

Herstellererklärung

Der Hersteller

**OPTIMAL SYSTEMS Gesellschaft für innovative Computertechnologien mbH**

Cicerostraße 26  
10709 Berlin

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

**OS|ECM Signaturmodul Version 6.0**

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 Signaturgesetzes<sup>1</sup> und der Signaturverordnung<sup>2</sup> genügt.

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.optimal-systems.de> veröffentlicht.

Per Januar 2010 liegt auch eine Version 6.10 der Teil- Signaturanwendungskomponente OS|ECM Signaturmodul vor.

Berlin, 25.03.2010

gez. Karsten Renz  
Geschäftsführer

<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 ..... 8

    2.4 Schnittstellen ..... 8

3. Funktionsbeschreibung ..... 8

    3.1 Erstellen einer qualifizierten Signatur ..... 10

    3.2 Erstellen qualifizierter Signaturen in einem Dokumentenstapel ..... 11

    3.3 Verifikation einer qualifizierten elektronischen Signatur ..... 12

        3.3.1 Ablauf der Verifikation einer qualifizierten elektronischen Signatur ..... 12

        3.3.2 Vertrauensanker ..... 15

        3.3.3 Inhalt des Verifikationsprotokolls ..... 16

    3.4 Anfordern qualifizierter Zeitstempel vom ZDA ..... 19

4. Erfüllung der Anforderungen des SigG und der SigV ..... 20

    4.1 Erfüllte Anforderungen ..... 20

        4.1.1 Erfüllte Anforderungen § 17 Abs. 2 Satz 1 SigG ..... 20

        4.1.2 Erfüllte Anforderungen § 15 Abs. 2 Nr. 1 SigV ..... 21

        4.1.3 Erfüllte Anforderungen § 17 Abs. 2 Satz 2 SigG ..... 22

        4.1.4 Erfüllte Anforderungen § 15 Abs. 2 Nr. 2 SigV ..... 23

        4.1.5 Erfüllte Anforderungen § 17 Abs. 2 Satz 3 SigG ..... 23

        4.1.6 Erfüllte Anforderungen § 15 Abs. 4 SigV ..... 24

5. Einsatzbedingungen ..... 24

    5.1.1 Potentielle Bedrohungen..... 24

    5.1.2 Maßnahmen in der Einsatzumgebung ..... 24

        a) Zulässige IT- Komponenten und Systeme für den Signaturbetrieb ..... 25

        b) Auflagen zur Anbindung an das Internet..... 25

        c) Auflagen zur Anbindung an ein Intranet..... 25

        d) Auflagen zur Sicherheit der IT-Plattform und Applikationen ..... 26

        e) Auflagen zur Auslieferung und Installation des Produktes..... 27

        f) Auflagen zur Nutzung von bestimmten Signaturkarten (SSEE) ..... 28

        g) Schutz vor unbefugter Veränderung ..... 28

        h) Maßnahmen zur Zugangskontrolle..... 30

        i) Absicherung von Schnittstellen ..... 30

    5.1.3 Wartung/Reparatur..... 30

6. Algorithmen und zugehörige Parameter..... 31

8. Gültigkeit der Herstellererklärung..... 32

9. Begleitende Dokumente ..... 32

| Dokumenten<br>-Version | Bearbeiter   | Inhalt                             | Datum           |
|------------------------|--------------|------------------------------------|-----------------|
| 2.01                   | Raoul Kirmes | Übernahme Stand 15.11.2006         | 06.06. 2008     |
| 2.02                   | Raoul Kirmes | Überarbeitung Algorithmen          | 09.06. 2008     |
| 2.03                   | Raoul Kirmes | Ergänzung SSEE/Leser               | 13.06. 2008     |
| 2.04                   | Raoul Kirmes | Umsetzung aktuelles Release        | 17.06. 2008     |
| 2.05                   | Raoul Kirmes | Zeitstempelkomponente              | 26.06. 2008     |
| 2.06                   | Raoul Kirmes | Anpassung BNetzA                   | bis 18.03. 2010 |
| 2.07                   | Reibis       | Prüfung                            | 18.03. 2010     |
| 2.08                   | Karsten Renz | Autorisierung zur Veröffentlichung | 18.03. 2010     |

### 1. Handelsbezeichnung

Die Handelsbezeichnung lautet: **OS|ECM Signaturmodul Version 6.0**

Per Januar 2010 liegt auch eine Version 6.10 der Teil- Signaturanwendungskomponente OS|ECM Signaturmodul vor.

Hersteller: OPTIMAL SYSTEMS Gesellschaft für innovative Computertechnologien mbH  
 Registergericht: Berlin Charlottenburg HRB 38560 B  
 Cicerostraße 26  
 10709 Berlin

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   | Ax.exe                 | 6.0 und 6.10 | 29.10.2009 | Siehe Kap. 5.1.2.e |
| Das Produkt benötigt keine externen Funktionsbibliotheken oder Komponenten von Drittanbietern. |                        |              |            |                    |
| Handbuch   | Handbuch_OS-Client.pdf | 6.0 und 6.10 | 29.10.2009 | Siehe Kap. 5.1.2.e |

Die Teil- Signaturanwendungskomponente OS|ECM Signaturmodul Version 6.0 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 STARCOS 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>6</sup>         |
| <b>Signaturkarte für Berufsträger der DATEV</b>          | DATEV eG Zertifizierungsstelle           | Z0004                               | SSEE STARCOS 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]                      |
| <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                              | [+]                    | [+]                                  | [+]                      |

