

Herstellereklärung

Der Hersteller

Mentana-Claimsoft AG

Spreenhagener Str. 16
D-15528 Spreenhagen

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

Kanzlei-Signer Version 2.1

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

- Daten dem Prozess der Erzeugung oder Prüfung qualifizierter elektronischer Signaturen zuzuführen und sicher anzuzeigen
 - qualifizierte elektronische Signaturen und qualifizierte Zertifikate zu prüfen und die Ergebnisse anzuzeigen
- und den Anforderungen des Signaturgesetzes¹ und der Signaturverordnung² genügt.

Diese Erklärung ersetzt die Herstellereklärung vom 19.12.2007 Amtsblatt der Bundesnetzagentur Nr. 24/2007 vom 19.12.2007, Mitteilung Nr. 1015, Seite 5201.

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 26.05.2008

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 Erstellen einer qualifizierten Signatur	4
2.2 Erstellen qualifizierter Signaturen in einem Dokumentenstapel	5
2.3 Verifikation einer qualifizierten elektronischen Signatur	6
2.3.1 Ablauf der Verifikation einer qualifizierten elektronischen Signatur.....	6
2.3.2 Vertrauensanker.....	8
2.3.3 Inhalt des Verifikationsprotokolls	9
2.4 Anfordern qualifizierter Zeitstempel vom ZDA	12
3. Erfüllung der Anforderungen des SigG und der SigV	12
3.1 Erfüllte Anforderungen	12
3.1.1 Erfüllte Anforderungen § 17 Abs. 2 Satz 1 SigG	12
3.1.2 Erfüllte Anforderungen § 17 Abs. 2 Satz 2 SigG	13
3.1.3 Erfüllte Anforderungen § 17 Abs. 2 Satz 3 SigG	13
3.1.4 Erfüllte Anforderungen § 15 Abs. 2 SigV	13
3.1.5 Erfüllte Anforderungen § 15 Abs. 4 SigV	14
3.2 Einsatzbedingungen	14
3.2.1 Potentielle Bedrohungen	14
3.2.2 Maßnahmen in der Einsatzumgebung	15
a) Auflagen zur Anbindung an das Internet.....	15
b) Auflagen zur Anbindung an ein Intranet.....	15
c) Auflagen zur Sicherheit der IT-Plattform und Applikationen	15
d) Auflagen zur Auslieferung und Installation des Produktes	16
e) Auflagen zur Nutzung von bestimmten Signaturkarten (SSEE)	18
f) Schutz vor unbefugter Veränderung	20
g) Maßnahmen zur Zugangskontrolle	22
3.2.3 Wartung/Reparatur.....	22
3.3 Algorithmen und zugehörige Parameter	23
4. Begleitende Dokumente	23
5. Referenz	23
6. Gültigkeit der Herstellereklärung	24

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: **Kanzlei-Signer Version 2.1**

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

2. Funktionsbeschreibung

Der Kanzlei-Signer Version 2.1 ist eine Teil- Signaturanwendungskomponente, die für die speziellen Bedürfnisse von Rechtsanwälten und Notaren konzipiert wurde. Kanzlei-Signer Version 2.1 unterstützt alle Belange des elektronischen Rechtsverkehrs in der Justiz einschließlich der sicheren Zustellung von Dokumenten an einen Justiz-Intermediär (EGVP-ELBA-ERVD). Die Zustellung an den Justiz-Intermediär ist nicht Bestandteil dieser Herstellereklärung.

Der Kanzlei-Signer 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 3075-3375

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)

Der Kanzlei-Signer Version 2.1 ist auch eine Teil- Signaturanwendungskomponente gemäß § 2 Nr. 11b SigG, die qualifizierte Signaturen zusammen mit den jeweiligen Originaldokumenten verifiziert.

