

Herstellereklärung  
Der Hersteller

**Mentana-Claimsoft AG**  
Spreenhagener Str. 16  
D-15528 Spreenhagen

erklärt hiermit gemäß § 17 Abs. 4 Satz 2 SigG<sup>1</sup>,  
in Verbindung mit § 15 Abs. 5 SigV<sup>2</sup>,  
dass sein Produkt

**M-Doc AutoSigner Version 2.1**

eine Teil- Signaturanwendungskomponente (Software) gemäß § 2 Nr. 11 a SigG ist, die es ermöglicht

- Daten dem Prozess der Erzeugung qualifizierter elektronischer Signaturen zuzuführen und sicher anzuzeigen

Unbeschadet der Veröffentlichung im Amtsblatt der Bundesnetzagentur (vormals Regulierungsbehörde für Post und Telekommunikation) gemäß § 17 Abs. 4 Satz 3 SigG wird ein Widerruf oder eine Erneuerung dieser Erklärung auch unter:

<http://www.mentana-claimsoft.de> veröffentlicht.

Spreenhagen, den 22.04.2010

Jürgen Ludyga  
Leiter Softwareentwicklung

Dipl. Ing. Axel Janhoff  
Vorstand

<sup>1</sup> Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz – SigG) vom 16. Mai 2001 (BGBl. S. 876, Jahrgang 2001 Teil I Nr. 22) in der Fassung des 1.SigÄndG vom 04. Januar 2005 zuletzt geändert durch Artikel 4 des Gesetzes vom 17. Juli 2009 (BGBl. I S. 2091).

<sup>2</sup> Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) vom 16. November 2001 (BGBl. Jahrgang 2001 Teil I Nr. 59) in der Fassung des 1.SigÄndG vom 04. Januar 2005 (BGBl. I S. 2) zuletzt geändert durch die Verordnung vom 17. Dezember 2009 (BGBl. I S. 3932).

## Inhaltsverzeichnis

Deckblatt.....	1
Herstellererklärung .....	1
1. Handelsbezeichnung .....	3
2. Lieferumfang und Versionsinformationen.....	3
2.1 Tabelle Lieferumfang des Produkts .....	3
2.2 Benötigte und bestätigte Produkte .....	4
2.3 Benötigte und „nicht bestätigte“ Produkte .....	9
2.4 Schnittstellen .....	9
3. Funktionsbeschreibung .....	10
3.1 Erstellen einer qualifizierten Signatur .....	13
3.2 Erstellen qualifizierter Signaturen in einem Dokumentenstapel oder als Massensignatur .....	14
4. Erfüllung der Anforderungen des SigG und der SigV .....	16
4.1 Erfüllte Anforderungen .....	16
4.1.1 Erfüllte Anforderungen § 17 Abs. 2 Satz 1 SigG .....	16
4.1.2 Erfüllte Anforderungen § 15 Abs. 2 Nr. 1 SigV .....	16
4.1.5 Erfüllte Anforderungen § 17 Abs. 2 Satz 3 SigG .....	17
4.1.6 Erfüllte Anforderungen § 15 Abs. 4 SigV .....	17
5. Einsatzbedingungen .....	18
5.1.1 Potentielle Bedrohungen.....	18
5.1.2 Maßnahmen in der Einsatzumgebung .....	18
a) Zulässige IT- Komponenten und Systeme für den Signaturbetrieb .....	19
b) Auflagen zur Anbindung an das Internet.....	19
c) Auflagen zur Anbindung an ein Intranet .....	20
d) Auflagen zur Sicherheit der IT-Plattform und Applikationen .....	20
e) Auflagen zur Auslieferung und Installation des Produktes.....	21
f) Auflagen zur Nutzung von bestimmten Signaturkarten (SSEE) .....	22
g) Schutz vor unbefugter Veränderung .....	22
h) Maßnahmen zur Zugangskontrolle.....	24
i) Absicherung von Schnittstellen .....	24
5.1.3 Wartung/Reparatur.....	24
6. Algorithmen und zugehörige Parameter.....	25
7. Gültigkeit der Herstellererklärung.....	25
8. Begleitende Dokumente .....	26

Dokumenten -Version	Bearbeiter	Inhalt	Datum
2.01	Raoul Kirmes	Übernahme Stand Amtsbaltt BNetzA	15.11.2007
2.02	Raoul Kirmes	Überarbeitung Algorithmen	30.03.2008
2.03	Raoul Kirmes	Ergänzung SSEE/Leser	15.05.2008
2.04	Raoul Kirmes	Umsetzung aktuelles Release	17.05.2008
2.05	Dr. Ralf Hesse	Prüfung/ Freigabe	18.05.2008
2.06	Axel Janhoff	Autorisierung zur Veröffentlichung	28.05.2008
2.07	Raoul Kirmes	Einarbeitung Prüfbericht BNetzA	12.12.2008
2.08	Dr. Ralf Hesse	Anpassung 2009 Unterversionen	25.04.2009
2.09	Raoul Kirmes	Prüfaussagen/Prüfbericht BNetzA	08.05.2009
2.10	Axel Janhoff	Autorisierung zur Veröffentlichung	11.05.2009
2.11	Raoul Kirmes	Umsetzung aktuelles Release	15.09.2009
2.12	Raoul Kirmes	Einarbeitung Prüfbericht BNetzA	04.11.2009
2.13	Axel Janhoff	Autorisierung zur Veröffentlichung	12.11.2009
2.14	Raoul Kirmes	Überarbeitung	06.02.bis 15.04.2010
2.15	Axel Janhoff	Autorisierung zur Veröffentlichung	22.04.2010

## 1. Handelsbezeichnung

Die Handelsbezeichnung lautet: **M-Doc AutoSigner Version 2.1**

Hersteller: Mentana-Claimsoft AG  
Registergericht Frankfurt/Oder HRB 9343 FF  
Spreenhagener Str. 16  
D-15528 Spreenhagen  
[support@mentana.de](mailto:support@mentana.de)

Auslieferung: Online per Download oder als DVD/CD.

## 2. Lieferumfang und Versionsinformationen

### 2.1 Tabelle Lieferumfang des Produkts

Lieferumfang der Signaturanwendungskomponente				
Produktart	Bezeichnung	Version	Datum	Auslieferung
Software	„Setup_AS_2.1.exe“ (Win)	2.1	16.09.2009	Siehe Kap. 5.1.2.e
Software	„Autosigner“ (Linux)	2.1	16.09.2009	Siehe Kap. 5.1.2.e
Das Produkt benötigt keine externen Funktionsbibliotheken oder Komponenten von Drittanbietern				
Handbuch	Handbuch für M-Doc Auto- Signer.pdf	1.029	15.04.2009	Siehe Kap. 5.1.2.e

Die Teil- Signaturanwendungskomponente M-Doc AutoSigner Version 2.1 wird vom Hersteller als Installationspaket über das Internet vertrieben. Nähere Angaben zum Verfahren werden in Kap. 5.1.2. lit. e) beschrieben.

## 2.2 Benötigte und bestätigte Produkte<sup>3</sup>

Sichere Signaturerstellungseinheiten (SSEE)/ Smart-Cards							
Handelsbezeichnung	ZDA	Reg-Nr. ZDA	Name der SSEE in der Bestätigungs-urkunde	Bestätigung der SSEE	unterstützt wird:		
					qualifizierte Signatur	Ver-/Entschlüsselung Authentisierung	Massen / Stapel-Signatur
<b>PKS- Card (E4 NetKey 3.01)</b>	Produktzentrum TeleSec Telekom AG	Z0001	SSEE TCOS 3.0 Signature Card, Version 1.0 with Philips chip P5CT072V0Q / P5CD036V0Q	TUVIT. 93119.TE.09.2006	[+] <sup>4</sup>	[+]	[-] <sup>5</sup>
<b>„Multisign“</b>	Produktzentrum TeleSec Telekom AG	Z0001	TCOS 3.0 Signature Card, Version 1.0 with Philips chip P5CT072V0Q / P5CD036V0Q	TUVIT. 93119.TE.09.2006	[+]	[+]	[+]
<b>Signaturkarte der Bundesnotarkammer</b>	Bundesnotarkammer, Zertifizierungsstelle	Z0003	SSEE STRACOS 3.0 with Electronic Signature Application V3.0	TUVIT.93100.TE.09.2005, Nachtrag vom 08.08.2006, 20.10.2006, 07.12.2006,15.06	[+]	[+]	[0] <sup>6</sup>
<b>Signaturkarte für Berufsträger der DATEV</b>	DATEV eG Zertifizierungsstelle	Z0004	SSEE STRACOS 3.0 with Electronic Signature Application V3.0	TUVIT.93100.TE.09.2005, Nachtrag vom 08.08.2006, 20.10.2006,07.12.2006,15.06.2007	[+]	[+]	[0]

<sup>3</sup> Nicht im Lieferumfang enthalten.

