

Herstellereklärung

Der Hersteller

Mentana-Claimsoft AG

Spreenhagener Str. 16
15528 Spreenhagen b. Berlin

erklärt hiermit gemäß § 17 Abs. 4 Satz 2 SigG¹,
in Verbindung mit § 15 Abs. 5 SigV²,
dass sein Produkt

M-Doc AutoVerifier Version 2.1

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

- qualifizierte elektronische Signaturen und qualifizierte Zertifikate zu prüfen sowie die Ergebnisse anzuzeigen und zu protokollieren

und den Anforderungen des Signaturgesetzes¹ und der Signaturverordnung² genügt.

Diese Erklärung ersetzt die Herstellereklärung vom 19.12.2007 veröffentlicht im Amtsblatt der Bundesnetzagentur Nr. 24/2007 Mitteilung Nr. 1016, Seite 5223.

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 b. Berlin, 28.05.2008
+

Dr. Inf. Ralf Hesse
Leiter Softwareentwicklung

Dipl. Ing. Axel Janhoff
Vorstand

¹ 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 26. Februar 2007 (BGBl. I S. 179).

² 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 Art. 9 Abs. 18 G v. 23.11.2007.

Inhaltsverzeichnis

Deckblatt.....	1
Herstellereklärung	1
1. Handelsbezeichnung	3
2. Funktionsbeschreibung.....	3
2.1 Verifikation einer qualifizierten elektronischen Signatur	4
2.1.1 Ablauf der Verifikation einer qualifizierten elektronischen Signatur.....	4
2.1.2 Vertrauensanker.....	6
2.1.3 Inhalt des Verifikationsprotokolls für qualifizierte Signaturen	7
3. Erfüllung der Anforderungen des SigG und der SigV	10
3.1 Erfüllte Anforderungen	10
3.1.1 Erfüllte Anforderungen § 17 Abs. 2 Satz 2 SigG	10
3.1.2 Erfüllte Anforderungen § 17 Abs. 2 Satz 3 SigG	10
3.1.3 Erfüllte Anforderungen § 15 Abs. 2 Nr. 2 SigV	10
3.1.4 Erfüllte Anforderungen § 15 Abs. 4 SigV	10
3.2 Einsatzbedingungen.....	11
3.2.1 Potentielle Bedrohungen	11
3.2.2 Maßnahmen in der Einsatzumgebung.....	11
a) Auflagen zur Anbindung an das Internet.....	12
b) Auflagen zur Anbindung an ein Intranet.....	12
c) Auflagen zur Sicherheit der IT-Plattform und Applikationen.....	12
d) Auflagen zur Auslieferung und Installation des Produktes.....	12
f) Schutz vor unbefugter Veränderung.....	13
g) Maßnahmen zur Zugangskontrolle	15
3.2.3 Wartung/Reparatur	15
3.3 Algorithmen und zugehörige Parameter.....	15
4. Begleitende Dokumente	16
5. Gültigkeit der Herstellereklärung	17

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	18.05.2008
2.06	Axel Janhoff	Autorisierung zur Veröffentlichung	26.05.2008

1. Handelsbezeichnung

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

Hersteller: Mentana-Claimsoft AG
Spreenhagener Str. 16
D- 15528 Spreenhagen
info@mentana.de

2. Funktionsbeschreibung

Die Teil-Signaturanwendungskomponente M-Doc AutoVerifier Version 2.1 ist eine Serversoftware die qualifizierte elektronische Signaturen von Dateien jeglichen Dateityps, unter Beachtung der Bestimmungen des Signaturgesetzes, überprüft (verifiziert) und die Ergebnisse der Verifikation dem Anwender in Protokollen anzeigt. Haupteinsatzzwecke der Anwendung sind z.B. die massenhafte, automatisierte Prüfung elektronischer Rechnungen gemäß § 15 UstG, die Verifikation eingescannter und signierter Belege im Anwendungsumfeld des § 110d SGB IV oder die Prüfung (Verifikation) elektronischer Post in einer virtuellen Poststelle.