Für die Verifikation 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

Kanzlei-Signer Version 2.1 verfügt über eine sichere Anzeige (Secure Viewer). Auf Aufforderung durch den Benutzer können beliebige Dokumentenformate in einem PDF-Viewer innerhalb von Kanzlei-Signer Version 2.1 vor der Signaturerzeugung sicher angezeigt werden. Dazu werden die Dateien in das Format PDF/A nach DIN ISO 19005 konvertiert und mittels eines PDF-Viewers angezeigt. 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. Kanzlei-Signer Version 2.1 ermöglicht auch die Anzeige von Zertifikatsinhalten über einen Zertifikatsviewer.

2.1 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 darauf hin, 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 3.2.2 lit.e) dieser Herstellereklärung werden die sicheren Signaturerstellungseinheiten aufgeführt die im Einsatz mit Kanzlei-Signer Version 2.1 erfolgreich getestet wurden.

Um den Signaturvorgang zu beginnen steckt der Signaturschlüssel-Inhaber seine Signaturkarte in den Chipkartenleser. Kanzlei-Signer 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 Aufforderungsdialog für die PIN-Eingabe zeigt den Hersteller und Typ des angesprochenen geprüften und bestätigten Kartenlesegerätes an um zu gewährleisten, dass ein geeignetes Gerät für die PIN-Eingabe verwendet wird. Nach erfolgreicher PIN-Authentifizierung übernimmt Kanzlei-Signer Version 2.1 die Zuführung der Daten zur SSEE.

2.2 Erstellen qualifizierter Signaturen in einem Dokumentenstapel

Der Benutzer erstellt zunächst einen Dokumentenstapel durch Markierung und Auswahl mehrerer Dokumente. Alle ausgewählten Dokumente werden zu einem Stapel verbunden und an Kanzlei-Signer 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.³ 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. 2.1 beschriebenen Ablauf, wobei Kanzlei-Signer Version 2.1 die Zuführung der Daten zur Signaturerstellungseinheit für den gesamten Dokumentenstapel innerhalb einer Krypto-Session durchführt. Ein Zwischenspeichern der PIN (PIN-Caching) ist weder zulässig noch wird es durch die Software technisch realisiert.

2.3 Verifikation einer qualifizierten elektronischen Signatur

2.3.1 Ablauf der Verifikation einer qualifizierten elektronischen Signatur

Der Verifikationsvorgang wird durch den Benutzer durch Auswahl eines Dokuments eingeleitet. Nach Aufforderung durch den Benutzer überprüft Kanzlei-Signer 2.1 die Dokumente auf ihre Integrität und die Signaturen auf Gültigkeit.

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 Kanzlei-Signer Version 2.1 zunächst den Zertifizierungspfad und assoziiert die Zertifikatskette. Kanzlei-Signer 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, indem die entsprechenden Einträge (Flag) in den Zertifikaten

³ 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.

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.

ausgewertet werden. Im Anschluss daran ermittelt Kanzlei-Signer Version 2.1 zur Sicherstellung der Zertifikatsgültigkeit durch Onlineabfrage bei jedem Aussteller der Zertifikate 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 Kanzlei-Signer Version 2.1 entsprechend dem Gültigkeitsmodell das Gesamturteil der Signaturprüfung.

Zur Onlineüberprüfung der Zertifikatsgültigkeit nutzt Kanzlei-Signer 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 Kanzlei-Signer 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 Kanzlei-Signer Version 2.1 hinterlegen.

Der Hersteller weist ausdrücklich darauf hin, dass verlässliche Informationen zur Zertifikatsgültigkeit nur über eine aktuelle Onlineabfrage auf den Verzeichnisdienst eines ZDA zu erlangen sind. Dies kann durch Kanzlei-Signer Version 2.1 nur bei den oben beschriebenen „OCSP“ oder „Sperrlistenprüfungen“ sichergestellt werden. Andere Verfahren bedürfen besonderer administrativer Maßnahmen, was eine entsprechende Qualifikation auf Anwenderseite erfordert.

