Herstellererklärung

Die

OpenLimit SignCubes GmbH

Saarbrücker Str. 38A

D – 10405 Berlin

erklärt hiermit gemäß § 17 Abs. 4 Satz 2 SigG[1]
in Verbindung mit § 15 Abs. 5 Satz 1 SigV[2],
dass die

OpenLimit SignCubes Basiskomponenten Version 2.10

als
Signaturanwendungskomponente
zur Erzeugung und Verifikation qualifizierter Signaturen
und zur Einholung qualifizierter Zeitstempel

die nachstehend genannten Anforderungen an das
Signaturgesetz[1] bzw. die Signaturverordnung[2] erfüllt.

gez. Maik Pogoda
Geschäftsführer
OpenLimit SignCubes GmbH

gez. Dr. Stephan Lachmann
Prokurist
OpenLimit SignCubes GmbH

Berlin, den 29.04.2016

Diese Herstellererklärung in Version 1.0 mit der Dokumentennummer *he_ol-v2-client_2.10_v1.0* besteht aus 44 Seiten.

[1] Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz – SigG) vom 16. Mai 2001 (BGBI. I S. 876), zuletzt geändert durch Artikel 4 des Gesetzes vom 17. Juli 2009 (BGBl. I S.2091)

[2] Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) vom 16. November 2001 (BGBI. I Seite 3074), zuletzt geändert durch die Verordnung vom 15. November 2010 (BGBl. I S.1542)

Dokumentenhistorie

Version	Datum	Autor	Bemerkung
1.0	29.04.2016	S. Dörpinghaus	Finale Version für v.2.10

Inhaltsverzeichnis

1 Handelsbezeichnung 5

2 Lieferumfang und Versionsinformationen 5

3 Funktionsbeschreibung 14

3.1 Allgemein 14

3.2 Unterstützung der Signaturerzeugung 15

3.3 Sichere Anzeige von Dokumenten 21

3.4 Anwendung von Zeitstempeln 22

3.5 Signaturverifikation 23

3.5.1 Prüfung digital signierter Objekte 23

3.5.2 Verarbeitbare Dokument- und Signaturformate 29

3.5.3 Erwarteter Aufbau von CMS-Objekten 29

3.5.4 Konformität von PDF-Dokumenten / PDF-Signaturen 30

3.5.5 Verarbeitung eingebetteter Zeitstempel und OCSP-Antworten 31

3.6 *Online Certificate Status Protocol* (OCSP) Anfrage gemäß RFC 2560 32

3.7 Sperrliste (CRL) gemäß RFC 3280 32

3.8 Vertrauenslisten 32

3.9 Zeitstempel gemäß RFC 3161 33

3.10 Unterstützte Algorithmen und Signaturverfahren 33

3.11 Kombination Hash- und Signaturalgorithmus 34

3.12 Sicherheitsbewertung von Algorithmen 35

3.13 Sicherung der Integrität 35

4 Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung 36

5 Maßnahmen in der Einsatzumgebung 40

5.1 Einrichtung der IT-Komponenten 40

5.2 Anbindung an ein Netzwerk 41

5.3 Auslieferung und Installation 41

5.4 Auflagen für den Betrieb des Produktes 42

6 Algorithmen und zugehörige Parameter 42

7 Gültigkeit der Herstellererklärung 43

8 Zusatzdokumente 43

1 Handelsbezeichnung

Die Handelsbezeichnung lautet: OpenLimit CC Sign 2.10

Hersteller: OpenLimit SignCubes GmbH
Saarbrücker Str. 38 A
D - 10405 Berlin

Auslieferung: Das Produkt *OpenLimit CC Sign 2.10* wird direkt vom Hersteller bzw. einem seiner Vertriebspartner online per Download und auf CD ausgeliefert. Die CDs werden entweder per Post versendet oder persönlich übergeben.

Handelsregisterauszug: HRB 86352 B

2 Lieferumfang und Versionsinformationen

Nachfolgend ist der Lieferumfang, einschließlich der Versionsinformationen, aufgelistet:

Produktart	**Bezeichnung**	**Version**	**Datum**	**Übergabe-form**
Installations-programm für das Produkt *OpenLimit CC Sign 2.10*	"*OL2101CCSign.exe*", " *OL2101CCSignEE.exe*" oder "*OL2101Reader.exe*" (abhängig von der gewünschten Lizenz)	2.10	14.04.2016	Download und auf CD
Installations-anleitung, *OpenLimit CC Sign 2.10* (deutsch)	*OpenLimit_CCSign_Getting_Started_2.10.pdf*	1.0	22.04.2016	Download und auf CD
Installations-anleitung, *OpenLimit CC Sign 2.10* (englisch)	*OpenLimit_CCSign_Getting_Started_2.10_EN.pdf*	1.0	22.04.2016	Download und auf CD

Tabelle 1: Lieferumfang und Versionsinformationen

In dem Installationspaket sind die folgenden Dokumentationen enthalten:

Bezeichnung	**Dateiname**	**Datum**	**Version**
Online Help (deutsch)	deuOPENLiMiT SignCubes.chm	22.04.2016	1.0

Bezeichnung	Dateiname	Datum	Version
Online Help (englisch)	engOPENLiMiT SignCubes.chm	22.04.2016	1.0

Tabelle 2: Übersicht über die mitgelieferten Handbücher

Die Herstellererklärung für die *OpenLimit SignCubes Basiskomponenten Version 2.10* erfolgt als Erweiterung des Nachtrags Nr. 4 zur Sicherheitsbestätigung BSI.02110.TE.12.2008 für die OPENLiMiT SignCubes base components 2.5, Version 2.5.0.4.

Gegenüber der Version 2.5.0.4 des Produkts wurde in der nun herstellererklärten Version 2.10 die Menge der zu unterstützenden Sicheren Signaturerstellungseinheiten (SSEE) gemäß

Bezeichnung	Registriernummer der Bestätigungs-ID
STARCOS 3.4 Health QES C2 (Einzel-, M100- und Massensignaturkarte; Handelsnamen: *D-TRUST Card V3.0, DATEV Card V3.0, Signaturkarte der Bundesagentur für Arbeit (BA))*	BSI.02120.TE.05.2009 Nachtrag vom 15.11.2010
STARCOS 3.5 ID ECC C1 (Einzelsignaturkarte)	SRC.00013.TE.10.2012
STARCOS 3.5 ID ECC C1R (Einzel-, M100- und Massensignaturkarte; Handelsnamen: *Signtrust Card 3.5, Signtrust MCard 3.5, Signtrust MCard100 3.5, DGN sprintCard, sprintCard, DGN businessCard, businessCard, elektronischer Arztausweis, eA, eArztausweis, eHBA für Ärzte, elektronischer Zahnarztausweis, eZAA, eZahnarztausweis, eHBA für Zahnärzte, elektronischer Psychotherapeutenausweis, ePTA, eHBA für Psychotherapeuten, eHBA für psychologische Psychotherapeuten und Kinder- und Jugendlichenpsychotherapeuten, medisign Card, medisignCard, ZOD-Signaturkarte für Zahnärzte, ZOD-Karte, ZOD-Card, Bundesnotarkammer - Stapelsignaturkarte 100, Bundesnotarkammer – Multisignaturkarte*)	SRC.00021.TE.05.2013 Korrigendum 1 vom 14.11.2013 Nachtrag 1 vom 23.09.2013
STARCOS 3.5 ID GCC C1 (Einzelsignaturkarte; Handelsnamen: *nPA-Signaturkarte*)	SRC.00008.TE.12.2010
STARCOS 3.5 ID GCC C1R (Einzelsignaturkarte; Handelsnamen: *nPA-Signaturkarte*)	SRC.00014.TE.02.2012

Bezeichnung	Registriernummer der Bestätigungs-ID
STARCOS 3.5 ID GCC C2 (Einzelsignaturkarte; Handelsnamen: *nPA-Signaturkarte*)	SRC.00012.TE.05.2013
TCOS Identity Card Version 1.0 Release 1/SLE78CLX1440P (Einzelsignaturkarte; Handelsnamen: *nPA-Signaturkarte*)	SRC.00006.TE.11.2010
TCOS 3.0 Signature Card, Version 1.1 (Einzel- und Massensignaturkarte)	TUVIT.93146.TE.12.2006 Nachtrag 1 vom 07.05.2010
TCOS 3.0 Signature Card, Version 2.0 Release 1/ SLE78CLX1440P (Einzel- und Massensignaturkarte)	SRC.00016.TE.11.2012
ZKA Banking Signature Card, Version 7.1.2 (Einzelsignaturkarte)	TUVIT.93166.TU.06.2008 Nachtrag 1 vom 15.09.2009 Nachtrag 2 vom 28.12.2010
ZKA Banking Signature Card, Version 7.1.3 (Einzelsignaturkarte)	TUVIT.93171.TU.06.2010
ZKA Banking Signature Card, Version 7.1.4 (Einzelsignaturkarte)	TUVIT.93181.TU.09.2010 Nachtrag 1 vom 28.12.2010
ZKA Banking Signature Card, Version 7.2.1 (Einzelsignaturkarte)	TUVIT.93174.TU.06.2010 Nachtrag 1 vom 28.12.2010
ZKA Banking Signature Card, Version 7.2.2 (Einzelsignaturkarte)	TUVIT.93172.TU.06.2010
ZKA Banking Signature Card, Version 7.2.3 (Einzelsignaturkarte)	TUVIT.93182.TU.09.2010
ZKA SECCOS Sig v2.6.4 R1.1.2 (Einzelsignaturkarte)	SRC.00009.TE.09.2010
ZKA-Signaturkarte, Version 6.21 (Einzelsignaturkarte)	TUVIT.93174.TU.06.2010
ZKA-Signaturkarte, Version 6.22 (Einzelsignaturkarte)	TUVIT.93183.TU.11.2010
ZKA-Signaturkarte, Version 6.30 (Einzelsignaturkarte)	TUVIT.93170.TU.07.2010 Nachtrag 1 vom 22.07.2010
ZKA-Signaturkarte, Version 6.31 (Einzelsignaturkarte)	TUVIT.93175.TU.08.2010
ZKA-Signaturkarte, Version 6.32 (Einzelsignaturkarte)	TUVIT.93184.TU.11.2010
ZKA-Signaturkarte, Version 6.32 M (Massensignaturkarte)	TUVIT.93176.TU.05.2011

Tabelle 3 erweitert. Zudem ist gemäß

Bezeichnung	**Registriernummer der Bestätigungs-ID**
STARCOS 3.4 Health QES C2 (Einzel-, M100- und Massensignaturkarte; Handelsnamen: *D-TRUST Card V3.0, DATEV Card V3.0, Signaturkarte der Bundesagentur für Arbeit (BA))*	BSI.02120.TE.05.2009 Nachtrag vom 15.11.2010
STARCOS 3.5 ID ECC C1 (Einzelsignaturkarte)	SRC.00013.TE.10.2012
STARCOS 3.5 ID ECC C1R (Einzel-, M100- und Massensignaturkarte; Handelsnamen: *Signtrust Card 3.5, Signtrust MCard 3.5, Signtrust MCard100 3.5, DGN sprintCard, sprintCard, DGN businessCard, businessCard, elektronischer Arztausweis, eA, eArztausweis, eHBA für Ärzte, elektronischer Zahnarztausweis, eZAA, eZahnarztausweis, eHBA für Zahnärzte, elektronischer Psychotherapeutenausweis, ePTA, eHBA für Psychotherapeuten, eHBA für psychologische Psychotherapeuten und Kinder- und Jugendlichenpsychotherapeuten, medisign Card, medisignCard, ZOD-Signaturkarte für Zahnärzte, ZOD-Karte, ZOD-Card, Bundesnotarkammer - Stapelsignaturkarte 100, Bundesnotarkammer – Multisignaturkarte*)	SRC.00021.TE.05.2013 Korrigendum 1 vom 14.11.2013 Nachtrag 1 vom 23.09.2013
STARCOS 3.5 ID GCC C1 (Einzelsignaturkarte; Handelsnamen: *nPA-Signaturkarte*)	SRC.00008.TE.12.2010
STARCOS 3.5 ID GCC C1R (Einzelsignaturkarte; Handelsnamen: *nPA-Signaturkarte*)	SRC.00014.TE.02.2012
STARCOS 3.5 ID GCC C2 (Einzelsignaturkarte; Handelsnamen: *nPA-Signaturkarte*)	SRC.00012.TE.05.2013
TCOS Identity Card Version 1.0 Release 1/SLE78CLX1440P (Einzelsignaturkarte; Handelsnamen: *nPA-Signaturkarte*)	SRC.00006.TE.11.2010
TCOS 3.0 Signature Card, Version 1.1 (Einzel- und Massensignaturkarte)	TUVIT.93146.TE.12.2006 Nachtrag 1 vom 07.05.2010
TCOS 3.0 Signature Card, Version 2.0 Release 1/ SLE78CLX1440P (Einzel- und Massensignaturkarte)	SRC.00016.TE.11.2012

Bezeichnung	Registriernummer der Bestätigungs-ID
ZKA Banking Signature Card, Version 7.1.2 (Einzelsignaturkarte)	TUVIT.93166.TU.06.2008 Nachtrag 1 vom 15.09.2009 Nachtrag 2 vom 28.12.2010
ZKA Banking Signature Card, Version 7.1.3 (Einzelsignaturkarte)	TUVIT.93171.TU.06.2010
ZKA Banking Signature Card, Version 7.1.4 (Einzelsignaturkarte)	TUVIT.93181.TU.09.2010 Nachtrag 1 vom 28.12.2010
ZKA Banking Signature Card, Version 7.2.1 (Einzelsignaturkarte)	TUVIT.93174.TU.06.2010 Nachtrag 1 vom 28.12.2010
ZKA Banking Signature Card, Version 7.2.2 (Einzelsignaturkarte)	TUVIT.93172.TU.06.2010
ZKA Banking Signature Card, Version 7.2.3 (Einzelsignaturkarte)	TUVIT.93182.TU.09.2010
ZKA SECCOS Sig v2.6.4 R1.1.2 (Einzelsignaturkarte)	SRC.00009.TE.09.2010
ZKA-Signaturkarte, Version 6.21 (Einzelsignaturkarte)	TUVIT.93174.TU.06.2010
ZKA-Signaturkarte, Version 6.22 (Einzelsignaturkarte)	TUVIT.93183.TU.11.2010
ZKA-Signaturkarte, Version 6.30 (Einzelsignaturkarte)	TUVIT.93170.TU.07.2010 Nachtrag 1 vom 22.07.2010
ZKA-Signaturkarte, Version 6.31 (Einzelsignaturkarte)	TUVIT.93175.TU.08.2010
ZKA-Signaturkarte, Version 6.32 (Einzelsignaturkarte)	TUVIT.93184.TU.11.2010
ZKA-Signaturkarte, Version 6.32 M (Massensignaturkarte)	TUVIT.93176.TU.05.2011

Tabelle 3 und

Cherry KC 1000SC, JK-A01, FW-Version: 2.0.0, HW-Version: 1.0	BSI-DSZ-CC-0970

Tabelle 4 die Unterstützung für einige SSEE und Kartenleser entfallen.