Der M-Doc AutoVerifier Version 2.1 ist eine Teil-Signaturanwendungskomponente gemäß § 2 Nr. 11b SigG, die qualifizierte Signaturen zusammen mit den jeweiligen Originaldokumenten verifiziert. Insbesondere werden folgende Signaturformate unterstützt:

- a) „signedData“ gemäß RFC 2630 (Dateiendungen *.pk7 und *.p7s)
- b) „signedData“ mit „multipart-signed“-Content gemäß RFC 2633 (Dateiendung *.p7m)
- c) PDF (PKCS#7-konforme Signatur entsprechend Adobe-Reference 1.4 bis 1.6)

- d) "XMLDsig" als "enveloped signature" oder "detached signature" gemäß RFC 3075-3375
- e) EDIFACT- Nachricht [INVOIC] nach DIN [ISO9735- 5]
- f) AUTACK- Nachricht nach DIN [ISO9735- 6]

2.1 Verifikation einer qualifizierten elektronischen Signatur

2. 1. 1 Ablauf der Verifikation einer qualifizierten elektronischen Signatur

M-Doc AutoVerifier Version 2.1 prüft, über definierte Schnittstellen³, eingelieferte Dateien (Dokumente) auf ihre Integrität und die enthaltenen Signaturen auf Gültigkeit. Die Schnittstellen, die zur Verfügung gestellt werden, sind kein Bestandteil dieser Herstellereklärung.

Im Rahmen der Prüfung (Verifikation) werden folgende Fragen untersucht und es wird ein Prüfurteil abgegeben:

- a) Wurde die signierte Datei (Dokument) seit dem Anbringen der Signatur verändert?
- b) Kann die Zertifikatskette bis zum ausstellenden ZDA aufgebaut werden?
- c) Kann die mathematische Korrektheit aller Zertifikate in der Kette bestätigt werden?
- d) Ist die ausstellende Organisation des Signaturzertifikats ein ZDA im Sinne des SigG und handelt es sich um ein qualifiziertes Zertifikat?
- e) Waren alle Zertifikate in der Kette zum ermittelten Zeitpunkt der Signaturerstellung⁴ entsprechend dem zulässigen Gültigkeitsmodell (Kette) gültig und nicht gesperrt?

Zur Verifikation der elektronischen Signatur ermittelt M-Doc AutoVerifier Version 2.1 zunächst den Zertifizierungspfad und assoziiert die Zertifikatskette. M-Doc AutoVerifier Version 2.1 überprüft die mathematische Korrektheit aller Signaturen in der Zertifikatskette. Soweit die mathematische Prüfung nicht zu Fehlern führt, wird überprüft, ob es sich bei allen Zertifikaten in der Kette um qualifizierte Zertifikate handelt, in dem die entsprechenden Einträge (Flag) in den Zertifikaten ausgewertet werden. Im Anschluss daran ermittelt M-Doc AutoVerifier Version 2.1 zur Sicherstellung der Zertifikatsgültigkeit durch Onlineabfrage bei jedem Aussteller eines Zertifikats in der Kette, ob das Zertifikat im Zeitpunkt der Anfrage bekannt, gültig und nicht gesperrt ist bzw. wann es gesperrt wurde. Aus diesen Informationen ermittelt Doc AutoVerifier Version 2.1 entsprechend dem Gültigkeitsmodell das Gesamturteil der Signaturprüfung.

³ Schnittstellen: Dateiverzeichnisse, SOAP, SMTP, SFTP, Kofax Capture Textplus, DB-Connect.

⁴ Der Signaturzeitpunkt der aus den Signaturinformationen extrahiert wird gibt in der Regel die Systemzeit des Rechners des Signaturschlüsselinhabers wieder. Die Zeitangabe ist nur in Verbindung mit einem Zeitstempel gemäß § 2 Nr. 14 SigG verlässlich.

