anzeige der Daten in dieser Form nicht möglich und hotSign quittiert dies mit einer entsprechenden Fehlermeldung.
- Bestimmte ASCII-Zeichen (<, &) in den Anzeigedaten zerstören die XML-Struktur eines XMLDSIG-Requests wenn diese uncodiert übergeben werden. Auch bestimmte Escapesequenzen (& < und >) werden immer interpretiert. Als Abhilfe müssen diese Anzeigedaten base64-codiert im Request übergeben werden.

Bei der Verwendung von XMLDSIG-Signaturen ist es beim Content-Type text/html möglich Bilddaten, mit Hilfe eines Image-Tags, einzubinden¹¹.

Grundsätzlich ist nur die Einbindung von Pixelgrafiken möglich, und zwar in den folgenden Formaten:

- **GIF¹²**: Vor der Anzeige im wird geprüft ob:
 - es sich um ein gültiges GIF-Format handelt,
 - es sich weder um ein animiertes noch transparentes GIF handelt, und
 - keine Zusatzinformationen vorhanden sind.
- **JPEG/JFIF¹³**: Vor der Anzeige im wird geprüft ob:
 - ob die Bilddaten ausschließlich im JFIF-Format vorliegen,
 - ob es sich um ein gültiges JFIF-Format handelt, und
 - ob undefinierte oder ungültige Marker (siehe Anhang E) vorhanden sind.

Nach dem Aufrufen eines der beiden oben beschriebenen Signatur-Requests durch eine geeignete Applikation wird der Signator vom Signatur-Client aufgefordert, eine geeignete Signaturkarte in das Chipkartenterminal zu stecken. Dann wird das Format der zu signierenden Daten geprüft. Ist das Format der Daten ungültig, wird der Vorgang abgebrochen und eine entsprechende Fehlermeldung erzeugt. Nach erfolgreicher Prüfung werden die Daten entsprechend ihres Formates im Fenster des Secure-Viewers angezeigt. Es besteht die Möglichkeit bis zu 6 Dokumente mit einem Signaturvorgang zu signieren, sollen mehrere Dokumente auf einmal signiert werden, wird eine entsprechende Anzahl von Registerkarten im Fenster des Secure-Viewers angezeigt. Wird eine Signaturkarte mit qualifiziertem Zertifikat verwendet, wird ein zusätzlicher Hinweis angezeigt, dass eine sichere Signatur erstellt wird. Der Signator kann dann durch Klicken eines entsprechenden Buttons den Signaturvorgang entweder starten oder abbrechen. Zusätzlich besteht die Möglichkeit, sich das Signaturzertifikat der verwendeten Signaturkarte anzeigen zu lassen. Zum endgültigen Auslösen des Signaturvorganges muss die Signatur-PIN am PIN-Pad des verwendeten Chipkartenterminals eingegeben werden. Nach erfolgreicher PIN-Prüfung wird vom Signatur-Client der Hashwert aus den zu signierenden Daten berechnet und an die Signaturkarte übertragen. Die Berechnung der Signatur aus dem Hashwert wird ausschließlich auf der verwendeten Signaturkarte durchgeführt.

Nach erfolgter Signaturberechnung liefert der Signatur-Client der aufrufenden Applikation das angeforderte Signatur-Format zurück (XMLDSIG bzw. CMS). Die Antwort des Signatur-Clients an die aufrufende Applikation erfolgt in den im Security-Layer Protokoll 1.1.0¹⁴ und 1.2.0¹⁵ spezifizierten Formaten.

Signieren von Dateien

Alternativ zur Übergabe der zu signierenden Daten in einem Security-Layer Signatur-Request besteht die Möglichkeit über das graphische User-Interface eine zu signierende Datei anzuwählen. Hier kann zwischen einfacher und sicherer Signatur gewählt werden. Wird die sichere Signatur gewählt, so wird die zu signierende Datei an den „Secure-Viewer“ zur Darstellung übergeben.

Dabei gelten folgende Einschränkungen:

- Die zu signierende Datei wird immer im Character-Encoding ISO-8859-1 und text/plain interpretiert, dargestellt und signiert.
- Die Signatur wird analog einem **CreateCMSSignatureRequest** erzeugt.

Die signierten Dateien können auf Wunsch als Datei abgespeichert werden.

Bei der Installation des Signatur-Clients besteht die Möglichkeit, Integritätsprüfmechanismen zu aktivieren, die die Integrität der verwendeten Programmbibliotheken überprüfen.

¹¹ ()

¹² Graphics Interchange Format, Version 89a. <http://www.w3.org/Graphics/GIF/spec-gif89a.txt>

¹³ JPEG File Interchange Format, Version 1.02. <http://www.w3.org/Graphics/JPEG/jif3.pdf>

¹⁴ <http://www.buergerkarte.at/konzept/securitylayer/spezifikation/20020831/>

¹⁵ <http://www.buergerkarte.at/konzept/securitylayer/spezifikation/20040514/>

Applikationen, die das Produkt hotSign, Version 2.0.0 nutzen, sind **nicht** Gegenstand dieses Gutachtens.

3. Befundaufnahme

Der Hersteller des Signatur-Clients hat das Referenzmuster und die erforderlichen Unterlagen zur Begutachtung eingereicht.

3.1. Referenzmuster

Der Hersteller hat

- den Signatur-Client hotSign, Version 2.0.0, Release vom 17.07.07 zur Begutachtung bereitgestellt.

3.2. Unterlagen

Der Hersteller hat folgende Dokumente zur Begutachtung bereitgestellt:

- „Deckblatt zur Hash-Implementierung“
- „Entwicklerhandbuch zur Hash-Implementierung“
- „Sicherheitskonzept zur Hash-Implementierung“
- „Testapplikation zur Hash-Implementierung“
- „hotSign-Deckblatt“
- „hotSign-Entwicklerhandbuch“
- „hotSign-Entwicklungsumgebung“
- „hotSign-Sicherheitskonzept“
- „hotSign-Testbericht“
- „hotSign-Viewer“
- „hotSign-Benutzerhandbuch“

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

Der Signatur-Client überprüft, ob die zu signierenden Daten einem der oben definierten Content-Formate (text/plain, text/html und text/xml) entsprechen und ermöglicht, dass dem Signator die zu signierenden Daten vor Auslösung des Signaturvorganges dargestellt werden. In den verwendeten Formaten können keine dynamischen Veränderungen codiert werden.

Der Signatur-Client ist damit unter den in Kapitel 5 angeführten 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 Signatur-Clients 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 der Signatur-Client installiert ist, sind zu verhindern. Es ist sicherzustellen, dass die Sicherheit der technischen Einsatzumgebung des Signatur-Clients 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. Insbesondere muss sich der Signator vergewissern, dass die Bildschirmauflösung und Farbtiefe korrekt gemäß den Benutzungsvorschriften des Herstellers eingestellt ist. Wird der Signatur-Client ohne aktivierte Integritätsprüfung installiert, ist die Integrität des Signatur-Clients, der verwendeten Programmbibliotheken und Treiber durch geeignete technische und/oder organisatorische Maßnahmen in der Einsatzumgebung sicherzustellen.
- (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 Signatur-Clients mit der Signaturerstellungseinheit ist ein Chipkartenterminal zu verwenden, das die Anforderungen von SigG und SigV erfüllt und vom Signatur-Client 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) Die verwendeten Formate zur Darstellung des Inhaltes der zu signierenden Daten (siehe auch Kapitel 2.4) müssen vom Zertifizierungsdiensteanbieter empfohlen sein.

6. Unterschriften

A-SIT Zentrum für sichere Informationstechnologie - Austria

Signaturwert	S0sbHWYLnB6HFRVuQcSD0SdvI5I1ICs0X7uAPtSlzegvcPBVyginubUMHw00fmas	
 GESCHÄFTSFÜHRER	Unterzeichner	Geschäftsführender Vorstand, Manfred Holzbach
	Datum/Zeit-UTC	2007-10-31T12:30:48Z
	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.	97349
	Methode	urn:pdfsigfilter:bka.gv.at:text:v1.1.0
	Parameter	etsi-bka-1.0@1193833848-13954453@8754-31744-0-9861-1583
Prüfhinweis	Informationen zur Signaturprüfung finden Sie unter: www.a-sit.at/de/dokumente/publikationen/a-sit_signaturen/index.php .	

Signaturwert	cwTSbYf19x43P0Sz2ZlPk059n7t9TC7kCO7rITTympjNUSj+3LUQkYXFor+dzkj3	
 GESCHÄFTSFÜHRER	Unterzeichner	Prof. Dr. Reinhard Posch, Wissenschaftlicher Gesamtleiter
	Datum/Zeit-UTC	2007-10-31T20:01:08Z
	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.	65090
	Methode	urn:pdfsigfilter:bka.gv.at:text:v1.1.0
	Parameter	etsi-bka-1.0@1193860868-427257843@31094-5822-0-8910-23763
Prüfhinweis	Prüfservice: http://demo.a-sit.at/el_signatur/verification	

Anhang A – Zulässige Zeichen und Character-Encodings bei text/plain

Folgende Zeichen (Unicode-Codepoints) sind zulässig:

Unicode Codepoint (dezimal)	Anmerkung
9, 10, 13	9 = TAB, 10 = LF, 13 = CR
32 - 127	Basic – Latin
160 - 255	Latin 1 - Supplement
256 – 383	Latin Extended - A
711, 728, 729, 731, 733	

Folgende Character-Encodings werden dabei unterstützt:

ANSI_X3.4-1968 (US-ASCII)	Cp869	Cp1124
Big5	Cp870	Cp1258
Big5-HKSCS	Cp871	Cp1381
Cp037	Cp874	Cp1383
Cp273	Cp875	Cp33722
Cp277	Cp918	EUC_CN
Cp278	Cp921	EUC_JP
Cp280	Cp922	EUC_JP_LINUX
Cp284	Cp930	EUC_KR
Cp285	Cp933	EUC_TW
Cp297	Cp935	ISO2022JP
Cp420	Cp937	ISO8859_1
Cp424	Cp939	ISO8859_2
Cp437	Cp942	ISO8859_3
Cp500	Cp942C	ISO8859_4
Cp737	Cp943	ISO8859_5
Cp775	Cp943C	ISO8859_6
Cp838	Cp948	ISO8859_7
Cp850	Cp949	ISO8859_8
Cp852	Cp949C	ISO8859_1
Cp855	Cp950	ISO8859_9
Cp856	Cp964	ISO8859_13
Cp857	Cp970	ISO8859_15_FDIS
Cp860	Cp1006	MS874
Cp861	Cp1025	MS932
Cp862	Cp1026	MS949
Cp863	Cp1097	KOI8_R
Cp864	Cp1098	SJIS
Cp865	Cp1112	TIS620
Cp866	Cp1122	UTF8
Cp868	Cp1123	UnicodeLittleUnmarked

Anmerkung: mit den angeführten Codepoints können nur die Zeichen der Character-Sets ISO8859_1 und ISO8859_2 in vollem Umfang dargestellt werden - die übrigen Character-Sets nur teilweise.