<sup>4</sup> [+] = unterstützt.

<sup>5</sup> [-] = nicht unterstützt.

<sup>6</sup> [0] = Funktionalität nicht vorhanden/gesperrt.

<b>D-Trust-Signaturkarte Version 2.2</b>	D-Trust GmbH	Z0017 und angezeigt § 4 Abs. 3 SigG	SSEE „Chipkarte mit Prozessor SLE66CX322P, CardOS V4.3B mit Applikation für digitale Signatur“	T-Systems .02122.TE.05.2005, Nachtrag vom 06.05.2008	[+]	[+]	[0]
<b>D-Trust-muticard</b>	D-Trust GmbH	Z0017 und angezeigt § 4 Abs. 3 SigG	SSEE „Chipkarte mit Prozessor SLE66CX322P, CardOS V4.3B mit Applikation für digitale Signatur“	T-Systems .02122.TE.05.2005, Nachtrag vom 06.05.2008	[+]	[+]	[+]
<b>SigntrustCard3.0/ Signtrust MCard100 3.0/ Signtrust MCard 3.0</b>	Deutsche Post Com GmbH Geschäftsfe Id Signtrust	Z0002	SSEE STARCOS 3.0 with Electronic Signature Application V3.0 der Giesecke & Devrient GmbH	TUVIT.93100.TE.09.2005, Nachtrag vom 08.08.2006, 20.10.2006, 07.12.2006,15.06.2007	[+]	[+]	[+]
<b>Signtrust Card 3.2</b>	Deutsche Post Com GmbH Geschäftsfe Id Signtrust	Z0002	SSEE STARCOS 3.2 QES Version 1.1	BSI.02102.TE.11.2008	[+]	[+]	[+]
<b>Signtrust MCard 3.2</b>	Deutsche Post Com GmbH Geschäftsfe Id Signtrust	Z0002	SSEE STARCOS 3.2 QES Version 2.0	BSI.02114.TE.12.2008	[+]	[+]	[+]
<b>Signtrust MCard100 3.2</b>	Deutsche Post Com GmbH Geschäftsfe Id Signtrust	Z0002	SSEE STARCOS 3.2 QES Version 2.0B	BSI.02115.TE.12.2008	[+]	[+]	[+]
<b>TC-Trustcenter Q-Sign-Card (limited)</b>	TC TrustCenter TrustCenter GmbH	Z0032	SSEE „Chipkarte mit Prozessor SLE66CX322P, CardOS V4.3B mit Applikation für digitale Signatur“	T-Systems .02122.TE.05.2005 Nachtrag vom 06.05.2008	[+]	[+]	[0]

<b>TC-Trustcenter Q-Sign-Card (unlimited)</b>	TC TrustCenter TrustCenter GmbH	Z0032	SSEE „Chipkarte mit Prozessor SLE66CX322P, CardOS V4.3B mit Applikation für digitale Signatur“	T-Systems .02122.TE.05.2005, Nachtrag vom 06.05.2008	[+]	[+]	[+]
<b>Chambersign Karte der IHK D- Trust-Card (2.02c)</b>	D-Trust GmbH	Z0017 und angezeigt § 4 Abs. 3 SigG	SSEE „Chipkarte mit Prozessor SLE66CX322P, CardOS V4.3B mit Applikation für digitale Signatur	T-Systems .02122.TE.05.2005 Nachtrag vom 06.05.2008	[+]	[+]	[0]
<b>Sparkassen-Card oder GeldKarte</b>	S-Trust	angezeigt § 4 Abs. 3 SigG	SSEE ZKA-Signaturkarte, Version 5.02 der Gemplus-mids GmbH	TUVIT .09385.TU.09.2004	[+]	[+]	[+]
	S-Trust	angezeigt § 4 Abs. 3 SigG	SSEE ZKA-Signaturkarte, Version 5.11	TUVIT. 93138.TE.11.2006			
	S-Trust	angezeigt § 4 Abs. 3 SigG	SSEE ZKA Banking Signature Card, Version 6.2b NP und 6.2f NP, Type 3 der Giesecke & Devrient GmbH	TUVIT .09395.TU.01.2005	[+]	[+]	[-]
	S-Trust	angezeigt § 4 Abs. 3 SigG	SSEE ZKA Banking Signature Card, Version 6.31 NP, Type 3 der Giesecke & Devrient GmbH	TUVIT .09397.TU.03.2005	[+]	[+]	[-]
	S-Trust	angezeigt § 4 Abs. 3 SigG	SSEE ZKA Banking Signature Card, Version 6.32 NP, Type 3 der Giesecke & Devrient GmbH	TUVIT .93125.TU.12.2005	[+]	[+]	[-]

	S-Trust	angezeigt § 4 Abs. 3 SigG	SSEE ZKA Banking Signature Card, Version 6.4 der Giesecke & Devrient GmbH	TUVIT .93123.TU. 12. 2006	[+]	[+]	[-]
	S-Trust	angezeigt § 4 Abs. 3 SigG	SSEE ZKA- Signaturkarte, Version 5.10 der Gemplus- mids GmbH	TUVIT.93132.TU .06.2006 20.06.2006	[+]	[+]	[-]
	S-Trust	angezeigt § 4 Abs. 3 SigG	SSEE ZKA Banking Signature Card, Version 6.6 der Giesecke & Devrient GmbH	TUVIT .93130.TU.05.20 06 Nachtrag vom 28.08.2006 und vom 18.10.2006	[+]	[+]	[-]
	S-Trust	angezeigt § 4 Abs. 3 SigG	SSEE ZKA Banking Signature Card, Version 6.51 der Giesecke & Devrient GmbH	TUVIT .93129.TU.03.20 06	[+]	[+]	[-]
	S-Trust	angezeigt § 4 Abs. 3 SigG	Signaturerstellu ngseinheit ZKA SECCOS Sig v1.5.2 und 1.5.3 der Sagem Orga GmbH	BSI.02075.TE.08 .2006 BSI.02076.TE.12 .2006	[+]	[+]	[-]
	S-Trust	angezeigt § 4 Abs. 3 SigG	ZKA- Signaturkarte, Version 5.11 M Gemplus GmbH (Gemalto)	TUVIT .93148.TU.06.20 07	[+]	[+]	[+]
	S-Trust	angezeigt § 4 Abs. 3 SigG	ZKA- Signaturkarte, Version 6	TUVIT. 93143.TE.11.200 7	[+]	[+]	[-]
	S-Trust	angezeigt § 4 Abs. 3 SigG	ZKA Banking Signature Card, Version 7.1	TUVIT. 93149.TE.09.200 7	[+]	[+]	[-]
	S-Trust	angezeigt § 4 Abs. 3 SigG	ZKA Banking Signature Card, Version 7.1.1	TUVIT. 93159.TE.09.200 7	[+]	[+]	[-]

# Herstellereklärung

Teil- Signaturanwendungskomponente  
M-Doc AutoSigner Version 2.1

Seite 8

Mentana- Claimsoft AG NL Berlin/Brandenburg

HP.BK.10.06.002

	S-Trust	angezeigt § 4 Abs. 3 SigG	SSEE ZKA Banking Signature Card, Version 7.2.1	TUVIT. 93157.TE.06.200 8	[+]	[+]	[-]
	S-Trust	angezeigt § 4 Abs. 3 SigG	ZKA Banking Signature Card, Version 7.1.2	TUVIT. 93166.TU.06.200 8	[+]	[+]	[-]
	S-Trust	angezeigt § 4 Abs. 3 SigG	SSEE ZKA- Signaturkarte, Version 6.01	TUVIT. 93169.TU.09.200 8	[+]	[+]	[-]
<b>Signaturkarte der Deutschen Rente Bund</b>	Deutsche Rentenversi- cherung Bund	angezeigt § 4 Abs. 3 SigG	SSEE „Chipkarte mit Prozessor SLE66CX322P, CardOS V4.3B mit Applikation für digitale Signatur“	T-Systems .02122.TE.05. 2005, Nachtrag vom 06.05.2008	[+]	[+]	[-]
	Deutsche Rentenversi- cherung Bund	angezeigt § 4 Abs. 3 SigG	SSEE "ACOS EMV- A04V1"	T-Systems. 02166.TE.07.200 8 Nachtrag 1 18.12.2008 und Nachtrag 2 vom 18.05.2009	[+]	[+]	[-]