Das Produkt *OpenLimit SignCubes Basiskomponenten Version 2.10* nutzt als Drittkomponenten die folgenden, nach SigG bestätigten Sicheren Signaturerstellungseinheiten (kurz: „SSEE“), für die eine Bestätigung wie angegeben vorliegt:

Bezeichnung	Registriernummer der Bestätigungs-ID

Bezeichnung	**Registriernummer der Bestätigungs-ID**
STARCOS 3.4 Health QES C2 (Einzel-, M100- und Massensignaturkarte; Handelsnamen: *D-TRUST Card V3.0*, *DATEV Card V3.*0, *Signaturkarte der Bundesagentur für Arbeit (BA))*	BSI.02120.TE.05.2009 Nachtrag vom 15.11.2010
STARCOS 3.5 ID ECC C1 (Einzelsignaturkarte)	SRC.00013.TE.10.2012
STARCOS 3.5 ID ECC C1R (Einzel-, M100- und Massensignaturkarte; Handelsnamen: *Signtrust Card 3.5, Signtrust MCard 3.5, Signtrust MCard100 3.5, DGN sprintCard, sprintCard, DGN businessCard, businessCard, elektronischer Arztausweis, eA, eArztausweis, eHBA für Ärzte, elektronischer Zahnarztausweis, eZAA, eZahnarztausweis, eHBA für Zahnärzte, elektronischer Psychotherapeutenausweis, ePTA, eHBA für Psychotherapeuten, eHBA für psychologische Psychotherapeuten und Kinder- und Jugendlichenpsychotherapeuten, medisign Card, medisignCard, ZOD-Signaturkarte für Zahnärzte, ZOD-Karte, ZOD-Card, Bundesnotarkammer - Stapelsignaturkarte 100, Bundesnotarkammer – Multisignaturkarte*)	SRC.00021.TE.05.2013 Korrigendum 1 vom 14.11.2013 Nachtrag 1 vom 23.09.2013
STARCOS 3.5 ID GCC C1 (Einzelsignaturkarte; Handelsnamen: *nPA-Signaturkarte*)	SRC.00008.TE.12.2010
STARCOS 3.5 ID GCC C1R (Einzelsignaturkarte; Handelsnamen: *nPA-Signaturkarte*)	SRC.00014.TE.02.2012
STARCOS 3.5 ID GCC C2 (Einzelsignaturkarte; Handelsnamen: *nPA-Signaturkarte*)	SRC.00012.TE.05.2013
TCOS Identity Card Version 1.0 Release 1/SLE78CLX1440P (Einzelsignaturkarte; Handelsnamen: *nPA-Signaturkarte*)	SRC.00006.TE.11.2010
TCOS 3.0 Signature Card, Version 1.1 (Einzel- und Massensignaturkarte)	TUVIT.93146.TE.12.2006 Nachtrag 1 vom 07.05.2010
TCOS 3.0 Signature Card, Version 2.0 Release 1/ SLE78CLX1440P (Einzel- und Massensignaturkarte)	SRC.00016.TE.11.2012

Bezeichnung	Registriernummer der Bestätigungs-ID
ZKA Banking Signature Card, Version 7.1.2 (Einzelsignaturkarte)	TUVIT.93166.TU.06.2008 Nachtrag 1 vom 15.09.2009 Nachtrag 2 vom 28.12.2010
ZKA Banking Signature Card, Version 7.1.3 (Einzelsignaturkarte)	TUVIT.93171.TU.06.2010
ZKA Banking Signature Card, Version 7.1.4 (Einzelsignaturkarte)	TUVIT.93181.TU.09.2010 Nachtrag 1 vom 28.12.2010
ZKA Banking Signature Card, Version 7.2.1 (Einzelsignaturkarte)	TUVIT.93174.TU.06.2010 Nachtrag 1 vom 28.12.2010
ZKA Banking Signature Card, Version 7.2.2 (Einzelsignaturkarte)	TUVIT.93172.TU.06.2010
ZKA Banking Signature Card, Version 7.2.3 (Einzelsignaturkarte)	TUVIT.93182.TU.09.2010
ZKA SECCOS Sig v2.6.4 R1.1.2 (Einzelsignaturkarte)	SRC.00009.TE.09.2010
ZKA-Signaturkarte, Version 6.21 (Einzelsignaturkarte)	TUVIT.93174.TU.06.2010
ZKA-Signaturkarte, Version 6.22 (Einzelsignaturkarte)	TUVIT.93183.TU.11.2010
ZKA-Signaturkarte, Version 6.30 (Einzelsignaturkarte)	TUVIT.93170.TU.07.2010 Nachtrag 1 vom 22.07.2010
ZKA-Signaturkarte, Version 6.31 (Einzelsignaturkarte)	TUVIT.93175.TU.08.2010
ZKA-Signaturkarte, Version 6.32 (Einzelsignaturkarte)	TUVIT.93184.TU.11.2010
ZKA-Signaturkarte, Version 6.32 M (Massensignaturkarte)	TUVIT.93176.TU.05.2011

Tabelle 3: Zusätzliche Produkte (SSEE), nach SigG bestätigt

Weiterhin kommen die in der folgenden

Cherry KC 1000SC, JK-A01, FW-Version: 2.0.0, HW-Version: 1.0	BSI-DSZ-CC-0970

Tabelle 4 aufgelisteten und nach SigG bzw. SigV bestätigten (resp. herstellererklärten) Kartenleser mit sicherer PIN-Eingabe als Drittkomponenten zum Einsatz:

Bezeichnung	Registriernummer der Bestätigung
Cherry SmartBoard xx44, Firmware-Version 1.04	BSI.02048.TE.12.2004
Cherry SmartTerminal ST-2xxx, Firmware Version 6.01 (ST-2000UCZ)	BSI.02124.TE.09.2010
Cherry SmartTerminal ST-2xxx, Firmware Version 6.01 (ST-2052UCZ)	BSI.02124.TE.09.2010
Fujitsu SmartCase KB SCR eSIG (S26381-K529-Vxxx), Hardware Version HOS:01, Firmware-Version 1.21	BSI.02107.TE.03.2010, Nachtrag
Fujitsu SmartCase KB SCR2 eSIG (S26381-K539-Lxxx), Hardware Version HOS:01, Firmware-Version 1.06	Herstellererklärung
Kobil KAAN Advanced, Firmware Version 1.19, Hardware Version K104R3	T-Systems.02207.TU.04.2008, Nachtrag
Reiner SCT cyberJack e-com, Version 3.0	TUVIT.93155.TE.09.2008
Reiner SCT cyberJack e-com plus, Version 3.0	TUVIT.93156.TE.09.2008
Reiner SCT cyberJack secoder, Version 3.0	TUVIT.93154.TE.09.2008
Reiner SCT cyberJack RFID standard, Version 1.2	TUVIT.93188.TU.07.2011
Reiner SCT cyberJack RFID komfort, Version 2.0	TUVIT.93180.TU.12.2011
SCM SPR332, Firmware Version 6.01	BSI.02117.TE.02.2010
Cherry KC 1000SC, JK-A01, FW-Version: 2.0.0, HW-Version: 1.0 [1]	BSI-DSZ-CC-0970

Tabelle 4: Zusätzliche Produkte (Kartenleser), nach SigG bestätigt

Das Produkt *OpenLimit CC Sign Version 2.10* ist für den Einsatz unter den Betriebssystemen

- Windows 7 32 Bit und 64 Bit
- Windows 8.1 32 Bit und 64 Bit
- Windows 10 32 Bit und 64 Bit
- Windows 2008 R2 Terminal Server
- Windows 2012 R2 Terminal Server

[1] Die vorliegende Erklärung gilt lediglich nach Abschluss des Zertifizierungsverfahrens BSI-DSZ-CC-0970.

freigegeben. Für den Einsatz auf anderen Betriebssystemen gilt diese Herstellerklärung nicht.

3 Funktionsbeschreibung

3.1 Allgemein

Die *OpenLimit SignCubes Basiskomponenten Version 2.10* sind eine Signaturanwendungskomponente, die gemäß § 2 Nr.11 und Nr. 14 SigG geeignet ist,

- Daten dem Prozess der Erzeugung oder Prüfung qualifizierter elektronischer Signaturen zuzuführen,
- qualifizierte elektronische Signaturen zu prüfen oder qualifizierte Zertifikate nachzuprüfen und die Ergebnisse anzuzeigen, oder
- qualifizierte Zeitstempel als elektronische Bescheinigungen eines Zertifizierungsdiensteanbieters einzuholen und zu prüfen.

Die *OpenLimit SignCubes Basiskomponenten Version 2.10* enthalten ausführbare Programmbestandteile, aber auch Funktionsbibliotheken, die eine Integration in weitere Anwendungen ermöglichen. Damit können die *OpenLimit SignCubes Basiskomponenten Version 2.10* auf zwei verschiedene Arten eingesetzt werden:

- Das Produkt kann als eigenständige Anwendung vom Benutzer dazu verwendet werden, qualifizierte elektronische Signaturen zu erzeugen.
- Mit Hilfe der Funktionsbibliotheken können die *OpenLimit SignCubes Basiskomponenten Version 2.10* in weitere Anwendungen integriert werden.

Die Integrität der *OpenLimit SignCubes Basiskomponenten Version 2.10* wird über das *OpenLimit SignCubes Integrity Tool* geprüft. Es wird festgestellt, ob sich die Programmbibliotheken noch in dem Zustand befinden, wie sie ursprünglich ausgeliefert und installiert wurden. Das Applet kann über die folgende URL aufgerufen werden: *https://www.openlimit.com/integritytool*.

Das Java-Applet berechnet die SHA-256-Hashwerte und vergleicht sie mit den vom Hersteller stammenden Referenzwerten. Nach erfolgter Prüfung wird ein Prüfbericht erstellt. Weitere Informationen dazu sind in dem Kapitel 3.13 enthalten.

Über die programmtechnisch ansteuerbare Schnittstelle werden den *OpenLimit SignCubes Basiskomponenten Version 2.10* die zu prüfenden Daten übergeben. Das Gesamtergebnis der Signaturprüfung wird an die aufrufende Anwendung in Form eines numerischen Werts ausgegeben.

Der Vorgang der Signaturprüfung erfolgt unter Benutzung von OCSP-Auskünften gemäß RFC 2560 (vgl. Abschnitt 3.6) oder Sperrlisten gemäß RFC 3280 (vgl. Abschnitt 3.7).

Ferner können an die Programmierschnittstelle Daten zwecks Erstellung eines Zeitstempels gemäß RFC 3161 übergeben werden, sodass in Folge dieses Aufrufs vom Produkt an der Programmierschnittstelle der erzeugte Zeitstempel an die aufrufende Anwendung

zurückgeliefert wird. Für die Anwendung von Zeitstempeln ist der Zugang zu einem Zeitstempeldiensteanbieter (*Timestamp Service Provider*, TSP) erforderlich.

Für den Empfang von OCSP-Auskünften, Sperrlisten und Zeitstempeln nutzt das Produkt die Betriebssystem-vermittelte Netzwerkschicht. Beim Import signierter Objekte wird die Quelle der Beschaffung nicht geprüft, da die Sicherheitsleistung des Produkts darin besteht, die Integrität der importierten Daten zu prüfen und somit sicherzustellen, dass keine manipulierten Daten importiert werden. Das Produkt verfolgt hierbei die Sicherheitspolitik ausschließlich signierte Datenobjekte zu importieren, nachdem diese erfolgreich verifiziert werden konnten. Nicht erfolgreich geprüfte signierte Objekte oder unsignierte Objekte werden nicht importiert.

Die *OpenLimit SignCubes Basiskomponenten Version 2.10* sind dazu ausgelegt, Signaturen im CMS-Format (gemäß RFC 5652) bzw. PKCS#7-Format zu prüfen. Dabei werden vorhandene elektronische Signaturen in den folgenden Containerformaten verarbeitet:

- Die Signatur liegt als abgesetzte Signatur zum Originaldokument vor.
- Die Signatur und das Dokument sind in einem zusammenhängenden Datencontainer kodiert.
- Die Signatur ist Teil eines PDF-Dokuments und als eingebettete PDF-Signatur in das Dokument eingebracht.