<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>SigntrustCard 3.0/<br/>Signtrust MCard100 3.0/<br/>Signtrust MCard 3.0</b> | Deutsche Post Com GmbH<br>Geschäftsfeld 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<br>Geschäftsfeld 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<br>Geschäftsfeld 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<br>Geschäftsfeld 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                               | SEE „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<br>§ 4 Abs. 3<br>SigG | SEE ZKA<br>Banking<br>Signature Card,<br>Version 6.2b NP<br>und 6.2f NP, Type<br>3 der Giesecke & | TUVIT<br>.09395.TU.01.2005   | [+] | [+] | [-] |
|  | S-Trust | angezeigt<br>§ 4 Abs. 3<br>SigG | SEE ZKA<br>Banking<br>Signature Card,<br>Version 6.31 NP,<br>Type 3 der<br>Giesecke &             | TUVIT<br>.09397.TU.03.2005   | [+] | [+] | [-] |
|  | S-Trust | angezeigt<br>§ 4 Abs. 3<br>SigG | SEE ZKA<br>Banking<br>Signature Card,<br>Version 6.32 NP,<br>Type 3 der<br>Giesecke &             | TUVIT<br>.93125.TU.12.2005   | [+] | [+] | [-] |
|  | S-Trust | angezeigt<br>§ 4 Abs. 3<br>SigG | SEE ZKA<br>Banking<br>Signature Card,<br>Version 6.4 der<br>Giesecke &                            | TUVIT<br>.93123.TU. 12.<br>2006  | [+] | [+] | [-] |
|  | S-Trust | angezeigt<br>§ 4 Abs. 3<br>SigG | SEE ZKA-<br>Signaturkarte,<br>Version 5.10 der<br>Gemplus-mids<br>GmbH                            | TUVIT.93132.TU.06.200<br>6 20.06.2006  | [+] | [+] | [-] |
|  | S-Trust | angezeigt<br>§ 4 Abs. 3<br>SigG | SEE ZKA<br>Banking<br>Signature Card,<br>Version 6.6 der<br>Giesecke &<br>Devrient GmbH           | TUVIT<br>.93130.TU.05.2006<br>Nachtrag vom<br>28.08.2006 und<br>vom 18.10.2006 | [+] | [+] | [-] |
|  | S-Trust | angezeigt<br>§ 4 Abs. 3<br>SigG | SEE ZKA<br>Banking<br>Signature Card,<br>Version 6.51 der<br>Giesecke &                           | TUVIT<br>.93129.TU.03.2006   | [+] | [+] | [-] |
|  | S-Trust | angezeigt<br>§ 4 Abs. 3<br>SigG | Signatuererstellung<br>seinheit ZKA<br>SECCOS Sig<br>v1.5.2 und 1.5.3<br>der Sagem Orga           | BSI.02075.TE.08.2006<br>BSI.02076.TE.12.2006                                   | [+] | [+] | [-] |
|  | S-Trust | angezeigt<br>§ 4 Abs. 3<br>SigG | ZKA-<br>Signaturkarte,<br>Version 5.11 M<br>Gemplus GmbH  | TUVIT<br>.93148.TU.06.2007   | [+] | [+] | [+] |
|  | S-Trust | angezeigt<br>§ 4 Abs. 3<br>SigG | ZKA-<br>Signaturkarte,<br>Version 6   | TUVIT.<br>93143.TE.11.2007   | [+] | [+] | [-] |
|  | S-Trust | angezeigt<br>§ 4 Abs. 3<br>SigG | ZKA Banking<br>Signature Card,<br>Version 7.1   | TUVIT.<br>93149.TE.09.2007   | [+] | [+] | [-] |

|   |   |                                 |   |  |     |     |     |
|---|---|---------------------------------|---|--|-----|-----|-----|
|   | S-Trust                                 | angezeigt<br>§ 4 Abs. 3<br>SigG | ZKA Banking<br>Signature Card,<br>Version 7.1.1   | TUVIT.<br>93159.TE.09.2007   | [+] | [+] | [-] |
|   | S-Trust                                 | angezeigt<br>§ 4 Abs. 3<br>SigG | SSEE ZKA<br>Banking<br>Signature Card,<br>Version 7.2.1   | TUVIT.<br>93157.TE.06.2008   | [+] | [+] | [-] |
|   | S-Trust                                 | angezeigt<br>§ 4 Abs. 3<br>SigG | ZKA Banking<br>Signature Card,<br>Version 7.1.2   | TUVIT.<br>93166.TU.06.2008   | [+] | [+] | [-] |
|   | S-Trust                                 | angezeigt<br>§ 4 Abs. 3<br>SigG | SSEE ZKA-<br>Signaturkarte,<br>Version 6.01   | TUVIT.<br>93169.TU.09.2008   | [+] | [+] | [-] |
| <b>Signaturkarte<br/>der Deutschen<br/>Rente Bund</b> | Deutsche<br>Rentenversic<br>herung Bund | angezeigt<br>§ 4 Abs. 3<br>SigG | SSEE „Chipkarte<br>mit Prozessor<br>SLE66CX322P,<br>CardOS V4.3B<br>mit Applikation für<br>digitale Signatur" | T-Systems<br>.02122.TE.05. 2005,<br>Nachtrag vom<br>06.05.2008                                 | [+] | [+] | [-] |
|   | Deutsche<br>Rentenversic<br>herung Bund | angezeigt<br>§ 4 Abs. 3<br>SigG | SSEE<br>"ACOS EMV-<br>A04V1"  | T-Systems.<br>02166.TE.07.2008<br>Nachtrag 1 18.12.2008<br>und<br>Nachtrag 2 vom<br>19.05.2009 | [+] | [+] | [-] |