Der Zugriff auf ein LDAP-Verzeichnis bei einem ZDA erfordert regelmäßig eine Zugriffsberechtigung. Das Vorliegen einer solchen Berechtigung kann Kanzlei-Signer Version 2.1 **nicht** prüfen. Das weitere Vorgehen für eine Verifikation gegen ein LDAP 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:

a) **"Signatur gültig"**

b) **"Signatur ungültig"**

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

2. 3. 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 sogenannte „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 dem öffentlichen Schlüssel („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 Kanzlei-Signer 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. 3. 3 Inhalt des Verifikationsprotokolls

Dem Benutzer der Verifikationsfunktion werden die folgenden Informationen als Ergebnis des Prüfvorganges 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:
- Attributsverweise:

Aus den Zertifikatserweiterungen (Extensions):

- authorityKeyIdentifier:
- OCSP-Quelle:
- Sperrlistenverteilungspunkt:

⁵ Der Verifikationszeitpunkt der für das Protokoll ausgegeben wird gibt in der Regel die Systemzeit des Rechners wieder auf dem Kanzlei- Signer Version 2.0 installiert wurde. Die Zeitangabe ist nur in Verbindung mit einem Zeitstempel gemäß § 2 Nr. 14 SigG verlässlich.

⁶ Wie Fußnote 3.

- qcStatements: (Flag zur Feststellung eines qualifizierten Zertifikats)
- subjectKeyIdentifier :
- keyUsage: (Nutzungsseigenschaften 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: (Signaturprüfchlüssel)
- Public Key Algorithmus: (Signaturalgorithmus)
- Schlüssellänge des Public Key:
- Attribute: (Beschränkungen/ Attributsangaben)
- id-isismtt-at-restriction:

Aus den Zertifikatserweiterungen (Extensions):

- authorityKeyIdentifier:
- certificatePolicies:
- Sperrlistenverteilungspunkt:
- OCSP-Quelle:
- authorityInfoAccess:
- qcStatements: (Flag zur Feststellung eines qualifizierten Zertifikats)

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: (Signaturprüfchlüssel)
- 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: (Signaturprüfschlüssel)
- 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:

Jeder Verifikationsvorgang kann durch Abspeichern eines beschreibenden XML-Dokumentes mit vorgena nntem Inhalt dokumentiert werden. Dieses XML -File enthält alle nach inhaltlichen Anforderungen der GDPdU/GOBS für die Prüfung elektronischer Rechnungen gem. § 15 UStG.

2.4 Anfordern qualifizierter Zeitstempel vom ZDA

Beliebige elektronische Dokumente (Dateien) können durch den Benutzer für Archivierungszwecke oder zur Feststellung der amtlichen Zeit gem. ZeitG mit einem qualifizierten Zeitstempel eines Zertifizierungsdiensteanbieters gesichert werden. Dazu wird über eine verschlüsselte Verbindung (HTTPS) auf einen passwort geschützten Benutzeraccount der geschlossenen Benutzergruppe bei www.signaturportal.de mittels eines Web-Service zugegriffen. Kanzlei-Signer Version 2.1 errechnet den Hashwert des Dokumentes⁷, der über den geschützten Benutzeraccount an den ZDA übertragen wird. Der empfangene Zeitstempel wird entweder als externe Zeitstempeldatei abgelegt oder in das Dokument eingebettet (nur für PDF-Dokumente verfügbar).