## Unterstützte Kartenlesegeräte

Handelsname	Angaben aus den veröffentlichten Bestätigungen bei der BNetzA			Schnittstelle
	Hersteller	Name	Reg. Nr.	
SPR 532 usb (Chipdrive pinpad pro)	SCM Microsystems GmbH	Chipkartenleser SPR132, SPR332, SPR532, Firmware Version 4.15	TUVIT.09370.TE. 03. 2003	USB, seriell
CardMan 3621	OMNIKEY	SAK Chipkartenterminal der Familie CardMan Trust CM3621, Firmware-Version 6.00	BSI.02057.TE.12 .2005	USB
CardMan 3821	OMNIKEY GmbH	SAK Chipkartenterminal der Familie CardMan Trust CM3821, Firmware-Version 6.00	BSI.02057.TE.12. 2005	USB
Cherry Smartboard G83-6744	Cherry GmbH	Chipkartenterminal der Familie SmartBoard xx44 Firmware-Version 1.04	BSI.02048.TE.12. 2004	USB
Cherry SmartTerminal 2000 U	Cherry GmbH	Chipkartenterminal der Familie SmartTerminal ST-2xxx, Firmware Version 5.08	BSI.02059.TE.02. 2006	USB
Kobil KAAN Advanced	Kobil Systems GmbH	Chipkartenterminal KAAN Advanced, Hardware Version K104R3, Firmware Version 1.19	BSI.02050.TE.12. 2006 vom 12.2006 und Nachtrag von T-Systems 02207.TU.04.2008	USB

### 2.3 Benötigte und „nicht bestätigte“ Produkte<sup>7</sup>

Allgemeine Aussagen über eine rechtswirksame Verwendbarkeit nicht bestätigter Produkte können vom Hersteller nicht abgegeben werden. Die Verwendung des Produktes im Umfeld der SigG, mit Einsatzkomponenten die nicht im Kap. 2.2. aufgeführt sind, erfordert eine herstellerseitige Einzelfallprüfung und ist nur nach ausdrücklicher schriftlicher Genehmigung durch den Hersteller zulässig.

### 2.4 Schnittstellen

M-Doc AutoSigner Version 2.1 verfügt über folgende Schnittstellen:

#### a) Schnittstelle zum Chipkartenleser:

Die Software sendet zu signierende Daten über eine Kabelverbindung zum Chipkartenleser und dieser die Daten an die Signaturkarte. Über diese Schnittstelle und empfängt M-Doc AutoSigner Version 2.1 die von der Signaturkarte verarbeiteten (signierten) Daten.

#### b) Schnittstelle zur grafischen Bedienungsfläche (Graphical User Interface – GUI):

<sup>7</sup> Nicht im Lieferumfang enthalten.

M-Doc AutoSigner Version 2.1 stellt eine grafische Oberfläche als Schnittstelle zum Signaturschlüssel-Inhaber bereit und visualisiert die Interaktion mit diesem.

### **c) Schnittstelle zur aufrufenden Anwendung/ Addon:**

M-Doc AutoSigner Version 2.1 kann über Kommando- Zeile (command-line) durch beliebige Anwendungen integriert werden. Über diese Schnittstelle werden die Software gestartet und Einstellungen vorgegeben. Über den Aufruf werden gleichzeitig die notwendigen Parameter (wie zu signierende Datei(en), Ablageort der signierten Dateien, Signaturformat) übergeben. Diese Schnittstelle dient auch zur Anbindung der Addon´s für M-Doc AutoSigner.

### **3. Funktionsbeschreibung**

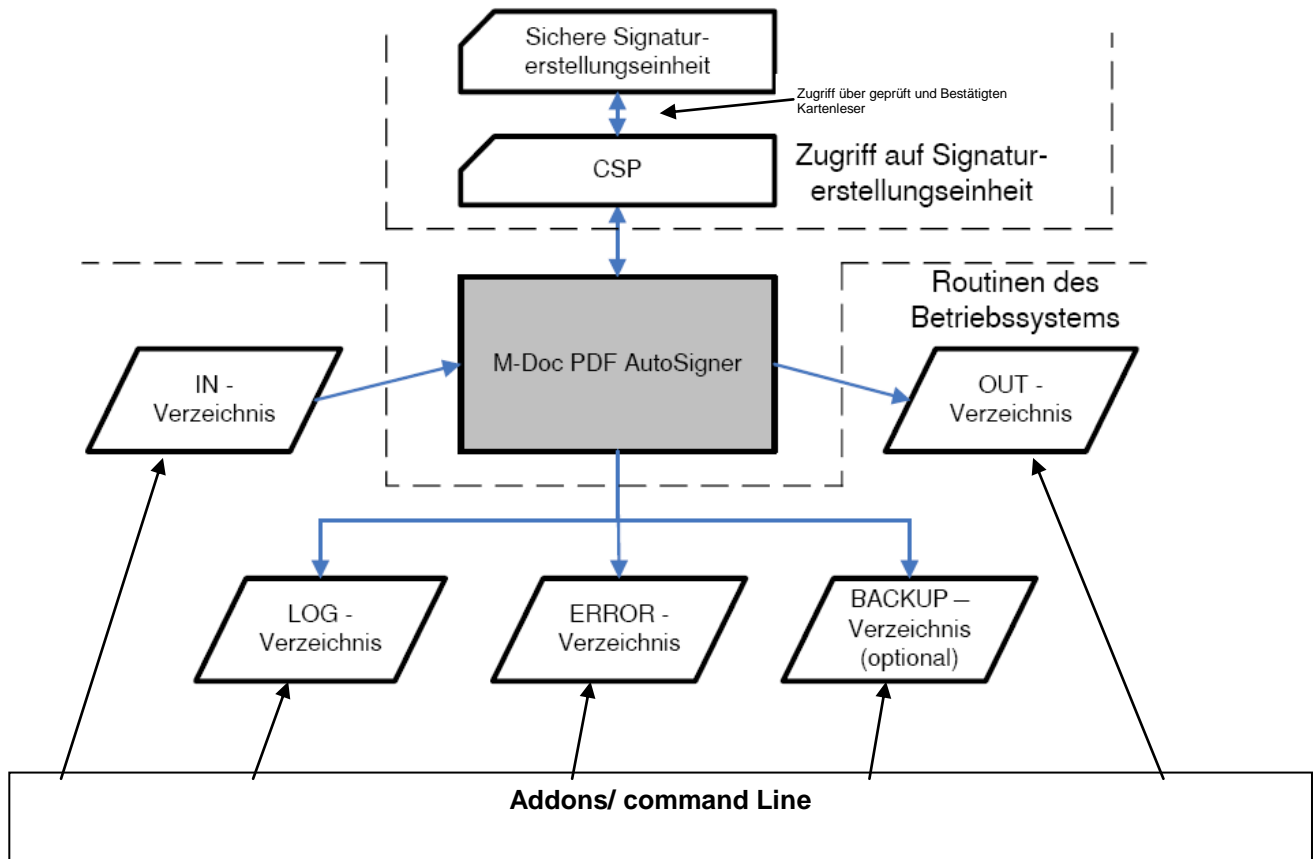
Der M-Doc AutoSigner Version 2.1 ist eine Teil- Signaturanwendungskomponente, die für die massenhafte Verarbeitung qualifizierter elektronischer Signaturen entwickelt wurde. Die Signaturanwendungskomponente M-Doc AutoSigner Version 2.1 kann bis zu 8 sichere Signaturerstellungseinheiten (SSEE) parallel ansprechen.

Für jede sichere Signaturerstellungseinheit kann eine Begrenzung der Signaturvorgänge -Anzahl- oder Zeitgesteuert- erfolgen. Die Signaturanwendungskomponente M-Doc AutoSigner Version 2.1 stellt sicher, dass die vorgegeben Einschränkungen für die Dauer bzw. die Anzahl der zu erstellenden Signaturen eingehalten werden. Ein Zwischenspeichern der PIN (PIN-Caching) ist weder zulässig, noch wird es durch Software technisch realisiert.

Das Entfernen einer sicheren Signaturerstellungseinheit (SSEE) aus dem jeweiligen Kartenlesegerät führt zur Beendigung des Signaturprozesses.

Der M-Doc AutoSigner Version 2.1 ist eine Teil- Signaturanwendungskomponente (Software), zur Erzeugung von elektronischen Dokumenten die den Formvorschriften der elektronischen Form im Sinne des § 126a BGB entsprechen. Der M-Doc AutoSigner Version 2.1 dient auch als Signaturkomponente im Anwendungsbereich einer virtuellen Poststelle (EGVP/ OSCI/De-Mail) zur Ausstellung von Eingangsbestätigungen.

