**Herstellererklärung**

Die

intarsys consulting GmbH

Kriegsstraße 100

D – 76133 Karlsruhe

erklärt hiermit gemäß § 17 Abs. 4 Satz 2 SigG[1]
in Verbindung mit § 15 Abs. 5 Satz 1 SigV[2]
unter Berücksichtigung der Übersicht über geeignete Algorithmen[3], dass ihr Produkt

*Sign Live! CC 7.0*

die nachstehend genannten Anforderungen des SigG bzw. der SigV erfüllt.

Karlsruhe, den 5.12.2016

Karl Kagermeier

Geschäftsführer

Diese Herstellererklärung in Version 1.0 mit der Dokumentennummer IS-SIGNLIVECC-7.0 besteht aus 37 Seiten.

---

[1] Signaturgesetz vom 16. Mai 2001 (BGBl. I S. 876), das durch Artikel 4 Absatz 111 des Gesetzes vom 7. August 2013 (BGBl. I S. 3154) geändert worden ist

[2] Signaturverordnung vom 16. November 2001 (BGBl. I S. 3074), die durch Artikel 4 Absatz 112 des Gesetzes vom 7. August 2013 (BGBl. I S. 3154) geändert worden ist

[3] Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen) vom 9. Dezember 2015, veröffentlicht auf den Internetseiten des Bundesanzeigers www.bundesanzeiger.de unter BAnz AT 01.02.2016 B5

**Dokumentenhistorie**

| Version | Datum | Autor | Bemerkung |
|---|---|---|---|
| 1.0 | 5.12.2016 | Jörg Steinbach | Initial eingereichte Version |
| | | | |
| | | | |

**Inhalt**


| | | |
|---|---|---|
| 1 | HANDELSBEZEICHNUNG | 5 |
| 2 | LIEFERUMFANG UND VERSIONSINFORMATIONEN | 6 |
| 2.1 | INTARSYS ZERTIFIKATE | 6 |
| 2.2 | INTARSYS PRODUKTBESTANDTEILE | 6 |
| 2.3 | DRITTPRODUKTE | 7 |
| 3 | FUNKTIONSBESCHREIBUNG | 12 |
| 3.1 | ÜBERBLICK | 12 |
| 3.2 | AUFBAU DES PRODUKTES | 12 |
| 3.2.1 | COMMAND LINE INTERFACE (CLI) | 13 |
| 3.2.2 | PKCS#11 | 13 |
| 3.2.3 | ACTIVEX | 14 |
| 3.2.4 | HTTP | 14 |
| 3.2.5 | GRAPHICAL USER INTERFACE (GUI) | 14 |
| 3.2.6 | FILE SYSTEM | 14 |
| 3.2.7 | PC/SC DRIVER | 14 |
| 3.2.8 | TCP/IP | 14 |
| 3.2.9 | CLIENT API | 14 |
| 3.3 | SICHERHEITSFUNKTIONEN IM DETAIL | 15 |
| 3.3.1 | EINZELDOKUMENT VERTRAUENSWÜRDIG ANZEIGEN | 15 |
| 3.3.2 | DOKUMENTENSTAPEL VERTRAUENSWÜRDIG BEARBEITEN | 15 |
| 3.3.3 | SIGNATUR ERSTELLEN | 15 |
| 3.3.3.1 | Signaturverfahren *signIT smartcard CC* | 15 |
| 3.3.3.2 | Signaturverfahren *signIT multisign* | 16 |
| 3.3.4 | ZEITSTEMPEL ERSTELLEN | 16 |
| 3.3.5 | SIGNATUR VALIDIEREN | 16 |
| 3.3.5.1 | Integrität prüfen | 17 |
| 3.3.5.2 | Zertifikat prüfen | 17 |
| 3.3.5.3 | QES prüfen | 17 |
| 3.3.5.4 | Zeitstempel prüfen | 18 |
| 3.3.5.5 | Ergebnisdarstellung | 18 |
| 3.3.5.6 | Qualifizierte Zeitstempel | 22 |
| 3.3.6 | DOKUMENTE IN MASSENVERARBEITUNGSPROZESSEN BEARBEITEN | 22 |
| 3.3.7 | MANIPULATIONEN DES PRODUKTS ERKENNBAR MACHEN | 22 |
| 3.3.8 | SIGNATUR-PIN/PUK INITIALISIEREN, ÄNDERN UND ZURÜCKSETZEN | 23 |
| 4 | ERFÜLLTE ANFORDERUNGEN DES SIGG UND DER SIGV | 24 |
| 5 | MAßNAHMEN IN DER EINSATZUMGEBUNG | 28 |
| 5.1 | EINRICHTUNG DER IT-KOMPONENTEN | 28 |
| 5.1.1 | ALLGEMEINE IT-KOMPONENTEN | 28 |
| 5.1.1.1 | Hardware | 28 |
| 5.1.1.2 | Betriebssystem | 28 |
| 5.1.1.3 | Java Runtime Environment (JRE) | 29 |
| 5.1.2 | WEITERE IT-KOMPONENTEN | 29 |
| 5.1.2.1 | IT-Komponenten für das Signaturverfahren signIT smartcard CC | 29 |
| 5.1.2.2 | IT-Komponenten für das Signaturverfahren signIT multisign | 29 |
| 5.2 | ANBINDUNG AN EIN NETZWERK | 29 |
| 5.3 | AUSLIEFERUNG UND INSTALLATION | 29 |
| 5.3.1 | INSTALLATIONSASSISTENTEN | 29 |
| 5.3.2 | AUSLIEFERUNG UND INSTALLATION IM WARTUNGSFALL | 30 |
| 5.4 | AUFLAGEN FÜR DEN BETRIEB DES PRODUKTES | 31 |
| 5.4.1 | ALLGEMEINE AUFLAGEN | 31 |

5.4.2 AUFLAGEN BEI ERSTELLUNG VON QUALIFIZIERTEN ZEITSTEMPELN 32
5.4.3 AUFLAGEN BEI ERSTELLUNG VON MASSENSIGNATUREN 32
5.4.4 AUFLAGEN BEI VERWENDUNG DES SIGNATURVERFAHRENS SIGNIT SMARTCARD CC 33
5.4.5 AUFLAGEN BEI VERWENDUNG DES SIGNATURVERFAHRENS SIGNIT MULTISIGN 33
6 ALGORITHMEN UND ZUGEHÖRIGE PARAMETER 35
7 GÜLTIGKEIT DER HERSTELLERERKLÄRUNG 36
8 ZUSATZDOKUMENTATION 37

## 1 Handelsbezeichnung

| | |
|---|---|
| Handelsbezeichnung: | *Sign Live! CC 7.0* |
| Versionsnummer: | 7.0 |
| Auslieferung: | Das Produkt ist per CD direkt vom Hersteller oder einem seiner Vertriebspartner erhältlich oder kann über die Homepage der intarsys http://www.intarsys.de heruntergeladen werden. |
| Hersteller: | intarsys consulting GmbH<br>Kriegsstraße 100<br>D-76133 Karlsruhe<br>Handelsregister HRB 107535,<br>Amtsgericht Mannheim Abteilung B |

Im Folgenden wird das Produkt, auf das sich die Herstellererklärung bezieht nur noch als *das Produkt* bzw. *Sign Live! CC* bezeichnet. In Situationen, die Missverständnisse möglich machen, wird die vollständige Handelsbezeichnung verwendet.

## 2 Lieferumfang und Versionsinformationen

Die von intarsys bereitgestellten Produkte sind zur Integritätssicherung mit den zum intarsys Code bzw. Component Signing Zertifikat gehörigen Signaturschlüsseln signiert. intarsys trägt die Verantwortung für die sichere Verwendung der Signaturschlüssel, die Funktionalität und korrekte Auslieferung der intarsys Produkte. Somit ist gewährleistet, dass der Benutzer den Hersteller der Produktbestandteile und den Originalzustand eindeutig identifizieren kann.

Für die Funktionalität und korrekte Auslieferung der in den jeweiligen Szenarien erforderlichen Drittprodukte ist der jeweilige Hersteller verantwortlich.

### 2.1 intarsys Zertifikate

Die folgenden Zertifikate werden verwendet:

| | |
|---|---|
| **Code Signing** | für Installationsassistenten |
| Ausgestellt von: | GlobalSign Extended Validation CodeSigning CA - SHA256 - G2 |
| Serienummer: | `11 21 b2 55 cc 44 e2 4d 8f 9e 98 18 6d 96 8e 0a 67 cd` |
| Fingerabdruck (SHA-1): | `5e c9 99 a3 e0 0e ca 1d dd b3 9b 4b 85 fc bb 24 33 a6 ce 07` |
| **Component Signing** | für Produktbestandteile |
| Ausgestellt von: | Thawte Code Signing CA - G2 |
| Serienummer: | `75 88 7b 91 bd 53 0c 40 bc 35 97 4e 79 b8 6c` |
| Fingerabdruck (SHA-1): | `a6 93 ec 1b f9 af f7 05 bb 0d 83 94 27 c4 27 d9 a6 ba de ff` |

### 2.2 intarsys Produktbestandteile

| Produktbestandteile | Bezeichnung | Version |
|---|---|---|
| Installationsassistent Windows | Sign Live! CC<br>Sign Live! CC Sparkassen Edition<br>Sign Live! CC Telekom Edition | 7.0.0 |
| Installationspaket Mac OS X | Sign Live! CC für Mac OS X | 7.0.0 |
| Installationspaket Linux | Sign Live! CC für Linux | 7.0.0 |
| Integritätsprüfroutine | Sign Live! CC Installation Verifier | 4.1 |

*Tabelle 1 Lieferumfang und Versionsinformationen*

#### INSTALLATIONSASSISTENTEN/INSTALLATIONSPAKET SIGN LIVE! CC

Installationsassistenten werden jeweils in Varianten

- mit und ohne integrierter JRE und
- für 32- und für 64 bit-Betriebssysteme

ausgeliefert.

Die Installationsassistenten mit JRE installieren alle für den Betrieb des Produktes notwendigen Dateien. Die Installationsassistenten/-pakete ohne JRE beinhalten keine JRE. In diesen Fällen muss der Benutzer selbst für die korrekte Installation der JRE sorgen bzw. die JRE ist bereits vorinstalliert. Weitere Informationen zur zu verwendenden JRE sind in Kapitel 5.1.1.3 dokumentiert.

Die auf Basis der Installationsassistenten installierte Anwendung heißt bis auf die noch zu nennenden Ausnahmen *Sign Live! CC*.

Der Installationsassistent *Sign Live! CC Telekom Edition* unterscheidet sich vom Installationsassistenten *Sign Live! CC* dadurch, dass das Produkt *Sign Live! CC* mit Telekom-spezifischem Branding und eingeschränktem Funktionsumfang installiert wird. Die so installierte Anwendung heißt *Sign Live! CC Telekom Edition.*

Der Installationsassistent *Sign Live! CC Sparkassen-Edition* unterscheidet sich vom Installationsassistenten *Sign Live! CC* dadurch, dass das Produkt *Sign Live! CC* mit Sparkassen-spezifischem Branding und eingeschränktem Funktionsumfang installiert wird. Die so installierte Anwendung heißt *Sign Live! CC Sparkassen Edition.*

Im Installationsassistent enthalten sind unter anderen EULA, Readme, Releasenotes, Online-Dokumentation.