Der Kanzlei-Signer Version 2.1 kann zur Anforderung qualifizierter Zeitstempel der folgenden Zertifizierungsdiensteanbieter verwendet werden:

a) **AuthentiDate International AG⁸**

Großenbaumer Weg 6

40472 Düsseldorf

b) **Deutsche Post Com GmbH⁹**

Geschäftsfeld Signtrust

Tulpenfeld 9

53113 Bonn

c) **D-TRUST GmbH¹⁰**

Kommandantenstr. 15

10969 Berlin

3. Erfüllung der Anforderungen des SigG und der SigV

3.1 Erfüllte Anforderungen

3.1.1 Erfüllte Anforderungen § 17 Abs. 2 Satz 1 SigG

Der Kanzlei-Signer Version 2.1 erfüllt die Anforderungen an Produkte für qualifizierte elektronische Signaturen nach § 17 Abs. 2 Satz 1 SigG. Er ermöglicht, dass die Erzeugung

⁷ Derzeit kann SHA 256 bis SHA 512 erzeugt u. übermittelt werden.

⁸ Gütezeichen RegTP Nr. Z0015, erteilt am 9. November 2001.

⁹ Gütezeichen RegTP Nr. Z0002, erteilt am 17. September 2004.

¹⁰ Gütezeichen RegTP Nr. Z0017, erteilt am 8. März 2002, zusätzlich auch angezeigtes ZDA.

einer qualifizierten elektronischen Signatur vorher eindeutig angezeigt wird und feststellbar ist, auf welche Daten sich die Signatur bezieht.

3.1.2 Erfüllte Anforderungen § 17 Abs. 2 Satz 2 SigG

Der Kanzlei-Signer 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
5. zu welchem Ergebnis die Nachprüfung von Zertifikaten nach § 5 Abs. 1 Satz 3 SigG geführt hat

3.1.3 Erfüllte Anforderungen § 17 Abs. 2 Satz 3 SigG

Der Kanzlei-Signer 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 zu signierenden oder signierten Daten hinreichend erkennen lässt.

3.1.4 Erfüllte Anforderungen § 15 Abs. 2 SigV

Der Kanzlei-Signer 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

Das Kanzlei-Signer Version 2.1 ist auch 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.

3.1.5 Erfüllte Anforderungen § 15 Abs. 4 SigV

Weiterhin sind für das Produkt Kanzlei-Signer Version 2. 1 durch de n Hersteller Maßnahme n gegen sich erheitstechnische Verän derung ergriffen worden, die gemäß § 15 Abs. 4 SigV sicherheitstechnische Veränderungen an der Anwendungskomponente für den Nutzer erkennbar machen. Voraussetzung dafür ist, dass die unter 3.2 ff spezifizierte n Einsatzbedingungen eingehalten werden. Es wird ein Betrieb in einem „geschützte n Einsatzbereich“¹¹ vorausgesetzt.

3.2 Einsatzbedingungen

3.2.1 Potentielle Bedrohungen

Die Sicherheit von Kanzlei-Signer Version 2.1 ist potentiell bedroht durch

- Angriffe über Kommunikationsnetze¹²,
- Angriffe über manuellen Zugriff Unbefugter/Datenaustausch per Datenträger¹³ und
- Fehler/Manipulationen bei Installation, Betrieb/Nutzung und Wartung/Reparatur.

Für den sicheren Einsatz von Kanzlei-Signer Version 2.1 und zur Verhinderung vo n erfolgreichen Angriffen mit den Zielen, dass:

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

¹¹ Definierter Einsatzbereich gemäß Nr. 4.2 RegTP Dokument: Einheitliche Spezifizierung der Einsatzbedingungen für Signaturanwendungskomponenten Version 1.1.

¹² Spezifizierte Bedrohung gemäß Fußnote 15 RegTP Dokument: Einheitliche Spezifizierung der Einsatzbedingungen für Signaturanwendungskomponenten Version 1.1.