## Schaubild Anwendungssystem M-Doc AutoSigner



Für die Signaturanwendungskomponente M-Doc AutoSigner Version 2.1 stehen für bestimmte häufig vorkommenden und vom Hersteller vorbereitete Addons zur Verfügung.

Bezeichnung des Addon	Kurz-Beschreibung
SOAP- Connector 1.3	Webservice –Schnittstelle
SMTP- Connector 1.1	Output via SMTP
Data Center Edition (DCE) 1.2	Umfangreiche Funktionen für den Einsatz in Rechenzentren und Großarchiven: <ul style="list-style-type: none"> <li>- Lastverteilung</li> <li>- Mandantenverwaltung</li> <li>- Queue-Transaktionskontrolle</li> <li>- Remoteüberwachung</li> <li>- High Availability -Unterstützung</li> <li>- Telesignatur</li> </ul>

SAM -SAP-Edition 1.1	Signaturmodul für SAP
Datatrain Signaturmodul for SAP 1.0	Signaturmodul für SAP
EDI- Connector 1.0	Schnittstelle für die Signatur von EDI Nachrichten EDIFACT und AUTACK
ASN.1-Connector	Signatur von ASN.1 Strukturen und DKIM nach RFC 5672 insbesondere für De-Mail Kommunikationsserver

Die Addons nutzen die Schnittstelle „command-line“ 2.4. c) des M-Doc AutoSigner Version 2.1 und sind deshalb im Rahmen dieser Herstellererklärung nicht näher zu erläutern.

Der M-Doc AutoSigner Version 2.1 ist eine Teil- Signaturanwendungskomponente gemäß § 2 Nr. 11 a SigG, die elektronische Daten dem Prozess der Erzeugung qualifizierter elektronischer Signaturen durch eine sichere Signaturerstellungseinheit (Chipkarte, nachfolgend als SSEE abgekürzt) zuführen und sicher anzeigen kann (secure Viewer).

Für die Signatur werden folgende Signaturformate unterstützt:

a) Bei beliebigem Eingangsformat der zu signierenden Datei:

1. „signedData“ gemäß RFC 2630 (Dateiendungen \*.pk7 \*.pkcs7 \*.p7b \*.CMS und \*.p7s)
2. „signedData“ mit „multipart-signed“-Content gemäß RFC 2633 (Dateiendung \*.p7m)
3. "XMLDsig" als "enveloped signature" oder "detached signature" gemäß RFC 3075-3275
4. EDIFACT- Nachricht [INVOIC] nach DIN [ISO9735- 5]
5. AUTACK- Nachricht nach DIN [ISO9735- 6]
6. ASN.1 Signatur auf Hash-String in den Bitlängen 256 bis 512

b) Bei Portable Document Format (PDF) 1.4-1.6 als Eingangsformat der zu signierenden Datei:

1. PDF (PKCS#7-konforme Signatur entsprechend Adobe-Reference 1.6)

M-Doc AutoSigner Version 2.1 verfügt über eine sichere Anzeige (Secure Viewer). Auf Aufforderung durch den Benutzer können beliebige druckbare Dokumentenformate in einem PDF-Viewer innerhalb von M-Doc AutoSigner Version 2.1 vor der Signaturerzeugung sicher angezeigt werden. Dazu werden die Dateien vom Ursprungsformat in das Format PDF/A nach DIN ISO 19005 konvertiert und mittels eines PDF- Viewers angezeigt und nach Autorisierung durch den Benutzer als PDF/A Dokument der SSEE zugeführt. Nicht durch den Secure-Viewer visualisierbare Dokumentenformate können durch Betätigung des Schalters "Datei anzeigen" mit Hilfe von Betriebssystemmitteln oder Programmen eines

Drittherstellers vor der Signaturerzeugung geöffnet werden, soweit eine sichere Anzeige gewährleistet ist (vgl. Kap. 4.1.2.c). M-Doc AutoSigner Version 2.1 ermöglicht auch die Anzeige von Zertifikatsinhalten über einen Zertifikatsviewer.

### 3.1 Erstellen einer qualifizierten Signatur

Beliebige elektronische Dateien (im Folgenden auch als Dokumente bezeichnet) können durch den Benutzer mit einer qualifizierten elektronischen Signatur versehen werden. Bei der Signatur von Dokumenten, die einem der Standards PDF 1.4, PDF 1.5, PDF 1.6 oder PDF/A entsprechen, wird die erstellte Signatur in das PDF- Dokument integriert. Die Möglichkeiten des PDF- Formates zur Darstellung von mehreren Signaturen über ein Dokument und die Signatur verschiedener, eingebetteter Dokumentenversionen innerhalb einer Datei werden vollständig unterstützt.

Der Hersteller weist daraufhin, dass zur Erzeugung einer qualifizierten elektronischen Signatur eine Kombination aus einem geprüften und bestätigten Kartenlesegerät und einer sicheren Signaturerstellungseinheit (SSEE) zum Einsatz kommen muss. In Kapitel 2.2.) dieser Herstellererklärung werden die sicheren Signaturerstellungseinheiten aufgeführt die im Einsatz mit M-Doc AutoSigner Version 2.1 erfolgreich getestet wurden.

Um den Signaturvorgang zu beginnen steckt der Signaturschlüssel-Inhaber seine Signaturkarte in den Chipkartenleser. M-Doc AutoSigner Version 2.1 überprüft ob die auf der SSEE verfügbaren Zertifikate ausweislich ihrer Schlüsselattribute zur Erstellung der elektronischen Signatur geeignet sind und zeigt nur diese dem Benutzer in einem Dialog zur Auswahl an.

In einem weiteren Dialog können einem PDF- Dokument zusätzliche Signaturinformationen (Ort/ Grund) hinzugefügt werden. Wegen der geltenden Beschränkungen des PKCS#7-Formates ist diese Funktion nur bei PDF- Dokumenten verfügbar.

Anschließend wird der Benutzer aufgefordert, die Nutzung des ausgewählten Signaturzertifikats durch die Eingabe des PIN über die Tastatur des geprüften und bestätigten Kartenlesegerätes zu autorisieren. Der Benutzer wird daraufhin gewiesen, dass nach Eingabe der PIN eine qualifizierte Signatur erzeugt wird. Der Aufforderungdialog für die PIN- Eingabe zeigt den Hersteller und Typ des angesprochenen geprüften und bestätigten Kartenlesegeräts an um für den Nutzer zu gewährleisten, das ein geeignetes Gerät für die PIN- Eingabe verwendet wird. Nach erfolgreicher PIN-Authentifizierung übernimmt M-Doc AutoSigner Version 2.1 die Zuführung der Daten zur SSEE.

Ein Zwischenspeichern der PIN (PIN- Caching) ist weder zulässig noch wird es durch die Software technisch realisiert.

### 3.2 Erstellen qualifizierter Signaturen in einem Dokumentenstapel oder als Massensignatur

Die Massensignatur wird Synonym auch als Mehrfach-, Batch-, Stapel- oder Multisignatur bezeichnet. Es ist unter bestimmten technischen Voraussetzungen grundsätzlich zulässig qualifizierte Signaturen nicht einzeln je Dokument zu erzeugen sondern eine Voreinstellung zu definieren, die entweder **a)** für ein festes Zeitfenster (**Massensignaturen**) oder **b)** eine bestimmte Anzahl von Dokumenten erzeugt werden (**Stapelsignatur**).

#### a) Massensignatursitzung

In Falle der Massensignatur Variante **a)** sind besondere Maßnahmen in der Einsatzumgebung zu ergreifen, die dass unberechtigte oder fehlerhafte einliefern von Dokumenten sicher verhindern. Es obliegt dem Nutzer sicher zu stellen, dass nur berechtigte Dokumente im Fall der Massensignatur eingeliefert werden (z.B. alle Rechnungen eines Tages oder jeweils der vom Schlüsselinhaber in der virtuellen Poststelle erzeugte Eingangsnachweis (Rückschein) jeweils beim Eingang von Nachrichten in die VPS). M-Doc AutoSigner Version 2.1 kann nicht den semantischen Inhalt von eingelieferten Dokumenten analysieren. Da auch die sichere Anzeige (vor/nach der Signatur) nicht sinnvoller Weise im Massensignaturbetrieb für jedes Dokument durchgeführt wird, kann M-Doc AutoSigner Version 2.1 so konfiguriert werden, das eine sichere Anzeige und ggf. erneute PIN-Eingabe nach einer festen Anzahl oder zufällig als **Stichprobenkontrolle** nach § 110d SGB IV und § 41 SRVwV erfolgt. Zusätzlich kann die eine max. Dauer der Signatursitzung konfiguriert werden. Um den Signaturvorgang zu beginnen steckt der Signaturschlüssel-Inhaber seine Signaturkarte in den Chipkartenleser. M-Doc AutoSigner Version 2.1 überprüft ob die auf der SSEE verfügbaren Zertifikate ausweislich ihrer Schlüsselattribute zur Erstellung der elektronischen Signatur geeignet sind und zeigt nur diese dem Benutzer in einem Dialog zur Auswahl an.