Zur Onlineüberprüfung der Zertifikatsgültigkeit nutzt M-Doc AutoVerifier Version 2.1 standardmäßig die durch die ZDA´s angebotenen OCSP-Responder gemäß RFC 2560 die im Zertifikat angegeben sind.

Die Abfragen erfolgen über eine HTTPS-Verbindung. Der OCSP-Responder des ZDA liefert als Antwort: "good" (Zertifikat gültig); "revoked" (Zertifikat gesperrt); "unknown" (Zertifikat unbekannt) sowie gegebenenfalls den Zeitpunkt einer Sperrung. Die Antwort des OCSP-Responders des ZDA ist signiert und wird ihrerseits auf Gültigkeit geprüft. Sofern im Zertifikat statt eines OCSP-Responders eine Sperrliste angegeben ist, prüft M-Doc AutoVerifier Version 2.1 gegen eine Sperrliste gemäß RFC 3280. Sind im Zertifikat weder OCSP-Responder noch Sperrlistenverteilungspunkte angegeben kann der Nutzer durch manuelle Konfiguration die LDAP-Verzeichnisse der ZDA´s in M-Doc AutoVerifier Version 2.1 hinterlegen. Der Zugriff auf ein LDAP-Verzeichnis bei einem ZDA erfordert regelmäßig eine Zugriffsberechtigung. Das Vorliegen einer solchen Berechtigung kann M-Doc AutoVerifier Version 2.1 **nicht** prüfen. Ist auch kein LDAP-Verzeichnis in M-Doc AutoVerifier Version 2.1 hinterlegt wird nur die mathematische Integrität von Signatur und Zertifikaten geprüft und das Gesamturteil gemäß 2.1.1 lit cc) „Status unbekannt“ ausgegeben.

Kann wegen speziellen Sicherheitsbedürfnissen des Nutzers eine Internetverbindung nicht hergestellt werden, kann M-Doc AutoVerifier Version 2.1 gegen lokal gespiegelte Sperrlisten prüfen, die ebenfalls manuell eingetragen werden müssen.

Der Hersteller weist ausdrücklich daraufhin, dass verlässliche Informationen nur über eine aktuelle Onlineabfrage auf den Verzeichnisdienst eines ZDA zu erlangen sind. Dies kann durch M-Doc AutoVerifier Version 2.1 nur bei den oben beschriebenen „OCSP“ oder „Sperrlistenprüfungen“ sichergestellt werden. Andere Verfahren (LDAP und lokal gespiegelte Sperrlisten) bedürfen besonderer administrativer Maßnahmen, was eine entsprechende Qualifikation auf Anwenderseite erfordert. Es wird weiterhin ausdrücklich darauf hingewiesen, dass die Verifikation gegen lokal gespiegelte Sperrlisten nur verlässlich ist, wenn durch administrative Maßnahmen des Nutzers von M-Doc AutoVerifier Version 2.1 eine Aktualität und Übereinstimmung dieser lokalen Sperrlisten mit denen beim ZDA geführten Sperrlisten gewährleistet wird. Die tatsächliche Aktualität einer Sperrliste kann M-Doc AutoVerifier Version 2.1 **nicht** prüfen. Das weitere Vorgehen für eine Verifikation gegen LDAP und lokale Sperrlisten wird im Handbuch beschrieben.

Als Ergebnis der Verifikationsvorgänge je Signatur wird dem Nutzer gemäß § 15 Abs. 2 Nr. 2 SigV das Gesamtergebnis der Prüfung angegeben, durch Anzeige der Urteile:

aa) **"Signatur gültig"**

bb) **"Signatur ungültig"**

cc) **„Status unbekannt“** --Mindestens eine Prüfung konnte nicht abschließend durchgeführt werden. Weitere Informationen finden Sie im Handbuch Abschnitt "Umgang mit Prüfergebnissen.--"