#### INSTALLATIONSPRÜFROUTINE SIGN LIVE! CC INSTALLATION VERIFIER

Mit Hilfe der Installationsprüfroutine prüft der Benutzer die Integrität der installierten Anwendung. Die Prüfroutine ist mit dem zum intarsys Component Signing Zertifikat gehörigen Signaturschlüssel signiert und ausschließlich auf der intarsys Homepage www.intarsys.de über eine SSL-gesicherte Verbindung erreichbar.

## 2.3 Drittprodukte

Das Produkt Sign Live! CC wird mit von Drittanbietern hergestellten Funktionsbibliotheken, Farbprofilen und Schriftarten ausgeliefert und benutzt diese. Dies sind:

| Bibliothek | Herausgeber |
|---|---|
| Apache Commons | Open Source |
| Apache CXF | Open Source |
| Apache Xalan | Open Source |
| Bouncycastle | Open Source |
| DejaVu Font Dateien | Open Source |
| Dom4j | Open Source |
| Eclipse Standard Widget Toolkit (SWT)/ JFace/Nebula | Open Source |
| exe4j | ej-technologies GmbH |
| Farbprofile | Adobe Systems Incorporated<br>Heidelberger Druckmaschinen AG<br>Hewlett Packard |
| Freetype Library | Open Source |
| Java Native Access (JNA) | Open Source |
| Java Runtime Environment (JRE) | Open Source |
| jPedal JBIG2 | Open Source |

| Bibliothek | Herausgeber |
|---|---|
| JLine | Open Source |
| Mozilla Rhino, JavaScript Interpreter | Open Source |
| tagsoup | Open Source |
| URW Schriftarten | URW++ Design & Development GmbH |

*Tabelle 2 Mit dem Produkt ausgelieferte und verwendete Funktionsbibliotheken, Farbprofile und Schriftarten*

Das Produkt Sign Live! CC nutzt die folgenden nach SigG bestätigten Produkte, die von Dritten hergestellt werden und nicht Bestandteil dieser Erklärung sind. Diese Drittprodukte werden in Abhängigkeit vom verwendeten Signaturverfahren eingesetzt.

#### SIGNATURVERFAHREN SIGNIT SMARTCARD CC

Bei Verwendung des Signaturverfahrens *signIT smartcard CC* muss eine Kombination aus Signaturkarte und Kartenleser der folgenden Tabellen eingesetzt werden.

| Herausgeber | Bezeichnung | Bestätigung |
|---|---|---|
| Deutscher Sparkassen Verlag GmbH (S-Trust) | Signaturerstellungseinheit<br>ZKA Banking Signature Card,<br>Version 7.1.3<br>Hersteller:<br>Giesecke und Devrient GmbH | TUVIT93171.TU.06.2010 |
| | Signaturerstellungseinheit<br>ZKA-Signaturkarte,<br>Version 6.32<br>Hersteller:<br>Giesecke und Devrient GmbH | TUVIT.93184.TU.11.2010<br>Nachtrag 1 12.11.2010<br>(19.05.2011)<br>Nachtrag 2 17.06.2013 |
| | Signaturerstellungseinheit<br>ZKA-Signaturkarte,<br>Version 6.32 M<br>Hersteller:<br>Giesecke und Devrient GmbH | TUVIT.93176.TU.05.2011<br>Nachtrag 1 17.06.2013 |
| Deutsches Gesundheits-netz Service GmbH<br>medisign GmbH | Signaturerstellungseinheit<br>STARCOS 3.2 QES Version 1.1<br>Hersteller:<br>Giesecke und Devrient GmbH | BSI.02102.TE.11.2008 |
| | Signaturerstellungseinheit<br>STARCOS 3.4 Health QES C1<br>Hersteller:<br>Giesecke und Devrient GmbH | BSI.02135.TE.08.2011 |
| DATEV eG<br>BNotK | Signaturerstellungseinheit<br>STARCOS 3.2 QES Version 2.0<br>Hersteller:<br>Giesecke und Devrient GmbH | BSI.02114.TE.12.2008<br>Nachtrag 1 08.03.2010 |

| Herausgeber | Bezeichnung | Bestätigung |
|---|---|---|
| | Signaturerstellungseinheit<br>STARCOS 3.5 ID ECC C1<br><br>Hersteller:<br>Giesecke und Devrient GmbH | SRC.00013.TE.10.2012 |
| D-TRUST GmbH<br><br>Swisscom AG<br><br>QuoVadis AG | Signaturerstellungseinheit<br>Chipkarte SLE66CX322P (oder SLE66CX642P), Software CardOS V4.3B Re_Cert with Application for Digital Signature<br><br>Hersteller:<br>Siemens AG | T-Systems.02182.TE.11.2006<br>Nachtrag 1 06.02.2007<br>Nachtrag 2 06.05.2008 |
| D-TRUST GmbH | Signaturerstellungseinheit<br>STARCOS 3.4 Health QES C1 und C2<br><br>Hersteller:<br>Siemens AG | BSI.<br>02120.TE.05.2009<br>Nachtrag 1<br>19.05.2009 |
| | Signaturerstellungseinheit<br>TCOS Identity Card Version 1.0 Release 1/SLE78CLX1440P | SRC.00006.TE.11.2010 |
| | Signaturerstellungseinheit<br>TCOS Identity Card<br>Version 1.0 Release 1/P5CD128/145<br><br>Hersteller:<br>T-Systems International GmbH | SRC.00007.TE.10.2010 |
| ZDA DTAG (Telesec) | Signaturerstellungseinheit<br>TCOS 3.0 Signature Card,<br>Version 1.0 with Philips chip P5CT072V0Q / P5CD036V0Q<br><br>Hersteller:<br>T-Systems Enterprise Services GmbH | TUVIT.93119.TE.09.2006 |
| | Signaturerstellungseinheit<br>TCOS 3.0 Signature Card,<br>Version 1.1<br><br>Hersteller:<br>T-Systems Enterprise Services GmbH | TUVIT.93146.TE.12.2006<br>Nachtrag 1 07.05.2010 |
| | Signaturerstellungseinheit<br>TCOS 3.0 Signature Card,<br>Version 2.0 Release 1/SLE78CLX1440P<br><br>Hersteller:<br>T-Systems Enterprise Services GmbH | SRC.<br>00016.TE.11.2012 |
| A-TRUST | Signaturerstellungseinheit<br>ACOS EMV-A04V1<br><br>Hersteller:<br>Austria Card Plastikkarten und Ausweissysteme GmbH | T-Systems.02166.TE.07.2008 |

*Tabelle 3 Zusätzliche bestätigte Produkte – Signaturkarten*

| Hersteller | Bezeichnung | Bestätigung |
|---|---|---|
| Cherry GmbH | Chipkartenterminal<br>Familie SmartBoard xx44<br>Firmware Version 1.04 | BSI.02048.TE.12.2004 |
| ZF Electronics GmbH | Chipkartenterminal<br>Familie SmartTerminal ST-2xxx<br>Firmware Version 5.11 | BSI.02095.TE.10.2007 |
| | Chipkartenterminal<br>Familie SmartTerminal ST-2xxx<br>Firmware Version 6.01 | BSI.02124.TE.09.2010<br>Nachtrag 1 02.11.2015 |
| Fujitsu | Chipkartenterminal<br>Familie SmartCase KB SCR eSIG<br>(S26381-K529-Vxxx)<br>Hardware Version HOS:01<br>Firmware Version 1.20 | BSI.02107.TE.03.2010<br>Nachtrag 1 04.02.2011 |
| KOBIL Systems GmbH | Chipkartenterminal<br>KAAN Advanced<br>Firmware Version 1.19 und<br>Hardware Version 1.04R3 | BSI.02050.TE.12.2006<br>Nachtrag 1 07.04.2008 |
| | KAAN<br>EMV-TriCAP Reader<br>(Artikel-Nr. HCPNCKS/A04,<br>Firmware-Version 82.23)<br>SecOVID Reader III<br>(Artikel-Nr. HCPNCKS/B07,<br>Firmware-Version 82.23)<br>TriB@nk<br>(Artikel-Nr. HCPNCKS/C08, Firmware-Version 79.23) | T-Systems.02246.TE.10.2010 |
| OMNIKEY GmbH | Chipkartenterminal<br>Familie CardMan Trust CM3621<br>Firmware Version 6.00 | BSI.02057.TE.12.2005 |
| | Chipkartenterminal<br>Familie CardMan Trust CM3821<br>Firmware Version 6.00 | |
| REINER Kartengeräte GmbH & Co. KG | Chipkartenterminal<br>cyberJack pin pad, Version 3.0 | TUVIT.93107.TU.11.2004 |
| | Chipkartenterminal<br>cyberJack e-com, Version 3.0 | TUVIT.93155.TE.09.2008 |
| | Chipkartenterminal<br>cyberJack e-com plus Version 3.0 | TUVIT.93156.TE.09.2008 |
| | Chipkartenterminal<br>cyberJack secoder Version 3.0 | TUVIT.93154.TE.09.2008 |
| | Chipkartenterminal<br>cyberJack RFID standard, Version 1.0<br>Nachtrag 1: Version 1.1 | TUVIT.93179.TU.12.2010<br>Nachtrag 1 vom 11.05.2011 |

| Hersteller | Bezeichnung | Bestätigung |
|---|---|---|
| | Chipkartenterminal<br>cyberJack RFID komfort, Version 1.0 | TUVIT.93187.TU.02.2011 |
| | Chipkartenterminal<br>cyberJack RFID standard, Version 1.2 | TUVIT.93188.TU.07.2011 |
| | Chipkartenterminal<br>cyberJack RFID komfort, Version 2.0 | TUVIT.93180.TU.12.2011 |
| SCM Microsystems GmbH | Chipkartenterminal<br>SPR532<br>Firmware Version 5.10 | BSI.02080.TE.10.2006 |
| | Chipkartenterminal<br>SPR332<br>Firmware Version 6.01 | BSI.02117.TE.02.2010 |

*Tabelle 4 Zusätzliche bestätigte Produkte - Kartenleser*

#### SIGNATURVERFAHREN SIGNIT MULTISIGN

Bei Verwendung des Signaturverfahrens *signIT multisign* muss ein Signaturserver laut folgender Tabelle eingesetzt werden. Dieses Verfahren ist nur unter den genannten Windows Betriebssystemen einsetzbar.

| Hersteller | Bezeichnung | Bestätigung/ Herstellererklärung |
|---|---|---|
| secunet Security Networks AG | multisign Enterprise, Version 4.1.4 | HE vom 01.12.2014 |

*Tabelle 5 Zusätzliche bestätigte/herstellererklärte Produkte – secunet multisign Enterprise*

# 3 Funktionsbeschreibung

## 3.1 Überblick

*Sign Live! CC* 7.0 ist gemäß SigG eine Signaturanwendungskomponente gemäß §2 Nr. 11 SigG. Das Produkt deckt die durch § 17 Abs. 2 SigG in Verbindung mit § 15 Abs. 2 und 4 SigV geforderte Funktionalität ab. Es ist in dieser Version nicht sicherheitsbestätigt, basiert jedoch auf dem nach den Common Criteria zertifizierten und vom Bundesamt für Sicherheit in der Informationstechnik sicherheitsbestätigten Produkt Sign Live! CC 3.2.3.