In einem weiteren Dialog können einem PDF- Dokument zusätzliche Signaturinformationen (Ort/ Grund) hinzugefügt werden die für die gesamte Sitzung<sup>8</sup> gelten. Wegen der geltenden Beschränkungen des PKCS#7-Formates ist diese Funktion nur bei PDF- Dokumenten verfügbar.

Zum Starten der Signatursitzung wird der Benutzer aufgefordert, die Nutzung des ausgewählten Signaturzertifikats durch die Eingabe des PIN über die Tastatur des geprüft und bestätigten Kartenlesegerätes zu autorisieren. Der Aufforderungsdialog für die PIN- Eingabe zeigt den Hersteller und Typ des angesprochenen geprüft und bestätigten Kartenlesegeräts an um zu gewährleisten, das ein geeignetes Gerät für die PIN- Eingabe verwendet wird. Nach erfolgreicher PIN-Authentifizierung übernimmt M-Doc AutoSigner Version 2.1 die Zuführung der Daten zur SSEE. Durch einen besonderen Warnhinweis ist dem Benutzer ersichtlich, dass er sich im „Massensignaturmodus“ befindet. Ein

<sup>8</sup> Eine Signatursitzung beschreibt den Zeitraum nach Eingabe der PIN bis zu Beendigung des Programms, des Auftrages oder bis zum entfernen der Signaturkarte, in der alle Dokumente nach vordefinierten Parametern signiert werden.

Zwischenspeichern der PIN (PIN- Caching) ist weder zulässig noch wird es durch die Software technisch realisiert.

Einsatz von M-Doc AutoSigner Version 2.1 in Verbindung mit einer Signaturerstellungseinheit (SSEE) erfolgt regelmäßig am selben Server, an dem der geprüfte und bestätigte Karteleser angeschlossen ist. Zulässig ist der Einsatz von M-Doc AutoSigner Version 2.1 auch in einer Microsoft Terminal Services und Windows 2003 Server Umgebung sowie auf Citrix Presentation Server in den unter (vgl. Kap 4.1.2. lit. d Abs. 3) angegebenen Versionen. Der Einsatz von M-Doc AutoSigner Version 2.1 im Rahmen der sog. „Telesignatur“ ist ebenfalls unter den in Kap 5.1.2. lit. a) gemachten Auflagen zulässig.

## b) Stapelsignatur

Der Benutzer erstellt zunächst einen Dokumentenstapel durch Markierung und Auswahl mehrerer Dokumente. Alle ausgewählten Dokumente werden zu einem Stapel verbunden und an M-Doc AutoSigner Version 2.1 übergeben. Durch einen besonderen Warnhinweis ist dem Benutzer ersichtlich, dass er sich im „Stapelmodus“ befindet. Das erste Dokument des Stapels wird automatisch angezeigt. Durch die Schalter 'Nächstes Dokument', 'Vorheriges Dokument', 'erstes Dokument', 'Letztes Dokument' kann der Benutzer durch den Dokumentenstapel navigieren und sich alle Dokumente anzeigen lassen. Innerhalb eines angezeigten Dokumentes kann zwischen den Seiten navigiert werden und damit der komplette Inhalt eines jeden Dokuments und damit insgesamt auch des Stapels vor der Signatur zur Anzeige gebracht werden.<sup>9</sup> Nachdem der Benutzer durch vorherige Anzeige und Prüfung die Zusammenstellung des Dokumentenstapels geprüft hat, kann er den Signaturmodus starten. Der folgende Ablauf ist identisch mit dem unter Kap. 3.1 beschriebenen Ablauf, wobei M-Doc AutoSigner Version 2.1 die Zuführung der Daten zur Signaturerstellungseinheit für den gesamten Dokumentenstapel innerhalb einer „Krypto-Session“<sup>10</sup> durchführt. Ein Zwischenspeichern der PIN (PIN- Caching) ist weder zulässig noch wird es durch die Software technisch realisiert.

Die vorbeschriebene sog. „Stapelsignatur“ erfordert den Einsatz sog. Massensignaturfähiger Signaturerstellungseinheiten (siehe Kap. 2.2. SSEE mit Kennzeichnung „[+]“).

<sup>9</sup> Der Signaturmodus ist erst aktiv, wenn mindestens ein Navigationsschalter „Nächstes Dokument“ oder „Letztes Dokument“ verwendet wurde um zu gewährleisten, dass immer eine Prüfung der Zusammenstellung des Stapels durch den Signaturschlüsselinhaber erfolgt.

<sup>10</sup> Mit „Krypto-Session“ wird in diesem Zusammenhang eine aktuelle Transaktion zwischen SAK und SSEE bezeichnet in der mehr als ein Hashwert zur Verschlüsselung übertragen wird, ohne dass die SAK die Liste der Hashwerte speichern kann. Nach Ablauf (vordefiniertes Time-out-Fenster) der Transaktion können die Hash-Werte nicht mehr rekonstruiert werden, sondern müssen beim fehlschlagen der Transaktion erneut sowohl an SAK also auch an SSEE übertragen werden.

## 4. Erfüllung der Anforderungen des SigG und der SigV

### 4.1 Erfüllte Anforderungen

#### 4.1.1 Erfüllte Anforderungen § 17 Abs. 2 Satz 1 SigG

##### Zitat § 17 Abs. 2 Satz 1 SigG

„(2) Für die Darstellung zu signierender Daten sind Signaturanwendungskomponenten erforderlich, die die Erzeugung einer qualifizierten elektronischen Signatur vorher eindeutig anzeigen und feststellen lassen, auf welche Daten sich die Signatur bezieht.“

Der M-Doc AutoSigner Version 2.1 erfüllt die Anforderungen an Produkte für qualifizierte elektronische Signaturen nach § 17 Abs. 2 Satz 1 SigG indem er ermöglicht, dass die Erzeugung einer qualifizierten elektronischen Signatur über einen Dialog in der GUI vorher eindeutig angezeigt wird und feststellbar ist, auf welche Daten sich die Signatur bezieht, wie in Kap. 3.1 und 3.2 beschrieben.

#### 4.1.2 Erfüllte Anforderungen § 15 Abs. 2 Nr. 1 SigV

##### Zitat § 15 Abs. 2 Nr. 1 SigV

„(2) Signaturanwendungskomponenten nach § 17 Abs. 2 des Signaturgesetzes müssen gewährleisten, dass

1. bei der Erzeugung einer qualifizierten elektronischen Signatur
  - a) die Identifikationsdaten nicht preisgegeben und diese nur auf der jeweiligen sicheren Signaturerstellungseinheit gespeichert werden,
  - b) eine Signatur nur durch die berechtigt signierende Person erfolgt,
  - c) die Erzeugung einer Signatur vorher eindeutig angezeigt wird“

Der M-Doc AutoSigner Version 2.1 erfüllt außerdem die Anforderungen an Produkte für qualifizierte elektronische Signaturen gemäß § 15 Abs. 2 SigV indem er gewährleistet, dass bei der Erzeugung einer qualifizierten elektronischen Signatur

- a. die Identifikationsdaten nicht preisgegeben und diese nur auf der jeweiligen sicheren Signaturerstellungseinheit gespeichert werden,
- b. eine Signatur nur durch die berechtigt signierende Person erfolgt,
- c. die Erzeugung einer Signatur vorher eindeutig angezeigt wird

M-Doc AutoSigner Version 2.1 erfüllt die Anforderungen unter a) und b) indem entsprechend der Vorgaben in Kap. 2.2 und der geeigneten Einsatzumgebung wie in Kap. 5.1.2 ff beschrieben nur geeignete Signaturerstellungseinheiten (SSEE) zum Einsatz kommen, die eine Preisgabe der Identifikationsdaten nachweislich verhindern. Die Berechtigung zur Auslösung einer qualifizierten Signatur nach § 2 Nr. 2 SigG durch den Nutzer, wird gesichert durch die Sicherheitsmerkmale „Besitz der

SSEE“ und alleiniges „Wissen“ der identifizierten Person um die sog. „PIN“ zu Auslösung einer Transaktion auf der SSEE. Insoweit wird auf die gesetzliche Belehrung durch den ZDA gem. § 6 SigG bei Ausgabe der SSEE, an die identifizierte Person verwiesen. M-Doc AutoSigner Version 2.1 unterlässt ein Speichern der PIN.