3.2 Unterstützung der Signaturerzeugung

Die *OpenLimit SignCubes Basiskomponenten Version 2.10* unterstützen die Erstellung fortgeschrittener und qualifizierter elektronischer Signaturen in Abhängigkeit vom für die Signaturerstellung verwendeten Signaturzertifikat. Die Erstellung qualifizierter elektronischer Signaturen unterliegt hierbei den Anforderungen gemäß SigG / SigV.

Der Vorgang der Erstellung elektronischer Signaturen kann wie folgt gestartet werden:

- über die Schaltfläche „Datei signieren“ der „Shell-Extension“-Anwendung und Betätigung der Schaltfläche „Signieren“ im „Signaturanforderungsdialog“ oder
- oder im „OpenLimit SignCubes Viewer“ durch Anklicken der Schaltfläche „Unterschreiben“.

Zur Erzeugung qualifizierter Signaturen muss der Benutzer die für das Produkt zugelassenen Sicheren Signaturerstellungseinheiten (SSEE, „Smartcard“) gemäß

Bezeichnung	**Registriernummer der Bestätigungs-ID**
STARCOS 3.4 Health QES C2 (Einzel-, M100- und Massensignaturkarte; Handelsnamen: *D-TRUST Card V3.0, DATEV Card V3.0, Signaturkarte der Bundesagentur für Arbeit (BA))*	BSI.02120.TE.05.2009 Nachtrag vom 15.11.2010

Bezeichnung	Registriernummer der Bestätigungs-ID
STARCOS 3.5 ID ECC C1 (Einzelsignaturkarte)	SRC.00013.TE.10.2012
STARCOS 3.5 ID ECC C1R (Einzel-, M100- und Massensignaturkarte; Handelsnamen: *Signtrust Card 3.5, Signtrust MCard 3.5, Signtrust MCard100 3.5, DGN sprintCard, sprintCard, DGN businessCard, businessCard, elektronischer Arztausweis, eA, eArztausweis, eHBA für Ärzte, elektronischer Zahnarztausweis, eZAA, eZahnarztausweis, eHBA für Zahnärzte, elektronischer Psychotherapeutenausweis, ePTA, eHBA für Psychotherapeuten, eHBA für psychologische Psychotherapeuten und Kinder- und Jugendlichenpsychotherapeuten, medisign Card, medisignCard, ZOD-Signaturkarte für Zahnärzte, ZOD-Karte, ZOD-Card, Bundesnotarkammer - Stapelsignaturkarte 100, Bundesnotarkammer – Multisignaturkarte*)	SRC.00021.TE.05.2013 Korrigendum 1 vom 14.11.2013 Nachtrag 1 vom 23.09.2013
STARCOS 3.5 ID GCC C1 (Einzelsignaturkarte; Handelsnamen: *nPA-Signaturkarte*)	SRC.00008.TE.12.2010
STARCOS 3.5 ID GCC C1R (Einzelsignaturkarte; Handelsnamen: *nPA-Signaturkarte*)	SRC.00014.TE.02.2012
STARCOS 3.5 ID GCC C2 (Einzelsignaturkarte; Handelsnamen: *nPA-Signaturkarte*)	SRC.00012.TE.05.2013
TCOS Identity Card Version 1.0 Release 1/SLE78CLX1440P (Einzelsignaturkarte; Handelsnamen: *nPA-Signaturkarte*)	SRC.00006.TE.11.2010
TCOS 3.0 Signature Card, Version 1.1 (Einzel- und Massensignaturkarte)	TUVIT.93146.TE.12.2006 Nachtrag 1 vom 07.05.2010
TCOS 3.0 Signature Card, Version 2.0 Release 1/ SLE78CLX1440P (Einzel- und Massensignaturkarte)	SRC.00016.TE.11.2012
ZKA Banking Signature Card, Version 7.1.2 (Einzelsignaturkarte)	TUVIT.93166.TU.06.2008 Nachtrag 1 vom 15.09.2009 Nachtrag 2 vom 28.12.2010

Bezeichnung	Registriernummer der Bestätigungs-ID
ZKA Banking Signature Card, Version 7.1.3 (Einzelsignaturkarte)	TUVIT.93171.TU.06.2010
ZKA Banking Signature Card, Version 7.1.4 (Einzelsignaturkarte)	TUVIT.93181.TU.09.2010 Nachtrag 1 vom 28.12.2010
ZKA Banking Signature Card, Version 7.2.1 (Einzelsignaturkarte)	TUVIT.93174.TU.06.2010 Nachtrag 1 vom 28.12.2010
ZKA Banking Signature Card, Version 7.2.2 (Einzelsignaturkarte)	TUVIT.93172.TU.06.2010
ZKA Banking Signature Card, Version 7.2.3 (Einzelsignaturkarte)	TUVIT.93182.TU.09.2010
ZKA SECCOS Sig v2.6.4 R1.1.2 (Einzelsignaturkarte)	SRC.00009.TE.09.2010
ZKA-Signaturkarte, Version 6.21 (Einzelsignaturkarte)	TUVIT.93174.TU.06.2010
ZKA-Signaturkarte, Version 6.22 (Einzelsignaturkarte)	TUVIT.93183.TU.11.2010
ZKA-Signaturkarte, Version 6.30 (Einzelsignaturkarte)	TUVIT.93170.TU.07.2010 Nachtrag 1 vom 22.07.2010
ZKA-Signaturkarte, Version 6.31 (Einzelsignaturkarte)	TUVIT.93175.TU.08.2010
ZKA-Signaturkarte, Version 6.32 (Einzelsignaturkarte)	TUVIT.93184.TU.11.2010
ZKA-Signaturkarte, Version 6.32 M (Massensignaturkarte)	TUVIT.93176.TU.05.2011

Tabelle 3 und die für das Produkt zugelassenen Kartenterminals gemäß

Cherry KC 1000SC, JK-A01, FW-Version: 2.0.0, HW-Version: 1.0	BSI-DSZ-CC-0970

Tabelle 4 benutzen. Wenn kein Kartenterminal und keine SSEE vorhanden sind, bricht das Produkt den Vorgang zur Erstellung einer elektronischen Signatur mit einer Fehlermeldung ab.

Die Kommunikation mit dem Kartenterminal und der Signaturerstellungseinheit erfolgt über die PC/SC-Schnittstelle. Diese Schnittstelle wird vom Betriebssystem bzw. der Umgebung des Produkts zur Verfügung gestellt. Die Kommunikation erfolgt immer im Transaktionsmodus, d.h., andere Anwendungen, die ebenfalls unter Verwendung der PC/SC-Schnittstelle auf die Signaturerstellungseinheit zugreifen wollen, können die Kommunikation zwischen dem Produkt und der Signaturerstellungseinheit nicht stören, soweit die PC/SC-Implementierung des Betriebssystems dies absichert.

Über diese Schnittstelle zum Terminal werden die zu signierenden Hashwerte an die SSEE übergeben und die erzeugten Signaturen von der SSEE empfangen. Ferner wird das Signaturzertifikat darüber abgefragt und erhalten.

Das Produkt unterstützt die Erstellung von Signaturen gemäß den folgenden Verfahren:

- RSA-Algorithmus oder
- ECDSA-Algorithmus.

Das konkret verwendete Signaturverfahren und die verwendete Schlüssellänge werden durch die Fähigkeiten der benutzten Signaturerstellungseinheit bestimmt, vgl. dazu

Bezeichnung	**Registriernummer der Bestätigungs-ID**
STARCOS 3.4 Health QES C2 (Einzel-, M100- und Massensignaturkarte; Handelsnamen: *D-TRUST Card V3.0, DATEV Card V3.0, Signaturkarte der Bundesagentur für Arbeit (BA))*	BSI.02120.TE.05.2009 Nachtrag vom 15.11.2010
STARCOS 3.5 ID ECC C1 (Einzelsignaturkarte)	SRC.00013.TE.10.2012
STARCOS 3.5 ID ECC C1R (Einzel-, M100- und Massensignaturkarte; Handelsnamen: *Signtrust Card 3.5, Signtrust MCard 3.5, Signtrust MCard100 3.5, DGN sprintCard, sprintCard, DGN businessCard, businessCard, elektronischer Arztausweis, eA, eArztausweis, eHBA für Ärzte, elektronischer Zahnarztausweis, eZAA, eZahnarztausweis, eHBA für Zahnärzte, elektronischer Psychotherapeutenausweis, ePTA, eHBA für Psychotherapeuten, eHBA für psychologische Psychotherapeuten und Kinder- und Jugendlichenpsychotherapeuten, medisign Card, medisignCard, ZOD-Signaturkarte für Zahnärzte, ZOD-Karte, ZOD-Card, Bundesnotarkammer - Stapelsignaturkarte 100, Bundesnotarkammer – Multisignaturkarte*)	SRC.00021.TE.05.2013 Korrigendum 1 vom 14.11.2013 Nachtrag 1 vom 23.09.2013
STARCOS 3.5 ID GCC C1 (Einzelsignaturkarte; Handelsnamen: *nPA-Signaturkarte*)	SRC.00008.TE.12.2010
STARCOS 3.5 ID GCC C1R (Einzelsignaturkarte; Handelsnamen: *nPA-Signaturkarte*)	SRC.00014.TE.02.2012
STARCOS 3.5 ID GCC C2 (Einzelsignaturkarte; Handelsnamen: *nPA-Signaturkarte*)	SRC.00012.TE.05.2013

Bezeichnung	Registriernummer der Bestätigungs-ID
TCOS Identity Card Version 1.0 Release 1/SLE78CLX1440P (Einzelsignaturkarte; Handelsnamen: *nPA-Signaturkarte*)	SRC.00006.TE.11.2010
TCOS 3.0 Signature Card, Version 1.1 (Einzel- und Massensignaturkarte)	TUVIT.93146.TE.12.2006 Nachtrag 1 vom 07.05.2010
TCOS 3.0 Signature Card, Version 2.0 Release 1/ SLE78CLX1440P (Einzel- und Massensignaturkarte)	SRC.00016.TE.11.2012
ZKA Banking Signature Card, Version 7.1.2 (Einzelsignaturkarte)	TUVIT.93166.TU.06.2008 Nachtrag 1 vom 15.09.2009 Nachtrag 2 vom 28.12.2010
ZKA Banking Signature Card, Version 7.1.3 (Einzelsignaturkarte)	TUVIT.93171.TU.06.2010
ZKA Banking Signature Card, Version 7.1.4 (Einzelsignaturkarte)	TUVIT.93181.TU.09.2010 Nachtrag 1 vom 28.12.2010
ZKA Banking Signature Card, Version 7.2.1 (Einzelsignaturkarte)	TUVIT.93174.TU.06.2010 Nachtrag 1 vom 28.12.2010
ZKA Banking Signature Card, Version 7.2.2 (Einzelsignaturkarte)	TUVIT.93172.TU.06.2010
ZKA Banking Signature Card, Version 7.2.3 (Einzelsignaturkarte)	TUVIT.93182.TU.09.2010
ZKA SECCOS Sig v2.6.4 R1.1.2 (Einzelsignaturkarte)	SRC.00009.TE.09.2010
ZKA-Signaturkarte, Version 6.21 (Einzelsignaturkarte)	TUVIT.93174.TU.06.2010
ZKA-Signaturkarte, Version 6.22 (Einzelsignaturkarte)	TUVIT.93183.TU.11.2010
ZKA-Signaturkarte, Version 6.30 (Einzelsignaturkarte)	TUVIT.93170.TU.07.2010 Nachtrag 1 vom 22.07.2010
ZKA-Signaturkarte, Version 6.31 (Einzelsignaturkarte)	TUVIT.93175.TU.08.2010
ZKA-Signaturkarte, Version 6.32 (Einzelsignaturkarte)	TUVIT.93184.TU.11.2010
ZKA-Signaturkarte, Version 6.32 M (Massensignaturkarte)	TUVIT.93176.TU.05.2011

Tabelle 3.

Die *OpenLimit SignCubes Basiskomponenten Version 2.10* unterstützen die Erstellung der folgenden Signaturtypen:

- CMS-Signaturen gemäß RFC 5652,
- XML-Signaturen gemäß RFC 3275,
- PDF-Signaturen und
- Zeitstempel gemäß RFC 3161

Die *OpenLimit SignCubes Basiskomponenten Version 2.10* unterstützen die Erstellung der folgenden CAdES-Signaturformate gemäß ETSI TS 101 733 mit den folgenden Profilen:

- CAdES-BES
- CAdES-T

Folgende Hash-Algorithmen werden unterstützt[2]:

- SHA-1, SHA-224, SHA-256, SHA-384 und SHA-512 sowie
- RIPEMD-160.

Bei der Erstellung einer qualifizierten elektronischen Signatur kann dem Produkt an der grafischen Benutzerschnittstelle (GUI) signalisiert werden, dass bei der Signaturerzeugung ein zum Benutzerzertifikat gehöriges Attributzertifikat in den Signaturcontainer eingebettet werden soll.

Vor dem eigentlichen Prozess der Signaturerstellung wird dem Benutzer (stets an der GUI) in Form des „Signaturanforderungsdialogs“ eindeutig signalisiert, dass dieser Prozess nun starten wird und welche Daten hierfür verwendet werden sollen. Diese Signalisierung an der GUI erfolgt auch, wenn die Signaturerzeugung über die SDK-Schnittstelle aufgerufen wurde.