Das Produkt dient der Bearbeitung von elektronischen Dokumenten in verschiedenen Formaten, wie z. B. PDF, Text, TIFF und XML, mit besonderem Fokus auf elektronischen Signaturen. In diesem Kontext bietet es die folgenden Funktionen:

- vertrauenswürdige Anzeige von Dokumenten im Format PDF, Text, TIFF und XML
- Validierung von elektronischen Signaturen für ein einzelnes Dokument, einen Dokumentstapel oder im Massenvalidierungsverfahren
- Erzeugung von qualifizierten, elektronischen Signaturen für ein einzelnes Dokument, einen Dokumentstapel oder im Massensignaturverfahren

Zur Erstellung einer qualifizierten Signatur ist eine sichere Signaturerstellungseinheit in Form einer Signaturkarte erforderlich. Um den unterschiedlichen Durchsatzanforderungen gerecht zu werden, bietet das Produkt folgende Signaturverfahren, für das die Signaturkarten in unterschiedlicher Weise an das Produkt angebunden werden:

- Signaturverfahren *signIT smartcard CC*: Signaturkarten werden über Standard Kartenleser der Klasse II und III direkt an den Arbeitsplatzrechner angeschlossen.
- Signaturverfahren *signIT multisign*: Eine oder mehrere Signaturkarten werden über den secunet multisign Enterprise Signaturserver angeschlossen.

Zusätzlich ermöglicht das Produkt, qualifizierte Zeitstempel über einen externen Zeitstempelserver eines Zeitstempeldiensteanbieters anzufordern und zu validieren.

Das Produkt bietet weitere Signaturverfahren – z. B. auf Basis von Software-Zertifikaten und biometrischen Informationen –, die jedoch nicht zur Erstellung von qualifizierten elektronischen Signaturen geeignet sind.

Das Produkt ist gleichermaßen über die graphische Benutzeroberfläche wie auch per Kommandozeile bedienbar.

Das Produkt ist konzipiert als Java Applikation. Es ist lauffähig auf den in Kapitel 5.1.1.2 aufgeführten Betriebssystemen. Das Produkt ist in einem geschützten Einsatzbereich[4] einzusetzen.

Das Produkt ist in deutscher und englischer Sprache bedienbar.

## 3.2 Aufbau des Produktes

Abbildung 1 Sign Live! CC Schnittstellen gibt einen Überblick über den Aufbau des Produktes und seine Schnittstellen.

**Windows:** Sign Live! CC ist realisiert als eigenständige Java-Anwendung, die durch den integrierten Windows-Exe-Wrapper für den Benutzer wie eine Windows Anwendung per Kommandozeile bedienbar ist. Durch einen weiteren Windows-Exe-Wrapper kann die Anwendung auch als Windows-Dienst betrieben werden. In diesem Fall wird die

[4] Definition gemäß dem von der Bundesnetzagentur veröffentlichten Dokument „Einheitliche Spezifizierung der Einsatzbedingungen für Signaturanwendungskomponenten“ Version 1.5, Stand 11.11.2011 (http://www.bundesnetzagentur.de).

Anwendung über Standard Mechanismen des Betriebssystems gestartet und gestoppt. Kommandozeilenparameter sind in diesem Fall über eine Kommandodatei verwendbar.

**Mac OS X:** Sign Live! CC ist realisiert als eigenständige Java-Anwendung, die durch den integrierten Application-Wrapper gestartet und per Kommandozeile bedienbar ist.

**Linux:** Sign Live! CC ist realisiert als eigenständige Java-Anwendung, die durch das mitgelieferte Programm *./signlivecc* per Kommandozeile bedienbar ist.

Durch das integrierte Plug-in Konzept, kann die Anwendung durch sogenannte Instruments flexibel an individuelle Anforderungen angepasst werden. Über das von der intarsys Homepage herunterladbare Applet *Installation Verifier* (nicht Bestandteil der Abbildung) kann der Benutzer jederzeit prüfen, ob die Installation dem Standardumfang entspricht oder erweitert bzw. manipuliert wurde.

Das security API stellt Signatur- und Validierungsfunktionen zur Verfügung, die über die Protokolle CLI, ActiveX und http aufgerufen werden können.

In Kombination mit dem Produkt *Sign Live! CC remote signer* stellt *Sign Live! CC* Teilfunktionen der über das security API bereitgestellten Signatur und Validierungsfunktionen zur Verfügung, um diese z. B. in verteilten Anwendungen zu nutzen. Diese sind nicht Bestandteil dieser Herstellererklärung.

### 3.2.1 Command Line Interface (CLI)

Der Benutzer startet das Produkt über den Standardkommandozeilenaufruf ohne Optionen. Durch die Verwendung von Optionen kann der Benutzer das Produkt veranlassen, komplexe Operationen durchzuführen, wie z. B. das Öffnen einer Datei und den Anstoß des Signatur-Assistenten.

Die mit dem Produkt ausgelieferte Online-Dokumentation gibt Auskunft über die zur Verfügung stehenden Optionen. Für den Aufruf des Produktes mit korrekten Optionen ist der Benutzer verantwortlich. Um ungewollte Aufrufe zu verhindern, ist der Rechner durch eine geeignete Benutzeradministration abzusichern.

Rückgabewert eines Kommandozeilenaufrufs ist ein Integer.

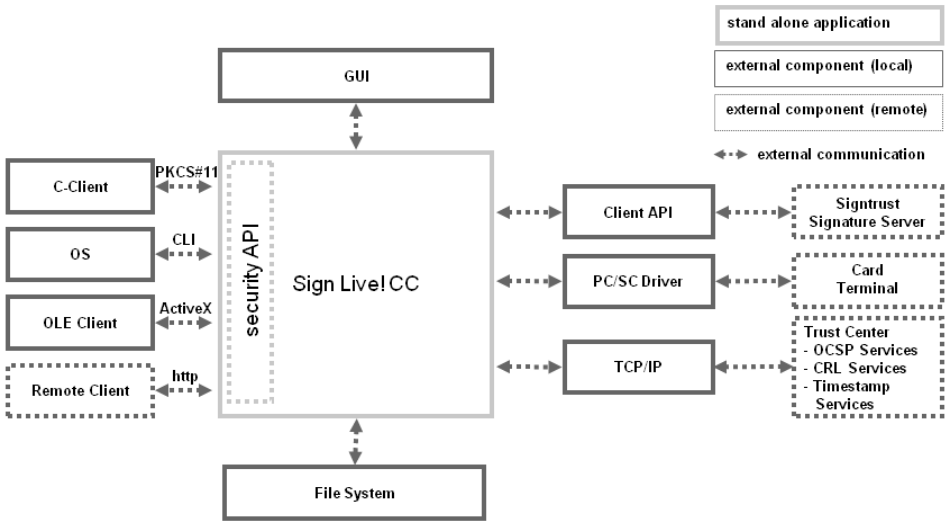


*Abbildung 1 Sign Live! CC Schnittstellen*

### 3.2.2 PKCS#11

Das Produkt bietet die Möglichkeit, auf Funktionen des security APIs via C-Aufruf gemäß PKCS#11 zuzugreifen. Die mit dem Produkt ausgelieferte Dokumentation und zugehörige

Beispiele geben Auskunft über die zur Verfügung stehenden Funktionen. Für den Aufruf des Produktes mit korrekten Optionen ist der Benutzer verantwortlich. Um ungewollte Aufrufe zu verhindern, ist der Rechner durch eine geeignete Benutzeradministration abzusichern.

### 3.2.3 ActiveX

Das Produkt bietet die Möglichkeit, auf Funktionen des security APIs via ActiveX zuzugreifen. Die mit dem Produkt ausgelieferte Dokumentation und zugehörige Beispiele geben Auskunft über die zur Verfügung stehenden Funktionen. Für den Aufruf des Produktes mit korrekten Optionen ist der Benutzer verantwortlich. Um ungewollte Aufrufe zu verhindern, ist der Rechner durch eine geeignete Benutzeradministration abzusichern.

### 3.2.4 http

Das Produkt bietet die Möglichkeit, auf Funktionen des security APIs via http zuzugreifen. Die mit dem Produkt ausgelieferte Dokumentation und zugehörige Beispiele geben Auskunft über die zur Verfügung stehenden Funktionen. Für den Aufruf des Produktes mit korrekten Optionen ist der Benutzer verantwortlich. Um ungewollte Aufrufe zu verhindern, ist der Rechner durch eine Firewall und geeignete Benutzeradministration abzusichern.

### 3.2.5 Graphical User Interface (GUI)

Das Produkt ist standardmäßig über seine graphische Benutzeroberfläche zu bedienen, die über die Graphikbibliotheken des Betriebssystems dargestellt wird. Über die Kommandozeile kann das Produkt dazu veranlasst werden, ohne graphische Oberfläche zu arbeiten.

### 3.2.6 File System

Zu verarbeitende Quelldateien liest das Produkt vom Dateisystem. Ergebnisdateien stellt das Produkt über das Dateisystem des Betriebssystems zur Verfügung. Um Manipulationen der Dateien während der Bearbeitung vorzubeugen, werden Dateien vollständig in den Speicher geladen.

### 3.2.7 PC/SC Driver

Das Produkt kommuniziert mit Kartenlesern/Signaturkarten über den PC/SC-Treiber des Betriebssystems. Das Produkt stellt sicher, dass die Verbindung zu einer Signaturkarte während der Nutzung durch das Produkt ausschließlich ist.

### 3.2.8 TCP/IP

Das Produkt kommuniziert mit externen Diensten (OCSP-, CRL-, Timestamp-Services) über die TCP/IP-Dienste des Betriebssystems. Das Verfahren ist sicher, da die erwarteten Ergebnisse signiert sind und die Signatur vom Produkt und anhand der mit dem Produkt ausgelieferten Zertifikate geprüft wird.

### 3.2.9 Client API

*Sign Live! CC* installiert und verwendet die zu der Signaturanwendungskomponente secunet multisign Enterprise gehörige Client API zur abgesicherten Kommunikation mit dem Signaturserver. Die Kommunikation zwischen *Sign Live! CC* und dem Client API erfolgt durch programminternen Aufruf. Das Client API selbst gewährleistet die sichere Übertragung der Daten. Zusätzlich sichert *Sign Live! CC* die Sicherheit der Übertragung, indem der übergebene Hashwert mit dem empfangenen, signierten Hashwert verglichen wird. Im Szenario mit *Sign Live! CC* übernimmt der Signaturserver die Rolle eines Kartenlesers.

## 3.3 Sicherheitsfunktionen im Detail

Im Folgenden werden die Sicherheitsfunktionen des Produktes detailliert erläutert. Die Erfüllung von SigG/SigV durch die Sicherheitsfunktionen ist in Kapitel 4 dargestellt.

### 3.3.1 Einzeldokument vertrauenswürdig anzeigen

Das Produkt bietet mit dem *Trusted Viewer* die Möglichkeit, Dokumente der Typen PDF, Text, TIFF, XML vertrauenswürdig und eindeutig anzuzeigen. XML Dateien werden ohne Umformung als Text dargestellt. Andere Dokumenttypen weist der *Trusted Viewer* als nicht darstellbar ab.

Der *Trusted Viewer* erlaubt zusätzlich die Analyse der angezeigten Dokumente. Er weist auf unbekannte, aktive und versteckte Inhalte hin.