¹³ Spezifizierte Bedrohung gemäß Fußnote 16 RegTP Dokument: Einheitliche Spezifizierung der Einsatzbedingungen für Signaturanwendungskomponenten Version 1.1.

sind die nachfolgenden **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.

a) Auflagen zur Anbindung an das Internet

Es wird vorausgesetzt, dass der Signaturrechner hinreichend gegen Bedrohungen durch Zugriff über das Internet abgeschottet ist.

b) Auflagen zur Anbindung an ein Intranet

Wenn der eingesetzte Signaturrechner in einem Intranet betrieben wird, so muss diese Netzverbindung über eine geeignete Firewall-Software auf dem Signaturrechner 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 Kanzlei-Signer 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 Rechner ein aktueller Virens Scanner 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 Inhaber möglich ist.

d) Auflagen zur Auslieferung und Installation des Produktes

Die Installation des Kanzlei-Signer 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 verwendet wird. Über die Konfiguration des Lesegerätes ist abzusichern, dass die PIN-Eingabe nur am Kartenleser möglich ist.

Vor der Installation hat sich die installierende Person von der korrekten Anwendung des Auslieferungsverfahrens zu überzeugen: Die Teil- Signaturanwendungskomponente Kanzlei-Signer Version 2.1 wird vom Hersteller als Produkt auf einer CD ausgeliefert oder als Installationspaket über das Internet vertrieben. Die dem Produkt beigelegte Überprüfungsroutine ist zur Sicherstellung der Produktintegrität einzusetzen (Prüfung der Code-Signatur).

Die Teil- Signaturanwendungskomponente Kanzlei-Signer 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).

- Kanzlei-Signer Version 2.1 kann unter den Betriebssystemen Windows 2000 Professional und Server, Windows XP Professional, Windows Server 2003 Standard und Enterprise Edition, Windows Vista eingesetzt werden.

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 nachfolgende geprüfte und bestätigte Kartenlesegeräte mit Kanzlei-Signer Version 2.1 erfolgreich getestet und empfiehlt deren Verwendung:

Handelsname	Angaben aus den veröffentlichten Bestätigungen bei der BNetzA			Schnittstelle
	Hersteller	Name	Reg. Nr.	
SPR 332	SCM Microsystems GmbH	Chipkartenleser SPR132, SPR332, SPR532, Firmware Version 4.15	TUVIT.09370.TE.03.2003	USB
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.122005	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 U	SB
Cherry SmartTerminal 2000 U	Cherry GmbH	Chipkartenterminal der Familie SmartTerminal ST-2xxx, Firmware Version 5.08	BSI.02059.TE.02.2006 U	SB
Kobil KAAAN Advanced	Kobil Systems GmbH	Chipkartenterminal KAAAN Advanced, Firmware Version 1.02, Hardware Version K104R3	BSI.02050.TE.12.2006 U	SB

Es sind auch die Anforderungen zu beachten, die der Hersteller des sich erheitsbestätigten Kartenlesegerätes und der Herausgeber der sicheren Signaturerstellungseinheit (SEEE) 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.

e) Auflagen zur Nutzung von bestimmten Signaturkarten (SSEE)

Der Hersteller hat die nachfolgend genannten Signaturerstellungseinheiten im Einsatz mit Kanzlei-Signer Version 2.1 erfolgreich getestet und empfiehlt dessen Einsatz:

Für die Erstellung von Signaturen wie unter Punkt 2.1 beschrieben empfiehlt der Hersteller den Einsatz nachfolgend genannter SSEE. Im „Stapel-signaturmodus“ wie unter Punkt 2.2 näher beschrieben dürfen nur sichere Signaturerstellungseinheiten (SSEE) verwendet werden, die vom ausstellenden Zertifizierungsdiensteanbieter dafür zugelassen sind.

In der nachfolgenden Übersichtstabelle sind diese in der Spalte "Stapel / Massensignatur" mit "[+]" gekennzeichnet worden.

