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 cloud suite 7.0

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

Karlsruhe, den 23.12.2016

Karl Kagermayer

Geschäftsführer

Diese Herstellererklärung in Version 1.0 mit der Dokumentennummer IS-SIGNLIVE_CS-7.0 besteht aus 27 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	Bermerkung
1.0	23.12.2016	Jörg Steinbach	Initial eingereichte Version

Inhalt

1 Handelsbezeichnung

Handelsbezeichnung:	*Sign Live! CC cloud suite* 7.0
Versionsnummer:	7.0
Auslieferung:	Der Hersteller liefert standardmäßig das Produkt per CD oder per Download von seiner Homepage http://www.intarsys.de direkt an den Lizenznehmer aus. Weitere Übertragungswege (E-Mail, FTP Download) sind individuell vereinbar. Das Produkt wird zusätzlich über autorisierte Vertriebspartner an Lizenznehmer ausgeliefert. Lizenznehmer stellen Teilkomponenten des Produktes für die tatsächliche Benutzung dem Anwender per HTTPS zur Verfügung.
Hersteller:	intarsys consulting GmbH Kriegsstraße 100 D-76133 Karlsruhe Handelsregister HRB 107535, Amtsgericht Mannheim

Im Folgenden wird das Produkt, auf das sich die Herstellererklärung bezieht nur noch als *das Produkt* bzw. *Sign Live! CC cloud suite* 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 dem zum intarsys Code Signing Zertifikat gehörigen Signaturschlüssel signiert. Somit ist gewährleistet, dass der Benutzer den Hersteller der Produktbestandteile und den Originalzustand eindeutig identifizieren kann. intarsys trägt die Verantwortung für die sichere Verwendung des Zertifikats und die Funktionalität und korrekte Auslieferung der intarsys Produkte.

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

2.1 intarsys Code Signing Zertifikat

Das intarsys Code Signing Zertifikat ist ein 2048 Bit Zertifikat:

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

2.2 intarsys Produktbestandteile

Produktbestandteile	Bezeichnung	Version
Installationspaket	SignLiveCloudSuite-7.0.0.zip	7.0.0
Signaturdatei	SignLiveCloudSuite-7.0.0.zip.p7s	7.0.0

Tabelle 1 Lieferumfang und Versionsinformationen

INSTALLATIONSPAKET SIGN LIVE CLOUD SUITE

Das Installationspaket umfasst

- die für den Betrieb notwendige Software
- weitere, optional nutzbare Software, um das Produkt in eine bestehende Anwendung zu integrieren
- das Entwicklerhandbuch (Developers Guide)
- Demo-Software

Die Software muss gemäß Entwicklerhandbuch in eine vorbereitete Umgebung installiert werden (s. hierzu Kapitel 5). Die so installierte Anwendung erscheint dem Anwender als *Sign Live! CC cloud suite 7.0.0*.

Es ist Aufgabe des Lizenznehmers, dem Anwender die notwendigen Informationen zur korrekten und sicheren Verwendung des Produkts zur Verfügung zu stellen.

2.3 Drittprodukte

Das Produkt *Sign Live! CC cloud suite* nutzt Funktionsbibliotheken und weitere nach SigG bestätigte/angezeigte Produkte, die von Dritten bzw. vom gleichen Hersteller hergestellt werden und nicht Bestandteil dieser Erklärung sind.

2.3.1 Funktionsbibliotheken

Bibliothek	Herausgeber
Apache Commons	Open Source
Bouncycastle	Open Source
Dom4j	Open Source
Java Native Access (JNA)	Open Source
Sign Live! CC security lib (Teil von SAK Sign Live! CC 7.0)	intarsys consulting GmbH

Tabelle 2 Mit dem Produkt ausgelieferte und verwendete Funktionsbibliotheken

2.3.2 Signaturanwendungskomponenten

Herausgeber	Bezeichnung	Bestätigung / Herstellererklärung
intarsys consulting GmbH	Signaturanwendungskomponente *Sign Live! CC* 7.0	Herstellererklärung

Tabelle 3 Zusätzliche Produkte – Signaturanwendungskomponenten

2.3.3 Sichere Signaturerstellungseinheiten (SSEE)

Eine Kombination aus SSEE und Kartenleser aus Tabelle 4 und Tabelle 5 muss eingesetzt werden.