### 3.3.2 Dokumentenstapel vertrauenswürdig bearbeiten

Das Produkt bietet über die integrierte Stapelverarbeitung die Möglichkeit, Dokumente zu einem Stapel zusammenzustellen, so dass Manipulationen an der Zusammenstellung des Stapels oder einzelner Dokumente, die während der Verarbeitung stattfinden, für den Benutzer erkennbar sind. Die Anwendung verarbeitet genau die Dokumente des Stapels. Somit ist die Begrenzung des Stapels hinsichtlich der Anzahl der Dokumente erfüllt.

Zusätzlich besteht die Möglichkeit, jedes Dokument des Stapels über den *Trusted Viewer* vor Verarbeitung zu inspizieren. Wenn der Benutzer dies nicht tut, ist er dazu angehalten, nur Dokumente zu verarbeiten, die den gleichen Zweck haben (z. B. elektronischer Rechnungsversand).

Der Ablauf der Signaturerstellung verhält sich wie unter 3.3.3 beschrieben.

### 3.3.3 Signatur erstellen

#### 3.3.3.1 Signaturverfahren *signIT smartcard CC*

Das Produkt bietet die Möglichkeit Einzel- und Stapelsignaturen mit Signaturkarten zu erstellen, die über einen direkt am Arbeitsplatzrechner angeschlossenen Kartenleser kontaktiert werden.

Vor Beginn des Signaturprozesses weist das Produkt den Benutzer eindeutig darauf hin, dass er im Begriff ist, eine qualifizierte Signatur zu erstellen. Das Produkt macht kenntlich, mit welcher Identität der Benutzer signiert und welche Daten er signiert.

Das Produkt ist zum Auslieferzeitpunkt so vorkonfiguriert, dass gültige Algorithmen zur Erstellung einer QES verwendet werden. Sollte dennoch – z. B. durch Umkonfigurieren des Benutzers – ein nicht mehr gültiger Algorithmus ausgewählt sein, weist das Produkt den Benutzer darauf hin. In diesem Fall erstellt das Produkt keine qualifizierte Signatur.

Die Anwendung kann folgende Signaturtypen erstellen:

- CAdES-BES, CAdES-EPES
- PAdES basic, PAdES-BES, PAdES-EPES
- XAdES (XMLDSig 1.0 mit RFC 4050 oder XMLDSig 1.1)

Die Erstellung der Signatur ist über die PIN Eingabe auf einem von der Bundesnetzagentur zugelassenen Klasse II oder Klasse III Leser zu autorisieren.

Bei der Erzeugung einer qualifizierten elektronischen Signatur ist die Verwendung dieser Leser sowie die Eingabe der PIN über die Tastatureinheit der Leser zwingend erforderlich. Die Anwendung hat keine Kenntnis der PIN und speichert diese nicht für eine spätere Verwendung zwischen.

Der Benutzer hat die Möglichkeit, die PIN auch über die Anwendung anzugeben, wird jedoch ausdrücklich darauf hingewiesen, dass dieses Vorgehen auf Grund der Vorgaben des SigG nicht für die Erstellung einer qualifizierten Signatur geeignet ist.

Um sicherzustellen, dass die SSEE die übergebenen Daten korrekt signiert hat, werden die signierten Daten entschlüsselt und der resultierende Hashwert mit dem zur Signatur übergebenen Hashwert verifiziert. Stellt das Produkt einen Fehler fest, wird der Benutzer mit einer Fehlermeldung per Oberfläche oder per Log in Kenntnis gesetzt.

#### 3.3.3.2 Signaturverfahren *signIT multisign*

Im Unterschied zum Verfahren *signIT smartcard CC* werden beim Verfahren *signIT multisign* eine oder mehrere Signaturkarten über den secunet multisign Enterprise Signaturserver angeschlossen. Die Signaturkarte(n) wird/werden auf dem Server durch PIN-Eingabe des Karteninhabers freigeschaltet. Für den Betrieb des Signaturservers sind dessen Einsatzvoraussetzungen zu berücksichtigen.

Am Arbeitsplatz prüft der Bearbeiter das oder die zu signierenden Dokumente und löst die Signatur durch die Eingabe von Zugangskennung/Kennwort aus. Der Signaturauslösende ist meistens nicht der Karteninhaber. Aus diesem Grund können nur zuvor vereinbarte, gleichartige Dokumente als Auftragsleistung signiert werden.

Um sicherzustellen, dass die SSEE die übergebenen Daten korrekt signiert hat und die Übertragung nicht manipuliert wurde, werden die signierten Daten entschlüsselt und der resultierende Hashwert mit dem zur Signatur übergebenen Hashwert verifiziert. Stellt das Produkt einen Fehler fest, wird der Benutzer mit einer Fehlermeldung per Oberfläche oder per Log in Kenntnis gesetzt.

Die Kommunikation zwischen Client und Server sichert die Client-Komponente des Signaturservers (Client-API) durch SSL und bereits zum Herstellzeitpunkt auf Client und Server verteilte Zertifikate (RSA-4096) ab. Das Produkt berücksichtigt sowohl die Client-Komponente als auch das Zertifikat in seiner Integritätsprüfung.

### 3.3.4 Zeitstempel erstellen

Das Produkt bietet die Möglichkeit, einen qualifizierten Zeitstempel gemäß § 2 Nr. 14 SigG eines Zertifizierungsdiensteanbieters anzufordern, zu prüfen und in eine QES zu integrieren. Dazu übermittelt das Produkt zunächst den Hashwert der erstellten Signatur per Time-Stamp Protocol (TSP gemäß RFC 3161) an den per Konfiguration ausgewählten ZDA. Anschließend prüft das Produkt die zurückgegebene, signierte Struktur hinsichtlich

- mathematischer Korrektheit,
- Übereinstimmung des gesendeten mit empfangenem Hashwert,
- Eignung des signierenden Zertifikats für die Zeitstempelerstellung und
- Gültigkeit der in der Zertifikatskette enthaltenen Zertifikate

Wenn die Struktur korrekt ist, wird sie in die QES integriert, andernfalls weist das Produkt den Benutzer mit einer Fehlermeldung auf die Situation hin.

Zusätzlich bietet das Produkt die Möglichkeit, die Zeitstempelinformation des ZDAs als separate Datei abzulegen.

### 3.3.5 Signatur validieren

Das Produkt bietet die Möglichkeit, Dokumente in Einzel- und Stapelverarbeitung zu validieren. Das Validierungsergebnis wird bei Einzelverarbeitung mit Hilfe der graphischen Benutzeroberfläche angezeigt. Optional kann ein Validierungsprotokoll als Dokument separat erstellt oder (nur bei PDF) an das validierte Dokument angehangen werden. Bei der Stapelverarbeitung wird das Validierungsergebnis als Sammelprotokoll dargestellt. Auch hier kann optional je Dokument zusätzlich ein Validierungsprotokoll erstellt werden.

Die Anwendung untersucht im Rahmen der Prüfung die folgenden Fragen:

- Wurden die signierten Daten seit dem Anbringen der Signatur verändert? (Integritätsprüfung)
- War das Zertifikat zum Zeitpunkt der Signaturerstellung gültig? (Zertifikatsprüfung)
- Handelt es sich um eine qualifizierte Signatur? (QES-Prüfung)

Die Ergebnisse der einzelnen Prüfroutinen ergänzen sich zu einem Gesamtergebnis. Das Produkt zeigt Gesamtergebnis und Einzelergebnisse dem Nutzer gemäß § 15 Abs. 2 Nr. 2 SigV zutreffend an.

#### 3.3.5.1 Integrität prüfen

Die Anwendung extrahiert und verifiziert den in der Signatur eines Dokuments enthaltenen Hashwert unter Anwendung des RSA Algorithmus sowie des im Signaturzertifikat enthaltenen öffentlichen Schlüssels. Dieser Hashwert wird mit dem Hashwert der signierten Daten verglichen, den das Produkt auf Basis eines der folgenden Algorithmen selbst ermittelt: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, RIPEMD-160. Bei Übereinstimmung der beiden Hashwerte ist die Integrität der signierten Daten sichergestellt.

#### 3.3.5.2 Zertifikat prüfen

Die Anwendung prüft, ob das Signaturzertifikat zum Referenzzeitpunkt - dem Zeitpunkt, zu dem die Signatur erstellt wurde - gültig war. Die Anwendung ermittelt den Referenzzeitpunkt abhängig von der Verfügbarkeit entsprechender Informationen, in der folgenden Reihenfolge:

1. Der Zeitpunkt, der im Zeitstempel der Signatur ausgewiesen ist. Sind mehrere Zeitstempel hinterlegt, so wird der erste gültige Zeitstempel verwendet.
2. Der Zeitpunkt, der in der Signatur-Datenstruktur dokumentiert ist.
3. Die aktuelle Systemzeit.

Für die Zertifikatsprüfung wird zunächst die Zertifikatskette zu einem vertrauenswürdigen Zertifikat ermittelt. Anschließend prüft die Anwendung jedes Zertifikat der Kette einzeln. Die Prüfung wird nach dem Kettenmodell durchgeführt. Jedes Zertifikat wird unter Verwendung lokal installierter Sperrlisten (CRL, Certificate Revocation List) oder OCSP-Antworten der OCSP-Dienste der Zertifikatsaussteller (Online Certificate Status Protocol) auf Sperrung gemäß § 8 SigG geprüft.

Das Produkt umfasst eine eigene Sperrlisten-Verwaltung. Werden bei der Prüfung abgelaufenen Sperrlisten verwendet, weist das Produkt den Benutzer darauf hin. Je nach Konfiguration aktualisiert das Produkt Sperrlisten selbstständig bzw. muss vom Benutzer dazu aufgefordert werden.

Falls dem Signaturzertifikat ein Attributzertifikat beigefügt ist, so wird auch dieses nach dem oben beschriebenen Verfahren geprüft.

#### 3.3.5.3 QES prüfen

Die Anwendung prüft, ob es sich um eine qualifizierte Signatur handelt. Dies ist gegeben, wenn die Signatur ausschließlich qualifizierte Signatur- und Attributzertifikate gemäß § 2 Nr. 7 SigG sowie qualifizierte Zeitstempel gemäß § 2 Nr. 14 SigG enthält. Ein Zertifikat wird als qualifiziertes Zertifikat ausgegeben, wenn die inhaltlichen Anforderungen an qualifizierte Zertifikate erfüllt sind sowie

- der ausstellende Zertifizierungsdiensteanbieter (ZDA) nach § 15 Abs. 1 SigG akkreditiert ist oder

- der ZDA die Ausstellung qualifizierter Zertifikate nach § 15 Abs. 1 SigG der zuständigen Behörde angezeigt hat.

Die Anwendung beinhaltet fest eingebaute Vertrauensanker der akkreditierten und angezeigten Zertifizierungsdiensteanbieter, die die o. g. Identifikation ermöglichen.

#### 3.3.5.4 Zeitstempel prüfen

Wenn die Signatur einen qualifizierten Zeitstempel gemäß § 2 Nr. 14 SigG enthält, prüft das Produkt diesen mit den gleichen Mechanismen, wie eine QES geprüft wird. Signierter Inhalt ist in diesem Fall der Hashwert der QES.

Zusätzlich prüft das Produkt, ob das Zertifikat, das den qualifizierten Zeitstempel erstellt hat, für die Erstellung von qualifizierten Zeitstempeln markiert ist.