M-Doc AutoSigner Version 2.1 erfüllt die Anforderungen des Punkte 4.1.2 c) indem beim Zugriff auf die SSEE in einem gesonderten, stets im Bildschirmvordergrund angeordneten, Dialogfenster der GUI die Aufforderung zur PIN-Eingabe angezeigt wird, verbunden mit dem Hinweis, der damit verbundenen Auslösung einer qualifizierten Signatur. Bei der PIN-Eingabe zum starten eines Massensignaturmodus wie in Kap. 3.2, wird ein Warnhinweis „Massensignatursitzung“ gegeben.

#### 4.1.5 Erfüllte Anforderungen § 17 Abs. 2 Satz 3 SigG

##### Zitat § 17 Abs. 2 Satz 3 SigG

„Signaturanwendungskomponenten müssen nach Bedarf auch den Inhalt der zu signierenden oder signierten Daten hinreichend erkennen lassen. Die Signaturschlüssel-Inhaber sollen solche Signaturanwendungskomponenten einsetzen oder andere geeignete Maßnahmen zur Sicherheit qualifizierter elektronischer Signaturen treffen.“

M-Doc AutoSigner Version 2.1 erfüllt die Anforderungen an Produkte für qualifizierte elektronische Signaturen nach § 17 Abs. 2 Satz 3 SigG indem nach Bedarf auch den Inhalt der zu signierenden oder signierten Daten hinreichend erkennen lässt. M-Doc AutoSigner Version 2.1 erfüllt die Anforderungen des § 17 Abs. 2 Satz 3 SigG wie angezeigt, indem dem Nutzer die Anzeige der Signaturobjekte vor der Auslösung der Signatur und auf Interaktion des Karteninhabers auch nach der Signatur ermöglicht wird wie in Kap. 3 Abs. 5 Seite 9 und Kap. 5.1.2. d) Nr. 9 im Einzelnen beschrieben. Insbesondere kann der Karteninhaber über eine Voreinstellung konfigurieren, dass jede Datei unmittelbar nach der Signatur mit Betriebssystemmitteln geöffnet und damit zur Anzeige gebracht wird. Im Massensignaturmodus wie in Kap.3.2 beschrieben ist die Anzeige jedes Dokumentes nicht sinnvoll, sondern wird als Stichprobenkontrolle durch das Produkt unterstützt.

#### 4.1.6 Erfüllte Anforderungen § 15 Abs. 4 SigV

##### Zitat § 15 Abs. 4 SigV

„(4) Sicherheitstechnische Veränderungen an technischen Komponenten nach den Absätzen 1 bis 3 müssen für den Nutzer erkennbar werden.“

Weiterhin sind für das Produkt M-Doc AutoSigner Version 2.1 durch den Hersteller Maßnahmen gegen sicherheitstechnische Veränderung ergriffen worden, die jede Veränderungen an der Anwendungskomponente für den Nutzer gemäß § 15 Abs. 4 SigV erkennbar machen. Voraussetzung für

die Zuverlässigkeit dieser technischen Schutzmaßnahmen ist, dass die unter 5.1.2 ff spezifizierten Einsatzbedingungen eingehalten werden. Es wird ein Betrieb in einem „geschützten Einsatzbereich“<sup>11</sup> vorausgesetzt. Der M-Doc AutoSigner Version 2.1 erfüllt die Anforderungen durch den Einsatz von Code-Signatur aller Komponentenbestandteile wie in Kap. 5.1.2 g) im Einzelnen beschrieben.

## 5. Einsatzbedingungen

### 5.1.1 Potentielle Bedrohungen

Die Sicherheit von M-Doc AutoSigner Version 2.1 ist potentiell bedroht durch

- Angriffe über Kommunikationsnetze<sup>12</sup>,
- Angriffe über manuellen Zugriff Unbefugter/Datenaustausch per Datenträger<sup>13</sup> und
- Fehler/Manipulationen bei Installation, Betrieb/Nutzung und Wartung/Reparatur.

Für den sicheren Einsatz von M-Doc AutoSigner Version 2.1 und zur Verhinderung von erfolgreichen Angriffen mit den Zielen, dass:

- Daten signiert werden, die nicht signiert werden sollen und
- die Geheimhaltung des Identifikationsmerkmals (PIN) nicht gewährleistet ist und

sind die nachfolgenden **Auflagen** zu beachten:

### 5.1.2 Maßnahmen in der Einsatzumgebung

Der Signaturrechner wird in einem geschützten Einsatzbereich eingesetzt, bei dem gegenüber den potentiellen Bedrohungen folgender Schutz besteht:

Potentielle Angriffe über

- das Internet,
- ein angeschlossenes Intranet,
- einen manuellen Zugriff Unbefugter und
- Datenaustausch per Datenträger

werden durch eine Kombination von Sicherheitsvorkehrungen in der Teil-Signaturanwendungskomponente selbst und der Einsatzumgebung mit hoher Sicherheit abgewehrt.

<sup>11</sup> Definierter Einsatzbereich gemäß Nr. 4.2 RegTP Dokument: Einheitliche Spezifizierung der Einsatzbedingungen für Signaturanwendungskomponenten Version 1.4.

<sup>12</sup> Spezifizierte Bedrohung gemäß Fußnote 15 RegTP Dokument: Einheitliche Spezifizierung der Einsatzbedingungen für Signaturanwendungskomponenten Version 1.4.

<sup>13</sup> Spezifizierte Bedrohung gemäß Fußnote 16 RegTP Dokument: Einheitliche Spezifizierung der Einsatzbedingungen für Signaturanwendungskomponenten Version 1.4.

## a) Zulässige IT- Komponenten und Systeme für den Signaturbetrieb

Die Teil- Signaturanwendungskomponente M-Doc AutoSigner Version 2.1 ist für die folgende technische Einsatzumgebungen vorgesehen:

- IBM-kompatibler PC/ Server lauffähig mit einem der unten genannten Betriebssysteme, mit Anschlussmöglichkeiten für ein Read-Only-Memory Laufwerk (z.B. ein DVD-ROM oder CD-ROM) sowie für einen Kartenleser (serielle oder USB-Schnittstelle).
- M-Doc AutoSigner Version 2.1 kann unter den Betriebssystemen Windows 2000 Professional und Server, Windows XP Home Edition, Windows XP Professional Edition, Windows XP Media Center Edition, Windows XP Tablet PC Edition, Windows Server 2003 Standard und Enterprise Edition, Windows Vista (32 und 64 Bit), Windows Server 2008 (32 und 64 Bit), Windows 7 (32 und 64 Bit), eingesetzt werden.
- M-Doc AutoSigner Version 2.1 kann in den Metaframeumgebungen „Microsoft Terminal Services“ ab Windows 2003 Server und „Citrix Presentation Server“ ab Version 4 eingesetzt werden.
- Sowie den Linuxdistributionen: Suse ab V. 9; RedHat Enterprise ab V. 4; Fedora Core ab V. 4; Debian ab V. 3.1; Ubuntu ab V. 5.1.

Der Einsatz von M-Doc AutoSigner Version 2.1 im Rahmen der sog. „**Telesignatur**“ bzw. mir „**Secure-Remote-PIN-Systemen**“, bei dem der geprüft und bestätigte Kartenleser nicht am Server angeschlossen ist sondern über ein LAN oder WAN <sup>14</sup> verbunden wird, ist nur unter folgenden Auflagen zulässig:

1) Die Verbindung des geprüft und bestätigte Kartenleser muss über die USB-Schnittstelle unter Verwendung der folgenden Komponente erfolgen:

- a) DIGI USBAnywhere / 5 (USB zu IP) (Typ: 91001219 /C1/208)  
Fa. Digi International  
France; 92200 Neuilly sur Seine; 31 rue des Poissonniers

Der Einsatz in der Telesignatur ist nur zulässig unter Verwendung der SSEE Multisign NetKey 3.01, TUVIT. 93119.TE.09.2006. Es ist durch entsprechende Konfiguration der SSEE sicher zu stellen, das die gesamte Kartenkommunikation verschlüsselt erfolgt.