2. 1. 2 Vertrauensanker

Der Hersteller weißt bezüglich der Gesamtaussage des Verifikationsergebnisses: „Signatur gültig“ und „Status unbekannt“ (wie unter 2.3.1 beschrieben) daraufhin, dass das Vertrauen in ein Zertifikat bzw. eine Zertifikatskette, auf dem Vertrauen in die Stelle welche das Zertifikat ausstellt basiert. Das Vertrauen in eine solche ausstellende Organisation (ZDA oder Bundesnetzagentur) wird als sog. "Vertrauensanker" (trustanchor) bezeichnet, welcher Ausgangspunkt für die Validierung eines Zertifikates oder einer Zertifikatskette ist. Für den vom Signaturgesetz erfassten Bereich gelten folgende Strukturen für die Ermittlung eines gültigen Vertrauensankers

I. qualifizierte Signaturen gemäß § 15 Abs.1 SigG:

a) Hierarchisches Top-Down-Modell

- Ebene 0: BNetzA als Wurzel (Top-Level-CA, Root-CA)
- Ebene 1: ZDA (Ausstellerzertifikat)
- Ebene 2: Teilnehmer (Unterzeichnerzertifikat)

b) Vertrauensanker:

Es kann nur den öffentlichen Schlüsseln (Public-Key RegTP) der BNetzA, vormals RegTP, vertraut werden, die im Bundesanzeiger veröffentlicht werden. Die Zertifikate können daneben elektronisch über <http://www.nrca-ds.de/> abgerufen werden.

II. qualifizierte Signaturen von ZDA nach § 4 Abs. 3 SigG (angezeigter Betrieb):

a) Hierarchisches Top-Down-Modell

- Ebene 0: ZDA als Wurzel (Top-Level-CA) u. (Ausstellerzertifikat)
- Ebene 1: Teilnehmer (Unterzeichnerzertifikat)

b) Vertrauensanker:

Es liegt im Verantwortungsbereich des Nutzers von M-Doc AutoVerifier Version 2.1, durch geeignete Maßnahmen sicher zu stellen, welchem ZDA und deren Zertifikat er vertrauen will. Eine vergleichbare Veröffentlichung von vertrauenswürdigen Zertifikaten, wie im Bereich der qualifizierten Signaturen gemäß § 15 Abs.1 SigG, ist **nicht existent**. Der Hersteller empfiehlt dem Nutzer sich mit dem betroffenen ZDA in Verbindung zu setzen und geeignete Maßnahmen abzustimmen.

2. 1. 3 Inhalt des Verifikationsprotokolls für qualifizierte Signaturen

Dem Benutzer der Verifikationsfunktion werden die folgenden Informationen als Ergebnis des Prüfungsvorganges jeder Signatur für ein Protokoll bereitgestellt:

Informationen zur Verifikation

- zur Verifikation genutzte Teil- Signaturanwendungskomponente und Version
- Datum und Zeitpunkt der Signaturprüfung⁵
- Im Rahmen der Verifikation genutztes Gültigkeitsmodell
- Gesamtergebnis der Signaturprüfung

Details zur Datei:

- Dateiname
- Dateigröße
- Aktuell berechneter Hashwert der Datei (Dokument)
- Verwendeter Hash-Algorithmus
- Ermittelter Zeitpunkt der Signaturerstellung⁶
- Begründung und Ort der Signaturerstellung (nur bei PDF- Dokumenten)

Aus dem Zertifikat der Signatur:

- Attributstyp: (Schlüsselzertifikat oder Attributzertifikat)
- Subject: (Eindeutiger Name des Signaturschlüsselinhabers (Distinguished Name, DN))
- Issuer: (Aussteller, eindeutiger Name des ZDA)
- Seriennummer des Zertifikates
- Fingerabdruck : (Hashwert des Zertifikats)
- Gültigkeitszeitraum des Zertifikats von/bis:
- Subject Public Key: (Signaturprüfchlüssel)
- Public Key Algorithmus: (Signaturalgorithmus)
- Schlüssellänge des Public Key

⁵ Der Verifikationszeitpunkt, der für das Protokoll ausgegeben wird, gibt in der Regel die Systemzeit des Rechners wieder auf dem M-Doc AutoVerifier Version 2.1 installiert wurde. Die Zeitangabe ist nur in Verbindung mit einem Zeitstempel gemäß § 2 Nr. 14 SigG verlässlich.