#### 3.3.5.5 Ergebnisdarstellung

Die Prüfergebnisse lassen sich in drei verschiedenen Varianten darstellen:

- Verdichtete Darstellung
- Detail-Darstellung
- Verifikationsprotokoll

Verdichtete und Detail-Darstellung werden über das GUI dargestellt. Die Detail-Darstellung detailliert die verdichtete Darstellung für jeweils eine Signatur. Das Verifikationsprotokoll wird als PDF-Dokument erzeugt und kann somit über das GUI dargestellt und gespeichert werden.

Die in Kap. 4 beschriebenen Regeln zur Darstellung der Prüfungsergebnisse bzgl. abgelaufener Algorithmen werden berücksichtigt.

##### VERDICHTETE DARSTELLUNG

Die verdichtete Darstellung gibt Aufschluss über die wichtigsten Aspekte einer Signatur:

- Name/Pfad der externen Signaturdatei bzw. Kennzeichnung als interne Signatur
- Signaturtyp (Signatur / qualifizierte Signatur)
- Erzeuger der Signatur
- Zeitpunkt der Signaturerstellung
- Gesamtstatus der Signatur
- Status der Datenintegrität
- Status des Signaturzertifikats
- Status der Attributzertifikate (falls vorhanden)
- Status der Zeitstempel (falls vorhanden)

##### DETAIL-DARSTELLUNG

Die Detail-Darstellung des Prüfergebnisses ermöglicht eine genaue Inspektion aller Signaturdaten. Dies sind je Signatur:

- Verdichtete Darstellung der Signaturdaten
- Status zur Datenintegrität
    - Hash-Algorithmus
    - Berechneter / signierter Hashwert
    - Signaturalgorithmus

    - Signaturbytes (hexadezimal)
- Status des verwendeten Unterschriftszertifikats
    - Allgemeine Daten
        - Status
        - Prüfzeitpunkt
        - Bestandteile des X500-Namens
    - Details
        - Gültigkeitszeitraum
        - Inhaber
        - Aussteller
        - Signaturalgorithmus
        - Seriennummer
        - Version
        - Öffentlicher Schlüssel (hexadezimal)
    - Attribute
        - OID
        - Name
        - Wert
    - Erweiterungen
        - OID
        - Name
        - Wert
        - kritisch (ja / nein)
    - Zertifikatsrichtlinien
    - Status des Zertifizierungspfads
        - Status
        - Validierungsmodell
        - Status der einzelnen Zertifikate
    - Sperrlistenstatus / Onlinestatus
    - Qualifiziertes Zertifikat
        - Status
        - Richtlinie (Common PKI / Common PKI SigG)
        - Vertrauensbasis (Akkreditierter ZDA / Angezeigter ZDA / Ausländischer ZDA)
        - QC-Aussagen
- Status je verwendetem Attributzertifikat (falls vorhanden)
    - Darstellung analog zum Unterschriftszertifikat
- Status je Zeitstempel (falls vorhanden)

    - Allgemein
        - Status
        - Erzeugungszeit
        - Herausgeber
    - Details
        - Erzeugungszeit
        - Policy-Identifikation
        - Hash-Algorithmus und -Wert
        - Seriennummer
        - Chronologisch
        - Anfrageidentifikation (nonce)
        - Ausstellende Autorität
    - Erweiterungen
        - OID
        - Name
        - Wert
        - kritisch (ja / nein)
    - Status der Signaturintegrität
    - Details der Zeitstempelunterschrift
    - Qualifizierter Zeitstempel
        - Status
        - Richtlinie (COMMON PKI / COMMON PKI SigG)
- Qualifizierte Signatur
    - Status
    - Richtlinie (COMMON PKI / COMMON PKI SigG)

Des Weiteren werden je Prüfaspekt die angefallenen Hinweise, Warnungen und Fehlermeldungen tabellarisch dargestellt.

#### VERIFIKATIONSPROTOKOLL

Das Verifikationsprotokoll enthält die folgenden Informationen:

- Einstellungen für die Signaturvalidierung
    - COMMON PKI-Profil (Standard / SigG)
    - Akzeptanzregel für nicht qualifizierte Zertifikate
    - CRL-Prüfung aktiv / inaktiv
    - OCSP-Prüfung aktiv / inaktiv
- Dokumenteigenschaften
    - Dateiname
    - Dateigröße
    - Prüfzeitpunkt

- Eigenschaften der Signaturdatei (bei externen Signaturen)
    - Dateiname
    - Datum der letzten Änderung
    - Dateigröße
- Signaturdaten je Signatur
    - Verdichtetes Prüfergebnis
        - Gesamtstatus der Signatur
        - Status der Datenintegrität
        - Status des Signaturzertifikats
        - Status der Attributzertifikate (falls vorhanden)
        - Status der Zeitstempel (falls vorhanden)
    - Angaben zur Unterschrift
        - Signaturersteller
        - Signaturzeitpunkt
        - Begründung der Signaturerstellung
        - Ort der Signaturerstellung
        - Signierter Hashwert und verwendeter Algorithmus
    - Angaben zum verwendeten Unterschriftszertifikat
        - Inhaber
        - Attribute
        - Seriennummer
        - Aussteller
        - Hashwert und -algorithmus
        - Gültigkeitszeitraum
        - Form der Sperrprüfung (OCSP / CRL / keine)
        - Validierungsmethode (Kettenmodell / Schalenmodell)
    - Angaben je verwendetem Attributzertifikat (falls vorhanden)
        - Attribute
        - Seriennummer
        - Aussteller
        - Hashwert und -algorithmus
        - Gültigkeitszeitraum
        - Form der Sperrprüfung (OCSP / CRL / keine)
        - Validierungsmethode (Kettenmodell / Schalenmodell)
    - Angaben je Zeitstempel (falls vorhanden)
        - Erzeugungszeit
        - Seriennummer
        - Ersteller

- Hinweise zur Prüfung (falls Warnungen vorliegen)

#### 3.3.5.6 Qualifizierte Zeitstempel

Die Anwendung kann Daten mit einem Qualifizierten Zeitstempel nach §2 Nr. 14 SigG versehen und validiert diesen korrekt.

Die Anwendung ist in der vorliegenden Version nicht in der Lage, Eigenschaften von qualifiziert signierten Daten, die nach §17 SigV im Sinne einer Übersignatur signiert wurden, so darzustellen, dass erkennbar ist, dass die Übersignatur den Beweiswert der signierten Daten erhält.

### 3.3.6 Dokumente in Massenverarbeitungsprozessen bearbeiten

Das Produkt erlaubt die Definition von *Services*. Ein Service definiert eine Aufgabe, welche über die angegebenen Protokolle (CLI, ActiveX, http) oder den in das Produkt integrierten Verzeichnisüberwachungsmechanismus wiederholt aufrufbar ist.

Der Verzeichnisüberwachungsmechanismus überwacht ein Eingangs-Verzeichnis, führt gefundene Dateien der definierten Aufgabe zu und stellt Ergebnisdokumente im Ausgabeverzeichnis zur Verfügung.

Alle Aufrufe des *securityAPIs* sind als Aufgaben definierbar.

#### MASSENSIGNATUR

Das Produkt erlaubt die Definition von *Signaturpools*. Ein Signaturpool verwaltet 1-n Signaturkarten. Nach Start eines Signaturpools müssen die zugeordneten Signaturkarten durch Eingabe der jeweiligen PINs über den jeweiligen Kartenleser freigeschaltet werden. Das Produkt implementiert einen Dialog, der bei Freigabe des Signaturprozesses anzeigt:

- Mit welchem Zertifikat signiert wird und
- ob es sich um ein qualifiziertes Zertifikat handelt.

Nach der Freigabe steht der Signaturpool für Massensignaturprozesse zur Verfügung. Die über einen Signaturpool erstellbaren Signaturen können zeitlich und mengenmäßig eingeschränkt werden. Durch Stoppen des Signaturpools werden alle zugeordneten Signaturkarten geschlossen und stehen für Signaturanforderungen nicht zur Verfügung.

Durch Definition eines Signaturservices in Verbindung mit einem Signaturpool als Signatur Device sind kontinuierlich arbeitende Massensignaturprozesse abbildbar. Die eigentliche Erstellung der Signatur erfolgt wie bei der Einzelsignatur mit dem Unterschied, dass die optische Kontrolle jedes einzelnen Dokuments entfällt.

Aus diesem Grund muss der Benutzer die notwendige Sicherheit durch organisatorische Maßnahmen gewährleisten. Zudem dürfen nur gleichartige Dokumente verarbeitet werden.

Für das Szenario Massensignatur müssen Multisignatur-fähige SSEE eingesetzt werden.

#### MASSENVALIDIERUNG

Durch Definition eines Validierungsservices sind kontinuierlich arbeitende Massenvalidierungsprozesse abbildbar. Das Produkt erzeugt Validierungsergebnisse im Format XML und PDF.

### 3.3.7 Manipulationen des Produkts erkennbar machen

#### PRÜFUNG DER INTEGRITÄT

Über die Installationsprüfroutine prüft der Benutzer die Integrität der installierten Dateien. Hierzu wurden bei Erstellung der Installationsassistenten die auszuliefernden Dateien unter Verwendung der Algorithmen RSA und SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, RIPEMD-160 mit einer hierarchisch konstruierten Verzeichnissignatur versehen. Der Hashwert der Top-Level-Signatur identifiziert das Produkt eindeutig. Der Benutzer startet

die Installationsprüfroutine online, validiert die Verzeichnissignaturen und prüft den Top-Level-Hashwert. Dazu ist eine Internet-Verbindung notwendig.

#### PRÜFUNG DER KONFIGURATION

Das Produkt prüft selbstständig die aktuelle Konfiguration und zeigt dem Benutzer über den „Trusted Mode“ Indikator in der Statuszeile an, ob die Konfiguration für einen sicheren Betrieb geeignet ist.

### 3.3.8 Signatur-PIN/PUK initialisieren, ändern und zurücksetzen

Das Produkt assistiert den Benutzer beim Initialisieren der Signatur-PIN, bei Änderung der Signatur-PIN bzw. -PUK und beim Zurücksetzen der Signatur-PIN. Die sichere Eingabe der Signatur-PIN/-PUK wird durch die Verwendung von bestätigten/herstellererklärten Kartenlesern gewährleistet. Das Datenblatt listet die Hardware-/Betriebssystemkombinationen auf, bei deren Verwendung ausschließlich die sichere Eingabe der Signatur-PIN bzw. -PUK über den Kartenleser erfolgt.