**Unterstützte Kartenlesegeräte**

| Handelsname                              | Angaben aus den veröffentlichten Bestätigungen bei der BNetzA |   |                             | Schnittstelle |
|--|---|---|-----------------------------|---------------|
|  | Hersteller  | Name  | Reg. Nr.                    |               |
| SPR 532 usb<br>(Chipdrive<br>pinpad pro) | SCM<br>Microsystems<br>GmbH                                   | Chipkartenleser SPR132, SPR332, SPR532,<br>Firmware Version 4.15                  | TUVIT.09370.TE<br>.03. 2003 | USB, seriell  |
| CardMan 3621                             | OMNIKEY<br>GmbH   | SAK Chipkartenterminal der Familie CardMan<br>Trust CM3621, Firmware-Version 6.00 | BSI.02057.TE.12<br>.2005    | USB           |
| CardMan 3821                             | OMNIKEY<br>GmbH   | SAK Chipkartenterminal der Familie CardMan<br>Trust CM3821, Firmware-Version 6.00 | BSI.02057.TE.12<br>.2005    | USB           |
| Cherry<br>Smartboard<br>G83-6744         | Cherry GmbH   | Chipkartenterminal der Familie SmartBoard<br>xx44 Firmware-Version 1.04           | BSI.02048.TE.12<br>. 2004   | USB           |
| Cherry<br>SmartTerminal<br>2000 U        | Cherry GmbH   | Chipkartenterminal der Familie SmartTerminal<br>ST-2xxx, Firmware Version 5.08    | BSI.02059.TE.02<br>. 2006   | USB           |

|                        |                       |   |  |     |
|------------------------|-----------------------|---|--|-----|
| Kobil KAAN<br>Advanced | Kobil Systems<br>GmbH | Chipkartenterminal KAAN Advanced, Hardware<br>Version K104R3, Firmware Version 1.19 | BSI.02050.TE.12<br>.2006 vom<br>12.2006 und<br>Nachtrag von<br>T-Systems<br>02207.TU.04.200<br>8 | 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

OS|ECM Signaturmodul Version 6.0 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 OS|ECM Signaturmodul Version 6.0 die von der Signaturkarte verarbeiteten (signierten) Daten.

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

OS|ECM Signaturmodul Version 6.0 stellt eine grafische Oberfläche als Schnittstelle zum Signaturschlüssel-Inhaber bereit und visualisiert die Interaktion mit diesem.

#### c) Schnittstelle zur aufrufenden Anwendung:

OS|ECM Signaturmodul Version 6.0 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.

## 3. Funktionsbeschreibung

**OS|ECM – Signaturmodul Version 6.0** ist ein Produktbestandteil von OS|ECM, einem Enterprise Content Management System, welches innerhalb der Produktpalette alle Funktionen zur Erzeugung, Verwaltung und Archivierung von Dokumenten bietet. Innerhalb des Enterprise Content Management Systems können unterschiedlichste Dokumentarten, z.B. Gebührenbescheide, Rechnungen und sonstige rechtsrelevante Schriftstücke verwaltet werden. OS|ECM – Signaturmodul Version 6.0 dient auch als

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

Signatur- und Verifikationskomponente im Anwendungsbereich einer mit **OS|ECM** integrierten virtuellen Poststelle (EGVP/ OSCI/De-Mail).

Auf Anforderung können Dokumente an das Signaturmodul übergeben werden, wo eine elektronische Signatur angebracht wird.

Der OS|ECM Signaturmodul Version 6.0 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

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 OS|ECM Signaturmodul Version 6.0 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 \*.pkcs7 \*.p7b \*.CMS 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 3075-3275

OS|ECM Signaturmodul Version 6.0 verfügt über eine sichere Anzeige (Secure Viewer). Auf Aufforderung durch den Benutzer können beliebige druckbare Dokumentenformate in einem PDF-Viewer innerhalb von OS|ECM Signaturmodul Version 6.0 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). OS|ECM Signaturmodul Version 6.0 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 Herstellereklärung werden die sicheren Signaturerstellungseinheiten aufgeführt die im Einsatz mit OS|ECM Signaturmodul Version 6.0 erfolgreich getestet wurden.

Um den Signaturvorgang zu beginnen steckt der Signaturschlüssel-Inhaber seine Signaturkarte in den Chipkartenleser. OS|ECM Signaturmodul Version 6.0 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 Aufforderungsdiallog 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 OS|ECM Signaturmodul Version 6.0 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

Der Benutzer erstellt zunächst einen Dokumentenstapel durch Markierung und Auswahl mehrerer Dokumente. Alle ausgewählten Dokumente werden zu einem Stapel verbunden und an OS|ECM Signaturmodul Version 6.0 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>8</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 OS|ECM Signaturmodul Version 6.0 die Zuführung der Daten zur Signaturerstellungseinheit für den gesamten Dokumentenstapel innerhalb einer „Krypto-Session“<sup>9</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 „[+]“). Die Stapelsignatur ist eine besondere Ausprägung der Massensignatur die Synonym auch als Mehrfach-, Batch-, Stapel- oder Multisignatur bezeichnet wird. 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). In Falle der Massensignatur Variante a) sind besondere Maßnahmen in der Einsatzumgebung zu ergreifen die dass unberechtigte einliefern von Dokumenten sicher verhindern. **Der Einsatz von OS|ECM Signaturmodul Version 6.0 nach Variante a) Massensignaturen ist unzulässig.** Der zulässige vorbeschriebene Einsatz von OS|ECM Signaturmodul Version 6.0 im sog. „Stapelsignaturmodus“ Variante b), erfasst nur die Einlieferung einer vorher durch den Nutzer mittels OS|ECM Signaturmodul Version 6.0 definierten und konkretisierten Anzahl von Dokumenten (Stapel) die der sicheren Signaturkarte (SSEE) im Mehrfachbetrieb<sup>10</sup> zugeführt

<sup>8</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>9</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.