⁶ Wie Fußnote 4.

- Attributsverweise:

Aus den Zertifikatserweiterungen (Extensions):

- authorityKeyIdentifier:
- OCSP-Quelle:
- Sperrlistenverteilungspunkt:
- qcStatements: (Flag zur Feststellung eines qualifizierten Zertifikats)
- subjectKeyIdentifier :
- keyUsage: (Nutzungseigenschaften der öffentlichen Schlüssel)
- certificatePolicies:
- subjectAltName: (2. Bezeichnung des Signaturschlüsselinhabers z.B. E-Mail)
- authorityInfoAccess:

Aus einem ggf. vorhandenen Attributzertifikat:

- Attributstyp:
- Subject: (eindeutiger Name des ZDA)
- Issuer: (Aussteller, eindeutiger Name des ZDA)
- Seriennummer des Zertifikates:
- Fingerabdruck des Zertifikates: (Hashwert des Zertifikats)
- Gültigkeitszeitraum des Zertifikates von/bis:
- Subject Public Key: (Signaturprüf Schlüssel)
- Public Key Algorithmus: (Signaturalgorithmus)
- Schlüssellänge des Public Key:
- Attribute: (Beschränkungen/ Attributsangaben)
- id-ismtt-at-restriction:

Aus den Zertifikatserweiterungen (Extensions):

- authorityKeyIdentifier:
- certificatePolicies:
- Sperrlistenverteilungspunkt:
- OCSP-Quelle:
- authorityInfoAccess:
- qcStatements:

aus dem CA Zertifikat des ZDA

- Attributstyp: (Schlüsselzertifikat oder Attributzertifikat)
- Subject: (eindeutiger Name des ZDA)
- Issuer: (Aussteller, Name der Root-CA/ RegTP/BNetzA)
- Seriennummer des Zertifikates

- Fingerabdruck des Zertifikates: (Hashwert des Zertifikats)
- Gültigkeitszeitraum des Zertifikates von/bis:
- Subject Public Key: (Signaturprüf Schlüssel)
- Public Key Algorithmus: (Signaturalgorithmus)
- Schlüssellänge des Public Key
- Attributsverweise:

Aus den Zertifikatserweiterungen (Extensions):

- authorityKeyIdentifier:
- Sperrlistenverteilungspunkt:
- OCSP-Quelle:
- qcStatements: (Flag zur Feststellung eines qualifizierten Zertifikats)
- subjectKeyIdentifier :
- keyUsage: (Nutzungseigenschaften der öffentlichen Schlüssel)
- certificatePolicies:
- subjectAltName:
- authorityInfoAccess:

aus dem Root-Zertifikat der BNetzA/ RegTP

- Attributstyp: (Schlüsselzertifikat oder Attributzertifikat)
- Subject: (Name der Root-CA/ RegTP/BNetzA)
- Issuer: (Aussteller, Name der Root-CA/ RegTP/BNetzA)
- Seriennummer des Zertifikates
- Fingerabdruck des Zertifikates: (Hashwert des Zertifikats)
- Gültigkeitszeitraum des Zertifikates von/bis:
- Subject Public Key: (Signaturprüf Schlüssel)
- Public Key Algorithmus: (Signaturalgorithmus)
- Schlüssellänge des Public Key

Aus den Zertifikatserweiterungen (Extensions):

- Sperrlistenverteilungspunkt:
- OCSP-Quelle:
- qcStatements: (Flag zur Feststellung eines qualifizierten Zertifikats)
- subjectKeyIdentifier :
- keyUsage: (Nutzungseigenschaften der öffentlichen Schlüssel)
- certificatePolicies:
- subjectAltName:
- authorityInfoAccess:

3. Erfüllung der Anforderungen des SigG und der SigV

3.1 Erfüllte Anforderungen

3.1.1 Erfüllte Anforderungen § 17 Abs. 2 Satz 2 SigG

M-Doc AutoVerifier Version 2.1 erfüllt die Anforderungen an Produkte für qualifizierte elektronische Signaturen nach § 17 Abs. 2 Satz 2 SigG.