Anhang B – Zulässige Zeichen und Character-Encodings bei text/xml und text/html

Folgende Zeichen (Unicode-Codepoints) sind zulässig:

Unicode Codepoint (dezimal)	Anmerkung
9, 10, 13	9 = TAB, 10 = LF, 13 = CR
32 - 127	Basic - Latin
160 - 255	Latin 1 - Supplement
256 – 383	Latin Extended - A
711, 728, 729, 731, 733	

Folgende Character-Encodings werden dabei unterstützt:

ANSI_X3.4-1968 (US-ASCII)	EBCDIC-CP-IT	ISO-8859-1
Big5	EBCDIC-CP-NL	ISO-8859-2
EBCDIC-CP-AR1	EBCDIC-CP-NO	ISO-8859-3
EBCDIC-CP-AR2	EBCDIC-CP-ROECE	ISO-8859-4
EBCDIC-CP-CA	EBCDIC-CP-SE	ISO-8859-5
EBCDIC-CP-CH	EBCDIC-CP-US	ISO-8859-6
EBCDIC-CP-DK	EBCDIC-CP-YU	ISO-8859-7
EBCDIC-CP-ES	EUC-JP	ISO-8859-8
EBCDIC-CP-FI	EUC-KR	ISO-8859-9
EBCDIC-CP-FR	GB2312	Shift_JIS
EBCDIC-CP-GB	KOI8-R	UTF-8
EBCDIC-CP-HE	ISO-2022-JP	Windows-31J
EBCDIC-CP-IS	ISO-2022-KR	

Anmerkung: mit den angeführten Codepoints können nur die Zeichen der Character-Sets ISO8859_1 und ISO8859_2 in vollem Umfang dargestellt werden - die übrigen Character-Sets nur teilweise.

CSS-Eigenschaften und zulässige bzw. unzulässige Werte für die Validierung durch Security-Layer 1.2 HTML Viewer:

CSS-Eigenschaften	Zulässige Werte	Anmerkungen
margin-top, margin-bottom, margin-left, margin-right	in, mm, cm, pc, px, (+keine Einheit – siehe Längenangaben)	Negative Werte dürfen nicht vorkommen
padding-top, padding-bottom, padding-left, padding-right	in, mm, cm, pc, px, (+keine Einheit – siehe Längenangaben)	Negative Werte dürfen nicht vorkommen
list-style-type	none, disc, circle, square, decimal, decimal-leading-zero, lower-roman, upper-roman, lower-alpha, lower-latin, upper-alpha, upper-latin	
color, background-color	<< Siehe Farbangaben >>	
font-family	serif, sans-serif, monospace	
font-style	normal, italic	
font-weight	normal, bold	

font-size	xx-small,x-small, small, medium, large, x-large, xx-large + Angabe in Pixel (px)	Negative Werte dürfen nicht vorkommen
text-align	left, right, center	
text-decoration	none, underline, line-through	
vertical-align	sub, super	

Längenangaben:

Die Default-Längeneinheit ist px. Daher ist es bei den entsprechenden Eigenschaften auch zugelassen wenn keine Längeneinheit angegeben ist.

Farbangaben:

- Black, Green, Silver, Lime, Gray, Olive, White, Yellow, Maroon, Navy, Red, Blue, Purple, Teal, Fuchsia, Aqua
- #f00: Werte von 0-f pro Stelle sind zugelassen
- #ff0000: Werte von 0-f pro Stelle sind zugelassen
- rgb(255,0,0): Werte von 0-255 sind zugelassen (pro Parameter), negative Werte ausgeschlossen, Whitespaces dazwischen dürfen vorkommen
- rgb(100%, 0%, 0%): Werte von 0-100 sind zugelassen (pro Parameter), negative Werte ausgeschlossen, Whitespaces dazwischen dürfen vorkommen

Anhang C – XML-Schema zur Validierung von HTML-Daten (BDC HTML Viewer¹⁶)

```
<?xml version='1.0' encoding='UTF-8'?>
<xs:schema targetNamespace='http://www.w3.org/1999/xhtml' xmlns:xs='http://www.w3.org/2001/XMLSchema'
xmlns='http://www.w3.org/1999/xhtml'>
  <xs:group name='Heading.class'>
    <xs:choice>
      <xs:choice minOccurs='0' maxOccurs='unbounded'>
        <xs:element ref='h1'/>
        <xs:element ref='h2'/>
        <xs:element ref='h3'/>
        <xs:element ref='h4'/>
        <xs:element ref='h5'/>
        <xs:element ref='h6'/>
      </xs:choice>
    </xs:choice>
  </xs:group>
  <xs:group name='List.class'>
    <xs:choice>
      <xs:choice minOccurs='0' maxOccurs='unbounded'>
        <xs:element ref='ul'/>
        <xs:element ref='ol'/>
        <xs:element ref='dl'/>
      </xs:choice>
    </xs:choice>
  </xs:group>
  <xs:group name='Block.class'>
    <xs:choice>
      <xs:choice minOccurs='0' maxOccurs='unbounded'>
        <xs:element ref='p'/>
        <xs:element ref='blockquote'/>
        <xs:element ref='table'/>
        <xs:element ref='pre'/>
        <xs:element ref='img'/>
        <xs:element ref='hr' minOccurs='0' maxOccurs='unbounded'/>
        <xs:group ref='List.class'/>
      </xs:choice>
    </xs:choice>
  </xs:group>
  <xs:group name='Block.mix'>
    <xs:choice>
      <xs:choice minOccurs='0' maxOccurs='unbounded'>
        <xs:group ref='Heading.class'/>
        <xs:group ref='Text.class'/>
        <xs:group ref='Block.class'/>
      </xs:choice>
    </xs:choice>
  </xs:group>
  <xs:group name='Flow.mix'>
    <xs:choice>
      <xs:choice minOccurs='0' maxOccurs='unbounded'>
        <xs:group ref='Block.class'/>
        <xs:group ref='Text.class'/>
      </xs:choice>
    </xs:choice>
  </xs:group>
  <xs:group name='Text.class'>
    <xs:choice>
      <xs:choice minOccurs='0' maxOccurs='unbounded'>
        <xs:element ref='font'/>
        <xs:element ref='br'/>
        <xs:element ref='tt'/>
        <xs:element ref='i'/>
        <xs:element ref='b'/>
        <xs:element ref='big'/>
        <xs:element ref='sub'/>
        <xs:element ref='sup'/>
      </xs:choice>
    </xs:choice>
  </xs:group>
</xs:schema>
```

¹⁶ Das XML-Schema zur Validierung von HTML-Daten nach dem Standard-Anzeigeformat zur Bürgerkarten-Umgebung der österreichischen Bürgerkarte ist unter <http://www.buergerkarte.at/konzept/securitylayer/spezifikation/aktuell/viewerformat/slxhtml.schemas.zip> öffentlich verfügbar.

```

</xs:choice>
</xs:group>
<xs:simpleType name='Color'>
  <xs:restriction base='xs:string'>
    <xs:enumeration value='Black'/>
    <xs:enumeration value='black'/>
    <xs:enumeration value='Silver'/>
    <xs:enumeration value='silver'/>
    <xs:enumeration value='Gray'/>
    <xs:enumeration value='gray'/>
    <xs:enumeration value='White'/>
    <xs:enumeration value='white'/>
    <xs:enumeration value='Maroon'/>
    <xs:enumeration value='maroon'/>
    <xs:enumeration value='Red'/>
    <xs:enumeration value='red'/>
    <xs:enumeration value='Purple'/>
    <xs:enumeration value='purple'/>
    <xs:enumeration value='Fuchsia'/>
    <xs:enumeration value='fuchsia'/>
    <xs:enumeration value='Green'/>
    <xs:enumeration value='green'/>
    <xs:enumeration value='Lime'/>
    <xs:enumeration value='lime'/>
    <xs:enumeration value='Olive'/>
    <xs:enumeration value='olive'/>
    <xs:enumeration value='Yellow'/>
    <xs:enumeration value='yellow'/>
    <xs:enumeration value='Navy'/>
    <xs:enumeration value='navy'/>
    <xs:enumeration value='Blue'/>
    <xs:enumeration value='blue'/>
    <xs:enumeration value='Teal'/>
    <xs:enumeration value='teal'/>
    <xs:enumeration value='Aqua'/>
    <xs:enumeration value='aqua'/>
  </xs:restriction>
</xs:simpleType>
<xs:simpleType name='FontSize'>
  <xs:restriction base='xs:string'>
    <xs:enumeration value='-1'/>
    <xs:enumeration value='+1'/>
    <xs:enumeration value='+2'/>
    <xs:enumeration value='+3'/>
    <xs:enumeration value='+4'/>
    <xs:enumeration value='2'/>
    <xs:enumeration value='3'/>
    <xs:enumeration value='4'/>
    <xs:enumeration value='5'/>
    <xs:enumeration value='6'/>
    <xs:enumeration value='7'/>
  </xs:restriction>
</xs:simpleType>
<xs:simpleType name='FontFace'>
  <xs:restriction base='xs:string'>
    <xs:enumeration value='Arial'/>
    <xs:enumeration value='arial'/>
    <xs:enumeration value='Times New Roman'/>
    <xs:enumeration value='times new roman'/>
    <xs:enumeration value='Verdana'/>
    <xs:enumeration value='verdana'/>
    <xs:enumeration value='courier new'/>
    <xs:enumeration value='Courier New'/>
  </xs:restriction>
</xs:simpleType>
<xs:simpleType name='Length'>
  <xs:restriction base='xs:integer'>
    <xs:minInclusive value='0'/>
    <xs:maxInclusive value='1000'/>
  </xs:restriction>
</xs:simpleType>
<xs:simpleType name='restrictedLength'>
  <xs:restriction base='xs:string'>
    <xs:pattern value='\d{2}%'/>
    <xs:pattern value='\d{1}%'/>
    <xs:pattern value='100%'/>
  </xs:restriction>
</xs:simpleType>