<sup>10</sup> das heißt unter Nutzung einer einmaligen Identifizierung (PIN) für die Einlieferung mehrerer Signaturen bzw. Zugriffe auf die SSEE.

werden. Die Erzeugung einer „Stapelsignatur“ in diesem Sinne wird dem Nutzer durch einen Warnhinweis und in einem gesonderten Menü deutlich angezeigt.

Einsatz von OS|ECM Signaturmodul Version 6.0 in Verbindung mit einer Signaturerstellungseinheit (SSEE) soll an dem Arbeitsplatz erfolgen, an dem auch das geprüft und bestätigte Kartenlesegerät installiert ist. Zulässig ist der Einsatz von OS|ECM Signaturmodul Version 6.0 auch in einer Microsoft Terminal Services und Windows 2003 Server Umgebung sowie auf Citrix Presentation Server in den unter (vgl. Kap 2.2. Tabelle 2) angegebenen Versionen. **Der Einsatz von OS|ECM Signaturmodul Version 6.0** im Rahmen der sog. „**Telesignatur**“, bei denen die Signaturanwendungskomponente und der geprüft und bestätigte Kartenleser ohne weitere Sicherheitsvorkehrungen über ein LAN verbunden sind, **ist unzulässig**.

### 3.3 Verifikation einer qualifizierten elektronischen Signatur

#### 3.3.1 Ablauf der Verifikation einer qualifizierten elektronischen Signatur

Der Verifikationsvorgang wird durch den Benutzer durch Auswahl eines Dokuments<sup>11</sup> eingeleitet. Nach Aufforderung durch den Benutzer überprüft OS|ECM Signaturmodul Version 6.0 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 Signaturerstellung<sup>12</sup> entsprechend dem zulässigen Gültigkeitsmodell (Kette) gültig und nicht gesperrt?
- f) Bei PKCS#7-konformen Signaturen die in den unsigned Attribut einen qualifiziert Zeitstempel nach § 2 Nr. 14 SigG enthalten, die gültige gesetzliche Signaturzeit und die Zertifikatsinformationen des Zeitstempeldiensteanbieters.
- g) Bei PKCS#7-konformen Signaturen die entsprechend Adobe-Reference 1.4 bis 1.6 in ein Portable Document Format (PDF) eingebettet wurden und bei deren Erzeugung ein Zeitstempel nach § 2 Nr. 14 SigG angefordert wurde, die gültige gesetzliche Signaturzeit und die Zertifikatsinformationen der

<sup>11</sup> Dokument bedeutet in diesem Zusammenhang, entweder ein Dokument mit interner oder externer Signaturdatei oder eine Zeitstempeldatei (.tsr) sein, welcher der Verifikation zugeführt werden kann.

<sup>12</sup> Der Signaturzeitpunkt der aus den Signaturinformationen extrahiert wird, gibt in der Regel die Systemzeit des Rechners des Signaturschlüsselhabers wieder. Die Zeitangabe ist nur in Verbindung mit einem Zeitstempel gemäß § 2 Nr. 14 SigG verlässlich.

Zeitstempelinstanz.

Zur Verifikation der elektronischen Signatur ermittelt OS|ECM Signaturmodul Version 6.0 zunächst den Zertifizierungspfad und assoziiert die Zertifikatskette. OS|ECM Signaturmodul Version 6.0 verifiziert die mathematische Korrektheit<sup>13</sup> aller Signaturen in der Zertifikatskette. Soweit die mathematische Verifizierung 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 OS|ECM Signaturmodul Version 6.0 zur Sicherstellung der Zertifikatsgültigkeit durch Onlineabfrage bei jedem Aussteller der Zertifikate in der Kette (Kettenmodell), ob das Zertifikat im Zeitpunkt der Anfrage bekannt, gültig und nicht gesperrt ist bzw. wann es gesperrt wurde. Aus diesen Informationen ermittelt OS|ECM Signaturmodul Version 6.0 entsprechend dem Gültigkeitsmodell das Gesamturteil der Signaturprüfung.

Zur Onlineüberprüfung der Zertifikatsgültigkeit nutzt OS|ECM Signaturmodul Version 6.0 standardmäßig die durch die ZDA 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 OS|ECM Signaturmodul Version 6.0 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 in OS|ECM Signaturmodul Version 6.0 hinterlegen.

Der Hersteller weist ausdrücklich daraufhin, dass verlässliche Informationen zur Zertifikatsgültigkeit nur über eine aktuelle Onlineabfrage auf den Verzeichnisdienst eines ZDA zu erlangen sind. Dies kann durch OS|ECM Signaturmodul Version 6.0 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 OS|ECM Signaturmodul Version 6.0 **nicht** prüfen. Das weitere Vorgehen für eine Verifikation gegen ein LDAP ist beim Kartenausgebenden ZDA zu erfragen.