Für die Überprüfung signierter Daten lässt sich feststellen:

1. auf welche Daten sich die Signatur bezieht,
2. ob die signierten Daten unverändert sind,
3. welchem Signaturschlüssel-Inhaber die Signatur zuzuordnen ist,
4. welche Inhalte das qualifizierte Zertifikat, auf dem die Signatur beruht, und zugehörige qualifizierte Attribut-Zertifikate aufweisen und

zu welchem Ergebnis die Nachprüfung von Zertifikaten nach § 15 Abs. 2 Nr. 2 SigV geführt hat.

3.1.2 Erfüllte Anforderungen § 17 Abs. 2 Satz 3 SigG

M-Doc AutoVerifier Version 2.1 erfüllt die Anforderungen an Produkte für qualifizierte elektronische Signaturen nach § 17 Abs. 2 Satz 3 SigG, indem es nach Bedarf auch den Inhalt der signierten Daten hinreichend erkennen lässt.

3.1.3 Erfüllte Anforderungen § 15 Abs. 2 Nr. 2 SigV

M-Doc AutoVerifier Version 2.1 ist eine Teil-Signaturanwendungskomponente nach § 17 Abs. 2 Satz 2 SigG und gewährleistet, dass bei der Prüfung einer qualifizierten elektronischen Signatur

- a. die Korrektheit der Signatur zuverlässig geprüft und zutreffend angezeigt wird
- b. eindeutig erkennbar wird, ob die nachgeprüften qualifizierten Zertifikate im jeweiligen Zertifikat-Verzeichnis zum angegebenen Zeitpunkt vorhanden und nicht gesperrt waren.

3.1.4 Erfüllte Anforderungen § 15 Abs. 4 SigV

Weiterhin sind für das Produkt M-Doc AutoVerifier Version 2.1 durch den Hersteller Maßnahmen gegen sicherheitstechnische Veränderung ergriffen worden, die gemäß

§ 15 Abs. 4 SigV sicherheitstechnische Veränderungen an den Anwendungskomponenten für den Nutzer erkennbar machen (Insb. 3.2.2.lit.f).

Voraussetzung dafür ist, dass die unter 3.2 ff spezifizierten Einsatzbedingungen eingehalten werden. Es wird ein Betrieb in einem „geschützten Einsatzbereich“⁷ vorausgesetzt.

3.2 Einsatzbedingungen

3.2.1 Potentielle Bedrohungen

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

- Angriffe über Kommunikationsnetze⁸,
- Angriffe über manuellen Zugriff Unbefugter/Datenaustausch per Datenträger⁹ und
- Fehler/Manipulationen bei Installation, Betrieb/Nutzung und Wartung/Reparatur.

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

- signierte Daten unvollständig oder falsch verifiziert werden

sind nachfolgende **Auflagen** zu beachten:

3.2.2 Maßnahmen in der Einsatzumgebung

Der Rechner 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.

⁷ Definierter Einsatzbereich gemäß Nr. 4.2 RegTP Dokument: Einheitliche Spezifizierung der Einsatzbedingungen für Signaturanwendungskomponenten Version 1.1.

⁸ Spezifizierte Bedrohung gemäß Fußnote 15 RegTP Dokument: Einheitliche Spezifizierung der Einsatzbedingungen für Signaturanwendungskomponenten Version 1.1.