Nachdem die *OpenLimit SignCubes Basiskomponenten Version 2.10* von der SSEE die erstellte Signatur erhalten haben, wird stets die Prüfung dieser Signatur durchgeführt. Auf diese Weise wird sichergestellt, dass sich die erzeugte Signatur auf die zu signierenden Daten bezieht. Schlägt diese Prüfung fehl, wird dies mitgeteilt und die Signatur verworfen.

Weitere Anwendungen, die von der OpenLimit SignCubes AG hergestellt werden, können ausschließlich über die Programmierschnittstelle die Funktionalität des Produktes nutzen, mit einer einmaligen Eingabe der PIN mehrere Dokumente qualifiziert elektronisch zu signieren. Wenn eine solche Anwendung diese Funktionalität verwendet, zeigen die *OpenLimit SignCubes Basiskomponenten Version 2.10* dem Anwender einen Signaturanforderungsdialog an, der die Liste der zu signierenden Dokumente enthält und die Anzeige eines jeden Dokuments über den *OpenLimit SignCubes Viewer* ermöglicht. Die Erzeugung der qualifizierten elektronischen Signaturen wird erst gestartet, wenn der Anwender dies in dem Dialog ausdrücklich bestätigt. Sind die *OpenLimit SignCubes*

[2] Die Hashalgorithmen SHA-1, SHA-224 und RIPEMD-160 sind nicht mehr zur Erzeugung qualifizierter elektronischer Signaturen gemäß Signaturgesetz und Signaturverordnung geeignet.

Basiskomponenten Version 2.10 entsprechend konfiguriert, muss der Anwender dann die PIN nicht für jede qualifizierte elektronische Signatur einzeln eingeben.

Die Signaturerzeugung über die programmierbare Schnittstelle (SDK) gemäß [SDK Documentation][3] erfolgt durch Aufruf eines der folgenden Jobs:

- SIQJOB_JOB_SIGNFILE zur Signatur einer Datei,
- SIQJOB_JOB_SIGNFILES zur Stapelsignatur,
- SIQJOB_JOB_SIGNDATA zur Signatur von Daten im Puffer oder
- SIQJOB_JOB_SIGNDIGEST zur Signatur eines Hashwertes.

Erfolgt die Signaturerzeugung im Stapelprozess unter Verwendung einer SSEE, die für Multisignaturen zulässig ist, wird für den Prozess der Signaturerzeugung die PIN, wie nachfolgend beschrieben, offen gehalten. Standardmäßig werden die *OpenLimit SignCubes Basiskomponenten Version 2.10* bei der Installation so eingestellt, dass die PIN für das qualifizierte Zertifikat bei jeder Signaturerzeugung eingegeben werden muss. Über die GUI der *OpenLimit SignCubes Basiskomponenten Version 2.10* kann der Anwender die Option zum Öffnen der Karte für mehrere Arbeitsschritte einstellen. Gleichzeitig wird der Anwender aufgefordert, diese Einstellung des Offenhaltens der PIN nach Zeit und/oder Anzahl der Signaturen zu begrenzen.

Im Prozess der Stapelerzeugung wird die PIN offengehalten bis zur Beendigung des Stapeljobs, sofern über die GUI der *OpenLimit SignCubes Basiskomponenten Version 2.10* die standardmäßig vorgenommene Einstellung nicht verändert wurde, d.h. für jeden Signaturerzeugung die PIN eingegeben werden muss. In dem Fall, dass durch den Anwender eine Einstellung zum Offenhalten der PIN vorgenommen wurde, gilt diese Einstellung für den Stapeljob.

PIN-Caching wird durch die *OpenLimit SignCubes Basiskomponenten Version 2.10* ausdrücklich nicht unterstützt. Weiterhin wird von der Komponente kein Mechanismus implementiert, der ein PIN-Caching oder einen vergleichbaren Betriebsmodus zulässt.

3.3 Sichere Anzeige von Dokumenten

Sowohl im Zuge der Signaturerstellung als auch der Signaturprüfung erhält der Benutzer die Möglichkeit, sich die zu signierenden bzw. signierten Daten anzeigen zu lassen. Bei dieser Anzeige stellen die *OpenLimit SignCubes Basiskomponenten Version 2.10* sicher, dass der

[3] „OPENLiMiT SignCubes SDK v2.5 Documentation, Version 1.5, OPENLiMiT SignCubes GmbH, 27.10.2008“ aus Nachtrag Nr. 4 zur Sicherheitsbestätigung BSI.02110.TE.12.2008. Dieses Dokument wird vom Hersteller nur auf Veranlassung durch den Benutzer an diesen ausgeliefert.

Inhalt der anzuzeigenden Daten eindeutig dargestellt wird. Zudem zeigt das Produkt dem Benutzer an, ob die Datei versteckte oder aktive Elemente enthält.

Für eine Sichere Anzeige müssen die anzuzeigenden Daten in einem der folgenden Dokumentenformate vorliegen:

- Text (7-Bit ASCII oder kodiert gemäß ISO-8859-15),
- XML,
- TIFF oder
- PDF bzw.PDF/A.

Das Produkt führt in Abhängigkeit vom Dateityp folgende Prüfungen durch:

- Textdatei: Vorhandensein unbekannter Symbole,
- TIFF-Datei: Vorhandensein unbekannter oder als bösartig bekannter Tags,
- PDF-Datei: Vorhandensein unbekannter oder als bösartig bekannter Elemente,

Der Benutzer wird über das Ergebnis der Prüfung informiert. Einzelheiten zum Gebrauch der Sicheren Anzeige entnimmt der Benutzer der „Online Help“.

3.4 Anwendung von Zeitstempeln

Die Anwendung von Zeitstempeln ist über die GUI- und SDK-Schnittstelle zugänglich. Der Vorgang der Anwendung von Zeitstempeln kann wie folgt gestartet werden:

- an der GUI-Schnittstelle „Shell-Extension“ durch Aufruf des Menüpunkts „Zeitstempel erzeugen“,
- im Signaturanforderungsdialog durch Anklicken der Option „Zeitstempel erzeugen“,
- über die GUI des *OpenLimit SignCubes Manager* durch Anklicken der Option „Signaturen automatisch mit Zeitstempel versehen“ oder
- an der SDK-Schnittstelle durch Aufruf eines der folgenden Jobs
    - SIQJOB_JOB_TIMESTAMPDIGEST,
    - SIQJOB_JOB_TIMESTAMPFILE,
    - SIQJOB_JOB_TIMESTAMPDATA,
    - SIQJOB_JOB_SIGNDATA oder
    - SIQJOB_JOB_SIGNFILE.

Sind im Produkt mehrere Zeitstempeldiensteanbieter konfiguriert, erscheint ein Auswahldialog, über den der Benutzer einen Zeitstempeldiensteanbieter auswählt. Anschließend fordert das Produkt den Zeitstempel an, der nach Erhalt (bei Anforderung über die „Shell-Extension“) als separate Datei gespeichert oder (bei Anforderung über die SDK-Schnittstelle) als Datenstrom zurückgegeben wird.

3.5 Signaturverifikation

Die *OpenLimit SignCubes Basiskomponenten Version 2.10* unterstützen die Prüfung der folgenden Signaturtypen:

- CMS-Signaturen gemäß RFC 5652,
- XML-Signaturen gemäß RFC 3275,
- PDF-Signaturen und
- Zeitstempel gemäß RFC 3161

3.5.1 Prüfung digital signierter Objekte

Die *OpenLimit SignCubes Basiskomponenten Version 2.10* sind in der Lage, elektronische Signaturen gemäß CMS und Zeitstempel gemäß RFC 3161 zu prüfen. Diese elektronischen Signaturen können dabei qualifizierte oder fortgeschrittene elektronische Signaturen gemäß SigG / SigV sein. Der Typ der zu prüfenden Signaturen wird gemäß dem Typ des Zertifikats des Signaturschlüsselinhabers ermittelt. Die Prüfung qualifizierter elektronischer Signaturen, bei denen das Signaturzertifikat von einem Zertifizierungsdiensteanbieter gemäß SigG / SigV ausgegeben worden ist, erfolgt die Prüfung nach dem sogenannte *Kettenmodell*. Die Gültigkeit der in der zu prüfenden qualifizierten elektronischen Signatur verwendeten Algorithmen wird hierbei unter Benutzung des sogenannten Algorithmenkatalogs bestimmt.

Die *OpenLimit SignCubes Basiskomponenten Version 2.10* zeigen bei der Prüfung von Signaturen an der grafischen Benutzerschnittstelle (GUI) im Dialogfenster zur Zusammenfassung des Prüfergebnisses sowie im Dialogfenster zu den Details des Prüfergebnisses zuverlässig an, wenn die zu prüfende Signatur Algorithmen verwendet, die gemäß Algorithmenkatalog als ungeeignet oder nicht mehr geeignet bewertet sind. Bei der Benutzung der programmierbaren Schnittstelle (SDK) erfolgt die Bewertung des verwendeten Algorithmen im XML-Verifikationsdatenstrom des Produkts durch Angabe des Werts „*secure*“ für einen gemäß Algorithmenkatalog geeigneten Algorithmus, „*insecure*“ für einen gemäß Algorithmenkatalog ungeeigneten Algorithmus oder „*unknown*“ (bzw. gleichbedeutend eine leere Zeichenkette), falls die *OpenLimit SignCubes Basiskomponenten Version 2.10* hierüber keine Aussage treffen können, jeweils bezüglich:

- des verwendeten Signaturalgorithmus in dem Element <*SignatureVerificationResult*> <*SignerInfos*> <*P72SignerInfo*> <*P72SignerInfoValidationResult*> <*P72SignerInfoValidationResult*> <*SignerRoleValidationResult*> <*Signer*> <*CertificateChainInfo*> <*CertificateInfo*> <*CertificateValidationResult*> <*CertSignatureInfo*> <*PKCS1SignatureInfo*> <*PKCS1SignatureValidationResult*> <*AlgorithmInfo*> <*AlgorithmSecurity*> bzw.
- des verwendeten Hashalgorithmus in dem Element <*SignatureVerificationResult*> <*SignerInfos*> <*P72SignerInfo*> <*P72SignerInfoValidationResult*>

<MessageDigestInfo> <MessageDigestValidationResult> <AlgorithmInfo> <AlgorithmSecurity>.

Das Ergebnis, ob der Algorithmus sicher ist oder nicht, wird bei der Benutzung der programmierbaren Schnittstelle (SDK) in dem Element *<AlgorithmSecurity>* angegeben. Die Informationen unter dem Element *<ExpirationInfo>* weisen die jeweilige Auslaufzeit der Sicherheit dieses Algorithmus mit den zugehörigen Schlüssellängen aus.

Bei der Prüfung eines digital signierten Objekts kann dieses auf einem SHA-1-, SHA-224-, SHA-256-, SHA-384-, SHA-512- oder RIPEMD-160-Hashwert beruhen. Während des Vorgangs der Prüfung digital signierter Objekte ist es unzweifelhaft, auf welche Daten sich die elektronische Signatur bezieht. Zum Zwecke der elektronischen Signaturprüfung wird der Hashwert des digital signierten Objekts unter Benutzung des zugehörigen Algorithmus berechnet und der ursprüngliche Hashwert aus der Signatur unter Benutzung des RSA-, DSA- bzw. ECDSA-Algorithmus und des öffentlichen Schlüssels des gegebenen Signaturzertifikats extrahiert. Gemäß den im Produkt definierten Parametern des DSA-Algorithmus ist die Prüfung von DSA-Signaturen nur für fortgeschrittene Signaturen anwendbar. Zusätzlich zu diesem Vorgang wird die Zertifikatskette unter Verwendung des Kettenmodells oder RFC 3280 geprüft.

Während des Prüfvorgangs wird der Herausgeber des Signaturzertifikats ermittelt und eine OCSP-Anfrage gestellt, um die Gültigkeit des zu untersuchenden Zertifikats zu prüfen. Die zugehörige OCSP-Auskunft kann hierbei in die zu untersuchenden Signaturdaten einkodiert sein. Falls eine existierende, gültige OCSP-Auskunft verfügbar ist (deren Erstellungszeit nach der Signaturerstellungszeit liegt), kann diese für die Signaturprüfung verwendet werden.

Alternativ zur Benutzung von OCSP kann eine Zertifikatssperrliste für den Prüfvorgang verwendet werden. Diese Sperrliste wird auf das Vorhandensein eines Sperrvermerks für das Signaturzertifikat geprüft. Falls dies zutrifft, wird diese Information verwendet. Falls das Zertifikat schon während der Signaturerstellung gesperrt war, wird dem Benutzer diese Information angezeigt.

Die wesentlichen Gültigkeitsprüfungen erfolgen stets unter Benutzung der Zeitangabe, die in den Signaturblock einkodiert ist. Diese Zeit ist normalerweise die Systemzeit, zu der die Signatur erstellt worden ist. Wenn bei der Prüfung einer qualifizierten Signatur kein Signaturerstellungszeitpunkt vorliegt (also in der Signatur enthalten ist), kann nicht sichergestellt werden, ob die qualifizierte Signatur zum Zeitpunkt ihrer Erstellung auf einem gültigen qualifizierten Zertifikat beruhte und dem Benutzer wird diesbezüglich ein entsprechender Hinweis gegeben. Bitte wenden Sie sich an die Bundesnetzagentur, um weiterführende Informationen zur Interpretation dieses technischen Umstands zu erhalten.

Die internen Prozesse der *OpenLimit SignCubes Basiskomponenten Version 2.10* sind wie folgt: Zuerst wird das Signaturzertifikat aus dem Signaturblock extrahiert. Der Prüfschlüssel

dieses Zertifikats wird für die Prüfung der digitalen Signatur verwendet. Alternativ kann das verwendete Signaturzertifikat bei der Anfrage zur Signaturprüfung durch die aufrufende Anwendung angegeben werden, sodass dieses zur Prüfung der elektronischen Signatur verwendet wird.