## 4 Erfüllte Anforderungen des SigG und der SigV

Das Produkt erfüllt die nachfolgend aufgeführten Anforderungen des SigG bzw. SigV. Falls notwendig, werden nicht erfüllte Teilabsätze explizit ausgeschlossen.

| § 17 Abs. 2 SigG | abgedeckt durch |
|---|---|
| *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.* | **Einzel-/Stapelsignatur:**<br>Das Produkt implementiert einen Signaturassistenten, der bei Freigabe des Signaturprozesses anzeigt:<br>- Mit welchem Zertifikat signiert wird,<br>- ob es sich um ein qualifiziertes Zertifikat handelt und<br>- welche Daten signiert werden sollen.<br>( s. auch Kap. 3.3.3)<br>**Massensignatur:**<br>Das Produkt implementiert einen Dialog, der bei Freigabe des Signaturprozesses anzeigt:<br>- Mit welchem Zertifikat signiert wird und<br>- ob es sich um ein qualifiziertes Zertifikat handelt.<br>Durch organisatorische Maßnahmen ist sicherzustellen, dass nur gewünschte Dokumente signiert werden und dass diese von gleicher Art sind. |
| *Für die Überprüfung signierter Daten sind Signaturanwendungskomponenten erforderlich, die feststellen lassen,*<br>*1. auf welche Daten sich die Signatur bezieht,*<br>*2. ob die signierten Daten unverändert sind,*<br>*3. welchem Signaturschlüssel-Inhaber die Signatur zuzuordnen ist,*<br>*4. welche Inhalte das qualifizierte Zertifikat, auf dem die Signatur beruht, und zugehörige qualifizierte Attribut-Zertifikate aufweisen und*<br>*5. zu welchem Ergebnis die Nachprüfung von Zertifikaten nach § 5 Abs. 1 Satz 3 geführt hat.* | Das Produkt zeigt die Ergebnisse der Signaturvalidierung in folgenden Formen an:<br>- Anzeige im GUI in Detail- und verdichteter Ansicht<br>- Validierungsprotokoll in den Formaten HTML, PDF, XML<br><br>Folgende Informationen werden angezeigt:<br>- Auf welche Daten sich die Signatur bezieht (im GUI implizit durch das parallel angezeigte, signierte Dokument; im Protokoll durch Pfadangabe des signierten Dokuments),<br>- ob die Daten der Signatur und die signierten Daten unverändert sind,<br>- welchem Signaturschlüsselinhaber die Signatur zuzuordnen ist,<br>- die Inhalte des qualifizierten Zertifikats, auf dem die Signatur beruht, und evtl. vorhandener, zugehöriger qualifizierter Attributzertifikate und<br>- ob die verwendeten Zertifikate gültig und nicht gesperrt sind.<br>- der Zeitpunkt der Signatur – im Falle eines qualifizierten Zeitstempels, die durch den Zeitstempel signierte Zeitangabe<br><br>(s. auch Kap. 3.3.5) |
| *Signaturanwendungskomponenten* | Das Dokument implementiert eine vertrauenswürdige Ansicht (*Trusted Viewer*) für die |

| § 17 Abs. 2 SigG | abgedeckt durch |
|---|---|
| *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.* | Dokumentformate PDF, TIFF, Text (XML). Diese steht dem Benutzer für bereits signierte Dokumente wie auch vor dem Signaturprozess zur Verfügung.<br>**Einzelsignatur:**<br>Bei Verwendung des Trusted Viewers im Einzelsignaturprozess wird durch Anzeige des vollständig im Speicher gehaltenen Dokuments sichergestellt, dass das angezeigte Dokument mit dem signierten übereinstimmt.<br>**Stapelsignatur:**<br>Bei Verwendung des *Trusted Viewers* im Stapelsignaturprozess wird durch Berechnung der Hashwerte vor Anzeige und Prüfung dieser vor Beginn des Signaturprozesses sichergestellt, dass die angezeigten Dokumente mit den signierten übereinstimmen.<br>**Massensignatur:**<br>Im Massensignaturprozess ist durch organisatorische Maßnahmen sicherzustellen, dass ausschließlich gewünschte Dokumente signiert werden und dass diese von gleicher Art sind.<br><br>(s. auch Kap. 3.3.1 und Kap. 3.3.2) |

| § 15 Abs. 2 SigV | abgedeckt durch |
|---|---|
| *Signaturanwendungskomponenten nach §17 Abs. 2 des Signaturgesetzes müssen gewährleisten, dass*<br><br>*1. bei der Erzeugung einer qualifizierten elektronischen Signatur*<br><br>*a) die Identifikationsdaten nicht preisgegeben und diese nur auf der jeweiligen sicheren Signaturerstellungseinheit gespeichert werden,*<br><br>*b) eine Signatur nur durch die berechtigt signierende Person erfolgt,*<br><br>*c) die Erzeugung einer Signatur vorher eindeutig angezeigt wird und* | zu a) b)<br>Die Geheimhaltung des Signaturschlüssels wird durch den ausschließlichen Einsatz von sicheren Kartenlesern der Klasse II/III und SSEEen zur Erstellung von elektronischen, qualifizierten Signaturen sichergestellt.<br><br>Um die Anforderungen umzusetzen, implementiert das Produkt Funktionen, die sicherstellen, dass die eingegebene Signatur-PIN sich immer nur auf das (Einzelsignatur) oder die (Stapelsignatur) zuvor angezeigten / aufgelisteten / im Trusted Viewer geprüften Dateien bezieht. Änderungen an den Dateien, würde das Produkt kenntlich machen.<br><br>Im Falle der Massensignatur ist durch organisatorische Maßnahmen sicherzustellen, dass nach zeitlich oder mengenmäßig begrenzter Freigabe der SSEE, nur solche Dateien signiert werden, die signiert werden sollen, und dass alle zu signierenden Dateien einem gleichartigen Zweck dienen (s. auch Kap. 5.4.3).<br><br>zu c)<br>Das Produkt informiert den Benutzer im Signaturassistenten eindeutig, dass die Erzeugung einer Signatur initiiert bzw. ein qualifiziertes Zertifikat für den |

| § 15 Abs. 2 SigV | abgedeckt durch |
|---|---|
| | Massensignaturprozess freigeschaltet wird.<br><br>Hierzu zeigt der Signaturassistent/-dialog des Produktes an:<br>- Mit welchem Zertifikat signiert wird und<br>- ob es sich um ein qualifiziertes Zertifikat handelt.<br><br>Im Kontext der Massensignatur muss der Benutzer durch organisatorische Maßnahmen sicherstellen, dass dem Produkt nur solche Dokumente übergeben bzw. zur Verfügung gestellt werden, die tatsächlich signiert werden sollen und dass diese Dokumente alle einem gleichartigen Zweck dienen (s. auch Kap. 3.3.3 und Kap. 3.3.6). |
| *2. bei der Prüfung einer qualifizierten elektronischen Signatur*<br><br>*a) die Korrektheit der Signatur zuverlässig geprüft und zutreffend angezeigt wird und*<br><br>*b) eindeutig erkennbar wird, ob die nachgeprüften qualifizierten Zertifikate im jeweiligen Zertifikat-Verzeichnis zum angegebenen Zeitpunkt vorhanden und nicht gesperrt waren.* | s. Begründung zu § 17 Abs. 2 SigG Satz 2 |

| § 15 Abs. 4 SigV | abgedeckt durch |
|---|---|
| *Sicherheitstechnische Veränderungen an technischen Komponenten nach den Absätzen 1 bis 3 müssen für den Nutzer erkennbar werden.* | Die Anforderungen zum Erkennen sicherheitstechnischer Veränderungen an der SAK werden umgesetzt durch die hierarchische Signatur der zum Produkt gehörigen Dateien und programminterner Routinen zur Prüfung der sicheren Konfiguration des Produktes. Durch die Auflagen zum Betrieb des Produktes ist der Benutzer aufgefordert, die Signatur des Produktes und dessen sichere Konfiguration regelmäßig zu prüfen.<br><br>(s. Kap. 3.3.7 und Kap. 5.4) |

Das Produkt erfüllt die Anforderungen an schwach werdende Algorithmen und qualifizierte Zeitstempel wie folgt:

| Anforderungen | abgedeckt durch |
|---|---|
| a) Abgelaufene Algorithmen:<br>Die Prüfung einer Signatur durch eine Signaturanwendungskomponente (SAK) für qualifizierte elektronische Signaturen i.S.v. § 2 Nr. 11b SigG muss bei abgelaufenen Algorithmen für den Nutzer deutlich anzeigen, dass die geprüfte Signatur mit einem Algorithmus erzeugt wurde, der nicht mehr dem Stand der Wissenschaft und Technik entspricht, und | Die Darstellung der Validierungsergebnisse berücksichtigt folgende Regeln:<br><br>- Wenn die geprüfte Signatur auf einem Algorithmus basiert, der zum Erstellzeitpunkt der Signatur nicht mehr gültig war, gibt die Anwendung als Validierungsergebnis „nicht qualifiziert“ aus und weist den Benutzer darauf hin, seit wann die Verwendung des Algorithmus nicht mehr |

| Anforderungen | abgedeckt durch |
|---|---|
| sie somit einen verminderten Beweiswert hinsichtlich der Authentizität und Integrität des verbundenen Dokuments gegenüber dem Signaturzeitpunkt besitzt. Weiter sollte der Zeitpunkt, zu dem der Algorithmus seine Eignung verloren hat, zutreffend angezeigt werden.<br>Unspezifische Aussagen zu abgelaufenen Algorithmen sind nicht zulässig. | zulässig ist.<br>- Wenn die geprüfte Signatur auf einem Algorithmus basiert, der zwar zum Erstellzeitpunkt aber nicht zum Prüfzeitpunkt gültig ist, gibt die Anwendung als Validierungsergebnis „qualifiziert mit Warnungen“ aus, weist den Benutzer darauf hin, seit wann die Verwendung des Algorithmus nicht mehr zulässig ist und dass das Dokument somit nur einen verminderten Beweiswert hinsichtlich Authentizität und Integrität hat. |
| b) Nicht implementierte Algorithmen:<br>Ist bei der Prüfung einer Signatur ein Algorithmus zu verwenden, der in der Verifikationskomponente der SAK nicht implementiert ist, so muss dies dem Nutzer zutreffend angezeigt werden.<br>Unspezifische Aussagen zu nicht implementierten Algorithmen sind nicht zulässig. | Die Darstellung der Validierungsergebnisse berücksichtigt folgende Regeln:<br>- Wenn die geprüfte Signatur auf einem Algorithmus basiert, den die Anwendung nicht implementiert, gibt die Anwendung als Validierungsergebnis „unbekannt“ aus und weist den Benutzer mit der Meldung „Der verwendete Algorithmus ist nicht implementiert“ darauf hin. |
| c) Qualifizierte Zeitstempel:<br>Tragen Daten einer qualifizierten Signatur, bei deren Verifikation zu erkennen ist, dass der Signaturprüfschlüssel zu einem Zeitstempel-Zertifikat gehört, so ist dies dem Nutzer zutreffend anzuzeigen. Der Zeitpunkt, der im qualifizierten Zeitstempel enthalten ist, ist dem Nutzer ebenfalls darzulegen.<br>Solange kein standardisiertes Verfahren für die Einbindung von qualifizierten Zeitstempeln existiert, ist es ausreichend, wenn das Produkt seine selbst integrierten qualifizierten Zeitstempel auswerten kann. Qualifizierte Zeitstempel, die aus Fremdprodukten und damit in einer evtl. proprietären Datenstruktur vorliegen, müssen nicht zwingend durch das Produkt ausgewertet werden.<br>Unspezifische Aussagen zu qualifizierten Zeitstempeln sind nicht zulässig. | Das Produkt kann Daten mit einem Qualifizierten Zeitstempel nach §2 Nr. 14 SigG versehen und validiert diesen korrekt.<br>Die Anwendung ist in der vorliegenden Version nicht in der Lage, Eigenschaften von qualifiziert signierten Daten, die nach §17 SigV im Sinne einer Übersignatur signiert wurden, so darzustellen, dass erkennbar ist, dass die Übersignatur den Beweiswert der signierten Daten erhält. |

# 5 Maßnahmen in der Einsatzumgebung

## 5.1 Einrichtung der IT-Komponenten

Das Produkt darf ausschließlich innerhalb der im Folgenden beschriebenen Einsatzumgebung eingesetzt werden. Die allgemeinen IT-Komponenten werden immer vorausgesetzt, die weiteren IT-Komponenten sind abhängig vom verwendeten Signaturverfahren erforderlich.