Handelsbezeichnung	ZDA	Reg-Nr. ZDA	Name der SSEE in der Bestätigungsurkunde	Bestätigung der SSEE	unterstützt wird:		
					qualifizierte Signatur	Ver-/Entschlüsselung Authentisierung	Massen/ Stapel-Signatur
PKS- Card (NetKey3.01)	Produktzentrum TeleSec Telekom AG	Z0001	SSEE TCOS 3.0 Signature Card, Version 1.0	TUVIT .09361.TE. 10.2001 Nachtrag vom 24.03.2004	[+] ¹⁴	[+]	[-] ¹⁵
„Multisign“	Produktzentrum TeleSec Telekom AG	Z0001	SSEE TCOS 3.0 Signature Card, Version 1.0	TUVIT .09361.TE. 10.2001 Nachtrag vom 24.03.2004	[+]	[+]	[+]
Signaturkarte der Bundesnotarkammer	Bundesnotarkammer, Zertifizierungsstelle	Z0003	SSEE STARCOS 3.0	TUVIT .93100.TE.09.2005	[+]	[+]	[0] ¹⁶
Signaturkarte für Berufsträger der DATEV	DATEV eG Zertifizierungsstelle	Z0004	SSEE STARCOS 3.0	TUVIT .93100.TE.09.2005	[+]	[+]	[0]
D-Trust-Signaturkarte Version 2.2	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	[+]	[+]	[0]

¹⁴ [+] = unterstützt.

¹⁵ [-] = nicht unterstützt.

¹⁶ [0] = Funktionalität nicht vorhanden/gesperrt.

D-Trust-multicard	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	[+]	[+]	[+]
Signtrust-Identity-Card	Deutsche Post Com GmbH Geschäftsfeld Signtrust	Z0002	SSEE STARCOS 3.0	TUVIT .93100.TE.09.2005	[+]	[+]	[0]
Signtrust-M-Card	Deutsche Post Com GmbH Geschäftsfeld Signtrust	Z0002	Signaturerstellungseinheit STARCOS 3.0 with Electronic Signature Application V3.0, Type 3B	TUVIT .09399.TE.10.2005	[+]	[+]	[+]
TC-Trustcenter Q-Sign-Card (limited)	TC TrustCenter TrustCenter GmbH	Z0032	SEE „Chipkarte mit Prozessor SLE66CX322P, CardOS V4.3B mit Applikation für digitale Signatur“	T-Systems .02122.TE.05. 2005	[+]	[+]	[0]
TC-Trustcenter Q-Sign-Card (unlimited)	TC TrustCenter TrustCenter GmbH	Z0032	SEE „Chipkarte mit Prozessor SLE66CX322P, CardOS V4.3B mit Applikation für digitale Signatur“	T-Systems .02122.TE.05. 2005	[+]	[+]	[+]
Chambersign Karte der IHK D- Trust-Card (2.02c)	D-Trust GmbH	Z0017 und angezeigt § 4 Abs. 3 SigG	SEE „Chipkarte mit Prozessor SLE66CX322P, CardOS V4.3B mit Applikation für digitale Signatur	T-Systems .02122.TE.05. 2005	[+]	[+]	[0]
Sparkassen-Card oder GeldKarte	S-Trust	angezeigt § 4 Abs. 3 SigG	SEE ZKA-Signaturkarte, Version 5.02 der Gemplus-mids GmbH	TUVIT .09385.TU.09.2004	[+]	[+]	[+]
			SEE ZKA Banking Signature Card, Version 6.2b NP und 6.2f NP, Type 3 der Giesecke & Devrient GmbH	TUVIT .09395.TU.01.2005	[+]	[+]	[-]
			SEE ZKA Banking Signature Card, Version 6.31 NP, Type 3 der Giesecke & Devrient GmbH	TUVIT .09397.TU.03.2005	[+]	[+]	[-]