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

Herausgeber	Bezeichnung	Bestätigung
	Hersteller: Giesecke und Devrient GmbH	
DATEV eG BNotK	Signaturerstellungseinheit STARCOS 3.2 QES Version 2.0 Hersteller: Giesecke und Devrient GmbH	BSI.02114.TE.12.2008 Nachtrag 1 08.03.2010
	Signaturerstellungseinheit STARCOS 3.5 ID ECC C1 Hersteller: Giesecke und Devrient GmbH	SRC.00013.TE.10.2012
D-TRUST GmbH Swisscom AG QuoVadis AG	Signaturerstellungseinheit Chipkarte SLE66CX322P (oder SLE66CX642P), Software CardOS V4.3B Re_Cert with Application for Digital Signature Hersteller: Siemens AG	T-Systems.02182.TE.11.2006 Nachtrag 1 06.02.2007 Nachtrag 2 06.05.2008
D-TRUST GmbH	Signaturerstellungseinheit STARCOS 3.4 Health QES C1 und C2 Hersteller: Siemens AG	BSI. 02120.TE.05.2009 Nachtrag 1 19.05.2009
	Signaturerstellungseinheit TCOS Identity Card Version 1.0 Release 1/SLE78CLX1440P	SRC.00006.TE.11.2010
	Signaturerstellungseinheit TCOS Identity Card Version 1.0 Release 1/P5CD128/145 Hersteller: T-Systems International GmbH	SRC.00007.TE.10.2010
ZDA DTAG (Telesec)	Signaturerstellungseinheit TCOS 3.0 Signature Card, Version 1.0 with Philips chip P5CT072V0Q / P5CD036V0Q Hersteller: T-Systems Enterprise Services GmbH	TUVIT.93119.TE.09.2006
	Signaturerstellungseinheit TCOS 3.0 Signature Card, Version 1.1 Hersteller: T-Systems Enterprise Services GmbH	TUVIT.93146.TE.12.2006 Nachtrag 1 07.05.2010
	Signaturerstellungseinheit TCOS 3.0 Signature Card, Version 2.0 Release 1/SLE78CLX1440P Hersteller: T-Systems Enterprise Services GmbH	SRC. 00016.TE.11.2012
A-TRUST	Signaturerstellungseinheit	T-Systems.02166.TE.07.2008

Herausgeber	Bezeichnung	Bestätigung
	ACOS EMV-A04V1 Hersteller: Austria Card Plastikkarten und Ausweissysteme GmbH	

Tabelle 4 Zusätzliche bestätigte Produkte – SSEE

2.3.4 Kartenleser

Eine Kombination aus SSEE und Kartenleser aus Tabelle 4 und Tabelle 5 muss eingesetzt werden.

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

Hersteller	Bezeichnung	Bestätigung
	Chipkartenterminal cyberJack e-com, Version 3.0	TUVIT.93155.TE.09.2008
	Chipkartenterminal cyberJack e-com plus Version 3.0	TUVIT.93156.TE.09.2008
	Chipkartenterminal cyberJack secoder Version 3.0	TUVIT.93154.TE.09.2008
	Chipkartenterminal cyberJack RFID standard, Version 1.0 Nachtrag 1: Version 1.1	TUVIT.93179.TU.12.2010 Nachtrag 1 vom 11.05.2011
	Chipkartenterminal cyberJack RFID komfort, Version 1.0	TUVIT.93187.TU.02.2011
	Chipkartenterminal cyberJack RFID standard, Version 1.2	TUVIT.93188.TU.07.2011
	Chipkartenterminal cyberJack RFID komfort, Version 2.0	TUVIT.93180.TU.12.2011
SCM Microsystems GmbH	Chipkartenterminal SPR532 Firmware Version 5.10	BSI.02080.TE.10.2006
	Chipkartenterminal SPR332 Firmware Version 6.01	BSI.02117.TE.02.2010

Tabelle 5 Zusätzliche bestätigte Produkte - Kartenleser

3 Funktionsbeschreibung

3.1 Überblick

Das Produkt *Sign Live! CC cloud suite* ist eine Signaturanwendungskomponente gemäß §2 Nr. 11a SigG. Es besteht aus Komponenten und APIs, die eine existierende Webanwendung um Sicherheitsfunktionen auf höchstem Sicherheitsniveau erweitern. Dazu deckt das Produkt die durch § 17 Abs. 2 Sätze 1 und 3 SigG in Verbindung mit § 15 Abs. 2 Nr 1 und Abs. 4 SigV geforderten Funktionen ab. Diese umfassen:

- Dokument sicher anzeigen oder zur sicheren Anzeige weiterleiten
- qualifizierte Signatur mit sicherer PIN-Eingabe erstellen
  als Einzel-, Stapel- oder Komfortsignatur
  in einem der folgenden Formate:
  CAdES-BES, CAdES-EPES,
  PAdES basic, PAdES-BES, PAdES-EPES,
  XAdES (XMLDSig 1.0 mit RFC 4050 oder XMLDSig 1.1)

Weitere bereitgestellte, nicht für diese Erklärung relevante Funktionen, sind:

- Benutzer mit Hilfe von Signaturkarten mit geeignetem Zertifikat sicher authentisieren
- Kartenstatus überwachen (Karte gesteckt/gezogen)
- PIN-Verwaltung
- Zugriff auf den neuen Personalausweis (nPa)

In den typischen Einsatzszenarien wird das Produkt im Kontext einer Webanwendung von einem zentralen Applikationsserver auf den Arbeitsplatzrechner geladen. Typischerweise liegen die zu signierenden Daten ebenfalls auf dem Server. Je nach Einsatzszenario wird lediglich der Hashwert der zu signierenden Daten oder das gesamte Dokument zur Signatur an die Signaturanwendungskomponente weitergeleitet. Die zur Erstellung der Signatur verwendete SSEE wird in den an den Arbeitsplatz des Mitarbeiters angeschlossenen Kartenleser gesteckt.

3.2 Aufbau des Produktes

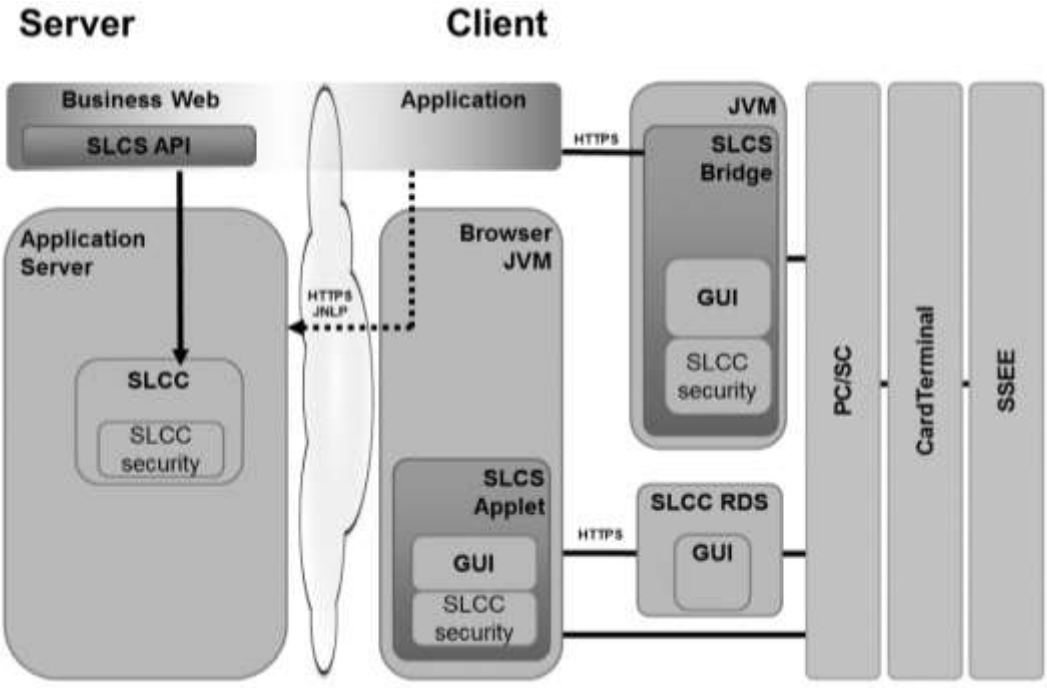

Abbildung 1 Sign Live! CC cloud suite

Abbildung 1 Sign Live! CC cloud suite gibt einen Überblick über den Aufbau des Produktes, seiner Teilkomponenten und seiner externen und internen Schnittstellen.

Das Produkt besteht aus Komponenten und APIs.

Die *Sign Live! CC cloud suite*-Komponenten sind als Java Applets (**SLCS Applet**) bzw. alternativ als Java Anwendung (**SLCS Bridge**) realisiert. Beide Komponententypen werden serverseitig in den Kontext eines Anwendungsservers (**Applicationserver**, z. B. Tomcat) installiert und von dort via JNLP auf den Client heruntergeladen. Der wesentliche Unterschied besteht darin, dass die Applets in einer vom Internet-Browser kontrollierten **Browser JVM** ablaufen und damit den Auswirkungen von Browser-Aktionen wie z. B. Seitenwechsel unterliegen, während die Bridge-Komponenten in einer eigenständigen **JVM** ablaufen. Die für die Erstellung einer qualifizierten Signatur relevanten Funktionen sind in einer Ausprägung der SLCS Applets, dem *Signaturapplet*, bzw. in der SLCS Bridge, der *Bridge Signaturkomponente*, realisiert. Beide Komponenten verwenden dazu die Sign Live! CC security lib (**SLCC security**).

Das *Sign Live!* ***Applet-API*** fasst die Konfigurationsmöglichkeiten der Applets zusammen, über die die Webanwendung die Applets ansteuert. Parallel bietet das *Sign Live!* **Bridge Client API** Zugriff auf die Bridge-Komponente.