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:

<sup>13</sup> Dazu wird der definierte Byte Range gemäß CMS Spezifikation (CMS= [Cryptographic Message Syntax gemäß RFC2630, RFC3369, RFC3852]) in der Version der Common PKI 2.1 (ehemals ISIMTT) extrahiert. Dieser referenzierte Byte-Bereich wird mit dem im Zertifikat angegebenen Hashwert-Algorithmus nachberechnet. Das Ergebnis wird mit dem entschlüsselten Wert aus dem „Signed-Data-Bereich“ der Signatur verglichen.

a) "Signatur gültig"

b) "Signatur ungültig"

c) „**Status unbekannt** Mindestens eine Prüfung konnte nicht abschließend durchgeführt werden.“

Zusätzlich zu den oben genannten Urteilen wird jeweils angegeben<sup>14</sup>:

- zu a)
1. Zeitraum der Sicherheitseignung des verwendeten Hash-Algorithmus
  2. Zeitraum der Sicherheitseignung des verwendeten Verschlüsselungs-Algorithmus
  3. (nur) wenn der **Prüfzeitpunkt** nach einem Ablaufdatum der Sicherheitseignung eines verwendeten Verschlüsselungs-Algorithmus oder Hash-Algorithmus liegt (Angaben zu Nr. 1 und Nr. 2) erfolgt folgender Warnhinweis:

*„Die bewertete Signatur erfüllt nur noch die Anforderungen des § 371a ZPO sofern das Dokument einschl. der Signatur im Rahmen der Archivierung durch eine Maßnahme<sup>15</sup> nach § 6 Abs. 1 Satz 2 SigG, § 17 Satz 3 SigV i. v. m. § 2 Nr. 14 SigG geschützt wurde. Die Gültigkeit der Signatur für den Vorsteuerabzug nach § 15 UStG [RL 2006/112 EG] beim Urteil a) [„Signatur gültig“] bleibt trotz des Ablaufs der Gültigkeit der angegebenen Algorithmen unter Nr.1 oder Nr. 2 uneingeschränkt bestehen (vgl. BMF- Rundschreiben IV B 7 - S 7280- 19/04 Rdn.70.)“*

<sup>14</sup> Zur Erfüllung der Forderungen der BNetzA aus FAQ Nr. 28.

<sup>15</sup> Eine geeignete Maßnahme ist die Übersignatur oder ein Archivsystem mit Archivzeitstempelfunktion, z.B. Hash-Safe.

- zu b)
1. Zeitraum der Sicherheitseignung des verwendeten Hash-Algorithmus
  2. Zeitraum der Sicherheitseignung des Verschlüsselungs-Algorithmus
  3. (nur) wenn der **Signaturzeitpunkt** nach dem Ablaufdatum der Sicherheitseignung eines verwendeten Verschlüsselungs-Algorithmus oder Hash-Algorithmus liegt, der Warnhinweis:

*„Die Signatur wurde mit unsicheren Algorithmen erzeugt. Ein Beweisprivileg nach § 371a ZPO für die beurteilte Signatur besteht nicht. Ein Vorsteuerabzug nach § 15 UStG [RL 2006/112 EG] ist nicht zulässig.“*

- zu c)
1. Zeitraum der Sicherheitseignung des verwendeten Hash-Algorithmus
  2. Zeitraum der Sicherheitseignung des Verschlüsselungs-Algorithmus oder Alternativ wenn ein Algorithmus verwendet wurde der von der SAK nicht unterstützt<sup>16</sup> wird der Warnhinweis:

*„Die überprüfte Signatur basiert auf mindestens einem Verschlüsselungs-Algorithmus der nicht durch diese Prüfsoftware verarbeitet werden kann. Bitte wenden Sie sich an den Aussteller der Signatur um zu erfahren mit welcher Software eine Prüfung erfolgen kann oder wenden Sie sich an den Hersteller.“*

### 3. 3. 2 Vertrauensanker

Der Hersteller weist bezüglich der Gesamtaussage des Verifikationsergebnisses: „Signatur gültig“ und „Status unbekannt“ (wie unter 3.3.1 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" (trust anchor) 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:

<sup>16</sup> Nicht unterstützt werden per 2009 DSA-Varianten, basierend auf elliptischen Kurven. Insbesondere die Verfahren: EC-DAS; EC-KDSA; EC-GDSA; Nyberg-Rueppel-Signaturen. Weitere Informationen zu diesen Algorithmen im BNetzA- Algorithmen-Katalog 2009, Seite 4 Pkt. 3.

**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/Zwischenzertifikate)
- 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 OS|ECM Signaturmodul Version 6.0 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.

**3. 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 Signaturprüfung<sup>17</sup>
- Im Rahmen der Verifikation genutztes Gültigkeitsmodell
- Gesamtergebnis der Signaturprüfung

**Details zur Datei:**

- Dateiname
- Dateigröße
- Aktuell berechneter Hashwert der Datei (Dokument)
- Verwendeter Hash-Algorithmus

<sup>17</sup> Der Verifikationszeitpunkt der für das Protokoll ausgegeben wird gibt in der Regel die Systemzeit des Rechners wieder auf dem OS|ECM Signaturmodul Version 6.0 installiert wurde. Die Zeitangabe ist nur in Verbindung mit einem Zeitstempel gemäß § 2 Nr. 14 SigG verlässlich.