```

```

        <xs:pattern value='\d{1}'/>
        <xs:pattern value='\d{2}'/>
        <xs:pattern value='\d{3}'/>
        <xs:pattern value='\d{4}'/>
        <xs:pattern value='10000'/>
        <xs:pattern value='\d{1}px'/>
        <xs:pattern value='\d{2}px'/>
        <xs:pattern value='\d{3}px'/>
        <xs:pattern value='\d{4}px'/>
        <xs:pattern value='10000px'/>
    </xs:restriction>
</xs:simpleType>
<xs:simpleType name='Pixels'>
    <xs:restriction base='xs:integer'>
        <xs:minInclusive value='0'/>
        <xs:maxInclusive value='1000'/>
    </xs:restriction>
</xs:simpleType>
<xs:simpleType name='Number'>
    <xs:restriction base='xs:nonNegativeInteger'/>
</xs:simpleType>
<xs:complexType name='empty.type'>
</xs:complexType>
<xs:attributeGroup name='CellVAlign.attrib'>
    <xs:attribute name='valign'>
        <xs:simpleType>
            <xs:restriction base='xs:NMTOKEN'>
                <xs:enumeration value='top'/>
                <xs:enumeration value='middle'/>
                <xs:enumeration value='bottom'/>
            </xs:restriction>
        </xs:simpleType>
    </xs:attribute>
</xs:attributeGroup>
<xs:attributeGroup name='CellHAlign.attrib'>
    <xs:attribute name='align'>
        <xs:simpleType>
            <xs:restriction base='xs:NMTOKEN'>
                <xs:enumeration value='left'/>
                <xs:enumeration value='center'/>
                <xs:enumeration value='right'/>
            </xs:restriction>
        </xs:simpleType>
    </xs:attribute>
</xs:attributeGroup>
<xs:complexType name='body.type' mixed='true'>
    <xs:group ref='Block.mix' />
    <xs:attribute name='bgcolor' type='Color' />
    <xs:attribute name='text' type='Color' />
</xs:complexType>
<xs:element name='body' type='body.type' />
<xs:simpleType name='FPI'>
    <xs:restriction base='xs:normalizedString' />
</xs:simpleType>
<xs:complexType name='html.type'>
    <xs:sequence>
        <xs:element ref='head' minOccurs='0' />
        <xs:element ref='body' />
    </xs:sequence>
    <xs:attribute name='version' type='FPI' fixed='XHTML1.1' />
</xs:complexType>
<xs:element name='html' type='html.type' />
<xs:element name='title' type='xs:string' />
<xs:group name='head.content'>
    <xs:sequence>
        <xs:element ref='title' minOccurs='0' />
    </xs:sequence>
</xs:group>
<xs:complexType name='head.type'>
    <xs:group ref='head.content' />
</xs:complexType>
<xs:element name='head' type='head.type' />
<xs:complexType name='blockquote.type' mixed='true'>
    <xs:group ref='Block.mix' />
</xs:complexType>
<xs:element name='blockquote' type='blockquote.type' />

```

```

<xs:complexType name='heading.type' mixed='true'>
  <xs:group ref='Text.class'/>
  <xs:attributeGroup ref='CellHAlign.attrib'/>
</xs:complexType>
<xs:element name='h1' type='heading.type'/>
<xs:element name='h2' type='heading.type'/>
<xs:element name='h3' type='heading.type'/>
<xs:element name='h4' type='heading.type'/>
<xs:element name='h5' type='heading.type'/>
<xs:element name='h6' type='heading.type'/>
<xs:complexType name='p.type' mixed='true'>
  <xs:group ref='Text.class'/>
  <xs:attributeGroup ref='CellHAlign.attrib'/>
</xs:complexType>
<xs:element name='p' type='p.type'/>
<xs:complexType name='dt.type' mixed='true'>
  <xs:group ref='Text.class'/>
</xs:complexType>
<xs:element name='dt' type='dt.type'/>
<xs:complexType name='dd.type' mixed='true'>
  <xs:group ref='Flow.mix'/>
</xs:complexType>
<xs:element name='dd' type='dd.type'/>
<xs:group name='dl.content'>
<xs:choice>
  <xs:element ref='dt'/>
  <xs:element ref='dd'/>
</xs:choice>
</xs:group>
<xs:complexType name='dl.type' mixed='true'>
<xs:group ref='dl.content' minOccurs='1' maxOccurs='unbounded'/>
</xs:complexType>
<xs:element name='dl' type='dl.type'/>
<xs:complexType name='li.type' mixed='true'>
  <xs:group ref='Flow.mix'/>
</xs:complexType>
<xs:element name='li' type='li.type'/>
<xs:complexType name='ol.type'>
  <xs:sequence>
    <xs:element ref='li' minOccurs='1' maxOccurs='unbounded'/>
  </xs:sequence>
</xs:complexType>
<xs:element name='ol' type='ol.type'/>
<xs:complexType name='ul.type'>
  <xs:sequence>
    <xs:element ref='li' minOccurs='1' maxOccurs='unbounded'/>
  </xs:sequence>
</xs:complexType>
<xs:element name='ul' type='ul.type'/>
<xs:attributeGroup name='table.attlist'>
  <xs:attribute name='width' type='restrictedLength'/>
  <xs:attribute name='border' type='Pixels'/>
  <xs:attribute name='cellspacing' type='Length'/>
  <xs:attribute name='cellpadding' type='Length'/>
  <xs:attribute name='bgcolor' type='Color'/>
  <xs:attribute name='align'>
    <xs:simpleType>
      <xs:restriction base='xs:NMTOKEN'>
        <xs:enumeration value='left'/>
        <xs:enumeration value='center'/>
        <xs:enumeration value='right'/>
      </xs:restriction>
    </xs:simpleType>
  </xs:attribute>
</xs:attributeGroup>
<xs:group name='table.content'>
  <xs:choice>
    <xs:element ref='tr' minOccurs='1' maxOccurs='unbounded'/>
  </xs:choice>
</xs:group>
<xs:complexType name='table.type' mixed='true'>
  <xs:group ref='table.content'/>
  <xs:attributeGroup ref='table.attlist'/>
</xs:complexType>
<xs:element name='table' type='table.type'/>
<xs:group name='pre.content'>

```

```

    <xs:choice>
      <xs:element ref='tt'/>
      <xs:element ref='i'/>
      <xs:element ref='b'/>
      <xs:element ref='font'/>
      <xs:element ref='br'/>
    </xs:choice>
  </xs:group>
  <xs:complexType name='pre.type' mixed='true'>
    <xs:group ref='pre.content' minOccurs='0' maxOccurs='unbounded'/>
  </xs:complexType>
  <xs:element name='pre' type='pre.type'/>
  <xs:attributeGroup name='tr.attlist'>
    <xs:attribute name='bgcolor' type='Color'/>
    <xs:attributeGroup ref='CellHAlign.attrib'/>
    <xs:attributeGroup ref='CellVAlign.attrib'/>
  </xs:attributeGroup>
  <xs:group name='tr.content'>
    <xs:choice>
      <xs:element ref='th' minOccurs='0' maxOccurs='unbounded'/>
      <xs:element ref='td' minOccurs='0' maxOccurs='unbounded'/>
    </xs:choice>
  </xs:group>
  <xs:complexType name='tr.type'>
    <xs:group ref='tr.content'/>
    <xs:attributeGroup ref='tr.attlist'/>
  </xs:complexType>
  <xs:element name='tr' type='tr.type'/>
  <xs:attributeGroup name='td.attlist'>
    <xs:attribute name='nowrap' fixed='nowrap'/>
    <xs:attribute name='bgcolor' type='Color'/>
    <xs:attribute name='text' type='Color'/>
    <xs:attribute name='rowspan' type='Length' default='1'/>
    <xs:attribute name='colspan' type='Length' default='1'/>
    <xs:attributeGroup ref='CellHAlign.attrib'/>
    <xs:attributeGroup ref='CellVAlign.attrib'/>
  </xs:attributeGroup>
  <xs:complexType name='td.type' mixed='true'>
    <xs:group ref='Block.mix'/>
    <xs:attribute name='height' type='restrictedLength'/>
    <xs:attribute name='width' type='restrictedLength'/>
    <xs:attributeGroup ref='td.attlist'/>
  </xs:complexType>
  <xs:element name='td' type='td.type'/>
  <xs:attributeGroup name='th.attlist'>
    <xs:attribute name='nowrap' fixed='nowrap'/>
    <xs:attribute name='bgcolor' type='Color'/>
    <xs:attribute name='width' type='restrictedLength'/>
    <xs:attribute name='height' type='restrictedLength'/>
    <xs:attribute name='rowspan' type='Length' default='1'/>
    <xs:attribute name='colspan' type='Length' default='1'/>
    <xs:attributeGroup ref='CellHAlign.attrib'/>
    <xs:attributeGroup ref='CellVAlign.attrib'/>
  </xs:attributeGroup>
  <xs:complexType name='th.type' mixed='true'>
    <xs:group ref='Block.mix'/>
    <xs:attributeGroup ref='th.attlist'/>
  </xs:complexType>
  <xs:element name='th' type='th.type'/>
  <xs:element name='br' type='empty.type'/>
  <xs:complexType name='Text.type' mixed='true'>
    <xs:group ref='Text.class' minOccurs='0' maxOccurs='unbounded'/>
  </xs:complexType>
  <xs:element name='b' type='Text.type'/>
  <xs:element name='big' type='Text.type'/>
  <xs:element name='i' type='Text.type'/>
  <xs:element name='sub' type='Text.type'/>
  <xs:element name='sup' type='Text.type'/>
  <xs:element name='tt' type='Text.type'/>
  <xs:element name='hr' type='empty.type'/>
  <xs:element name='img' type='img.type'/>
  <xs:attributeGroup name='font.attlist'>
    <xs:attribute name='size' type='FontSize'/>
    <xs:attribute name='color' type='Color'/>
    <xs:attribute name='face' type='FontFace'/>
  </xs:attributeGroup>