⁹ Spezifizierte Bedrohung gemäß Fußnote 16 RegTP Dokument: Einheitliche Spezifizierung der Einsatzbedingungen für Signaturanwendungskomponenten Version 1.1.

a) Auflagen zur Anbindung an das Internet

Es wird vorausgesetzt, dass der Verifikationsrechner hinreichend gegen Bedrohungen, durch Zugriff über das Internet, abgeschottet ist. Die Internetverbindung muss über eine geeignete Firewall-Software auf dem Verifikationsrechner abgesichert sein, so dass Online-Angriffe aus dem Internet auf den Computer erkannt bzw. unterbunden werden.

b) Auflagen zur Anbindung an ein Intranet

Wenn der eingesetzte Verifikationsrechner in einem Intranet betrieben wird, so muss diese Netzverbindung über eine geeignete Firewall-Software auf dem Verifikationsrechner abgesichert sein, so dass Online-Angriffe aus dem Intranet auf den Computer erkannt bzw. unterbunden werden.

c) Auflagen zur Sicherheit der IT-Plattform und Applikationen

Der Benutzer des M-Doc AutoVerifier Version 2.1 muss sich davon überzeugen, dass keine Angriffe auf den Rechner 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,
2. auf dem Verifikationsrechner ein aktueller Virenschanner läuft, so dass keine Viren oder Trojanischen Pferde unentdeckt bleiben können,
3. die Hardware des Rechners nicht unzulässig verändert werden kann,
4. eine Benutzerauthentifizierung am Betriebssystem des Verifikationsrechners erforderlich ist,
5. nach Abschluss der Arbeiten eine Konsolensperrung erfolgt, die eine erneute Authentifizierung bei nächsten Arbeiten erforderlich macht.

d) Auflagen zur Auslieferung und Installation des Produktes

Die Installation des M-Doc AutoVerifier 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. Vor der Installation hat sich die installierende Person von der korrekten Anwendung des Auslieferungsverfahrens zu überzeugen: Die Teil-Signaturanwendungskomponente M-Doc AutoVerifier Version 2.1 wird vom Hersteller als Produkt auf einer CD ausgeliefert oder als Installationspaket über das Internet vertrieben. Die

dem Produkt beigefügte Überprüfungsroutine ist zur Sicherstellung der Produktintegrität einzusetzen (Prüfung der Code-Signatur).

M-Doc AutoVerifier Version 2.1 ist für die folgende technische Einsatzumgebung 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) .
- Unterstützte Betriebssysteme sind: Windows 2000 Professional, Windows 2000 Server, Windows Server 2003 Standard Edition, Windows Server 2003 Enterprise Edition, Windows XP Professional, Windows Vista und den Linuxdistributionen Debian ab V. 3.0, Ubuntu ab V. 5.1, RedHat Enterprise ab V. 4, Fedora Core ab V. 4 und Suse ab V. 9.0.

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) Schutz vor unbefugter Veränderung

Es werden alle sicherheitskritischen Komponenten der Anwendung von der Mentana-Claimsoft AG mit einer Codesignatur versehen. Die Prüfung der Signaturen kann auf Betriebssystemebene bei jedem Programmstart automatisch erfolgen. Folgendes Zertifikat wird für die Code-Signatur verwendet.

Zertifikat für Mentana-Claimsoft AG (Code-Sign-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

Datei	Version	Zertifikat
Windows-Version		
AutoVerfier.exe	2.1	Zertifikat 1
mentalgocsp.dll	1.1	Zertifikat 1
mdocapiext.dll	2.1	Zertifikat 1
MdocExtWx.dll	2.1	Zertifikat 1
mdocapi.dll	2.1	Zertifikat 1
mdocapissl.dll	2.1	Zertifikat 1
mdocpdf.dll	2.1	Zertifikat 1
mdoccrypto.dll	2.1	Zertifikat 1
mdoccryptossl.dll	2.1	Zertifikat 1
libeay32.dll	2.1	Zertifikat 1
ssleay32.dll	2.1	Zertifikat 1
pkcs15init.dll	2.1	Zertifikat 1
opensc-pkcs11.dll	2.1	Zertifikat 1
opensc.dll	2.1	Zertifikat 1
engine_pkcs11.dll	2.1	Zertifikat 1
opensc-pkcs11.dll	2.1	Zertifikat 1