- Ermittelter Zeitpunkt der Signaturerstellung<sup>18</sup>
- 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:
- Zeitraum der Sicherheitseignung des verwendeten Hash-Algorithmus
- Zeitraum der Sicherheitseignung des verwendeten RSA-Algorithmus

**Aus den Zertifikatserweiterungen (Extensions):**

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

**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)

<sup>18</sup> Wie Fußnote 3 ober bei Adobe PDF 1.4 bis 1.6 konformen PKCS#7 Zeitstempel, ein Verweis auf die Zertifikatsinformationen des Zeitstempels der wie eine Signaturprüfung unter Pkt. 2.3.3 dargestellt wird, jedoch unter weiterer Angabe der aus dem Zeitstempel ermittelten Zeit.

- Public Key Algorithmus: (Signaturalgorithmus)
- Schlüssellänge des Public Key:
- Attribute: (Beschränkungen/ Attributsangaben)
- id-ismtt-at-restriction:
- Zeitraum der Sicherheitseignung des verwendeten Hash-Algorithmus
- Zeitraum der Sicherheitseignung des verwendeten RSA-Algorithmus

**Aus den Zertifikatserweiterungen (Extensions):**

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

**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:
- Zeitraum der Sicherheitseignung des verwendeten Hash-Algorithmus
- Zeitraum der Sicherheitseignung des verwendeten RSA-Algorithmus
- Attributsverweise:

**Aus den Zertifikatserweiterungen (Extensions):**

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

- alternative Widerrufsquelle:

**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: (Signaturprüfchlüssel)
- Public Key Algorithmus: (Signaturalgorithmus)
- Schlüssellänge des Public Key:
- Zeitraum der Sicherheitseignung des verwendeten Hash-Algorithmus
- Zeitraum der Sicherheitseignung des verwendeten RSA-Algorithmus

**Aus den Zertifikatserweiterungen (Extensions):**

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

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

**3.4 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 passwortgeschützten Benutzeraccount der geschlossenen Benutzergruppe bei [www.signaturportal.de](http://www.signaturportal.de) mittels eines Web-Service zugegriffen. OS|ECM Signaturmodul Version 6.0 errechnet den Hashwert des Dokumentes<sup>19</sup>, der über den geschützten Benutzeraccount an den ZDA

<sup>19</sup> Derzeit kann SHA 256 bis SHA 512 erzeugt u. übermittelt werden.

übertragen wird. Der empfangene Zeitstempel wird entweder als externe Zeitstempeldatei abgelegt oder in das Dokument eingebettet (nur für PDF-Dokumente verfügbar).

Der OS|ECM Signaturmodul Version 6.0 kann zur Anforderung qualifizierter Zeitstempel der folgenden Zertifizierungsdiensteanbieter verwendet werden:

- a) **AuthentiDate International AG<sup>20</sup>**  
Großenbaumer Weg 6  
40472 Düsseldorf
- b) **Deutsche Post Com GmbH<sup>21</sup>**  
Geschäftsfeld Signtrust  
Tulpenfeld 9  
53113 Bonn
- c) **D-TRUST GmbH<sup>22</sup>**  
Kommandantenstr. 15  
10969 Berlin

#### 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 OS|ECM Signaturmodul Version 6.0 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 beschrieben. Zusätzlich kann über ein Voreinstellung konfiguriert werden, dass mittels des secure Viewer das Signaturobjekt angezeigt wird und damit feststellbar ist, auf welche Daten sich die Signatur bezieht, wie in Kap. 3.1 und 3.2 beschrieben.

<sup>20</sup> Gütezeichen RegTP Nr. Z0015, erteilt am 9. November 2001.

<sup>21</sup> Gütezeichen RegTP Nr. Z0002, erteilt am 17. September 2004.

<sup>22</sup> Gütezeichen RegTP Nr. Z0017, erteilt am 8. März 2002, zusätzlich auch angezeigtes ZDA.

**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 OS|ECM Signaturmodul Version 6.0 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

OS|ECM Signaturmodul Version 6.0 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. OS|ECM Signaturmodul Version 6.0 unterlässt ein Speichern der PIN.

OS|ECM Signaturmodul Version 6.0 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.

**4.1.3 Erfüllte Anforderungen § 17 Abs. 2 Satz 2 SigG**

**Zitat § 17 Abs. 2 Satz 2 SigG**

„Für die Überprüfung signierter Daten sind Signaturanwendungskomponenten erforderlich, die feststellen lassen,

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 2 geführt hat.“

Der OS|ECM Signaturmodul Version 6.0 erfüllt die Anforderungen an Produkte für qualifizierte elektronische Signaturen nach § 17 Abs. 2 Satz 2 SigG in dem er für die Überprüfung signierter Daten eine Feststellung zulässt:

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

Der OS|ECM Signaturmodul Version 6.0 erfüllt die Anforderungen an Produkte für qualifizierte elektronische Signaturen nach § 17 Abs. 2 Satz 2 SigG wie deklariert indem: zu1) der Hashwert der Bestandteil der Signatur ist, mit dem Hashwert des Prüfobjekts verglichen wird; zu 2) die mathematische Integrität des Hashwertes des Prüfobjektes, mit dem Hashwert der der Signatur zugrunde lag verglichen wird; und zu 3) indem aus dem Zertifikat, das der Signatur zugrunde lag, im Feld „Subject“ der „Distinguished Name“(DN) des qualifizierten Zertifikats, sonstige Zertifikatsattribute und der „subject Key Identifier“ ermittelt wird. Mit diesen Informationen kann gegenüber dem, die SSEE ausgebendem ZDA, eine Identifizierung ermöglicht werden, soweit nicht bereits durch den „DN“ eindeutig erfolgt. Die Daten werden nach der Extraktion, nur angezeigt wenn ein Integritätsprüfung auf Zertifikatsebene eine „substitution attack“ ausgeschlossen hat. Die weiteren Ergebnisse und Anzeigen der Auswertung der Zertifikate, Attributzertifikate sowie Sperr- und Gültigkeitsprüfungen werden im Einzelnen unter Kap. 3.3.1 beschrieben.