### 5.1.1 Allgemeine IT-Komponenten

Die Einsatzumgebung muss den folgenden Anforderungen in jedem Einsatzszenario genügen.

#### 5.1.1.1 Hardware

**PROZESSOR**

Intel Pentium 1 GHz oder gleichwertiger Prozessor

**FREIER HAUPTSPEICHER**

Minimum 256 MB, empfohlen 512 MB

**FREIER FESTPLATTENSPEICHER**

Sign Live! CC mit JRE: ca. 250 MB,
zusätzlich ca. 150 MB zum Entpacken der Installationsdateien

**MONITORAUFLÖSUNG**

Minimum 800 x 600, empfohlen 1024 x 768

#### 5.1.1.2 Betriebssystem

**Windows**

- Windows 7
- Windows 8.1
- Windows 10
- Windows 2008, 2012 Server

**Linux**

- Cent OS 6
- Open Suse 12.3
- Suse Linux Enterprise Server 11
- Ubuntu 14.04, 16.04

**Mac OS X**

- Mac OS X 10.11, 10.12

Die folgenden VDI (Virtual Desktop Infrastructure) Kombinationen sind möglich:

- Windows 2008 Terminal Server mit Windows 7 Clients
- Windows 2008 Terminal Server mit Ubuntu 16.04 Clients

#### 5.1.1.3 Java Runtime Environment (JRE)

Die Anwendung benötigt eine JVM Version 1.8 Ein Java Runtime Environment (JRE) ist ausreichend. Wir empfehlen, den Installationsassistenten mit integrierter JRE zu verwenden und das integrierte JRE zu installieren.

Der Installation Verifier benötigt einen Browser mit integrierter JVM Version 1.5, 1.6, 1.7 oder 1.8.

### 5.1.2 Weitere IT-Komponenten

Abhängig vom verwendeten Signaturverfahren sind die folgenden IT-Komponenten erforderlich. Ausschließlich die genannten Signaturverfahren erlauben die Erstellung von QES.

#### 5.1.2.1 IT-Komponenten für das Signaturverfahren signIT smartcard CC

Bei Verwendung des Signaturverfahrens *signIT smartcard CC* muss die Einsatzumgebung zusätzlich folgenden Anforderungen genügen:

- Verwendet werden muss eine Signaturkarte gemäß Tabelle 3 Zusätzliche bestätigte Produkte – Signaturkarten. Der Benutzer muss die Auflagen der zugehörigen Sicherheitsbestätigung berücksichtigen.
- Verwendet werden muss ein Kartenleser gemäß Tabelle 4 Zusätzliche bestätigte Produkte - Kartenleser. Der Benutzer muss die Auflagen der zugehörigen Sicherheitsbestätigung berücksichtigen.

Die IT-Komponente für das Signaturverfahren *signIT smartcard CC* ist im Produkt enthalten. Enthaltene Funktionen werden über Lizenzschlüssel freigeschaltet.

#### 5.1.2.2 IT-Komponenten für das Signaturverfahren signIT multisign

Bei Verwendung des Signaturverfahrens *signIT multisign* muss die Einsatzumgebung keinen weiteren Anforderungen genügen, da die benötigte Komponente *Client API* durch den *Sign Live! CC* Installationsassistenten mitinstalliert wird und der Benutzer dessen Integrität durch den *Sign Live! CC Installation Verifier* überprüfen kann.

Die IT-Komponente für das Signaturverfahren *signIT multisign* ist im Produkt enthalten. Enthaltene Funktionen werden über Lizenzschlüssel freigeschaltet.

## 5.2 Anbindung an ein Netzwerk

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

Das Produkt darf nur in Verbindung mit einer Firewall an ein Netzwerk angeschlossen werden, so dass Angriffe aus dem Intra- oder Internet erkannt und verhindert werden können.

Das Produkt darf nur in Verbindung mit einem Virenscanner an ein Netzwerk angeschlossen werden, so dass auf dem Signaturrechner installierte, bösartige Programme erkannt werden können.

## 5.3 Auslieferung und Installation

### 5.3.1 Installationsassistenten

#### AUSLIEFERUNG

Die Installationsassistenten werden auf der intarsys Homepage zum Download angeboten oder per CD vom Hersteller selbst oder einem seiner Vertriebspartner ausgeliefert.

Die Installationsassistenten installieren alle für den Betrieb des Produktes notwendigen Dateien. Lediglich der Installationsassistent *Sign Live! CC ohne JRE* beinhaltet keine JRE. In diesem Fall muss der Benutzer selbst dafür sorgen, dass die JRE korrekt installiert ist.

Das installierte Produkt umfasst die Administrator- und Benutzeranleitung in Form einer Online-Dokumentation.

Ein Teil der in den Installationsassistenten enthaltenen Dateien wird zum besseren Zugriff für den Benutzer zusätzlich losgelöst auf CD oder im Web angeboten. Dazu gehören:

- readme (de/en)
- releasenotes (en)
- limitations (en)
- EULA (de/en)

#### INSTALLATION

Der Benutzer installiert das Produkt gemäß dem in der mitgelieferten readme Datei beschriebenen Verfahren. Es wird vorausgesetzt, dass der Benutzer entsprechende Voraussetzungen zur Bedienung eines Rechners besitzt.

Zusätzlich sind die im Kapitel 5.4 genannten Auflagen zu berücksichtigen.

#### SICHERHEIT DER AUSLIEFERUNG

**Windows:** Die Installationsassistenten sind mit dem zum intarsys Code Signing Zertifikat gehörigen Signaturschlüssel (s. Kapitel 2.1) signiert. Die Signatur ist mit Betriebssystem-mitteln prüfbar.

**Linux/Mac OS X:** Das Installationspaket ist nicht signiert. Jedoch wird auf der intarsys Homepage im zugehörigen Downloadeintrag der Hashwert des Pakets angezeigt. So kann der Benutzer prüfen, ob er ein nicht manipuliertes Installationspaket verwendet.

Alle installierten Produktbestandteile sind mit dem zum intarsys Component Signing Zertifikat gehörigen Signaturschlüssel (s. Kapitel 2.1) signiert. Die zugehörigen Hashwerte sind über **einen** hierarchisch konstruierten Hashwert prüfbar. Dieser ist mit Hilfe der Installationsprüfroutine prüfbar.

#### ÜBERPRÜFUNG DER INTEGRITÄT DER INSTALLATIONSASSISTENTEN

Der Benutzer ist angehalten, die Integrität des zu verwendenden Installationsassistenten/-pakets vor Installation zu prüfen. Die *readme* Datei des Produktes beschreibt das Vorgehen detailliert.

#### ÜBERPRÜFUNG DER INTEGRITÄT DES INSTALLIERTEN PRODUKTES

Der Benutzer ist angehalten, die Integrität der Installation mit Hilfe der Installationsprüf-routine nach Installation, nach Nachinstallation und zusätzlich in regelmäßigen Abständen zu prüfen. Die Online-Dokumentation des Produktes beschreibt das Vorgehen detailliert.

### 5.3.2 Auslieferung und Installation im Wartungsfall

Im Wartungsfall erhält der Benutzer vom Hersteller eine ZIP-Datei oder einen Installations-assistenten. Entweder kopiert er selbst oder der Installationsassistent die auszutauschen-den Dateien in die bestehende Installation. Nach abgeschlossenem Update soll der Be-nutzer in jedem Fall die Integrität der Installation prüfen wie unter Kapitel 5.3.1 beschrie-ben.

Bei einem solchen Update verliert diese Herstellererklärung ihre Gültigkeit.

## 5.4 Auflagen für den Betrieb des Produktes

Das Produkt ist in einem geschützten Einsatzbereich[5] einzusetzen.

Während des Betriebs sind die folgenden Auflagen für den sachgemäßen Einsatz zu beachten. Die allgemeinen Auflagen sind immer zu erfüllen, die weiteren nur bei Verwendung des entsprechenden Signaturverfahrens. Es muss eines der genannten Signaturverfahren eingesetzt werden. Andere mit dem Produkt verfügbare Signaturverfahren sind für die Erstellung qualifizierter elektronischer Signaturen nicht geeignet.

Wird eine der geforderten Auflagen nicht erfüllt, kann mit dem Produkt keine qualifizierte Signatur erstellt werden.

### 5.4.1 Allgemeine Auflagen

Die folgenden Auflagen sind immer zu erfüllen:

#### ZUGANGSKONTROLLE

Der Benutzer hat die vollständige Kontrolle über die im Rechner befindlichen Speichermedien.

Es ist nicht möglich, über existierende Netzwerkverbindungen auf *Sign Live! CC* – Verzeichnisse zuzugreifen, außer in der vom Benutzer beabsichtigten Weise. Dies sind:

- Installationsverzeichnis - Verzeichnis, in das Sign Live! CC installiert ist (<CABHOME>).
  Vorgabewert: C:\Programme\SignLive CC <Version>)
- Konfigurationsverzeichnis - Verzeichnis, in dem Sign Live! CC seine Konfigurationsdaten, Zertifikate und Sperrlisten ablegt (<CABPROFILE>).
  Vorgabewert: C:\Dokumente und Einstellungen\<Benutzername>\.SignLiveCC_<Version>
- Arbeitsverzeichnisse - alle Verzeichnisse, in denen Dateien für Signatur- und Validierungsprozesse zur Verfügung gestellt und verarbeitet werden.
  Vorgabewert: <CABPROFILE>\batch und alle zugehörigen Unterverzeichnisse.

Falls Sie ein Signaturverfahren ohne Benutzeroberfläche einsetzen, müssen Sie zusätzlich ausreichende Vorkehrungen treffen, die Arbeitsverzeichnisse der Anwendung gegen nicht autorisierte Manipulation zu schützen. Nur so sind Sie sicher, dass die zu signierenden Dateien zwischen kontrollierter Bereitstellung und Start des Signaturprozesses nicht unbemerkt manipuliert werden können.

#### PERSONAL

Benutzer und Administratoren der Anwendung müssen vertrauenswürdig sein. Sie kennen den Inhalt der zum Produkt gehörigen mit dem Produkt ausgelieferten Online-Dokumentation und berücksichtigen insbesondere die darin gegebenen Sicherheitshinweise. Andere Personen haben keinen Zugriff auf das System.

#### ALGORITHMEN

Benutzer und Administratoren der Anwendung sind angewiesen, mit Hilfe der Veröffentlichungen der Bundesnetzagentur regelmäßig zu prüfen, ob die verwendeten Algorithmen noch sicher sind. Ist dies nicht der Fall, soll der entsprechende Algorithmus nicht mehr verwendet werden

[5] Definition gemäß dem von der Bundesnetzagentur veröffentlichten Dokument „Einheitliche Spezifizierung der Einsatzbedingungen für Signaturanwendungskomponenten“ Version 1.5, Stand 11.11.2011 (http://www.bundesnetzagentur.de).