```

```

<xs:complexType name='font.type' mixed='true'>
  <xs:group ref='Text.class' minOccurs='0' maxOccurs='unbounded' />
  <xs:attributeGroup ref='font.attlist' />
</xs:complexType>
<xs:element name='font' type='font.type' />
<xs:complexType name='img.type'>
  <xs:attributeGroup ref='img.attlist' />
</xs:complexType>
<xs:attributeGroup name='img.attlist'>
  <xs:attribute name='src' type='xs:anyURI' />
</xs:attributeGroup>
</xs:schema>

```

Beschreibung zum XML - Schema

Element: ****

Verwendung: Mit diesem Tag werden Texte fett formatiert.

Attribute: Keine

Das Element **muss** folgende Elemente beinhalten: keine

Das Element **kann** folgende Elemente beinhalten:

	(0 bis n mal)
 	(0 bis n mal)
<tt>	(0 bis n mal)
<i>	(0 bis n mal)
	(0 bis n mal)
<big>	(0 bis n mal)
<sub>	(0 bis n mal)
<sup>	(0 bis n mal)

Das Element **kann** beliebigen Text beinhalten: ja

Element: **<big>**

Verwendung: Mit diesem Tag wird die Schriftgröße um einen Grad erhöht (die maximale Schriftgröße ist 7).

Attribute: Keine

Das Element **muss** folgende Elemente beinhalten: keine

Das Element **kann** folgende Elemente beinhalten:

	(0 bis n mal)
 	(0 bis n mal)
<tt>	(0 bis n mal)
<i>	(0 bis n mal)
	(0 bis n mal)
<big>	(0 bis n mal)
<sub>	(0 bis n mal)
<sup>	(0 bis n mal)

Das Element **kann** beliebigen Text beinhalten: ja

Element: **<blockquote>**

Verwendung: Da innerhalb des Elementes Blockquote alle "Body-Elemente" erlaubt sind, können mit diesem Element mehrere Dokumente zusammengeführt werden.

Attribute: Keine

Das Element **muss** folgende Elemente beinhalten: keine

Das Element **kann** folgende Elemente beinhalten:

<H1>, <H2>, ... <H6>	(0 bis n mal)
<p>	(0 bis n mal)
<blockquote>	(0 bis n mal)
<table>	(0 bis n mal)
<hr>	(0 bis n mal)
	(0 bis n mal)
	(0 bis n mal)
<dl>	(0 bis n mal)
	(0 bis n mal)

 (0 bis n mal)
 <tt> (0 bis n mal)
 <i> (0 bis n mal)
 (0 bis n mal)
 <big> (0 bis n mal)
 <sub> (0 bis n mal)
 <sup> (0 bis n mal)
 <pre> (0 bis n mal)
 (0 bis n mal)
 Das Element **kann** beliebigen Text beinhalten: ja

Element: <body>
 Verwendung: Dieses Tag definiert den sichtbaren Teil des HTML-Dokumentes
 Attribute: bgcolor - (Hintergrundfarbe alle 16 Grundfarben sind möglich)der Standartwert ist weiss
 text - (Textfarbe alle 16 Grundfarben sind möglich) der Standartwert ist schwarz

Der Fontstandartwert ist Times New Roman, Größe 3
 Das Element **muss** folgende Elemente beinhalten: keine
 Das Element **kann** folgende Elemente beinhalten:

<H1>, <H2>,... <H6> (0 bis n mal)
 <p> (0 bis n mal)
 <blockquote> (0 bis n mal)
 <table> (0 bis n mal)
 <hr> (0 bis n mal)
 (0 bis n mal)
 (0 bis n mal)
 <dl> (0 bis n mal)
 (0 bis n mal)

 (0 bis n mal)
 <tt> (0 bis n mal)
 <i> (0 bis n mal)
 (0 bis n mal)
 <big> (0 bis n mal)
 <sub> (0 bis n mal)
 <sup> (0 bis n mal)
 <pre> (0 bis n mal)
 (0 bis n mal)
 Das Element **kann** beliebigen Text beinhalten: ja

Element:

 Verwendung: Zeilenumbruch erzwingen
 Attribute: keine
 Das Element **muss** folgende Elemente beinhalten: keine
 Das Element **kann** folgende Elemente beinhalten: keine
 Das Element **kann** beliebigen Text beinhalten: nein

Element: <dd>
 Verwendung: leitet eine Definition eines Ausdrucks ein
 Attribute: keine
 Das Element **muss** folgende Elemente beinhalten: keine
 Das Element **kann** folgende Elemente beinhalten:

<p> (0 bis n mal)
 <blockquote> (0 bis n mal)
 <table> (0 bis n mal)
 <hr> (0 bis n mal)
 (0 bis n mal)
 (0 bis n mal)
 <dl> (0 bis n mal)
 (0 bis n mal)

 (0 bis n mal)
 <tt> (0 bis n mal)

<i> (0 bis n mal)
 (0 bis n mal)
<big> (0 bis n mal)
<sub> (0 bis n mal)
<sup> (0 bis n mal)
Das Element **kann** beliebigen Text beinhalten: ja

Element: <dl>
Verwendung: leitet eine Definitionsliste ein
Attribute: keine
Das Element **muss** zumindest **eines** der folgenden Elemente beinhalten:
<dt>
<dd>
Das Element **kann** folgende Elemente beinhalten:
<dt> (0 bis n mal)
<dd> (0 bis n mal)
Das Element **kann** beliebigen Text beinhalten: ja

Element: <dt>
Verwendung: leitet einen zu definierenden Ausdruck ein
Attribute: keine
Das Element **muss** folgende Elemente beinhalten: keine
Das Element **kann** folgende Elemente beinhalten:
 (0 bis n mal)

 (0 bis n mal)
<tt> (0 bis n mal)
<i> (0 bis n mal)
 (0 bis n mal)
<big> (0 bis n mal)
<sub> (0 bis n mal)
<sup> (0 bis n mal)
Das Element **kann** beliebigen Text beinhalten: ja

Element:
Verwendung: Markiert Text mit Schriftgröße, Schriftfarbe, Schriftart
Attribute: size - Schriftgröße (Größe 2 bis 7, rel.Größen -1,+1,+2,+3, +4)
face - Schriftart (Arial, TimesNewRoman, Verdana, Courier New)
color - Schriftfarbe (alle 16 Grundfarben)
Das Element **muss** folgende Elemente beinhalten: keine
Das Element **kann** folgende Elemente beinhalten:
 (0 bis n mal)

 (0 bis n mal)
<tt> (0 bis n mal)
<i> (0 bis n mal)
 (0 bis n mal)
<big> (0 bis n mal)
<sub> (0 bis n mal)
<sup> (0 bis n mal)
Das Element **kann** beliebigen Text beinhalten: ja

Element: <h1>, <h2>, ...<h6>
Verwendung: Markiert eine Überschrift 1. bis 6. Ordnung
Attribute: align - horizontale Ausrichtung (left, center, right)
Das Element **muss** folgende Elemente beinhalten: keine
Das Element **kann** folgende Elemente beinhalten:
 (0 bis n mal)

 (0 bis n mal)
<tt> (0 bis n mal)
<i> (0 bis n mal)

 (0 bis n mal)
<big> (0 bis n mal)
<sub> (0 bis n mal)
<sup> (0 bis n mal)
Das Element **kann** beliebigen Text beinhalten: ja

Element: <head>
Verwendung: Markiert den Kopfbereich einer HTML-Datei
Attribute: keine
Das Element **muss** folgende Elemente beinhalten:
<title> (genau 1 mal)
Das Element **kann** beliebigen Text beinhalten: nein

Element: <hr>
Verwendung: Erzeugt eine horizontale Trennlinie
Attribute: keine
Das Element **muss** folgende Elemente beinhalten: keine
Das Element **kann** folgende Elemente beinhalten: keine
Das Element **kann** beliebigen Text beinhalten: nein

Element: <html>
Verwendung: Basiselement einer HTML-Datei
Das Element **muss** folgende Elemente beinhalten:
<title> (genau 1 mal und immer an 1. Stelle)
<body> (genau 1 mal und immer an 2. Stelle)
Das Element **kann** beliebigen Text beinhalten: nein