Bei der Prüfung von CMS-Signaturen sind je nach der Kodierung des CMS-Containers zwei verschiedene Verfahren zu unterscheiden:

Kodierung ohne authentisierte Attribute: Das Produkt bestimmt den für die Signatur der Daten benutzten Signaturalgorithmus anhand der OID (wie z. B. „*SHA256withRSA*“ oder „1.2.840.113549.1.1.11“), die in dem Signaturcontainer enthalten sein muss, und durch den ebenfalls der verwendete Hash-Algorithmus angegeben wird. Das Produkt berechnet den Hashwert der Daten, auf die sich die Signatur bezieht. Das Produkt wendet das Verfahren, nach dem die Signatur erzeugt wurde (also RSA, DSA oder ECDSA), unter Benutzung des Prüfschlüssels des Signaturzertifikats an und vergleicht den für den Hashwert der signierten Daten angegebenen Wert mit dem im vorangehenden Schritt errechneten Wert. Stimmen diese beiden Werte nicht überein, wird im Verifikationsdatenstrom der Rückgabewert SIQ_E_VRF_WRONGMESSAGEDIGEST ausgegeben. Wurde die Prüfung über die grafische Benutzerschnittstelle angestoßen, erscheint eine entsprechende Warnung im Ergebnisfenster.

Kodierung mit authentisierten Attributen: Enthält der Signaturcontainer authentisierte Attribute, bezieht sich die Signatur im technischen Sinne auf diese authentisierten Attribute. Diese enthalten unter anderem den Hashwert der ursprünglich signierten Daten. Das Produkt bestimmt den benutzten Hash-Algorithmus anhand der angegebenen OID, berechnet den Hashwert der ursprünglichen DTBS (*„**D**ata **t**o **b**e **s**igned“*) und verifiziert die PKCS#1-Signatur gegen den neu errechneten Hashwert über die DTBS. Im zweiten Schritt prüft das Produkt, ob der in den DTBS angegebene Hashwert, der sich auf das ursprüngliche Dokument bezieht, identisch mit dem neu errechneten Hashwert über das Dokument ist. Stimmen diese beiden Werte nicht überein, geben die *OpenLimit SignCubes Basiskomponenten Version 2.10* eine dementsprechende Information an der grafische Benutzerschnittstelle (GUI) im Dialogfenster zur Zusammenfassung des Prüfergebnisses sowie im Dialogfenster zu den Details des Prüfergebnisses wieder. Bei Benutzung der programmierbaren Schnittstelle (SDK) wird im Verifikationsdatenstrom der Rückgabewert SIQ_E_VRF_WRONGMESSAGEDIGEST ausgegeben.

Durch das angegebene Verfahren stellt das Produkt sicher, dass die kryptografische Bindung zwischen Signatur und signierten Daten mathematisch korrekt ist. Der hierbei verwendete Algorithmus muss vom Produkt unterstützt werden, da ansonsten die Signatur nicht geprüft werden kann. In diesem Fall gibt das Produkt an der grafischen Benutzerschnittstelle (GUI) eine dementsprechende Information im Dialogfenster zur Zusammenfassung des Prüfergebnisses sowie im Dialogfenster zu den Details des Prüfergebnisses bzw. an der programmierbaren Schnittstelle (SDK) den Fehlercode

SIQ_E_VRF_UNKNOWNSIGNATUREALG bei unbekanntem Signaturalgorithmus bzw. SIQ_E_VRF_UNKNOWNDIGESTALG bei unbekanntem Hashalgorithmus aus.

Wurde diese mathematische Korrektheit erfolgreich festgestellt, ermittelt das Produkt die zwischen dem Signaturzertifikat, dem CA-Zertifikat und dem Wurzel-Zertifikat bestehenden Abhängigkeiten.

Erweist sich das Signaturzertifikat hierbei als ungültig, also z. B. indem das Signaturzertifikat nicht zu dem CA-Zertifikat gehört, zu dem es vorgibt zu gehören, wird eine entsprechende Information an der grafischen Benutzerschnittstelle (GUI) im Dialogfenster zur Zusammenfassung des Prüfergebnisses sowie im Dialogfenster zu den Details des Prüfergebnisses ausgegeben. Der Vorgang der Signaturprüfung wird beendet. An der SDK-Schnittstelle werden je nach Fehlersituation folgende Rückgabewerte ausgegeben:

- SIQ_E_VRF_CERTCHAIN_INCOMPLETE - Der Zertifikatspfad konnte nicht vollständig geprüft werden, da er unvollständig ist.
- SIQ_E_VRF_CERTCHAIN_NOCHAIN - Der Zertifikatspfad konnte nicht ermittelt werden und ist daher unvollständig.
- SIQ_E_VRF_INCOMPLETE - Die Zertifikatskette konnte nicht aufgebaut werden, da das CA- und / oder Wurzelzertifikat nicht ermittelt werden konnte.

Nachfolgend wird die Gültigkeit des Zertifikatspfads unter Benutzung aktueller Statusauskünfte geprüft. Um die Gültigkeit einer Signatur beurteilen zu können, muss das Produkt die möglichen Zertifikatspfade des Zertifikatsbaums aufbauen. Hierfür ermitteln die *OpenLimit SignCubes Basiskomponenten Version 2.10* aus dem Signaturzertifikat den Namen des Zertifikatsherausgebers und versuchen durch einen Namensvergleich eine vollständige Kette bis hin zu einem vertrauenswürdigen Zertifikat aufzubauen. Hierfür stellen die *OpenLimit SignCubes Basiskomponenten Version 2.10* fest, ob der „Signaturblock“ außer dem Signaturzertifikat weitere Zertifikate enthält. Für den Aufbau der Zertifikatspfade verwendet das Produkt zudem qualifiziert signierte Listen vertrauenswürdiger Statusquellen (*Trust-Service Status List* TSL) gemäß ETSI TS 102 231. In PKCS#7-signierten Listen vertrauenswürdiger Statusquellen des Produkt-Herstellers (also einer Zertifikatvertrauensliste „*Certificate Trust Lists*“ CTL, in Form von *SignCubes Trust Lists* STL) verwaltet das Produkt die CA-Zertifikate der angezeigten und akkreditierten Zertifizierungsdiensteanbieter. Vor der Verwendung von TSL-Dateien muss deren PKCS#1-Signatur erfolgreich geprüft sein. Die Qualität dieser Vertrauensanker wird anhand einer „Trust-OID“ bewertet, ob es sich um CA-Zertifikate angezeigter und akkreditierter ZDAs handelt. Die *OpenLimit SignCubes Basiskomponenten Version 2.10* prüfen also für jedes Ende eines gebildeten Zertifikatspfads, ob dieses Zertifikat Teil einer solchen Zertifikatvertrauensliste ist.

Das Produkt prüft die Authentizität der TSL an Hand ihrer Signatur (sofern vorhanden). Nachfolgend wird die kryptografische Korrektheit jedes Paars von Zertifikaten der einzelnen Zertifikatspfade geprüft sowie festgestellt, ob Informationen zur Sperrung eines Zertifikats

vorliegen. Das Produkt kann auch Zertifikatspfade bilden, die „Cross-Zertifikate“ enthalten und hierüber mit anderen Zertifikatsbäumen verbunden sind, wobei jeder derartige Pfad separat bis zur Wurzel geprüft wird. Die Darstellung der hierbei ermittelten Prüfergebnisse erfolgt für jeden Zertifikatspfad. In dem Dialogfenster zur Anzeige der Prüfergebnisse werden hierbei zuerst die Ergebnisse des „besten Pfads“ angezeigt, wobei dies i. A. der kürzeste Pfad bzw. der mit der besten „Trust-OID“ ist. Die Ergebnisse bzgl. weiterer aufgebauter Pfade, für die ebenfalls Prüfergebnisse vorliegen, werden dann wiederum zuerst in einem Zusammenfassungsdialog angezeigt, wobei für jeden gefundenen Pfad ein Reiter in dem Dialogfenster erscheint.

Für diesen Verarbeitungsschritt werden gültige OCSP-Auskünfte resp. CRL-Listen benötigt. Fehlen derlei aktuelle Statusauskünfte oder ist eines der Zertifikate des Zertifikatspfads nicht mehr gültig, wird die Signatur nicht als gültig, aber mathematisch korrekt klassifiziert.

Als Ergebnis der Prüfung der digitalen Signatur geben die *OpenLimit SignCubes Basiskomponenten Version 2.10* an der grafischen Benutzerschnittstelle (GUI) ein Dialogfenster aus, in dem alle bezüglich der Signaturprüfung relevanten Informationen gemäß §17 SigG eindeutig angezeigt werden, und die Aussage getroffen wird, ob die untersuchte Signatur gültig oder ungültig ist, oder ob keine solche Entscheidung getroffen werden kann. Die Anzeige des Prüfergebnisses erfolgt in einem separaten Anzeigefenster an der grafischen Benutzerschnittstelle (GUI), das eine Übersicht über die wichtigsten Fakten der Prüfung liefert, wobei durch Betätigung der entsprechend benannten Schaltfläche alle verfügbaren Detailinformationen angezeigt werden.

Bei Veranlassung einer Signaturprüfung an der programmierbaren Schnittstelle (SDK) erfolgt auch die Ausgabe eines XML-Datenstroms von Prüfergebnissen an der programmierbaren Schnittstelle (SDK). Das Produkt gibt gemäß §17 SigG eine eindeutige Information aus, ob der in die Signatur einkodierte Hashwert und der Hashwert der zu prüfenden Daten übereinstimmen oder nicht. Hierdurch ist es unzweifelhaft, ob die Originaldaten verändert wurden oder nicht. Die Korrektheit der elektronischen Signatur wird zuverlässig festgestellt und das Ergebnis im bereitgestellten Verifikationsdatenstrom bekanntgegeben. Das Ergebnis der Prüfung einer Signatur beschreibt hierbei gemäß §17 SigG

- in dem Element <*SignatureVerificationResult*> <*SignerInfos*> <*P72SignerInfo*> <*P72SignerInfoValidationResult*> <*MessageDigestInfo*> <*MessageDigest*> des XML-Verifikationsdatenstroms auf welche Daten sich die Signatur bezieht, und
- in dem Element <*SignatureVerificationResult*> <*SignerInfos*> <*P72SignerInfo*> <*P72SignerInfoValidationResult*> <*MessageDigestInfo*> <*MessageDigest*> <*MessageDigestValidationResult*> <*Value*> des XML-Verifikationsdatenstroms ob die Daten unverändert sind. <*Value*> kann hierbei die folgenden Werte enthalten: „*no_content*“ (der Hashwert konnte nicht berechnet werden, weil das Element *Content* in *MessageDigest* leer ist oder nicht gefunden werden konnte) , „*no_provider*“ (es konnte

kein Provider ermittelt werden, weil das Element *Provider* in *MessageDigest* leer ist oder nicht gefunden werden konnte), „*no_digest*“ (der Hashwert gegen den in den *signedAttributes* geprüft werden soll, konnte nicht gefunden werden), „*invalid*“ (der signierte Hashwert aus den *signedAttributes* entspricht nicht dem berechneten Hashwert. Entweder stimmt die Länge oder der Inhalt nicht überein.), „*valid*“ (der Hashwert aus den *signedAttributes* entspricht dem berechneten Hashwert über die die signierten Daten.), „*old_style*“ (es handelt sich um eine alte PKCS #7-Signatur ohne das Feld *signedAttributes* gemäß RFC 5652, sodass kein Hashwert geprüft werden kann) oder „*unknown*“ (keiner der oben genannten Fälle liegt vor).

- in dem Element <*SignatureVerificationResult*> <*SignerInfos*> <*P72SignerInfo*> <*P72SignerInfoValidationResult*> <*SignerRoleValidationResult*> <*Signer*> <*CertificateChainInfo*> <*CertificateInfo*> <*CertMgrData*> <*Certificate*> <*Subject*> des XML-Verifikationsdatenstroms welchem Signaturschlüsselinhaber die Signatur zuzuordnen ist,
- in dem Element <*SignatureVerificationResult*> <*SignerInfos*> <*P72SignerInfo*> <*P72SignerInfoValidationResult*> <*SignerRoleValidationResult*> <*Signer*> <*CertificateChainInfo*> <*CertificateInfo*> <*CertMgrData*> <*Certificate*> des XML-Verifikationsdatenstroms welche Inhalte das qualifizierte Zertifikat, auf dem die Signatur beruht, aufweist,
- in dem Element <*SignatureVerificationResult*> <*SignerInfos*> <*P72SignerInfo*> <*P72SignerInfoValidationResult*> <*SignerRoleValidationResult*> <*Signer*> <*CertificateChainInfo*> <*CertificateInfo*> <*AttrData*> <*AttrCert*> <*AttrCertificateInfo*> des XML-Verifikationsdatenstroms welche Inhalte zugehörige Attribut-Zertifikate aufweisen und
- unterhalb des Elements <*SignatureVerificationResult*> <*SignerInfos*> <*P72SignerInfo*> <*P72SignerInfoValidationResult*> <*SignerRoleValidationResult*> <*Signer*> <*CertificateChainInfo*> <*CertificateInfo*> <*CertificateValidationResult*> <*RevocCheckBase*>
    - für eine Nachprüfung eines Zertifikats gemäß OCSP in dem Element <*OCSPRevocationInfo*> <*RevocationState*> bzw.
    - für eine Nachprüfung eines Zertifikats gemäß CRL in dem Element <*CRLRevocationInfo*> <*RevocationState*>

  des XML-Verifikationsdatenstroms zu welchem Ergebnis die Nachprüfung von Zertifikaten führte, durch die die Zuordnung eines Signaturprüfschlüssels zu einer identifizierten Person durch ein qualifiziertes Zertifikat zu bestätigen und dieses jederzeit für jeden über öffentlich erreichbare Kommunikationsverbindungen nachprüfbar und abrufbar zu halten ist. Die möglichen Werte des Elements <*RevocationState*> können sein: „*Revoked*“ für zurückgezogene Zertifikate, „*Not_Revoked*“ für nicht zurückgezogene Zertifikate,

„*Unknown*“ falls über den Zertifikatszustand keine Aussage möglich ist, „*Failed*“, falls keine Informationen erhalten werden konnten, und „*Not_Revoked_Information*“, falls die erhaltene Auskunft zum Zustand des Zertifikats jünger ist, als die Angabe „Valid from“ des Zertifikats. Durch diese Angaben werden die Anforderungen gemäß § 17 Abs. 2 Nr. 2 b.) SigV erfüllt.