**4.1.4 Erfüllte Anforderungen § 15 Abs. 2 Nr. 2 SigV**

**Zitat § 15 Abs. 2 Nr. 2 SigV**

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

Der OS|ECM Signaturmodul Version 6.0 ist auch eine Teil- Signaturanwendungskomponente nach § 15 Abs. 2 Nr. 2 SigV und gewährleistet, dass bei der Prüfung einer qualifizierten elektronischen Signatur:

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

Der OS|ECM Signaturmodul Version 6.0 erfüllt die Anforderungen wie deklariert, indem er eine Zertifikatsprüfung durch Anfrage an einen OCSP-Server und /oder eine Sperrlistenabfrage beim zertifikatsausgebenden ZDA wie in Kap. 3.3.1 beschrieben durchführt und dem Nutzer im Rahmen der Zertifikatsauswahl (Kap. 3.1, 3.2) und bei der Ergebnisanzeige für die Verifikation (Kap. 3.3.1) von qualifizierten Signaturen anzeigt.

**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.“

OS|ECM Signaturmodul Version 6.0 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. OS|ECM Signaturmodul Version 6.0 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.

#### 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 OS|ECM Signaturmodul Version 6.0 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>23</sup> vorausgesetzt. Der OS|ECM Signaturmodul Version 6.0 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 OS|ECM Signaturmodul Version 6.0 ist potentiell bedroht durch

- Angriffe über Kommunikationsnetze<sup>24</sup>,
- Angriffe über manuellen Zugriff Unbefugter/Datenaustausch per Datenträger<sup>25</sup> und
- Fehler/Manipulationen bei Installation, Betrieb/Nutzung und Wartung/Reparatur.

Für den sicheren Einsatz von OS|ECM Signaturmodul Version 6.0 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
- Verifikationsergebnisse falsch angezeigt werden

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

<sup>23</sup> Definiertes Einsatzbereich gemäß Nr. 4.2 RegTP Dokument: Einheitliche Spezifizierung der Einsatzbedingungen für Signaturanwendungskomponenten Version 1.4.

<sup>24</sup> Spezifizierte Bedrohung gemäß Fußnote 15 RegTP Dokument: Einheitliche Spezifizierung der Einsatzbedingungen für Signaturanwendungskomponenten Version 1.4.

<sup>25</sup> Spezifizierte Bedrohung gemäß Fußnote 16 RegTP Dokument: Einheitliche Spezifizierung der Einsatzbedingungen für Signaturanwendungskomponenten Version 1.4.

- 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) Zulässige IT- Komponenten und Systeme für den Signaturbetrieb**

Die Teil- Signaturanwendungskomponente OS|ECM Signaturmodul Version 6.0 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).
- OS|ECM Signaturmodul Version 6.0 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.
- OS|ECM Signaturmodul Version 6.0 kann in den Metaframeumgebungen „Microsoft Terminal Services“ ab Windows 2003 Server und „Citrix Presentation Server“ ab Version 4 eingesetzt werden.

**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-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>26</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 OS|ECM Signaturmodul Version 6.0 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 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 Konsolensperre 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-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. Hashsummenvergleich) 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

<sup>26</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)

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 OS|ECM Signaturmodul Version 6.0 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 OS|ECM Signaturmodul Version 6.0 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 OS|ECM Signaturmodul Version 6.0 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 OS|ECM Signaturmodul Version 6.0 erfolgreich getestet. Zu Erzeugung von qualifizierten Signaturen ist die Verwendung der dort angegebenen 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 OS|ECM Signaturmodul Version 6.0 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 OS|ECM Signaturmodul Version 6.0 von der OPTIMAL SYSTEMS Gesellschaft für innovative Computertechnologien mbH 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 1 für OS – Komponenten:**

Ausgestellt für: OPTIMAL SYSTEMS GmbH  
 Ausgestellt: VeriSign Class 3 Code Signing 2004 CA  
 Seriennummer: 733B A6C9 3692 92E0 AF55 35F8 A561 E046

**Zertifikat 2 für Mentana-Claimsoft AG :**

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 3 für Mentana-Claimsoft AG [ab 11/2009]:**

Ausgestellt für: Mentana-Claimsoft AG Gesellschaft für innovative Computertechnologien mbH  
 Ausgestellt von: Commodo UTN-USERFirst-Object  
 Seriennummer: 00b50a7da137c127eafb6a7a067c8cbd91

| Datei           | Version  | Hersteller      | Zertifikat   |
|-----------------|----------|-----------------|--------------|
| Axdigisignm.dll | 6.0/6.10 | OPTIMAL SYSTEMS | Zertifikat 1 |
| Ax.exe          | 6.0/6.10 | OPTIMAL SYSTEMS | Zertifikat 1 |