Element: <i>
Verwendung: Markiert kursiv gedruckten Text
Attribute: keine
Das Element **muss** folgende Elemente beinhalten: keine
Das Element **kann** folgende Elemente beinhalten:
 (0 bis n mal)

 (0 bis n mal)
<tt> (0 bis n mal)
<i> (0 bis n mal)
 (0 bis n mal)
<big> (0 bis n mal)
<sub> (0 bis n mal)
<sup> (0 bis n mal)
Das Element **kann** beliebigen Text beinhalten: ja

Element:
Verwendung: implementiert ein Bild
Attribute: src=url
Das Element **muss** folgende Elemente beinhalten: keine
Das Element **kann** folgende Elemente beinhalten: keine
Das Element **kann** beliebigen Text beinhalten: nein

Element:
Verwendung: Markiert einen Listeneintrag
Attribute: keine
Das Element **muss** folgende Elemente beinhalten: keine
Das Element **kann** folgende Elemente beinhalten:
<p> (0 bis n mal)
<blockquote> (0 bis n mal)
<table> (0 bis n mal)
<hr> (0 bis n mal)
 (0 bis n mal)
 (0 bis n mal)
<dl> (0 bis n mal)

 (0 bis n mal)

 (0 bis n mal)
<tt> (0 bis n mal)
<i> (0 bis n mal)
 (0 bis n mal)
<big> (0 bis n mal)
<sub> (0 bis n mal)
<sup> (0 bis n mal)
<pre> (0 bis n mal)
 (0 bis n mal)
Das Element **kann** beliebigen Text beinhalten: ja

Element:
Verwendung: Markiert eine nummerierte Liste
Attribute: keine
Das Element **muss** folgende Elemente beinhalten:
 (1 mal)
Das Element **kann** folgende Elemente beinhalten:
 (1 bis n mal)
Das Element **kann** beliebigen Text beinhalten: nein

Element: <p>
Verwendung: Markiert einen Textabsatz
Attribute: align - horizontale Ausrichtung (left, center, right)
Das Element **muss** folgende Elemente beinhalten: keine
Das Element **kann** folgende Elemente beinhalten:
 (0 bis n mal)

 (0 bis n mal)
<tt> (0 bis n mal)
<i> (0 bis n mal)
 (0 bis n mal)
<big> (0 bis n mal)
<sub> (0 bis n mal)
<sup> (0 bis n mal)
<pre> (0 bis n mal)
 (0 bis n mal)
Das Element **kann** beliebigen Text beinhalten: ja

Element: <pre>
Verwendung: Formatiert einen Bereich wie im Editor eingegeben (präformatierter Text).
Attribute: keine
Das Element **muss** folgende Elemente beinhalten: keine
Das Element **kann** folgende Elemente beinhalten:
 (0 bis n mal)

 (0 bis n mal)
<tt> (0 bis n mal)
<i> (0 bis n mal)
 (0 bis n mal)
Das Element **kann** beliebigen Text beinhalten: ja

Element: <sup>
Verwendung: Markiert einen Text als hochgestellt
Attribute: keine
Das Element **muss** folgende Elemente beinhalten: keine
Das Element **kann** folgende Elemente beinhalten:
 (0 bis n mal)

 (0 bis n mal)
<tt> (0 bis n mal)
<i> (0 bis n mal)
 (0 bis n mal)
<big> (0 bis n mal)

<sub> (0 bis n mal)
<sup> (0 bis n mal)
Das Element **kann** beliebigen Text beinhalten: ja

Element: <sub>
Verwendung: Markiert einen Text als tiefgestellt
Attribute: keine
Das Element **muss** folgende Elemente beinhalten: keine
Das Element **kann** folgende Elemente beinhalten:
 (0 bis n mal)

 (0 bis n mal)
<tt> (0 bis n mal)
<i> (0 bis n mal)
 (0 bis n mal)
<big> (0 bis n mal)
<sub> (0 bis n mal)
<sup> (0 bis n mal)
Das Element **kann** beliebigen Text beinhalten: ja

Element: <table>
Verwendung: Erzeugt eine Tabelle
Attribute: width - Anzeigebreite der Tabelle in Pixel oder Prozent Wertebereich ganze Zahl von 1 bis 10000 und von 1 bis 100%
border - Rahmendicke der Tabelle in Pixel Wertebereich ganze Zahl von 1 bis 1000
cellspacing - Abstand zwischen zwei Zellen in Pixel Wertebereich ganze Zahl von 1 bis 1000
cellpadding - Innenabstand Zellenrand zu Inhalt in Pixel Wertebereich ganze Zahl von 1 bis 1000
bgcolor - Hintergrundfarbe (alle 16 Grundfarben sind möglich)
align - vertikale Ausrichtung der Tabelle (left, center, right)
Das Element **muss** folgende Elemente beinhalten:
<tr> (1 mal)
Das Element **kann** folgende Elemente beinhalten:
<tr> (1 bis n mal)
Das Element **kann** beliebigen Text beinhalten: nein

Element: <td>
Verwendung: Markiert eine Tabellenzelle
Attribute: width - Anzeigebreite in Pixel oder Prozent Wertebereich ganze Zahl von 1 bis 10000 und von 1 bis 100 %
height - Anzeigehöhe in Pixel oder Prozent Wertebereich ganze Zahl von 1 bis 10000 und von 1 bis 100 %
nowrap - Zeilenumbruch in Tabellenzelle verhindern Der Inhalt muss nowrap sein
bgcolor - Hintergrundfarbe (alle 16 Grundfarben sind möglich)
text - Textfarbe (alle 16 Grundfarben sind möglich)
rowspan - Anzahl wie viele Zellen vertikal verbunden werden die Defaulteinstellung ist 1 Wertebereich ganze Zahl von 1 bis 10000
colspan - Anzahl wie viele Zellen horizontal verbunden werden; die Defaulteinstellung ist 1; ganze positive Zahl Wertebereich ganze Zahl von 1 bis 10000

align - vertikale Ausrichtung der Tabelle
(left, center, right)
valign - horizontale Ausrichtung der Tabelle (
top, middle, bottom)

Das Element **muss** folgende Elemente beinhalten: keine

Das Element **kann** folgende Elemente beinhalten:

<H1>, <H2>, ... <H6> (0 bis n mal)
<p> (0 bis n mal)
<blockquote> (0 bis n mal)
<table> (0 bis n mal)
<hr> (0 bis n mal)
 (0 bis n mal)
 (0 bis n mal)
<dl> (0 bis n mal)
 (0 bis n mal)

 (0 bis n mal)
<tt> (0 bis n mal)
<i> (0 bis n mal)
 (0 bis n mal)
<big> (0 bis n mal)
<sub> (0 bis n mal)
<sup> (0 bis n mal)
<pre> (0 bis n mal)
 (0 bis n mal)

Das Element **kann** beliebigen Text beinhalten: ja

Element:

<th>

Verwendung:

Markiert eine Tabellenkopfzelle

Attribute:

width - Anzeigebreite in Pixel oder Prozent
Wertebereich ganze Zahl von 1 bis 10000 und
von 1 bis 100 %
height - Anzeigehöhe in Pixel oder Prozent
Wertebereich ganze Zahl von 1 bis 10000 und
von 1 bis 100 %
nowrap - Zeilenumbruch in Tabellenzelle
verhindern, der Inhalt muss nowrap sein
bgcolor - Hintergrundfarbe (alle 16
Grundfarben sind möglich)
text - Textfarbe (alle 16 Grundfarben sind
möglich)
rowspan - Anzahl wie viele Zellen vertikal
verbunden werden die Defaulteinstellung ist 1
Wertebereich ganze Zahl von 1 bis 10000
colspan - Anzahl wie viele Zellen horizontal
verbunden werden; die Defaulteinstellung ist
1; ganze positive Zahl Wertebereich ganze
Zahl von 1 bis 10000
align - vertikale Ausrichtung der Tabelle
(left, center, right)
valign - horizontale Ausrichtung der Tabelle
(top, middle, bottom)

Das Element **muss** folgende Elemente beinhalten: keine

Das Element **kann** folgende Elemente beinhalten:

<H1>, <H2>, ... <H6> (0 bis n mal)
<p> (0 bis n mal)
<blockquote> (0 bis n mal)
<table> (0 bis n mal)
<hr> (0 bis n mal)
 (0 bis n mal)
 (0 bis n mal)
<dl> (0 bis n mal)
 (0 bis n mal)

 (0 bis n mal)
<tt> (0 bis n mal)
<i> (0 bis n mal)
 (0 bis n mal)

<big> (0 bis n mal)
 <sub> (0 bis n mal)
 <sup> (0 bis n mal)
 <pre> (0 bis n mal)
 (0 bis n mal)
 Das Element **kann** beliebigen Text beinhalten: ja

Element: <title>
 Verwendung: Definiert den Titel einer HTML-Datei
 Attribute: keine
 Das Element **muss** folgende Elemente beinhalten: keine
 Das Element **kann** folgende Elemente beinhalten: keine
 Das Element **kann** beliebigen Text beinhalten: ja

Element: <tr>
 Verwendung: Definiert eine Tabellenzeile
 Attribute: bgcolor - Hintergrundfarbe (alle 16 Grundfarben sind möglich)
 align - vertikale Ausrichtung der Tabellenzeile (left, center, right)
 valign - horizontale Ausrichtung der Tabellenzeile (top, middle, bottom)
 Das Element **muss** folgende Elemente beinhalten: keine
 Das Element **kann** folgende Elemente beinhalten:
 <th> (0 bis n mal)
 <td> (0 bis n mal)
 Das Element **kann** beliebigen Text beinhalten: ja

Element: <tt>
 Verwendung: Markiert einen Text, der im Schreibmaschinenstil dargestellt wird
 Attribute: keine
 Das Element **muss** folgende Elemente beinhalten: keine
 Das Element **kann** folgende Elemente beinhalten:
 (0 bis n mal)