3.5.2 Verarbeitbare Dokument- und Signaturformate

Die *OpenLimit SignCubes Basiskomponenten Version 2.10* verarbeiten Signaturen im CMS-Format nach RFC 5652.

Dabei kann die Signatur wie folgend präsentiert werden:

- als abgesetzte Signatur (Signaturdatei, separiert von der Originaldatei (p7s)),
- als verbundene Signatur (Signaturdatei, bettet die Originaldaten ein (p7m)),
- als eingebettete Signatur in einer PDF-Datei gemäß der PDF/A-Spezifikation.

Darüber hinaus wird die Kombination PDF-Dateien mit eingebetteten Signaturen und zusätzlicher abgesetzter Signaturdatei verarbeitet.

3.5.3 Erwarteter Aufbau von CMS-Objekten

Im Folgenden wird auf die strukturellen Eigenschaften der verarbeiteten Signaturen eingegangen, basierend auf den RFCs und ISO-Standards, die von den *OpenLimit SignCubes Basiskomponenten Version 2.10* berücksichtigt werden.

Bei der Prüfung elektronischer Signaturen erwarten die *OpenLimit SignCubes Basiskomponenten Version 2.10* einen ASN.1-codierten Container im CMS-Format, der die eigentliche Signatur beinhaltet. Die Software geht dabei so vor, dass gemäß RFC 5652 geprüft wird, ob der angegebene *ContentType* vom Typ *SignedData* ist. Andere Typen werden von der Software nicht verarbeitet bzw. in der Verarbeitung von der Software abgewiesen.

Die *OpenLimit SignCubes Basiskomponenten Version 2.10* berücksichtigen aus dieser Datenstruktur die folgenden Elemente:

- *encapContentInfo* vom Typ *EncapsulatedContentInfo*
- *certificates* vom Typ *CertificateSet*
- *signerInfos* vom Typ *SignerInfos*

Das Element vom Typ *EncapsulatedContentInfo* beinhaltet eine OID (*Object Identifier*), die Auskunft über das vom CMS-Container adressierte Datenobjekt gibt.

Die Unterscheidung, ob es sich um eine verbundene Signatur oder eine abgesetzte Signatur handelt, wird von der Software anhand des Vorhandenseins des Feldes *eContent* definiert. Ist

dieses Feld nicht vorhanden, so handelt es sich um eine abgesetzte Signatur. Für PDF-Signaturen gilt, dass das Element *eContent* nicht gesetzt sein darf.

Das Element *certificates* vom Typ *CertificateSet* beinhaltet eine Auflistung der in dem vorliegenden CMS-Umschlag beinhalteten X.509-Zertifikate. Die *OpenLimit SignCubes Basiskomponenten Version 2.10* benötigen zwingend mindestens das für den Signaturvorgang verwendete Zertifikat als Bestandteil des präsentierten CMS-Containers zur Prüfung der beinhalteten elektronischen Signaturen. Durch entsprechende Ansteuerung an der programmierbaren Schnittstelle der Software können auch Signaturen geprüft werden, bei denen das ursprünglich verwendete Signaturzertifikat kein Bestandteil des CMS-Containers ist.

Das Element *SignerInfos* adressiert die letztendlich verarbeiteten Signaturen im CMS-Container. Dabei wird davon ausgegangen, dass sich die Signaturen auf das gleiche *Content*-Objekt beziehen. Dies schließt eine „Counter-Signatur“, bei der sich nachfolgende *SignerInfo*-Objekte auf das *Content*-Objekt zuzüglich bereits vorhandener *SignerInfos* beziehen, aus.

3.5.4 Konformität von PDF-Dokumenten / PDF-Signaturen

Voraussetzung für die Prüfung von Signaturen in PDF-Dateien mit den *OpenLimit SignCubes Basiskomponenten Version 2.10* ist die korrekte Verarbeitung eingebetteter Signaturen entsprechend Kapitel 2.2 der TechNote TN0006, die durch das PDF/A Competence Center veröffentlicht wurden. Dabei wird insbesondere die Konformität zu ISO 19005-1 verlangt, die für eine erfolgreiche Erkennung und Findung des Signaturobjektes innerhalb des PDF-Dokuments erforderlich ist. Weicht das zu prüfende Dokument von der PDF/A-Konformität ab, so kann nicht in jedem Falle eine erfolgreiche Signaturprüfung gewährleistet werden, da in diesem Falle strukturelle Fehler und Abweichungen von der ISO-Norm innerhalb des geprüften Dokuments eine weitere Verarbeitung verhindern. Ist das PDF-Dokument strukturell jedoch derart technisch intakt, dass ein Signaturobjekt gefunden werden kann, erfolgt durch die *OpenLimit SignCubes Basiskomponenten Version 2.10* eine zuverlässige Gültigkeitsprüfung.

So wie in TN0006 beschrieben, sollen die folgenden SubFilter für die Beschreibung der digitalen Signatur im PDF-Dokument verwendet werden:

- *adbe.pkcs7.detached*
- *adbe.pkcs7.sha1*

Andere Signaturen in PDF-Dokumenten werden von den *OpenLimit SignCubes Basiskomponenten Version 2.10* nicht verarbeitet.

Ist das Dokument strukturell beschädigt, kann es bei der Signaturprüfung dazu führen, dass vorhandene Signaturen nicht gefunden werden oder nicht erfolgreich geprüft werden können.

3.5.5 Verarbeitung eingebetteter Zeitstempel und OCSP-Antworten

Die *OpenLimit SignCubes Basiskomponenten Version 2.10* bieten die Möglichkeit, eingebettete Zeitstempel und OCSP-Antworten zu verarbeiten. Dabei muss der CMS-Umschlag so aufbereitet sein, dass die OCSP-Antworten als unsignierte Attribute (*UnsignedAttributes*) der jeweiligen *SignerInfo* zugeordnet sind. In diesem Falle erkennen die *OpenLimit SignCubes Basiskomponenten Version 2.10* automatisch die eingebetteten OCSP-Antworten und ziehen diese zur Prüfung der Zertifikatskette heran. Die Bedingung ist dabei, dass die OCSP-Antwort zu dem geprüften Zertifikat nach dem eigentlichen Signaturerstellungszeitpunkt (*Signing Time*) abgefragt wurde.

Ebenso kann eine Signatur einen Zeitstempel beinhalten, der als unsigniertes Attribut der *SignerInfo* zugeordnet ist. Dabei bezieht sich der Zeitstempel direkt auf die PKCS#1-Signatur. Neben diesem Format werden auch die eingebetteten Zeitstempel CAdES-konformer Kodierungen, wie CAdES-C und CAdES-T, gemäß RFC 5126 verarbeitet. Dabei ist zu beachten, dass die folgenden Formate verarbeitet werden:

- CAdES-BES
- CAdES-EPES
- CAdES-T
- CAdES-C

Weitere CAdES-Formate werden nicht unterstützt. Der in den jeweiligen CAdES-Containern enthaltene Zeitstempel, also das *SignatureTimeStampToken*, wird hierbei unabhängig von der Vollständigkeit der RFC-5126-Implementation stets zuverlässig korrekt geprüft.

Das Einbringen eines gültigen Zeitstempels in einen CMS-Container hat zur Folge, dass die Signatur nun zu einem weiteren Zeitpunkt geprüft wird. Die Signatur wird einerseits einer Prüfung zum angegebenen Signaturerstellungszeitpunkt unterzogen, zum anderen wird die Signatur zum im Zeitstempel angegebenen Zeitpunkt geprüft. Dies bedeutet auch – und das ist für die Verarbeitung der Signaturprüfergebnisse relevant – dass eine Signatur mit einem Zeitstempel zwei Einzelprüfergebnisse beinhaltet, die von einem jeweils anderen Signaturzeitpunkt ausgehen.

Ebenso werden eingebettete Objekte, wie ein Zeitstempel oder eine OCSP-Antwort, einer technischen und inhaltlichen Gültigkeitsprüfung unterzogen.

Informationen zu OCSP-Antworten (eingebettet oder neu geholt) sowie zu vorhandenen Zeitstempeln werden in das abrufbare Prüfprotokoll eingebettet.

Liegt zu einer Signatur ein Zeitstempel vor, der nicht als signiertes Attribut eingebettet wurde, muss dieser separat geprüft werden und wird nicht im Verifikationslauf der ursprünglichen Signatur mit verifiziert. Dies ist insbesondere dann relevant, wenn Zeitstempel als Übersignatur zu Signaturdateien vorliegen.

3.6 *Online Certificate Status Protocol* (OCSP) Anfrage gemäß RFC 2560

Die *OpenLimit SignCubes Basiskomponenten Version 2.10* stellen die Funktion der OCSP-Anfrage (Online-Gültigkeitsstatus) zur Verfügung.

Eine OCSP-Antwort ist eine Aussage zu dem Gültigkeitsstatus eines Zertifikats. Diese muss gemäß RFC 2560 von einer der folgenden Vergabestellen ausgestellt sein:

- dem Zertifizierungsdiensteanbieter (ZDA), der dieses Zertifikat ausgegeben hat, oder
- einem Drittanbieter, der von dem ZDA speziell zur Vergabe von Online-Gültigkeitsstati zu diesem Zertifikat autorisiert wurde.

Für die Funktion der OCSP-Anfrage verwenden die *OpenLimit SignCubes Basiskomponenten Version 2.10* die externen TCP/IP-Dienste des Betriebssystems.

Die Verfahrensweise der Beschaffung der OCSP-Antwort ist nicht Bestandteil dieser Herstellerklärung.

Das Verfahren der OCSP-Anfrage ist sicher, da die erwarteten Ergebnisse signiert sind und die Signatur vom Produkt geprüft wird.

3.7 Sperrliste (CRL) gemäß RFC 3280

Die *OpenLimit SignCubes Basiskomponenten Version 2.10* stellen über das SDK optional die Funktion des Downloads und der Bereitstellung von Sperrlisten (CRL) zur Verfügung, die zur Prüfung der Gültigkeit eines elektronischen Zertifikats verwenden können. Dieser Mechanismus wird genutzt, wenn keine OCSP-Antwort verfügbar ist.

Die Verfahrensweise der Beschaffung der Sperrlisten ist nicht Bestandteil dieser Herstellerklärung.

Das Verfahren der Sperrlistenbeschaffung und der Verwendung derart beschaffter Sperrlisten zur Signaturprüfung ist sicher, da die beschafften Sperrlisten signiert sind und diese Signaturen vom Produkt geprüft werden. *OpenLimit SignCubes Basiskomponenten Version 2.10* prüfen die elektronische Signatur jeder Sperrliste und importieren diese nur nach erfolgreicher Prüfung dieser Signatur. Auf diese Wiese ist die Integrität der Sperrinformationen sichergestellt.

3.8 Vertrauenslisten

Mit den *OpenLimit SignCubes Basiskomponenten Version 2.10* werden Vertrauenslisten ausgeliefert und können nachträglich über die GUI aktualisiert werden.

Das Verfahren der Aktualisierung der Vertrauenslisten und ihrer Verwendung ist sicher, da die beschafften Vertrauenslisten vom Produkthersteller signiert sind und diese Signaturen vom Produkt geprüft werden. Die *OpenLimit SignCubes Basiskomponenten Version 2.10* prüfen

die elektronische Signatur jeder Vertrauensliste und importieren diese nur nach erfolgreicher Prüfung ihrer Signatur. Auf diese Wiese ist die Integrität und Authentizität der Vertrauenslisten sichergestellt.

3.9 Zeitstempel gemäß RFC 3161

Die *OpenLimit SignCubes Basiskomponenten Version 2.10* stellen die Funktion des Einholens von Zeitstempeln an der grafischen und an der programmierbaren Schnittstelle zur Verfügung. Zeitstempel dienen als Nachweis für die Existenz von Daten zu einem bestimmten Zeitpunkt. Dieser Zeitpunkt wird von einer Zeitstempelvergabestelle in Form eines Zeitstempeldiensteanbieters (*Time Stamping Authority*, TSA) vergeben.

Die Verfahrensweise der Beschaffung der Zeitstempel ist nicht Bestandteil dieser Herstellerklärung.

Das Verfahren des Einholens der Zeitstempel ist sicher, da die erwarteten Ergebnisse signiert sind und die Signatur vom Produkt geprüft wird. Die *OpenLimit SignCubes Basiskomponenten Version 2.10* prüfen, ob der eingeholte Zeitstempel zum ursprünglich ausgewählten Datenmaterial passt, das mit einem Zeitstempel versehen werden sollte. Die elektronische Signatur eines eingeholten Zeitstempels wird stets geprüft wird. Die Weitergabe eines Zeitstempels erfolgt durch die *OpenLimit SignCubes Basiskomponenten Version 2.10* ausschließlich, falls der Zeitstempel gültig war.