			SEE ZKA Banking Signature Card, Version 6.32 NP, Type 3 der Giesecke & Devrient GmbH	TUVIT .93125.TU.12.2005	[+]	[+]	[-]
			SEE ZKA Banking Signature Card, Version 6.4 der Giesecke & Devrient GmbH	TUVIT .93123.TU. 12. 2006	[+]	[+]	[-]
			SEE ZKA-Signaturkarte, Version 5.10 der Gemplus-mids GmbH	wird in Kürze veröffentlicht	[+]	[+]	[-]
			SEE ZKA Banking Signature Card, Version 6.6 der Giesecke & Devrient GmbH	TUVIT .93130.TU.05.2006	[+]	[+]	[-]
			SEE ZKA Banking Signature Card, Version 6.51 der Giesecke & Devrient GmbH	TUVIT .93129.TU.03.2006	[+]	[+]	[-]
			Signaturerstellungseinheit ZKA SECCOS Sig v1.5.3 der Sagem Orga GmbH	BSI .02075.TE.08.2006	[+]	[+]	[-]
			ZKA-Signaturkarte, Version 5.11 M Gemplus GmbH (Gemalto)	TUVIT .93148.TU.06.2007	[+]	[+]	[+]
Signaturkarte der Deutschen Rente Bund	Deutsche Rentenversicherung Bund	angezeigt § 4 Abs. 3 SigG	SEE „Chipkarte mit Prozessor SLE66CX322P, CardOS V4.3B mit Applikation für digitale Signatur“	T-Systems .02122.TE.05. 2005	[+]	[+]	[0]

f) Schutz vor unbefugter Veränderung

Es werden alle sicherheitskritischen Komponenten von Kanzlei-Signer Version 2.1 von der Mentana-Claimsoft AG mit einer Codesignatur versehen. Die Prüfung der Code-Signaturen erfolgt auf Betriebssystemebene bei jedem Programmstart automatisch. Folgendes Zertifikat wird für die Code-Signatur verwendet.

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

Datei	Version	Zertifikat
kanzleisigner.exe	2.1	Zertifikat 1
Mdocapi.dll 1.5		Zertifikat 1
Base-CSP (mentcsp.dll)	1.1	Zertifikat 1
Algo-CSP (mentalgocsp.dll)	1.1	Zertifikat 1
mentmdcardos43b.dll	1.1	Zertifikat 1
mentmdtcos20.dll	1.1	Zertifikat 1
mentmdtcos30.dll	1.1	Zertifikat 1
mentmdseccos.dll	1.1	Zertifikat 1
mentmdsetcos.dll	1.1	Zertifikat 1
mentmdstarcos30.dll	1.1	Zertifikat 1
mentmdmcrd21.dll	1.1	Zertifikat 1
mentmdcardos401a.dll	1.1	Zertifikat 1
mdocapi.dll	2.1	Zertifikat 1
MdocExtWx.dll	2.1	Zertifikat 1
MdocTSAClient.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

g) 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.

Ein Installations- und Administrationshandbuch, in dem entsprechende Maßnahmen dokumentiert werden, liegen 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 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 Inverkehrbringen einer neuen Softwareversion des Kanzlei-Signer 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 Kanzlei-Signer Version 2.1 verwendet zur Erstellung und 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. 1 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). Für die Erzeugung von Signaturen wird empfohlen nur noch den RSA Algorithmus mit der Schlüssellänge von 2048-Bit zu nutzen. Dieser gilt bis Ende 2014 als sicher. Weiterhin kann Kanzlei-Signer 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 Kanzlei-Signer (EVG) Version 2.1, Stand 10.04.2008.
2. Spezifikation der Test- und Entwicklungsumgebung für Kanzlei-Signer (EVG) Version 2.1, Stand 10.04.2008.

5. Referenz

Diese Erklärung ersetzt die Herstellereklärung vom 19.12.2007 Amtsblatt der Bundesnetzagentur Nr. 24/2007 vom 19.12.2007, Mitteilung Nr. 1015, Seite 5201.

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 dem Punkt 3.3 angezeigt)- jeweils angezeigt durch die Bundesnetzagentur (www.bundesnetzagentur.de) – gültig, längstens jedoch bis zum **31.12.2014**.

Dieses Dokument umfasst 24 Seiten.

Ende der Herstellereklärung.