| Datei                      | Version | Hersteller            | Zertifikat          |
|----------------------------|---------|-----------------------|---------------------|
| Mdocapi.dll                | 1.5     | Mentana- Claimsoft AG | Zertifikat 2 oder 3 |
| Base-CSP (mentcsp.dll)     | 1.1     | Mentana- Claimsoft AG | Zertifikat 2 oder 3 |
| Algo-CSP (mentalgocsp.dll) | 1.1     | Mentana- Claimsoft AG | Zertifikat 2 oder 3 |
| mentmdcardos43b.dll        | 1.1     | Mentana- Claimsoft AG | Zertifikat 2 oder 3 |
| mentmdtcos20.dll           | 1.1     | Mentana- Claimsoft AG | Zertifikat 2 oder 3 |
| mentmdtcos30.dll           | 1.1     | Mentana- Claimsoft AG | Zertifikat 2 oder 3 |
| mentmdseccos.dll           | 1.1     | Mentana- Claimsoft AG | Zertifikat 2 oder 3 |
| mentmdsetcos.dll           | 1.1     | Mentana- Claimsoft AG | Zertifikat 2 oder 3 |
| mentmdstarcos30.dll        | 1.1     | Mentana- Claimsoft AG | Zertifikat 2 oder 3 |
| mentmdmcrd21.dll           | 1.1     | Mentana- Claimsoft AG | Zertifikat 2 oder 3 |
| mentmdcardos401a.dll       | 1.1     | Mentana- Claimsoft AG | Zertifikat 2 oder 3 |
| mdocapi.dll                | 2.2     | Mentana- Claimsoft AG | Zertifikat 2 oder 3 |
| MdocExtWx.dll              | 2.2     | Mentana- Claimsoft AG | Zertifikat 2 oder 3 |
| MdocTSAClient.dll          | 2.2     | Mentana- Claimsoft AG | Zertifikat 2 oder 3 |
| mdocapissl.dll             | 2.2     | Mentana- Claimsoft AG | Zertifikat 2 oder 3 |
| mdocpdf.dll                | 2.2     | Mentana- Claimsoft AG | Zertifikat 2 oder 3 |
| mdoccrypto.dll             | 2.2     | Mentana- Claimsoft AG | Zertifikat 2 oder 3 |
| mdoccryptossl.dll          | 2.2     | Mentana- Claimsoft AG | Zertifikat 2 oder 3 |
| libeay32.dll               | 2.2     | Mentana- Claimsoft AG | Zertifikat 2 oder 3 |

|                    |     |                       |                     |
|--------------------|-----|-----------------------|---------------------|
| ssleay32.dll       | 2.2 | Mentana- Claimsoft AG | Zertifikat 2 oder 3 |
| pkcs15init.dll     | 2.2 | Mentana- Claimsoft AG | Zertifikat 2 oder 3 |
| opencsc-pkcs11.dll | 2.2 | Mentana- Claimsoft AG | Zertifikat 2 oder 3 |
| opencsc.dll        | 2.2 | Mentana- Claimsoft AG | Zertifikat 2 oder 3 |
| engine_pkcs11.dll  | 2.2 | Mentana- Claimsoft AG | Zertifikat 2 oder 3 |
| opencsc-pkcs11.dll | 2.2 | Mentana- Claimsoft AG | Zertifikat 2 oder 3 |

**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 Bedienungsfläche (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 OS|ECM Signaturmodul Version 6.0 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 OPTIMAL SYSTEMS Gesellschaft für innovative Computertechnologien mbH umgehend aktualisierte Versionen der Programmkomponenten zur Verfügung. Die Anwender des Programms werden über die Webseite der OPTIMAL SYSTEMS Gesellschaft für innovative Computertechnologien mbH ([www.os.de](http://www.os.de)) über das Auftreten einer solchen Situation informiert. Mit dem Inverkehrbringen einer neuen Softwareversion des OS|ECM Signaturmodul Version 6.0 hinterlegt die OPTIMAL SYSTEMS Gesellschaft für innovative Computertechnologien mbH umgehend einen Nachtrag zu dieser Herstellereklärung bei der Bundesnetzagentur.

## 6. Algorithmen und zugehörige Parameter

Das Produkt OS|ECM Signaturmodul Version 6.0 verwendet zur Erstellung und Prüfung 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 wird empfohlen nur noch den RSA Algorithmus mit der Schlüssellänge von 2048-Bit zu nutzen. 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). Weiterhin kann OS|ECM Signaturmodul Version 6.0 zu Prüfungszwecken im Rahmen der Verifikation die RSA Algorithmen mit der Schlüssellänge 2048-Bit und der Zwischenstufen (1280 Bit; 1536 Bit, ab dem Ende des Jahres 2010 nur noch die Zwischenstufen 1728 Bit und 1976 Bit) sowie DAS nach ISO/IEC 14888-3 und NIST: FIPS Publication 186-2: Digital Signature Standard (DSS), Januar 2000 und Change Notice 1, Oktober 2001 verarbeiten. Zu Prüfzwecken ist Hashfunktion SHA-224 nur noch bis Ende 2015 für die Anwendung bei qualifizierten elektronischen Signaturen geeignet. Für die Verifikation 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. OS|ECM Signaturmodul Version 6.0 meldet dem Nutzer einen Warnhinweis wenn die Verifikation wegen eines nicht unterstützten Algorithmus nicht erfolgreich abgeschlossen werden kann (vgl. Pkt. 3.3.1 zu c) und Fußnote 14 und 16).

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 OPTIMAL SYSTEMS Gesellschaft für innovative Computertechnologien mbH 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 OS Client incl. OS|ECM Signaturmodul Version 6.0, 190 Seiten.
2. Sicherheitstechnische Produktvorgaben OS|ECM Signaturmodul Version 6.0, Stand 01.12. 2009, 30 Seiten.
3. Spezifikation der Test- und Entwicklungsumgebung für OS|ECM - Signaturmodul Version 6.0, Stand 01.12.2009, 15 Seiten.

Dieses Dokument umfasst 32 Seiten.

Ende der Herstellererklärung.