3.10 Unterstützte Algorithmen und Signaturverfahren

Grundsätzlich werden ausschließlich Algorithmen unterstützt, die nach aktuellem Algorithmenkatalog der Bundesnetzagentur für den jeweiligen Zweck geeignet sind. Zum Zeitpunkt der Abgabe dieser Herstellererklärung gilt der Algorithmenkatalog vom 13.01.2014. Eine Erneuerung der im Produkt vorliegenden Informationen zur Eignung der Algorithmen muss vom Administrator oder Benutzer des Produkts durch Aktualisierung der Vertrauenslisten oder Durchführung des Updates vollzogen werden.

Die folgende Tabelle gibt an, welche Algorithmen technisch unterstützt werden und wie die jeweilige zugeordnete OID lautet. Für die Verarbeitung von Hashwerten ist es wichtig, dass die korrekte OID verwendet wird, da sonst ein Hashwert nicht verifiziert oder nachgerechnet werden kann.

In der folgenden Tabelle werden diejenigen OIDs aufgeführt, die bei der Verarbeitung elektronischer Signaturen Berücksichtigung finden. Werden Signaturen geprüft, die mit einer anderen als der angegebenen OID erstellt wurden, so sind diese Signaturen nicht erfolgreich prüfbar und werden als ungültig angezeigt. Demzufolge werden alle dem Produkt nicht bekannten Algorithmen als ungültig angezeigt. Die Ausgabe der Information zur

Sicherheitseignung eines Algorithmus an die aufrufende Anwendung ist in Kap. 3.5 beschrieben.

Algorithmus	OID	Unterstützung bei Signaturprüfung
SHA-1	1.3.14.3.2.26	Ja (gültig nur für fortgeschrittene Signaturen)
SHA-224	2.16.840.1.101.3.4.2.4	Ja
SHA-256	2.16.840.1.101.3.4.2.1	Ja
SHA-384	2.16.840.1.101.3.4.2.2	Ja
SHA-512	2.16.840.1.101.3.4.2.3	Ja
RIPEMD-160	1.3.36.3.2.1	Ja (gültig nur für fortgeschrittene Signaturen)
MD-5	1.2.840.113549.2.5	Ja (ungültig für qualif. und fortg. Signaturen)

Tabelle 5: Unterstützte Algorithmen

Die von den *OpenLimit SignCubes Basiskomponenten Version 2.10* unterstützten OIDs entsprechen den Bezeichnungen, die in verschiedenen Quellen angegeben sind. In dem Fall, dass andere OIDs, d.h. abweichend von den in der Tabelle aufgeführten OIDs, verwendet wurden, sind die Signaturen durch die *OpenLimit SignCubes Basiskomponenten Version 2.10* nicht erfolgreich prüfbar und werden als ungültig angezeigt.

Für RSA-Signaturen gemäß RFC 3447 („PKCS #1“) werden die folgenden Padding-Verfahren unterstützt:

- EMSA-PKCS1-v1_5 gemäß RFC 3447,
- EMSA-PSS gemäß RFC 3447 und
- Signaturformat gemäß DIN-Sig.

3.11 Kombination Hash- und Signaturalgorithmus

Die *OpenLimit SignCubes Basiskomponenten Version 2.10* gehen standardmäßig davon aus, dass gemäß RFC 5652 der verwendete Hashalgorithmus bei der Berechnung der Prüfsumme über das Datenobjekt identisch mit dem Hashalgorithmus ist, der zur Berechnung der Prüfsumme über die signierten Attribute (*SignedAttributes*) verwendet wurde.

Es ist jedoch zulässig, dass beide Algorithmen voneinander verschieden sind. So kann der Hashwert über das Datenobjekt beispielsweise unter Verwendung von „SHA-256“ erstellt worden sein, der verwendete Signaturalgorithmus kann hingegen „*sha512WithRSAEncryption*“ sein. In diesem Fall wird durch *OpenLimit SignCubes Basiskomponenten Version 2.10* der Hashalgorithmus zur Verifikation der Prüfsumme des Dokuments verwendet, der entsprechend der OID in den signierten Attributen hinterlegt ist.

Die Verifikation der elektronischen Signatur und die damit im Zusammenhang stehende Berechnung der Prüfsumme über die signierten Attribute erfolgt ausschließlich unter Verwendung der angegebenen Signatur-OID.

Lediglich wenn als Signaturalgorithmus nur „*rsaEncryption*“ angegeben wurde, wird die Kombination aus angegebener OID für die Dokumentprüfsumme herangezogen, um das Verfahren für die Verifikation der elektronischen Signatur zu bestimmen.

3.12 Sicherheitsbewertung von Algorithmen

Die *OpenLimit SignCubes Basiskomponenten Version 2.10* führen bei jeder Signaturprüfung auch eine Prüfung der Sicherheitseignung der verwendeten Algorithmen durch. Grundlage dieser Sicherheitsbewertung ist der vom Bundesamt für Sicherheit in der Informationstechnik erstellte und von der Bundesnetzagentur jährlich veröffentlichte sog. Algorithmenkatalog, in dem die für die Hashwertberechnung bei qualifizierten elektronischen Signaturen als geeignet eingestuften Algorithmen vorgegeben werden. Eine Erneuerung der im Produkt vorliegenden Informationen zur Sicherheitsbewertung der verwendeten Algorithmen erfolgt durch entsprechende Aktualisierung der Vertrauenslisten bzw. über den Updatecheck durch den Administrator oder Benutzer des Produkts, sofern der Benutzer über Administratorrechte verfügt.

3.13 Sicherung der Integrität

Die *OpenLimit SignCubes Basiskomponenten Version 2.10* bieten die Funktion zum Erkennen von Manipulationen an den ausgelieferten Bibliotheken und ausführbaren Dateien. Das Prüfmodul ermittelt die Hashwerte aller Bibliotheken und ausführbaren Dateien und vergleicht diese mit den Signaturen der einzelnen Dateien. Bei Abweichungen werden die *OpenLimit SignCubes Basiskomponenten Version 2.10* deaktiviert und der Benutzer durch eine Textmeldung informiert.

Es wird automatisch sichergestellt, dass das Prüfmodul nur von einer berechtigten Anwendung geladen werden kann. Das bedeutet, dass diese Anwendung mit dem gleichen Schlüssel signiert sein muss, wie das installierte, zu prüfende Produkt.

Stellt das Prüfmodul eine Beschädigung der Modulsignaturen fest, werden die *OpenLimit SignCubes Basiskomponenten Version 2.10* deaktiviert. Der sichere Zustand der Anwendung ist nicht mehr gewährleistet, da offensichtlich eine Manipulation eingetreten ist. Mit einer Textmeldung wird der Benutzer auf diesen Zustand hingewiesen.

Die *OpenLimit SignCubes Basiskomponenten Version 2.10* bieten die Funktion zum Prüfen der Integrität der installierten Programm-Module. Diese Sicherheitsfunktion wird durch das *OpenLimit SignCubes Integrity Tool* realisiert. Das *OpenLimit SignCubes Integrity Tool* ist ein Java-Applet, das die Hash-Werte an den ausgelieferten sicherheitsrelevanten Modulen

überprüft und somit sicherstellt, dass sich die Module noch in dem Zustand befinden, wie sie ursprünglich ausgeliefert und installiert wurden.

Für die Nutzung des *OpenLimit SignCubes Integrity Tool* ist das Java-Plugin notwendig, das über die Internetseite *www.openlimit.com/integritytool* geladen wird. Das Java-Plugin sollte grundsätzlich erst nach positiver Prüfung der Signatur des Applets gestartet werden.

Das Ergebnis der Prüfung durch das *OpenLimit SignCubes Integrity Tool* wird in einer Textmeldung angezeigt. Stellt das Prüfmodul eine Beschädigung der Modulsignaturen fest, ist der sichere Zustand der Anwendung nicht mehr gewährleistet und das Produkt sollte auf dem Rechner neu installiert werden.

Die Überprüfung der Unversehrtheit der Programm-Module sollte regelmäßig, d.h. mindestens einmal im Monat, durchgeführt werden.

4 Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

Erfüllte Anforderungen des Signaturgesetzes

§ 17 SigG, Abs. 2 Satz 1

„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."

Die Erfüllung dieser Anforderung wird im Kapitel 3.2 ausführlich erläutert. Die *OpenLimit SignCubes Basiskomponenten Version 2.10* zeigen die Erzeugung qualifizierter elektronischer Signaturen in dem Signaturanforderungsfenster eindeutig an. Gleichzeitig wird dem Anwender angezeigt, auf welche Daten sich die zu erzeugende elektronische Signatur bezieht.

§ 17 SigG, Abs. 2 Satz 2

„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 3 geführt hat."*

Die *OpenLimit SignCubes Basiskomponenten Version 2.10* stellen die Funktion der Verifikation elektronischer Signaturen in Einzeldokumenten über die Programmierschnittstelle des OpenLimit SDK zur Verfügung. Das Ergebnis der Signaturprüfung wird der aufrufenden Anwendung an die Programmierschnittstelle *OpenLimit SDK* zurückgegeben. Die Erfüllung

der Anforderungen gemäß § 17 SigG, Absatz 2 Satz 2 wird auf Seite 27 ff. in Verbindung mit den Angaben zur Algorithmen-Sicherheitseignung auf Seite 23 beschrieben.

§ 17 SigG, Abs. 2 Satz 3
"Signaturanwendungskomponenten müssen nach Bedarf auch den Inhalt der zu signierenden oder signierten Daten hinreichend erkennen lassen."

Diese Anforderung wird dadurch erfüllt, dass die zu signierenden Dateien gemäß Kapitel 3.3 mit der Sicheren Anzeige der *OpenLimit SignCubes Basiskomponenten Version 2.10* geöffnet und angezeigt werden können.

Erfüllte Anforderungen der Signaturverordnung
§ 15 SigV, Abs. 2 Satz 1
„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 […]“

Die *OpenLimit SignCubes Basiskomponenten Version 2.10* dürfen ausschließlich mit den in

Bezeichnung	**Registriernummer der Bestätigungs-ID**
STARCOS 3.4 Health QES C2 (Einzel-, M100- und Massensignaturkarte; Handelsnamen: *D-TRUST Card V3.0, DATEV Card V3.0, Signaturkarte der Bundesagentur für Arbeit (BA))*	BSI.02120.TE.05.2009 Nachtrag vom 15.11.2010
STARCOS 3.5 ID ECC C1 (Einzelsignaturkarte)	SRC.00013.TE.10.2012

Bezeichnung	Registriernummer der Bestätigungs-ID
STARCOS 3.5 ID ECC C1R (Einzel-, M100- und Massensignaturkarte; Handelsnamen: *Signtrust Card 3.5, Signtrust MCard 3.5, Signtrust MCard100 3.5, DGN sprintCard, sprintCard, DGN businessCard, businessCard, elektronischer Arztausweis, eA, eArztausweis, eHBA für Ärzte, elektronischer Zahnarztausweis, eZAA, eZahnarztausweis, eHBA für Zahnärzte, elektronischer Psychotherapeutenausweis, ePTA, eHBA für Psychotherapeuten, eHBA für psychologische Psychotherapeuten und Kinder- und Jugendlichenpsychotherapeuten, medisign Card, medisignCard, ZOD-Signaturkarte für Zahnärzte, ZOD-Karte, ZOD-Card, Bundesnotarkammer - Stapelsignaturkarte 100, Bundesnotarkammer – Multisignaturkarte*)	SRC.00021.TE.05.2013 Korrigendum 1 vom 14.11.2013 Nachtrag 1 vom 23.09.2013
STARCOS 3.5 ID GCC C1 (Einzelsignaturkarte; Handelsnamen: *nPA-Signaturkarte*)	SRC.00008.TE.12.2010
STARCOS 3.5 ID GCC C1R (Einzelsignaturkarte; Handelsnamen: *nPA-Signaturkarte*)	SRC.00014.TE.02.2012
STARCOS 3.5 ID GCC C2 (Einzelsignaturkarte; Handelsnamen: *nPA-Signaturkarte*)	SRC.00012.TE.05.2013
TCOS Identity Card Version 1.0 Release 1/SLE78CLX1440P (Einzelsignaturkarte; Handelsnamen: *nPA-Signaturkarte*)	SRC.00006.TE.11.2010
TCOS 3.0 Signature Card, Version 1.1 (Einzel- und Massensignaturkarte)	TUVIT.93146.TE.12.2006 Nachtrag 1 vom 07.05.2010
TCOS 3.0 Signature Card, Version 2.0 Release 1/ SLE78CLX1440P (Einzel- und Massensignaturkarte)	SRC.00016.TE.11.2012
ZKA Banking Signature Card, Version 7.1.2 (Einzelsignaturkarte)	TUVIT.93166.TU.06.2008 Nachtrag 1 vom 15.09.2009 Nachtrag 2 vom 28.12.2010
ZKA Banking Signature Card, Version 7.1.3 (Einzelsignaturkarte)	TUVIT.93171.TU.06.2010

Bezeichnung	Registriernummer der Bestätigungs-ID
ZKA Banking Signature Card, Version 7.1.4 (Einzelsignaturkarte)	TUVIT.93181.TU.09.2010 Nachtrag 1 vom 28.12.2010
ZKA Banking Signature Card, Version 7.2.1 (Einzelsignaturkarte)	TUVIT.93174.TU.06.2010 Nachtrag 1 vom 28.12.2010
ZKA Banking Signature Card, Version 7.2.2 (Einzelsignaturkarte)	TUVIT.93172.TU.06.2010
ZKA Banking Signature Card, Version 7.2.3 (Einzelsignaturkarte)	TUVIT.93182.TU.09.2010
ZKA SECCOS Sig v2.6.4 R1.1.2 (Einzelsignaturkarte)	SRC.00009.TE.09.2010
ZKA-Signaturkarte, Version 6.21 (Einzelsignaturkarte)	TUVIT.93174.TU.06.2010
ZKA-Signaturkarte, Version 6.22 (Einzelsignaturkarte)	TUVIT.93183.TU.11.2010
ZKA-Signaturkarte, Version 6.30 (Einzelsignaturkarte)	TUVIT.93170.TU.07.2010 Nachtrag 1 vom 22.07.2010
ZKA-Signaturkarte, Version 6.31 (Einzelsignaturkarte)	TUVIT.93175.TU.08.2010
ZKA-Signaturkarte, Version 6.32 (Einzelsignaturkarte)	TUVIT.93184.TU.11.2010
ZKA-Signaturkarte, Version 6.32 M (Massensignaturkarte)	TUVIT.93176.TU.05.2011

Tabelle 3 aufgeführten, SigG-bestätigten Sicheren Signaturerstellungseinheiten (SSEE) betrieben werden. Des Weiteren unterstützt das Produkt ausschließlich die in

Cherry KC 1000SC, JK-A01, FW-Version: 2.0.0, HW-Version: 1.0	BSI-DSZ-CC-0970

Tabelle 4 aufgeführten, SigG-bestätigten Kartenleser mit sicherer PIN-Eingabe.