## b) Auflagen zur Anbindung an das Internet

Es wird vorausgesetzt, dass der Signaturrechner hinreichend gegen Bedrohungen durch Zugriff über das Internet abgeschottet ist. Wir verweisen für konkrete Maßnahmen auf die Empfehlungen der BSI-

<sup>14</sup> Local Area Network(LAN) oder Wide Area Network (WAN)

Standards zum Informationssicherheitsmanagement, die IT-Grundschutz-Kataloge und die ISO-27002 sowie den "Maßnahmenkatalog Kommunikation" M 5.

### **c) Auflagen zur Anbindung an ein Intranet**

Wenn der eingesetzte Signaturrechner in einem Intranet betrieben wird, so muss diese Netzverbindung über eine geeignete Firewall abgesichert sein, so dass unberechtigte Zugriffe aus dem Intranet auf den Signaturrechner erkannt bzw. unterbunden werden. Wir verweisen für konkrete Maßnahmen auf die Empfehlungen der BSI<sup>15</sup>-Standards zum Informationssicherheitsmanagement, die IT-Grundschutz-Kataloge und die ISO-27002 sowie den "Maßnahmenkatalog Kommunikation" M 5.

### **d) Auflagen zur Sicherheit der IT-Plattform und Applikationen**

Der Benutzer des M-Doc AutoSigner Version 2.1 muss sich davon überzeugen, dass keine Angriffe auf den Signaturrechner und die dort vorhandenen Applikationen durchgeführt werden können. Insbesondere muss gewährleistet sein, dass:

1. die Prüffunktion des Produktes, die die Integrität der installierten Software überprüft regelmäßig angewendet wird (Codesignaturprüfung durch Betriebssystem),
2. auf dem Signaturrechner ein aktueller Virenschanner läuft, so dass keine Viren oder Trojanischen Pferde unentdeckt bleiben können,
3. die Hardware des Signaturrechners nicht unzulässig verändert werden kann,
4. der verwendete Kartenleser weder böswillig manipuliert noch in irgendeiner anderen Form verändert wurde, um dadurch Daten (z.B. PIN, zu signierende Daten, Hashwerte etc.) auszuforschen, zu verändern oder die Funktion anderer Programme unzulässig zu verändern,
5. eine Benutzerauthentifizierung am Betriebssystem des Signaturrechners erforderlich ist,
6. nach Abschluss der Arbeiten ist eine Konsolensperrung erfolgt, die eine erneute Authentifizierung bei nächsten Arbeiten erforderlich macht
7. die PIN- Eingabe ausschließlich am Kartenleser erfolgt,
8. die Nutzung von installierten Signaturschlüsseln und Zertifikaten ausschließlich dem rechtmäßigen Karteninhaber möglich ist (keine Weitergabe von Karte und /oder PIN).
9. soweit nicht die Möglichkeit genutzt wird, die Ausgangsdaten vor der Signatur in das PDF-

<sup>15</sup> Bundesamt für Sicherheit in der Informationstechnologie:  
[https://www.bsi.bund.de/clin\\_164/DE/Themen/ITGrundschutz/itgrundschutz\\_node.html](https://www.bsi.bund.de/clin_164/DE/Themen/ITGrundschutz/itgrundschutz_node.html)

Format zu konvertieren und sicher anzuzeigen (siehe Kap. 3 Abs. 5) sondern die Anzeige einer zu signierenden Datei mit externen Programmen oder Betriebssystemmitteln erfolgt, ist zu beachten, das es in der Verantwortung des Nutzers liegt für eine sichere Anzeige/Identifizierung der zu signierenden Datei auf technischer Ebene (z.B. Hahssummenvergleich) zu sorgen um den Anforderungen des SigG zu genügen( z.B. bei „X-Justiz“ Datensätzen oder im Online-Mahnverfahren bei „.eda Dateien“).

Wir verweisen für konkrete Maßnahmen zur Umsetzung daneben auf die Empfehlungen der BSI-Standards zum Informationssicherheitsmanagement, die IT-Grundschutz-Kataloge und die ISO-27002 sowie den "Maßnahmenkatalog Hardware und Software" M 4. Für Telearbeitsplätze und Metaframeumgebungen verweisen wir auf die Empfehlungen M 5.51 Sicherheitstechnische Anforderungen an die Kommunikationsverbindung Telearbeitsrechner – Institution.

## **e) Auflagen zur Auslieferung und Installation des Produktes**

Die Installation des M-Doc AutoSigner Version 2.1 erfolgt durch den Kunden bzw. einen betreuenden Techniker des Herstellers. Es muss vorausgesetzt werden, dass diejenige Person, die das System installiert, die entsprechende Eignung zur Installation und Inbetriebnahme besitzt. Es ist sicherzustellen, dass ein geprüftes und bestätigtes Kartenlesegerät (siehe Kap. 2.2. Tabelle 2) verwendet wird. Über die Konfiguration des Lesegerätes ist abzusichern, dass die PIN-Eingabe nur am Kartenleser möglich ist.

Die zulässige (siehe Kap. 2.2.2 Tabelle 1) Signaturerstellungseinheit (SSEE) muss sich zwingend an einem lokal am Arbeitsplatz installierten geprüft und bestätigten Kartenlesegerät befinden. Der Einsatz von M-Doc AutoSigner Version 2.1 im Rahmen der sog. „Telesignatur“ bzw. „Secure-Remote-PIN-Systemen“, bei der sich der geprüft und bestätigte Kartenleser nicht am Arbeitsplatzrechner des Karteninhabers befindet, ist unzulässig. Auch bei Telearbeitsplätzen und in Metaframeanwendungen ist zwingend ein Kartenterminal am Arbeitsplatz (Client) vorzuhalten.

Vor der Installation hat sich die installierende Person von der korrekten Anwendung des Auslieferungsverfahrens zu überzeugen: Die Teil- Signaturanwendungskomponente M-Doc AutoSigner Version 2.1 wird vom Hersteller als Installationspaket über das Internet vertrieben. Das Produkt unterstützt eine von den Betriebssystemen angebotene Überprüfungsroutine zur Sicherstellung der Produktintegrität (Prüfung der Code-Signatur und des Herstellerzertifikats).

Es ist ein geprüft und bestätigter Kartenleser der Sicherheitsklassen 2 bis 4 mit PIN-Eingabefeld, der die sichere Eingabe der PIN unterstützt einzusetzen. Die PIN- Eingabe darf nur an der Tastatur des Kartenlesers erfolgen. Der Hersteller hat die in Kap. 2.2.2 geprüft und bestätigten Kartenlesegeräte mit M-Doc AutoSigner Version 2.1 erfolgreich getestet. Zu Erzeugung von qualifizierten Signaturen ist die Verwendung der dort angegeben Komponenten zwingend.

Es sind auch die Anforderungen zu beachten, die der Hersteller des sicherheitsbestätigten Kartenlesegerätes und der Herausgeber der sicheren Signaturerstellungseinheit (SSEE) für den Einsatz im Signaturbetrieb formuliert haben. Es ist eine, über die Standardkonfiguration hinausgehende, Absicherung des Signaturrechners durchzuführen, so dass nur die für den Betrieb notwendigen Protokolle, Ports und Dienste zur Verfügung stehen.

## **f) Auflagen zur Nutzung von bestimmten Signaturkarten (SSEE)**

Der Hersteller hat die in Kap. 2.2. genannten Signaturerstellungseinheiten im Einsatz mit M-Doc AutoSigner Version 2.1 erfolgreich getestet. Zu Erzeugung von qualifizierten Signaturen wie unter Punkt 3.1 beschrieben ist die Verwendung der dort angegebenen Komponenten (SSEE) zwingend. Im „Stapelsignaturmodus“ wie unter Punkt 3.2 näher beschrieben dürfen nur sichere Signaturerstellungseinheiten (SSEE) verwendet werden, die vom ausstellenden Zertifizierungsdiensteanbieter dafür zugelassen sind. In der Übersichtstabelle in Kap. 2.2. sind diese in der Spalte: "Stapel/ Massensignatur" mit "[+]" gekennzeichnet worden.

## **g) Schutz vor unbefugter Veränderung**

Es werden alle sicherheitskritischen Komponenten von M-Doc AutoSigner Version 2.1 von der Mentana-Claimsoft AG mit einer Code-Signatur versehen. Die Signatur wird in das Binary integriert und nachfolgend mit einem fortgeschrittenen Zeitstempel der TC-Trust versehen.

Die Prüfung der Code-Signaturen erfolgt auf Betriebssystemebene bei jedem Programmstart automatisch. Folgendes Zertifikat wird für die Code-Signatur verwendet und muss vom Betriebssystem als „gültig“ angezeigt werden.