Linux- Version		
AutoVerifier	2.1	Zertifikat 1
libMdocApiExt.Wx.a	2.1	Zertifikat 1
libssl.so.0.9.8	2.1	Zertifikat 1
libcrypto.so.0.9.8	2.1	Zertifikat 1
libopencsc.so.2	2.1	Zertifikat 1
libp11.so.0	2.1	Zertifikat 1
libscconf.so.2	2.1	Zertifikat 1
engine_pkcs11.so	2.1	Zertifikat 1
opencsc-pkcs11.so	2.1	Zertifikat 1

g) Maßnahmen zur Zugangskontrolle

Zum Schutz vor manuellen Zugriffen Unbefugter und über Datenaustausch per Datenträger ist der Signaturrechner so zu betreiben, dass eine Zugangskontrolle zur Konsole und zum sicheren Kartenlesegerät des Signatursystems aktiv ist.

Ein Installations- und Administrationshandbuch, in dem entsprechende Maßnahmen dokumentiert werden, liegt der Software in elektronischer Form bei.

3.2.3 Wartung/Reparatur

Bei der Wartung und der Reparatur des Signaturrechners gelten die Voraussetzungen der Erstinstallation (vergleiche Punkt 3.2.). Bei dem 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) über das Auftreten einer solchen Situation informiert. Mit dem in Verkehr bringen einer neuen Softwareversion des M-Doc AutoVerifier Version 2.1 hinterlegt die Mentana-Claimsoft AG umgehend einen Nachtrag zu dieser Herstellereklärung bei der Bundesnetzagentur.

3.3 Algorithmen und zugehörige Parameter

Das Produkt M-Doc AutoVerifier Version 2.1 verarbeitet zur Prüfung qualifizierter Signaturen die Hashverfahren SHA-256, SHA-512 und RIPEMD-160 sowie das Signaturverfahren RSA

mit variablen Schlüssellängen ab 2048 Bit. Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung reicht für SHA-256 und SHA-512 mindestens bis Ende 2014. Für RIPEMD-160 mindestens bis Ende des Jahres 2010 (Veröffentlicht am 05. Februar 2008 im Bundesanzeiger Nr. 19, Seite 376). Weiterhin kann M-Doc AutoVerifier Version 2.1 zu Prüfungszwecken im Rahmen der Verifikation die RSA Algorithmen mit der Schlüssellänge 2048-Bit und der Zwischenstufen (für den Zeitraum bis Ende 2008 1280 Bit; bis Ende 2009 bei 1536 Bit, bis Ende 2010 bei 1728 Bit und bis 2014 bei 1976 Bit) verarbeiten. Der RSA Algorithmus mit der Schlüssellänge 2048 Bit wird von der Bundesnetzagentur als „langfristig sicher“ eingestuft (siehe BAnz. (Veröffentlicht am 05. Februar 2008 im Bundesanzeiger Nr. 19, Seite 376).

Der aktuell gültige sowie die jährlichen Aktualisierungen des Algorithmenkatalogs können auf der Website der Bundesnetzagentur unter www.bundesnetzagentur.de eingesehen werden.

4. Begleitende Dokumente

Für diese Herstellereklärung gelten folgende Begleitdokumente:

1. Sicherheitstechnische Produktvorgaben AutoVerifier Version 2.1, Stand 10.04.2008.
2. Spezifikation der Test- und Entwicklungsumgebung für AutoVerifier (EVG) Version 2.1, Stand 10.04.2008.

5. Referenz

Diese Erklärung ersetzt die Herstellereklärung vom 19.12.2007 veröffentlicht im Amtsblatt der Bundesnetzagentur Nr. 24/2007 Mitteilung Nr. 1016, Seite 522.

6. Gültigkeit der Herstellereklärung

Diese Herstellereklärung ist bis zum Widerruf durch Mentana-Claimsoft AG bzw. 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) – gültig, längstens jedoch bis zum **31.12.2014**.

Dieses Dokument umfasst 15 Seiten.

Ende der Herstellereklärung.