Die Verarbeitung der für die Erzeugung einer qualifizierten elektronischen Signatur verwendeten Identifikationsdaten erfolgt in der IT-Umgebung des Produkts, daher ist diese Anforderung für das Produkt selbst nicht anwendbar.

Die Berechtigungsprüfung für die Erzeugung einer qualifizierten elektronischen Signatur wird durch die IT-Umgebung des Produkts durchgeführt (durch eine Sichere Signaturerstellungseinheit, mit der das Produkt kommuniziert), daher ist diese Anforderung für das Produkt selbst nicht anwendbar.

Die Signatur kann durch die Annahme an Besitz und Wissen auch nur durch die berechtigt signierende Person erfolgen. Das System implementiert keinerlei Mechanismen, welche die Zuführung der Identifikationsdaten an die Sichere Signaturerstellungseinheit ermöglichen.

Die *OpenLimit SignCubes Basiskomponenten Version 2.10* zeigen die Erzeugung qualifizierter elektronischer Signaturen in dem Signaturanforderungsdialog eindeutig an. Gleichzeitig wird dem Anwender angezeigt, auf welche Daten sich die elektronische Signatur bezieht und welche PIN zur Erzeugung der qualifizierten elektronischen Signatur verifiziert werden muss oder bereits verifiziert worden ist.

§ 15 SigV, Abs. 2 Satz 2
„Signaturanwendungskomponenten nach § 17 Abs. 2 des Signaturgesetzes müssen gewährleisten, dass […]
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 Zertifikatsverzeichnis zum angegebenen Zeitpunkt vorhanden und nicht gesperrt waren.“

Die Erfüllung dieser Anforderungen wird auf Seite 27 ff. in Verbindung mit den Angaben zur Algorithmen-Sicherheitseignung auf Seite 23 f. beschrieben.

§ 15 SigV, Abs. 4
„Sicherheitstechnische Veränderungen an Produkten für qualifizierte elektronische Signaturen nach den Absätzen 1 bis 3 müssen für den Nutzer erkennbar werden.“

Für die *OpenLimit SignCubes Basiskomponenten Version 2.10* stellt OpenLimit das *OpenLimit SignCubes Integrity Tool* über die URL https://www.openlimit.com/integritytool bereit.

Das *OpenLimit SignCubes Integrity Tool* überprüft die Hash-Werte an den installierten sicherheitsrelevanten Programmbibliotheken. Es wird festgestellt, ob sich die Programmbibliotheken noch in dem Zustand befinden, wie sie ursprünglich ausgeliefert und installiert wurden. Nach erfolgter Prüfung wird ein Prüfbericht erstellt.

5 Maßnahmen in der Einsatzumgebung

5.1 Einrichtung der IT-Komponenten

Für die *OpenLimit SignCubes Basiskomponenten Version 2.10* gelten die in der Benutzerdokumentation der *OpenLimit SignCubes Basiskomponenten Version 2.10* sowie die in der Installationsanleitung "Getting_Started_2_10.pdf" vorgegebenen Sicherheitsmaßnahmen.
Darüber hinaus ist der Anwender verpflichtet, mit den einstellbaren Optionen zur PIN-Eingabe sensibel und sorgsam umzugehen, um den Missbrauch der Signaturkarte zu verhindern. Insbesondere ist beim Verlassen des Arbeitsplatzes grundsätzlich die Signaturkarte aus dem Kartenleser zu entfernen.

Weiterhin muss der Anwender durch geeignete Art und Weise sicherstellen, dass nur er als Zertifikatsinhaber den Prozess der Signaturerzeugung anstoßen kann und keine andere Person physischen Zugriff auf den Rechner hat.
Die *OpenLimit SignCubes Basiskomponenten Version 2.10* dürfen ausschließlich innerhalb der in diesem Kapitel beschriebenen Hard- und Softwarevoraussetzungen und Konfigurationen eingesetzt werden.

5.2 Anbindung an ein Netzwerk

Als Einsatzumgebung der *OpenLimit SignCubes Basiskomponenten Version 2.10* ist der geschützte Einsatzbereich entsprechend den Vorgaben in der "Einheitlichen Spezifizierung der Einsatzbedingungen für Signaturanwendungskomponente, Version 1.5, Stand 11.11.2011, veröffentlicht unter www.bundesnetzagentur.de, vorgesehen. Das bedeutet, dass der Anwender durch Virenscanner und Firewall Vorkehrungen treffen muss, um potentielle Angriffe über das Internet bzw. über ein angeschlossenes Intranet abzuwehren. Ebenso muss durch geeignete Maßnahmen abgesichert werden, dass durch Unbefugte kein manueller Zugriff auf die Programm- und Dateiverzeichnisse ermöglicht wird, die für die *OpenLimit SignCubes Basiskomponenten Version 2.10* eingerichtet sind. Darüber hinaus ist abzusichern, dass kein Datenaustausch per Datenträger für diese Verzeichnisse durch Unbefugte erfolgen kann.

Der Anwender ist verpflichtet, die Integrität der Plattform sowie der eingesetzten zusätzlichen Softwareprodukte, wie Virenscanner und Firewall, sicherzustellen. Der Betreiber des Produktes trägt dafür Sorge, dass auf der Plattform regelmäßig Sicherheitsupdates installiert werden.

Die in diesem Abschnitt gemachten Auflagen müssen eingehalten werden.

5.3 Auslieferung und Installation

Die *OpenLimit SignCubes Basiskomponenten Version 2.10* werden vom Hersteller oder seinen Vertriebspartnern als Download oder auf CD ausgeliefert. Die CDs werden entweder per Post versendet oder persönlich übergeben.

Die Installation der OpenLimit SignCubes Basiskomponenten Version 2.10 erfolgt – abhängig von der erworbenen Lizenz - unter Verwendung eines der folgenden Installationspakete „*OL2801CCSign.exe*“, „*OL2801CCSignEE.exe*“ bzw. „*OL2801Reader.exe*“.

Der Installationsprozess ist in dem mitgelieferten Handbuch des Produkts „*Getting_Started_2_10.pdf*“ detailliert beschrieben. Das Auslieferungsverfahren des Produkts sowie das im „*Getting Started*” beschriebene Installationsverfahren sind zwingend einzuhalten.

5.4 Auflagen für den Betrieb des Produktes

Als Einsatzumgebung der *OpenLimit SignCubes Basiskomponenten Version 2.10* ist der geschützte Einsatzbereich entsprechend den Vorgaben in der "Einheitlichen Spezifizierung der Einsatzbedingungen für Signaturanwendungskomponente, Version 1.4, Stand 19.07.2005, veröffentlicht unter www.bundesnetzagentur.de, vorgesehen. Das bedeutet, dass der Anwender durch Virenscanner und Firewall Vorkehrungen treffen muss, um potentielle Angriffe über das Internet bzw. über ein angeschlossenes Intranet abzuwehren. Ebenso muss durch geeignete Maßnahmen abgesichert werden, dass kein manueller Zugriff und keine Datenaustausch per Datenträger durch Unbefugte erfolgen kann.

Die angewendeten organisatorischen Maßnahmen müssen sicherstellen, dass die Anforderungen des Signaturgesetzes und der Signaturverordnung sicher gestellt werden.

Da für die Signaturverifikation die Systemzeit verwendet wird, muss der Anwender sichern, dass die Systemzeit korrekt eingestellt ist.

Der Anwender ist verpflichtet, die Integrität der Plattform sowie der eingesetzten zusätzlichen Softwareprodukte, wie Virenscanner und Firewall, sicherzustellen. Der Betreiber des Produktes trägt dafür Sorge, dass auf der Plattform regelmäßig Sicherheitsupdates installiert werden.

Mit Auslieferung der *OpenLimit SignCubes Basiskomponenten Version 2.10* ist der Anwender auf die Einhaltung der oben genannten Einsatzbedingungen hinzuweisen.

6 Algorithmen und zugehörige Parameter

Die von den *OpenLimit SignCubes Basiskomponenten Version 2.10* technisch unterstützten Hash-Algorithmen samt dem zugehörigen Hinweis bzgl. der Verwendbarkeit im Bereich qualifizierter Signaturen sind in Tabelle 5 aufgeführt. Für die Verifikation qualifizierter elektronischer Signaturen werden von den *OpenLimit SignCubes Basiskomponenten Version 2.10* die folgenden Hash-Algorithmen unterstützt:

- SHA-224, SHA-256, SHA-384 und SHA-512

Die gemäß Anlage 1 Abs. 1 Nr. 2 SigV festgestellte Eignung für die verwendeten kryptografischen Algorithmen sind gemäß den im Bundesanzeiger (www.bundesanzeiger.de) unter "BAnz AT 14.04.2016 B11" veröffentlichten Angaben der Bundesnetzagentur vom 17.03.2016 wie folgt als geeignet eingestuft:

Algorithmus	Schlüssellänge	Gültig bis
SHA-224	-	Ende 2015
SHA-256	-	Ende 2022

Algorithmus	Schlüssellänge	Gültig bis
SHA-384	-	Ende 2022
SHA-512	-	Ende 2022
RSA	≥ 1976	Ende 2022
EC-DSA	q = 224	Ende 2015
EC-DSA	q ≥ 250, basierend auf Gruppen $E(F_p)$	Ende 2022
EC-DSA	q ≥ 250, basierend auf Gruppen $E(F_2^m)$	Ende 2022

Tabelle 6: Details zu den Algorithmen

Weitere Informationen zu den durch die *OpenLimit SignCubes Basiskomponenten Version 2.10* verwendeten Hashwerte sind in dem Abschnitt 3.10 beschrieben.

7 Gültigkeit der Herstellererklärung

Diese Erklärung ist bis zu ihrem Widerruf, längstens jedoch bis zum 31.12.2023 gültig. Die Gültigkeit der Herstellererklärung ist weiterhin beschränkt durch die im Kapitel 6 aufgeführten Gültigkeiten der Algorithmen. Die Gültigkeit kann sich verkürzen, wenn z.B. neue Feststellung hinsichtlich der Sicherheit des Produktes oder der Eignung der Algorithmen im Bundesanzeiger veröffentlicht werden.

Die Herstellererklärung kann durch die OpenLimit SignCubes GmbH oder die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahn als zuständige Behörde widerrufen werden.

Der aktuelle Status der Gültigkeit der Erklärung ist bei der zuständigen Behörde (Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahn, Referat Qualifizierte Elektronische Signatur - Technischer Betrieb) zu erfragen.

8 Zusatzdokumente

Folgende Bestandteile der Herstellererklärung wurden aus dem Veröffentlichungstext ausgegliedert und sind bei der zuständigen Behörde hinterlegt:

Bezeichnung des Dokumentes	Dateiname	Version	Datum	Seitenzahl
Getting Started OpenLimit CC Sign 2.10 (deutsch)	*OpenLimit_CCSign_Getting_Started_2.10.pdf*	1.0	22.04.2016	16

Bezeichnung des Dokumentes	Dateiname	Version	Datum	Seitenzahl
Getting Started OpenLimit CC Sign 2.10 (englisch)	*OpenLimit_CCSign_Getting_ Started_2.10_EN.pdf*	1.0	22.04.2016	16
Online Help (deutsch)	*deuOPENLiMiT SignCubes.chm*	1.0	22.04.2016	- [4] (3.191.633 B)
Online Help (englisch)	*engOPENLiMiT SignCubes.chm*	1.0	22.04.2016	- (2.500.164 B)
Testplan, *OpenLimit SignCubes Basiskomponenten Version 2.10*	*Test Plan OpenLimit Version 2_10.pdf*	1.0	06.03.2016	2701
Testreport, *OpenLimit SignCubes Basiskomponenten Version 2.10*	*Testreport_OL_2_10.pdf*	Version 2	27.04.2016	157

Tabelle 7: Zusatzdokumente

Ende der Herstellererklärung

[4] Die Online-Help-Dateien liegen lediglich in Form von „kompilierten HTML-Hilfedateien“ vor, die keine Seitenzahl haben, sodass hier anstelle dessen die Dateigröße in Byte angegeben wird.