### **Zertifikat für Mentana-Claimsoft AG (Zertifikat 1):**

Ausgestellt für: Mentana-Claimsoft AG

Ausgestellt von: GeoTrust Trustcenter CodeSigning CA I

Seriennummer: 00 d2 1a 00 01 00 20 c0 b7 f9 3c b4 12 ea ed

### **Zertifikat für Mentana-Claimsoft AG (Zertifikat 2) [ab 11/2009]:**

Ausgestellt für: Mentana-Claimsoft AG

Ausgestellt von: Commodo UTN-USERFirst-Object

Seriennummer: 00b50a7da137c127eafb6a7a067c8cbd91

Datei	Version	Zertifikat
<b>Windows-Version</b>		
AutoSigner.exe	2.1	Zertifikat 1 oder 2
mentalgocsp.dll	1.1	Zertifikat 1 oder 2
mdocapiext.dll	2.1	Zertifikat 1 oder 2
MdocExtWx.dll	2.1	Zertifikat 1 oder 2
MdocTSAClient.dll	2.1	Zertifikat 1 oder 2
mdocapi.dll	2.1	Zertifikat 1 oder 2
mdocapissl.dll	2.1	Zertifikat 1 oder 2
mdocpdf.dll	2.1	Zertifikat 1 oder 2
mdoccrypto.dll	2.1	Zertifikat 1 oder 2
mdoccryptossl.dll	2.1	Zertifikat 1 oder 2
libeay32.dll	2.1	Zertifikat 1 oder 2
ssleay32.dll	2.1	Zertifikat 1 oder 2
pkcs15init.dll	2.1	Zertifikat 1 oder 2
opensc-pkcs11.dll	2.1	Zertifikat 1 oder 2
opensc.dll	2.1	Zertifikat 1 oder 2
engine_pkcs11.dll	2.1	Zertifikat 1 oder 2
opensc-pkcs11.dll	2.1	Zertifikat 1 oder 2

<b>Linux- Version</b>		
AutoSigner	2.1	Zertifikat 1 oder 2
libMdocApiExt.Wx.a	2.1	Zertifikat 1 oder 2
libssl.so.0.9.8	2.1	Zertifikat 1 oder 2
libcrypto.so.0.9.8	2.1	Zertifikat 1 oder 2
libopensc.so.2	2.1	Zertifikat 1 oder 2
libp11.so.0	2.1	Zertifikat 1 oder 2
libsconf.so.2	2.1	Zertifikat 1 oder 2
engine_pkcs11.so	2.1	Zertifikat 1 oder 2
opensc-pkcs11.so	2.1	Zertifikat 1 oder 2

## **h) Maßnahmen zur Zugangskontrolle**

Zum Schutz vor manuellen Zugriffen Unbefugter und vor Datenaustausch per Datenträger, ist der Signaturrechner so zu betreiben, dass eine Zugangskontrolle zur Konsole und zum sicheren Kartenlesegerät des Signatursystems aktiv ist. Dazu muss der Signaturrechner mindestens an einem Ort aufgestellt werden, für den eine sichere Zugangskontrolle gewährleistet werden kann. Anhaltspunkte zur Sicherstellung einer sicheren Zugangskontrolle sind den Standards BSI 7550 und BSI 7551 zu entnehmen.

## **i) Absicherung von Schnittstellen**

### **zu 2.4. a) Schnittstelle zum Chipkartenleser:**

Die Absicherung der Schnittstelle zum Kartenleser wird durch das Sicherheitskonzept des Kartenlesers abgedeckt. Es sind jeweils die Auflagen und Angaben des Herstellers zum Einsatz bei USB und seriellen Anschlüssen zu beachten. Der Nutzer muss lediglich für die Manipulationsfreiheit der Kabelverbindung sorgen.

### **zu 2.4 b) Schnittstelle zur grafischen Bedienungsoberfläche (Graphical User Interface – GUI):**

Die GUI ist Bestandteil der geschützten Signaturkomponente und wird wie in 5.1.2 lit. g) beschrieben vor Manipulation geschützt.

### **zu 2.4 c) Schnittstelle zur aufrufenden Anwendung:**

Für Aufrufe per command line stellt M-Doc AutoSigner Version 2.1 eine API (application programming interface) bereit, die Bestandteil der geschützten Signaturkomponente ist und wird wie in 5.1.2 lit. g) beschrieben vor Manipulation geschützt wird.

## **5.1.3 Wartung/Reparatur**

Bei der Wartung und der Reparatur des Signaturrechners gelten die Voraussetzungen der Erstinstallation (vergleiche Kap. 5.1.1 und 5.1.2). Bei Erkennen von Fehlern, die die Sicherheit der Teil-Signaturanwendungskomponente betreffen können, stellt die Mentana-Claimsoft AG umgehend aktualisierte Versionen der Programmkomponenten zur Verfügung. Die Anwender des Programms werden über die Webseite der Mentana-Claimsoft AG ([www.mentana-claimsoft.de](http://www.mentana-claimsoft.de)) über das Auftreten einer solchen Situation informiert. Mit dem Inverkehrbringen einer neuen Softwareversion des M-Doc AutoSigner Version 2.1 hinterlegt die Mentana-Claimsoft AG umgehend einen Nachtrag zu dieser Herstellererklärung bei der Bundesnetzagentur.

## 6. Algorithmen und zugehörige Parameter

Das Produkt M-Doc AutoSigner Version 2.1 verwendet zur Erstellung qualifizierter Signaturen die Hashverfahren SHA-256, SHA-512 und RIPEMD-160 sowie das Signaturverfahren RSA mit variablen Schlüssellängen ab 1976 bis 2048 Bit. Die gemäß Anlage 1 Abs. 1 Nr. 2 SigV festgestellte Eignung reicht für SHA-256 und SHA-512 mindestens bis Ende 2016. Für RIPEMD-160 mindestens bis Ende des Jahres 2010 (Vom 06. Januar 2010 Veröffentlicht am 04. Februar 2010 im Bundesanzeiger Nr. 19, Seite 426). Für die Erzeugung von Signaturen für den Zeitraum bis Ende 2010 muss eine Länge von mindestens 1728 Bit und ab Anfang 2011 von mindestens 1976 Bit genutzt werden. Für die Gewährleistung eines langfristigen Sicherheitsniveaus wird grundsätzlich die Erhöhung auf 2048 Bit empfohlen. Dieser gilt bis Ende 2016 als sicher. Der RSA Algorithmus mit der Schlüssellänge 2048 Bit wird von der Bundesnetzagentur als „langfristig sicher“ eingestuft (Vom 06. Januar 2010 Veröffentlicht am 04. Februar 2010 im Bundesanzeiger Nr. 19, Seite 426). Nicht unterstützt werden Algorithmen in DSA-Varianten, basierend auf elliptischen Kurven. Insbesondere die Verfahren: EC-DAS; EC-KDSA; EC-GDSA; Nyberg-Rueppel-Signaturen.

Weitere Informationen zu diesen Algorithmen werden veröffentlicht im Bundesanzeiger, „Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung“ (nachfolgend bezeichnet als „BNetzA- Algorithmen-Katalog“) BNetzA- Algorithmen-Katalog 2010, Seite 4 Pkt. 3. Der aktuell gültige sowie die jährlichen Aktualisierungen des BNetzA- Algorithmen-Katalog können auf der Website der Bundesnetzagentur unter [www.bundesnetzagentur.de](http://www.bundesnetzagentur.de) eingesehen werden.

## 7. Gültigkeit der Herstellererklärung

Diese Herstellererklärung ist bis zum Widerruf durch Mentana-Claimsoft AG bzw. die Bundesnetzagentur oder im Falle des vorzeitigen Ablaufs der Vertrauenswürdigkeit der Hashalgorithmen SHA-256, SHA-512, RIPEMD-160 - oder des Signaturverfahrens (RSA 2048 Bit) (gegenüber dieser Erklärung wie unter den Punkt 3.3 angezeigt)- jeweils angezeigt durch die Bundesnetzagentur ([www.bundesnetzagentur.de](http://www.bundesnetzagentur.de)) – gültig, längstens jedoch bis zum **31.12.2010**.

## 8. Begleitende Dokumente

Für diese Herstellererklärung gelten folgende Begleitdokumente:

1. Handbuch für M-Doc Auto-Signer, Version 1.0.29, vom 15.04.10, 28 Seiten.
2. Sicherheitstechnische Produktvorgaben M-Doc AutoSigner (EVG) Version 2.1, vom 06.02.2010, 27 Seiten.
3. Spezifikation der Test- und Entwicklungsumgebung für M-Doc AutoSigner 2.1 (EVG), vom 06.02.2010, 15 Seiten.

Dieses Dokument umfasst 26 Seiten.

Ende der Herstellererklärung.