#### INTEGRITÄT DER INSTALLATION

Der Benutzer ist angewiesen, die Integrität des installierten Produkts regelmäßig zu überprüfen (s. auch Kapitel 5.3.1 Überprüfung der Integrität des installierten Produktes).

#### SICHERHEIT DER KONFIGURATION

Das Produkt prüft selbständig seine Konfiguration und zeigt dem Benutzer in der Statuszeile an, ob diese für einen sicheren Betrieb geeignet ist. Der Benutzer ist angewiesen, das Ergebnis zu berücksichtigen und die Konfiguration entsprechend anzupassen.

Durch die Gestaltung von *readme* Datei, Installationsassistent und Online-Dokumentation wird der Benutzer auf die Einhaltung der oben genannten Einsatzbedingungen hingewiesen.

#### ERSTELLUNG EIGENER STAPELVERARBEITUNGSDEFINITIONEN

Die Installationsprüfroutine der Anwendung kann die vom Benutzer selbst erstellten Stapelverarbeitungsdefinitionen nicht prüfen. Sobald der Benutzer solche verwendet, trägt er selbst die Verantwortung für die korrekte Verwendung dieser und die Prüfung auf Manipulationen.

#### VERWENDUNG API

Das API der Anwendung kann per Kommandozeile, ActiveX oder http verwendet werden. Die korrekte Erstellung der Aufrufe kann von der Anwendung nicht überwacht werden. Sobald der Benutzer solche Aufrufe verwendet, trägt er selbst die Verantwortung für die korrekte Erstellung dieser.

#### NETZANBINDUNG

Für das Herunterladen von Sperrlisten, Absetzen von OCSP-Anfragen und Zeitstempelanforderungen muss das Produkt eine IP-Verbindung zum entsprechenden Dienst aufbauen können.

### 5.4.2 Auflagen bei Erstellung von qualifizierten Zeitstempeln

Die folgenden Auflagen sind beim Erstellen von qualifizierten Zeitstempeln zu erfüllen.

#### AUFLAGEN DER DRITTPRODUKTE

Die durch den qualifizierten Zeitstempeldienst gegebenen Auflagen sind zu berücksichtigen.

#### NETZANBINDUNG

Für das Absetzen Zeitstempelanforderungen muss das Produkt eine IP-Verbindung zum entsprechenden Dienst aufbauen können.

### 5.4.3 Auflagen bei Erstellung von Massensignaturen

Die folgenden Auflagen sind beim Erstellen von Massensignaturen zu erfüllen. Massensignatur bezeichnet das Verfahren, durch einmalige PIN-Eingabe eine Signaturkarte für die Signatur von gleichartigen Dokumenten freizuschalten. Die Kontrolle, dass nur gewollte Signaturen erstellt werden, wird nicht durch individuelle Kontrolle jedes einzelnen, zu signierenden Dokuments gewährleistet, sondern durch einen dazu eingerichteten Prozess.

#### SCHUTZ GEGEN MANIPULATION DES SYSTEMS

Stellen Sie durch organisatorische bzw. technische Maßnahmen sicher, dass das Signatursystem nur von authorisiertem Personal konfiguriert und bedient wird.

#### DAUER DER SIGNATURSESSION

Eine sinnvolle Zeitdauer für eine Signatursession ist die Arbeitszeit des das System überwachenden Administrators, z. B. 8h.

#### KONTROLLE DER ZU VERARBEITENDEN DOKUMENTE

Stellen Sie durch organisatorische bzw. technische Maßnahmen sicher, dass nur solche Dokumente in das Eingangsverzeichnis gelangen, die tatsächlich signiert werden sollen. Dazu dienen z. B. Schreibrechte auf Dateisystemebene.

#### SIGNATURERSTELLUNG FÜR EINEN EINHEITLICHEN ZWECK

Erstellen Sie mit dem Massensignatur-Verfahren ausschließlich Signaturen für einen bestimmten Zweck - z. B. Rechnungssignatur. Verwenden Sie zur Signatur ein Attributzertifikat, welches diesen Zweck kenntlich macht.

#### MULTISIGNATUR-FÄHIGE SSEE

Zur Erstellung von Massensignaturen muss eine Multisignatur-fähige SSEE eingesetzt werden.

### 5.4.4 Auflagen bei Verwendung des Signaturverfahrens signIT smartcard CC

Die folgenden Auflagen sind zu erfüllen, wenn das Signaturverfahren *signIT smartcard CC* verwendet wird:

#### AUFLAGEN DER DRITTPRODUKTE

Die durch Kartenleser und Signaturkarte gegebenen Auflagen sind zu berücksichtigen.

#### UMGANG MIT DER SIGNATURKARTE

Die PIN für die Verwendung der Signaturkarte ist unbedingt vertraulich zu behandeln.

### 5.4.5 Auflagen bei Verwendung des Signaturverfahrens signIT multisign

Die folgenden Auflagen sind zu erfüllen, wenn das Signaturverfahren *signIT multisign* verwendet wird:

#### AUFLAGEN DER DRITTPRODUKTE

Stellen Sie sicher, dass im gehosteten Betrieb, die durch den secunet multisign Enterprise Signaturserver gegebenen Auflagen berücksichtigt werden.

#### VERFÜGBARKEIT DES SECUNET MULTISIGN SIGNATURSERVERS 4.1.4

Stellen Sie sicher, dass der secunet multisign Enterprise Signaturserver 4.1.4 von SLCC via Client API erreichbar ist.

Der secunet multisign Enterprise Signaturserver darf nur mit dem durch das Produkt installierte Client API kontaktiert werden. Andernfalls verliert diese Herstellererklärung ihre Gültigkeit.

#### KONFIGURATION DES SIGNATURSERVERS

Der Betreiber des secunet multisign Enterprise Signaturservers ist für die korrekte Konfiguration des Signaturservers verantwortlich.

#### UMGANG MIT DEM ZUGANGSKENNWORT

Die Authentifizierungsdaten für die Anmeldung an der zentralen Server-Komponente sind vertraulich zu behandeln.

## 6 Algorithmen und zugehörige Parameter

Das Produkt verwendet zum Erstellen und Prüfen qualifizierter Signaturen Hash-, Hashwert-Formatierungs- und Signatur-Algorithmen. Die folgenden Tabellen bezeichnen die verwendeten Algorithmen und geben an, bis wann diese Algorithmen laut Algorithmenkatalog der Bundesnetzagentur vom 9. Dezember 2015, veröffentlicht am 1. Februar 2016 als geeignet eingestuft werden.

Das Produkt beinhaltet alle zum Zeitpunkt der Veröffentlichung der Software von der BNetzA bekannt gegebenen, auch die zukünftig ablaufenden, Gültigkeitsbereiche der verwendeten Algorithmen. Diese Informationen werden folgendermaßen verwendet:

- Vor Erstellung einer Signatur weist die Software den Benutzer auf einen abgelaufenen Algorithmus hin.
- Bei Validierung einer Signatur:
  War der verwendete Algorithmus zum Zeitpunkt der Signaturerstellung abgelaufen, markiert die Software die Signatur als nicht gültig.
- Bei Validierung einer Signatur:
  Ist der verwendete Algorithmus zum Zeitpunkt der Validierung abgelaufen, weist die Software den Benutzer auf den verminderten Beweiswert der Signatur hin.

| Gültig bis | Erzeugung QES | Prüfung QES |
|---|---|---|
| abgelaufen | SHA-1, RIPEMD-160, SHA-224 | |
| Ende 2022 | SHA-256<br>SHA-384<br>SHA-512 | SHA-256<br>SHA-384<br>SHA-512 |

*Tabelle 6 Hash-Algorithmen und deren Eignung gemäß BNetzA*

| Gültig bis | Erzeugung QES | Prüfung QES |
|---|---|---|
| abgelaufen | RSA n<1976 bit<br>DSA-Elliptische Kurven q<250 bit | |
| Ende 2022 | RSA n>=1976 bit<br>DSA-Elliptische Kurven q>=250 bit | RSA n>=1976 bit<br>DSA-Elliptische Kurven q>=250 bit |

*Tabelle 7 Signatur-Algorithmen und deren Eignung gemäß BNetzA*

RSA: Für die Gewährleistung eines langfristigen Sicherheitsniveaus wird grundsätzlich die Erhöhung auf 2048 Bit empfohlen.

Der aktuell gültige Algorithmenkatalog sowie die jährlichen Aktualisierungen veröffentlicht die Bundesnetzagentur unter http://www.bundesnetzagentur.de .

## 7 Gültigkeit der Herstellererklärung

Diese Erklärung ist bis zu ihrem Widerruf, längstens jedoch bis zum 31.12.2022 gültig.

Die Gültigkeit der Herstellererklärung ist weiter beschränkt durch die in Kapitel 6 aufgeführten Gültigkeiten der Algorithmen; die Gültigkeit kann sich verkürzen, wenn z.B. neue Feststellungen hinsichtlich der Sicherheit des Produktes oder der Eignung der Algorithmen im Bundesanzeiger veröffentlicht werden.

Der aktuelle Status der Gültigkeit der Erklärung ist bei der zuständigen Behörde (Bundesnetzagentur, Referat Qualifizierte Elektronische Signatur – Technischer Betrieb) zu erfragen.

## 8 Zusatzdokumentation

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

1. Entwicklungsrichtlinien (Process Guide Version 1.3, 52 Seiten)
2. Testbeschreibung (Testing Guide Version 1.4, 48 Seiten)
3. Testpläne (Test Plan Design Report) zu der erklärten Version
   insgesamt 12 Testpläne für
   Sign Live! CC Linux Version 1.0
   Sign Live! CC Mac OS X Version 1.0
   Sign Live! CC Windows 7 Version 1.0
   Sign Live! CC Windows 8.1 Version 1.0
   Sign Live! CC Windows 10 Version 1.0
   Sign Live! CC Windows 2008 Server TS – Client Ubuntu Version 1.0
   Sign Live! CC Windows 2008 Server TS – Client Win 7 Version 1.0
   Sign Live! CC Windows 2012 Server Version 1.0
4. Testergebnisse zu der erklärten Version
   jeweils eine Testergebnistabelle je Testplan
   Erstellung: November 2016
5. Sign Live! CC Datenblatt 7.0 (Version 1.0, 22 Seiten)
6. Sign Live! CC Benutzerhandbuch 7.0 als PDF Export (Version 1.0)

Das Benutzer- und Administratorhandbuch wird als Online Dokumentation mit dem Produkt ausgeliefert. Releasenotes und Readme Datei ebenso.

Die in Kapitel 2.3 aufgeführten Drittprodukte sind Gegenstand der Testpläne und während des Produkttests erfolgreich getestet worden.

Das zu meldende Produkt Sign Live! CC 7.0 ist nicht sicherheitsbestätigt, basiert jedoch auf dem nach den Common Criteria zertifizierten und vom Bundesamt für Sicherheit in der Informationstechnik sicherheitsbestätigten Produkt Sign Live! CC 3.2.3. Der Hersteller bestätigt, dass das zu meldende Produkt unter Einhaltung der gleichen Entwicklungsrichtlinien produziert wird, wie das sicherheitsbestätigte Produkt. Die berücksichtigten Entwicklungsrichtlinien sind als Zusatzdokumentation (1) eingereicht.

---

Ende der Herstellererklärung