 (0 bis n mal)
 <tt> (0 bis n mal)
 <i> (0 bis n mal)
 (0 bis n mal)
 <big> (0 bis n mal)
 <sub> (0 bis n mal)
 <sup> (0 bis n mal)
 Das Element **kann** beliebigen Text beinhalten: ja

Element:
 Verwendung: Markiert eine Aufzählungsliste
 Attribute: keine
 Das Element **muss** folgende Elemente beinhalten:
 (1 mal)
 Das Element **kann** folgende Elemente beinhalten:
 (1 bis n mal)
 Das Element **kann** beliebigen Text beinhalten: nein

Anhang D – Zulässige Farben und unzulässige Farbkombination in HTML-Daten

Zulässige Farben

Folgende Farben können wahlweise als Text- und Hintergrundfarbe verwendet werden:

| |
|---------|
| Black |
| Silver |
| Gray |
| White |
| Maroon |
| Red |
| Purple |
| Fuchsia |
| Green |
| Lime |
| Olive |
| Yellow |
| Navy |
| Blue |
| Teal |
| Aqua |

Unzulässige Farbkombinationen

Die Verwendung einer Farbe sowohl für den Text als auch für den Hintergrund wird ausgeschlossen. Zusätzlich werden noch folgende Farbkombinationen ausgeschlossen:

| | |
|--------|---------|
| Navy | Black |
| Olive | Gray |
| Yellow | White |
| Purple | Maroon |
| Red | Fuchsia |
| Teal | Green |
| Aqua | Lime |

Anhang E - Tabelle aller JPEG-Marker

| Kurzbezeichnung | Definition | Beschreibung | Secure-Viewer Einschränkung |
|-----------------|---------------------------------|--|-----------------------------|
| SOI | Start of Image | Dateiheader | 1 x |
| EOI | End of Image | Dateitrailer | 1 x |
| DAC | Define arithmetic Table | Arithmetische Tabelle | n x |
| DHT | Define Huffmann Table | Huffmann-tabelle | n x |
| DQT | Define Quantiation Table | Quantisierungstabelle | n x |
| SOS | Start of Scan | komprimierte Pixeldaten | n x |
| EXP | Expand reference components | nicht definiert | n x |
| DNL | Define number of lines | wird benötigt | n x |
| DRI | Define restart interval | wird benötigt | n x |
| DHP | Define hierarchical progression | wird benötigt | n x |
| COM | Comment | Kommentar | 0 x |
| TEM | Temporary arithmetic coding | nicht definiert | 0 x |
| JPG | Reserved for JPEG extensions | nicht definiert | 0 x |
| JPGn | Reserved for JPEG extensions | nicht definiert | 0 x |
| RSTn | Restart | nicht definiert | 0 x |
| APP0 | Application Marker 0 | JFIF-Marker | 1 x |
| APPn | Application Marker 1-15 | verschieden (undefiniert) | 0 x |
| SOF0 | Start of frame | Baseline DCT, Huffmann | 1 x |
| SOF1 | Start of frame | Extended sequential DCT, Huffmann | 1 x |
| SOF2 | Start of frame | Progressive DCT, Huffmann | 1 x |
| SOF3 | Start of frame | Spatial sequential lossless, Huffmann | 1 x |
| SOF5 | Start of frame | Differential sequential DCT, Huffmann | 1 x |
| SOF6 | Start of frame | Differential progressive DCT, Huffmann | 1 x |
| SOF7 | Start of frame | Differential spatial, Huffmann | 1 x |
| SOF9 | Start of frame | Extended sequential DCT, Huffmann | 1 x |
| SOF10 | Start of frame | Progressive DCT, Arithmetic | 1 x |
| SOF11 | Start of frame | Spatial sequential lossless, Arithmetic | 1 x |
| SOF13 | Start of frame | Differential sequential DCT, Arithmetic | 1 x |
| SOF14 | Start of frame | Differential progressive DCT, Arithmetic | 1 x |
| SOF15 | Start of frame | Differential spatial, Arithmetic | 1 x |

Anmerkungen: 0x = nie, 1x = ein mal, nx = beliebig oft; (es darf auch nur einmal ein SOF-Marker vorkommen)

Anhang F – Sektionen und Parameter der signierten Konfigurationsdatei

Beschreibung KOBIL KAAN Professional / Advanced

Diese Section enthält folgende Parameter, die zur Authentifizierung des KOBIL KAAN Professional Chipkartenterminals benötigt werden:

- SectionName: KOBIL KAAN professional
- Name: file:beschreibung kobil kaan professional
- Digest-Algorithms: SHA-1 Digest
- SHA-1 Digest: 2j mj715rSw0yVb/vlWAYkK/YBwk=
- Magic: UsesMetaData
- isSecure: Yes
- Port0: 1
- ctapi: CT-API KOBIL Systems
- Status0: 4445787878435433393956322e3038
- Status1: 4445787878435420433256312e3032
- UseGUI0: Yes

Hinweis: Im Installationspackage sind 2 Ausprägungen für die jeweiligen Kartenleser vorhanden. Diese Dateien unterscheiden sich durch den Parameter Port0. Dieser ist jeweils auf den Wert „1“ (entspricht CTAPI Port 1) bzw. „2“ (entspricht CTAPI Port 2) gesetzt. Während der Installation muss der Benutzer den verwendeten CTAPI-Port auswählen. Das Installationsprogramm installiert dementsprechend die richtige ESW-Datei.

Beschreibung REINER SCT cyberJack™ e-com

Diese Section enthält folgende Parameter, die zur Authentifizierung des REINER SCT cyberJack™ e-com Chipkartenterminals benötigt werden:

- SectionName: cyberJack e-com
- Name: file:beschreibung cyberjack e-com
- Digest-Algorithms: SHA-1
- SHA-1-Digest: 2j mj715rSw0yVb/vlWAYkK/YBwk=
- MAGIC: UsesMetadata
- isSecure: Yes
- ctapi: CT-API REINER SCT
- Manufacturer: REINER SCT
- Port0: 1
- Status0: 444553435445435553422056322e30
- Status1: 444553435445434c50542056322e30
- UseGUI1: No

Beschreibung REINER SCT cyberJack™ KB

Diese Section enthält folgende Parameter, die zur Authentifizierung des REINER SCT cyberJack™ e-com Chipkartenterminals benötigt werden:

- SectionName: cyberJack KB
- Name: file:beschreibung cyberjack kb
- Digest-Algorithms: SHA-1
- SHA-1-Digest: 2j mj7l5rSw0yVb/vlWAYkK/YBwk=
- MAGIC: UsesMetadata
- isSecure: Yes
- ctapi: CT-API REINER SCT
- Port0: 1
- Status0: 4445534354202020202056332e3520
- UseGUI0: No

Beschreibung REINER SCT cyberJack™ Pinpad

Diese Section enthält folgende Parameter, die zur Authentifizierung des REINER SCT cyberJack™ Pinpad Chipkartenterminals benötigt werden:

- SectionName: cyberJack pinpad
- Name: file:beschreibung cyberjack pinpad
- Digest-Algorithms: SHA-1
- SHA-1-Digest: 2j mj7l5rSw0yVb/vlWAYkK/YBwk=
- MAGIC: UsesMetadata
- isSecure: Yes
- ctapi: CT-API REINER SCT
- Port0: 1
- Status0: 444553435450505553422056322e30
- Status1: 444553435450504c50542056322e30
- Status2: 4445534354434a5050412056332e30
- Status3: 4445534354434a5050412056342e30
- UseGUI1: No

Beschreibung SCM SPR 532

Diese Section enthält folgende Parameter, die zur Authentifizierung des SCM SPR 532 Chipkartenterminals benötigt werden:

- SectionName: SCM SPR 532
- Name: file:beschreibung scm spr 532
- Digest-Algorithms: SHA-1

- SHA-1-Digest: 2j mj715rSw0yVb/vlWAYkK/YBwk=
- MAGIC: UsesMetadata
- isSecure: Yes
- ctapi: CT-API SCM
- Port0: 1
- Status0: 444553434d535052783346342e3135
- Status1: 444553434d535052783346352e3038
- Status2: 444553434d535052783346352e3130
- Status3: 444553434d535052783346352e3039
- UseGUI0: No

Beschreibung Cherry Smartboards

Diese Section enthält folgende Parameter, die zur Authentifizierung der Cherry Smartboards benötigt werden:

- SectionName: Cherry Kartenleser
- Name: file:beschreibung cherry kartenleser
- Digest-Algorithms: SHA-1
- SHA-1-Digest: 2j mj715rSw0yVb/vlWAYkK/YBwk=
- MAGIC: UsesMetadata
- isSecure: Yes
- ctapi: CT-API Cherry
- Port0: 1
- Status0: 444543594d50432f53430000000000
- Status1: 444543594d50432f53430100000000
- UseGUI0: Yes

Beschreibung Fujitsu-Siemens SCR Keyboard

Diese Section enthält folgende Parameter, die zur Authentifizierung des Fujitsu-Siemens SCR Keyboard benötigt werden:

- SectionName: Reader
- Name: file:beschreibung Fujitsu_Siemens_KBPC_CX
- Digest-Algorithms: SHA-1
- SHA-1-Digest: 2j mj715rSw0yVb/vlWAYkK/YBwk=
- MAGIC: UsesMetadata
- isSecure: Yes
- ctapi: CT-API Cardman
- Status0: 444555449434d20202030342e3030
- Port0: 1
- UseGUI: No

Beschreibung Omnikey Cardman 3621

Diese Section enthält folgende Parameter, die zur Authentifizierung des Omnikey Cardman 3621 benötigt werden:

- Name: file:beschreibung omnikey3621
- SectionName: Reader
- Digest-Algorithms: SHA-1
- SHA-1-Digest: 2jmj7l5rSw0yVb/vlWAYkK/YBwk=
- isSecure: Yes
- ctapi: PCSC
- Status0: 4f4d4e494b455920436172644d616e2033363231
- Port0: none
- MAGIC: UsesMetadata
- UseGUI: Yes
- UseBeep: Yes
- UserMessage: 1

Beschreibung Omnikey Cardman 3821

Diese Section enthält folgende Parameter, die zur Authentifizierung des Omnikey Cardman 3821 benötigt werden:

- Name: file:beschreibung omnikey3821
- SectionName: Reader
- Digest-Algorithms: SHA-1
- SHA-1-Digest: 2jmj7l5rSw0yVb/vlWAYkK/YBwk=
- isSecure: Yes
- ctapi: PCSC
- Status0: 4f4d4e494b455920436172644d616e2033383231
- Port0: none
- MAGIC: UsesMetadata
- UseGUI: Yes
- UseBeep: Yes
- UserMessage: 1

BDC hotSign

Diese Section enthält folgende Parameter, die zur Authentifizierung und zur Konfigurierung von hotSign benötigt werden:

- Name: executable:hotsign.exe
- SectionName: hotSign
- Digest-Algorithms: SHA-1
- SHA-1-Digest: V26AEs6psQKnvIuEe2BJK5p/l0=
- Logging: Disabled
- TrustSign0: 07+UAIEx/mVF'TFUgQXVzdHJpYSAxLjI4
- TrustMark0: NotSupported

- Reader0: Reader
- BankCard0: O78RAIEx/kVFUEE=
- BankCard1: O78RAIEx/kVNQ0E=
- MAGIC: UsesMetadata
- AllowedOS: 2000;2003;XP;Vista
- Main-Class: at.hotSign.secsign.responder.WebClient
- ClassPath: w3c_http.jar;iaik_ssl.jar;iaik_jce_full.jar;ixsil-20020912.jar;iaik_cms.jar;hotSign.jar;iaik_ecc.jar;jh.jar;help.jar;ss_css2.jar
- BankCardHash0: SHA1
- BankCardHash1: SHA1
- TrustSignHash0: SHA1

AbsoluteLayout.jar

- Name: file:jre\lib\endorsed\AbsoluteLayout.jar
- SectionName: AbsoluteLayout JAR
- Digest-Algorithms: SHA-1
- SHA-1-Digest: 16kTCaS/uu057LvJ5pBUZQJljPI=

dcpr.dll

- Name: file:jre\bin\dcpr.dll
- SectionName: dcpr DLL
- Digest-Algorithms: SHA-1
- SHA-1-Digest: 7N1llQx1xdGjdftdXAHIdiDH4YM=

jce.jar

- Name: file:jre\lib\jce.jar
- SectionName: jce JAR
- Digest-Algorithms: SHA-1
- SHA-1-Digest: ApHDdoktcVGJBblrFWg00JoNomw=

jpeg.dll

- Name: file:jre\bin\jpeg.dll
- SectionName: jpeg DLL
- Digest-Algorithms: SHA-1
- SHA-1-Digest: s+46eWiNtsoble4HAn1RF4Ea17c=

nio.dll

- Name: file:jre\bin\nio.dll
- SectionName: nio DLL
- Digest-Algorithms: SHA-1
- SHA-1-Digest: gvik6rPQgj5zye+9xlrkPGur2b4=

profile.xml

- Name: file:config\profile.xml
- SectionName: profile XML
- Digest-Algorithms: SHA-1
- SHA-1-Digest: yHvAd/vWCUCDJKxy49TclKqgG4U=

resources.jar

- Name: file:jre\lib\resources.jar
- SectionName: resources JAR
- Digest-Algorithms: SHA-1
- SHA-1-Digest: HxzWHeuTGSmxxRb6M2D+oHepmYQ=

ss_css2.jar

- Name: file:ss_css2.jar
- SectionName: ss_css2 JAR
- Digest-Algorithms: SHA-1
- SHA-1-Digest: GFhm5q9mFAGGP7udnSaYyoqWb2o=

Java Virtuelle Maschine

Diese Section enthält folgende Parameter, die zur Authentifizierung und Konfiguration der Java Virtuellen Maschine benötigt werden:

- Name: executable:jre\bin\client\jvm.dll
- SectionName: JVM
- Digest-Algorithms: SHA-1
- SHA-1-Digest: bimZ+3AL3OhIpnSKBKuJnuileYO=
- MAGIC: UsesMetadata
- Files0: verify DLL;zip DLL;hpi DLL;awt DLL;fontmanager DLL;net DLL;rt JAR;jsse JAR;charsets JAR;xalan JAR;xercesImpl JAR;xml-apis JAR;Launcher JAR;dnsns JAR;localedata JAR;w3c_http JAR;iaik_ssl JAR;iaik_jce_full JAR;ixsil-20020912 JAR;iaik_cms JAR;hotSign JAR;iaik_ecc JAR;jh JAR;help JAR;ss_css2 JAR;java DLL;jce JAR;resources JAR
- Files1: AbsoluteLayout JAR;nio DLL;jpeg DLL;dcpr DLL;profile XML
- Directorys: Endorsed;Extension;Settings

Directory Extension

Diese Section enthält folgende Parameter, die zur Authentifizierung des Inhalts des Erweiterungsverzeichnisses der Java Virtuellen Maschine benötigt werden:

- Name: file:directory extension
- SectionName: Extension
- Digest-Algorithms: SHA-1

- SHA-1-Digest: 2j mj715rSw0yVb/vlWAYkK/YBwk=
- MAGIC: UsesMetadata
- Files: .;.;Launcher.jar;dnsns.jar;localedata.jar
- Path: jre\lib\ext

Directory Settings

Die Section enthält folgende Parameter, die zur Authentifizierung des Inhalts des Konfigurationsverzeichnis benötigt werden:

- Name: file:directory settings
- SectionName: Settings
- Digest-Algorithms: SHA-1
- SHA-1-Digest: 2j mj715rSw0yVb/vlWAYkK/YBwk=
- MAGIC: UsesMetadata
- Files: .;.;ca.xml;certs.xml;proxy.conf;xsl.dat;hotsign.p12;auth.conf;ti
- pps.txt
- Path: config\settings

Endorsed Settings

Die Section enthält folgende Parameter, die zur Authentifizierung des Inhalts des Konfigurationsverzeichnis benötigt werden:

- Name: file:directory endorsed
- SectionName: Endorsed
- Digest-Algorithms: SHA-1
- SHA-1-Digest: 2j mj715rSw0yVb/vlWAYkK/YBwk=
- MAGIC: UsesMetadata
- Files: .;.;xalan.jar;xercesImpl.jar;xml-apis.jar;AbsoluteLayout.jar
- Path: jre\lib\endorsed

java.dll

Die Section enthält folgende Parameter, die zur Authentifizierung des Inhalts eines Teils der Implementierung des Core APIs der Java Virtuellen Maschine benötigt werden:

- Name: file:jre\bin\java.dll
- SectionName: java DLL
- Digest-Algorithms: SHA-1
- SHA-1-Digest: BGkB+dji+yhE0CCfRoahogx4EV0=

awt.dll

Die Section enthält folgende Parameter, die zur Authentifizierung des Inhalts eines Teils der Implementierung des Core APIs der Java Virtuellen Maschine benötigt werden:

- Name: file:jre\bin\awt.dll
- SectionName: awt DLL
- Digest-Algorithms: SHA-1
- SHA-1-Digest: i2snPL4xTSHAmf0hMhbd/FnkQP4=

fontmanager.dll

Die Section enthält folgende Parameter, die zur Authentifizierung des Inhalts eines Teils der Implementierung des Core APIs der Java Virtuellen Maschine benötigt werden:

- Name: file:jre\bin\fontmanager.dll
- SectionName: fontmanager DLL
- Digest-Algorithms: SHA-1
- SHA-1-Digest: Sy9n7iWQhf9SuIZfxHvdlOxWQks=

net.dll

Die Section enthält folgende Parameter, die zur Authentifizierung des Inhalts eines Teils der Implementierung des Core APIs der Java Virtuellen Maschine benötigt werden:

- Name: file:jre\bin\net.dll
- SectionName: net DLL
- Digest-Algorithms: SHA-1
- SHA-1-Digest: Ei8LRSS4/Ibj4j+MJ70gO+A8WHc=

hpi.dll

Die Section enthält folgende Parameter, die zur Authentifizierung des Inhalts eines Teils der Implementierung des Core APIs der Java Virtuellen Maschine benötigt werden:

- Name: file:jre\bin\hpi.dll
- SectionName: hpi DLL
- Digest-Algorithms: SHA-1
- SHA-1-Digest: KC7hUBJ2ws3rk/kOf3WzyAxdhIw=

zip.dll

Die Section enthält folgende Parameter, die zur Authentifizierung des Inhalts eines Teils der Implementierung des Core APIs der Java Virtuellen Maschine benötigt werden:

- Name: file:jre\bin\zip.dll
- SectionName: zip DLL
- Digest-Algorithms: SHA-1
- SHA-1-Digest: ua2OaTbYtV1EQtCBmDiiiuyfxXs=

verify.dll

Die Section enthält folgende Parameter, die zur Authentifizierung des Inhalts eines Teils der Implementierung des Core APIs der Java Virtuellen Maschine benötigt werden:

- Name: file:jre\bin\verify.dll
- SectionName: verify DLL
- Digest-Algorithms: SHA-1
- SHA-1-Digest: ZtHk4Dd9BzZkO12jYdh0q53d/i4=

rt.jar

Die Section enthält folgende Parameter, die zur Authentifizierung des Inhalts eines Teils der Implementierung des Core APIs der Java Virtuellen Maschine benötigt werden:

- Name: file:jre\lib\rt.jar
- SectionName: rt JAR
- Digest-Algorithms: SHA-1
- SHA-1-Digest: Ocr2GkTBusmIVty6q78MCjkIJNM=

jsse.jar

Die Section enthält folgende Parameter, die zur Authentifizierung des Inhalts eines Teils der Implementierung des Core APIs der Java Virtuellen Maschine benötigt werden:

- Name: file:jre\lib\jsse.jar
- SectionName: jsse JAR
- Digest-Algorithms: SHA-1
- SHA-1-Digest: pwKTXk3OCnA55PFn9IDUVFOGJeE=

charsets.jar

Die Section enthält folgende Parameter, die zur Authentifizierung des Inhalts eines Teils der Implementierung des Core APIs der Java Virtuellen Maschine benötigt werden:

- Name: file:jre\lib\charsets.jar
- SectionName: charsets JAR
- Digest-Algorithms: SHA-1
- SHA-1-Digest: LE3FkQ05BZF4i9fXRoepXlGiE9o=

sunrsasign.jar

Die Section enthält folgende Parameter, die zur Authentifizierung des Inhalts eines Teils der Implementierung des Core APIs der Java Virtuellen Maschine benötigt werden:

- Name: file:jre\lib\sunrsasign.jar
- SectionName: sunrsasign JAR
- Digest-Algorithms: SHA-1
- SHA-1-Digest: FI5kJ/mSFFIK1WELTSE/QFTXqk8=

Launcher.jar

Die Section enthält folgende Parameter, die zur Authentifizierung des Inhalts eines Teils der Implementierung des Application Launchers des hot:Sign Signatur Clients benötigt werden:

- Name: file:jre\lib\ext\launcher.jar
- SectionName: Launcher JAR

- Digest-Algorithms: SHA-1
- SHA-1-Digest: JP2Auyyk4I3zHonlJps7Oyprbto=

dnsns.jar

Die Section enthält folgende Parameter, die zur Authentifizierung des Inhalts eines Teils der Implementierung der Architecture Extension der Java Virtuellen Maschine benötigt werden:

- Name: file:jre\lib\ext\dnsns.jar
- SectionName: dnsns JAR
- Digest-Algorithms: SHA-1
- SHA-1-Digest: B5EstZYzWB3VqhkoOjWmupUs6dM=

ldapsec.jar

Die Section enthält folgende Parameter, die zur Authentifizierung des Inhalts eines Teils der Implementierung der Architecture Extension der Java Virtuellen Maschine benötigt werden:

- Name: file:jre\lib\ext\ldapsec.jar
- SectionName: ldapsec JAR
- Digest-Algorithms: SHA-1
- SHA-1-Digest: Ilue+Sdl9fztReonXHEvDOowX3s=

localedata.jar

Die Section enthält folgende Parameter, die zur Authentifizierung des Inhalts eines Teils der Implementierung der Architecture Extension der Java Virtuellen Maschine benötigt werden:

- Name: file:jre\lib\ext\localedata.jar
- SectionName: localedata JAR
- Digest-Algorithms: SHA-1
- SHA-1-Digest: VK2AfEvd6qxPqnhp3vKqTdUDBCY=

iaik_jce_full.jar

Die Section enthält folgende Parameter, die zur Authentifizierung des Inhalts eines Teils der Implementierung des BDC hot:Sign Signatur Clients benötigt werden:

- Name: file:iaik_jce_full.jar
- SectionName: iaik_jce_full JAR
- Digest-Algorithms: SHA-1
- SHA-1-Digest: +hhyAdPXhReEj1BF3zQXAxhN1p8=

iaik_cms.jar

Die Section enthält folgende Parameter, die zur Authentifizierung des Inhalts eines Teils der Implementierung des BDC hot:Sign Signatur Clients benötigt werden:

- Name: file:iaik_cms.jar
- SectionName: iaik_cms JAR
- Digest-Algorithms: SHA-1
- SHA-1-Digest: FBW0QvbAZklUgs2FGf9r6BNi+lM=

xalan.jar

Die Section enthält folgende Parameter, die zur Authentifizierung des Inhalts eines Teils der Implementierung des BDC hot:Sign Signatur Clients benötigt werden:

- Name: file:jre\lib\endorsed\xalan.jar
- SectionName: xalan JAR
- Digest-Algorithms: SHA-1
- SHA-1-Digest: 4EdTdxMhZc//ewkiKjMAuzv1PI=

xercesImpl.jar

Die Section enthält folgende Parameter, die zur Authentifizierung des Inhalts eines Teils der Implementierung des BDC hot:Sign Signatur Clients benötigt werden:

- Name: file:jre\lib\endorsed\xercesimpl.jar
- SectionName: xercesImpl JAR
- Digest-Algorithms: SHA-1
- SHA-1-Digest: w67fxuWtpJnUab6wQv5VNBFSsgc=

xml-apis.jar

Die Section enthält folgende Parameter, die zur Authentifizierung des Inhalts eines Teils der Implementierung des BDC hot:Sign Signatur Clients benötigt werden:

- Name: file:jre\lib\endorsed\xml-apis.jar
- SectionName: xml-apis JAR
- Digest-Algorithms: SHA-1
- SHA-1-Digest: CRe0oJUC9pF9/rlpx9WaulJ8HKY=

ixsil-20020912

Die Section enthält folgende Parameter, die zur Authentifizierung des Inhalts eines Teils der Implementierung des BDC hot:Sign Signatur Clients benötigt werden:

- Name: file:ixsil-20020912.jar
- SectionName: ixsil-20020912 JAR
- Digest-Algorithms: SHA-1
- SHA-1-Digest: bhIzqmUDCPakhsvch45vJ/wPjLw=

iaik_ecc.jar

Die Section enthält folgende Parameter, die zur Authentifizierung des Inhalts eines Teils der Implementierung des BDC hot:Sign Signatur Clients benötigt werden:

- Name: file:iaik_ecc.jar
- SectionName: iaik_ecc JAR
- Digest-Algorithms: SHA-1
- SHA-1-Digest: aA2zL5a3gCfj0aCuRA0Xygt9UgE=

iaik_ssl.jar

Die Section enthält folgende Parameter, die zur Authentifizierung des Inhalts eines Teils der Implementierung des BDC hot:Sign Signatur Clients benötigt werden:

- Name: file:iaik_ssl.jar
- SectionName: iaik_ssl JAR
- Digest-Algorithms: SHA-1
- SHA-1-Digest: n1fC5fnEqbbXdIOIggqirSQfQzA=

w3c_http.jar

Die Section enthält folgende Parameter, die zur Authentifizierung des Inhalts eines Teils der Implementierung des BDC hot:Sign Signatur Clients benötigt werden:

- Name: file:w3c_http.jar
- SectionName: w3c_http JAR
- Digest-Algorithms: SHA-1
- SHA-1-Digest: tCyXj4ckJEd0+0L4qS1vFQHGgBE=

jh.jar

Die Section enthält folgende Parameter, die zur Authentifizierung des Inhalts eines Teils der Implementierung des BDC hot:Sign Signatur Clients benötigt werden:

- Name: file:jh.jar
- SectionName: jh JAR
- Digest-Algorithms: SHA-1
- SHA-1-Digest: DCyfvAmDHx9eFLpeuk2DJ4B2n80=

help.jar

Die Section enthält folgende Parameter, die zur Authentifizierung des Inhalts eines Teils der Implementierung des BDC hot:Sign Signatur Clients benötigt werden:

- Name: file:help.jar
- SectionName: help JAR
- Digest-Algorithms: SHA-1
- SHA-1-Digest: VUGCqSUMEjw0FjYcIb4D62S1ldI=

hotSign.jar

Die Section enthält folgende Parameter, die zur Authentifizierung des Inhalts eines Teils der Implementierung des BDC hot:Sign Signatur Clients benötigt werden:

- Name: file:hotsign.jar
- SectionName: hotSign JAR
- Digest-Algorithms: SHA-1
- SHA-1-Digest: o1b720k3XJEHetsJqIjNWAiIK2s=

Property Settings

Die Section enthält folgende Parameter, die der virtuellen Maschine beim Starten mitgegeben werden. Es handelt sich dabei um Environment-Variablen, die im OS gesetzt werden können.

- Name: file:beschreibung properties

- SectionName: Properties
- Digest-Algorithms: SHA-1
- SHA-1-Digest: 2jmj7l5rSw0yVb/vlWAYkK/YBwk=
- MAGIC: UsesMetadata
- Key0: CITIZENCARD.Security-Layer.HTTP.PORT
- Key1: CITIZENCARD.Security-Layer.HTTP.HOST
- Key2: BDC.Security-Layer.HTTP.PORT
- Key3: CITIZENCARD.Security-Layer.TCPIP.PORT
- Key4: CITIZENCARD.Security-Layer.TCPIP.HOST
- Key5: DCITIZENCARD.Security-Layer.HTTPS.PORT
- Key6: DCITIZENCARD.Security-Layer.TLS.PORT
- Key7: DCITIZENCARD.Security-Layer.HTTPS.HOST
- Key8: DCITIZENCARD.Security-Layer.TLS.HOST
- Property0: %CITIZENCARD.Security-Layer.HTTP.PORT%
- Property1: %CITIZENCARD.Security-Layer.HTTP.HOST%
- Property2: %BDC.Security-Layer.HTTP.PORT%
- Property3: %CITIZENCARD.Security-Layer.TCPIP.PORT%
- Property4: %CITIZENCARD.Security-Layer.TCPIP.HOST%
- Property5: %CITIZENCARD.Security-Layer.HTTPS.PORT%
- Property6: %CITIZENCARD.Security-Layer.TLS.PORT%
- Property7: %CITIZENCARD.Security-Layer.HTTPS.HOST%
- Property8: %CITIZENCARD.Security-Layer.TLS.HOST%