Über das *Sign Live! CC cloud suite-API* (**SLCS-API**) kann die Webanwendung auf Funktionen der Signaturanwendungskomponente Sign Live! CC (**SLCC**) zugreifen, um z. B. Parameter für die Verwendung in den *Sign Live! CC cloud suite*-Komponenten aufbereiten zu können oder das Ergebnis des Signaturprozesses zu validieren.

Für den Betrieb der Lösung sind neben der fachlichen Webanwendung und deren Voraussetzungen geeignete Hardware mit geeigneten Betriebsmitteln, ein SigG-konformer Kartenleser (**CardTerminal**) und eine SigG-konforme, sichere Signaturerstellungseinheit (**SSEE**) notwendig. Die genauen Einsatzvoraussetzungen sind dem Kapitel 5 zu entnehmen.

Im Regelfall greifen die *Sign Live! CC cloud suite*-Komponenten direkt via PC/SC auf die SSEE zu. Für das Szenario Komfortsignatur[4] ist es notwendig, dass die Signaturkomponente über längere Zeit die Verbindung zur SSEE aufrechterhalten kann. Wegen möglicher Browser-Interaktionen kann das Signatur Applet dies nicht garantieren. Daher stellt in diesem Fall das Signaturapplet die Verbindung zur SSEE über die externe Komponente SLCC RDS her. SLCC RDS ist eine speziell konfigurierte Installation der Signaturanwendungskomponente *Sign Live! CC 7.0*, welche es erlaubt, außerhalb des Signaturapplets eine Verbindung zur SSEE via PC/SC aufzubauen und zu halten. Bei Einsatz der Bridge Signaturkomponente ist dies nicht notwendig.

Durch das Verwenden von HTTPS und einem eindeutigen Token, welches nur den Teilkomponenten Webanwendung/Bridge Signaturkomponente und Signaturapplet/SLCC RDS bekannt ist, ist sichergestellt, dass keine andere Komponente Kontakt zur SSEE aufbauen kann.

3.3 Externe Schnittstellen

Das Produkt hat die folgenden externen Schnittstellen:

[4] Komfortsignatur bezeichnet das Szenario, in dem für die erste Signatur analog zur Einzelsignatur die PIN auf dem Kartenleser eingegeben werden muss und alle weiteren Signaturen zwar angezeigt werden, aber ohne PIN-Eingabe erfolgen.

Die Signatursession wird beendet durch Ziehen der Karte, Ablauf eines definierbaren Zeitintervalls, Erreichen einer definierbaren Anzahl von Signaturen.

SCHNITTSTELLE WEBANWENDUNG – SIGNATURANWENDUNGSKOMPONENTE (CLOUDSUITE-API)

Über das CloudSuite-API hat die Webanwendung die Möglichkeit auf die Signaturanwendungskomponente *Sign Live! CC* zuzugreifen. Hierüber stehen z. B. Funktionen zur Berechnung von Hashwerten und Validierung von Signaturen zur Verfügung.

SCHNITTSTELLE WEBANWENDUNG – SIGNATURAPPLET (APPLET-API)

Das Signaturapplet wird als Java Applet oder über Java Web Start (JNLP) im Kontext einer Webanwendung gestartet. Die verfügbaren Parameter und Rückgabemechanismen werden als Applet-API bezeichnet.

SCHNITTSTELLE SIGNATURAPPLET –SLCC RDS

Das Signaturapplet kommuniziert via HTTPS mit Sign Live! CC remote device service (SLCC RDS), welches außerhalb des Signaturapplets die Verbindung zur gesteckten SSEE aufbaut und aufrechterhält.

SCHNITTSTELLE WEBANWENDUNG – BRIDGE (BRIDGE CLIENT-API)

Die Bridge Signaturkomponente wird als Java-Anwendung über Java Web Start (JNLP) im Kontext einer Webanwendung gestartet. Die verfügbaren Parameter und Rückgabemechanismen werden als Bridge Client-API bezeichnet. Die Kommunikation zwischen Webanwendung und Bridge Signaturkomponente erfolgt via HTTPS.

SCHNITTSTELLE BRIDGE – GRAPHISCHE BEDIENUNGSOBERFLÄCHE (GUI)

Über das GUI erfolgt die Kommunikation zwischen Anwender und der Bridge Signaturkomponente.

SCHNITTSTELLE BRIDGE – KARTENLESER (CARDTERMINAL)

Die Bridge Signaturkomponente kommuniziert via PC/SC über den Kartenleser mit der gesteckten SSEE.

3.4 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.

3.4.1 Signatur erstellen

Das Produkt bietet die Möglichkeit, im Kontext von fachlichen Web Anwendungen Einzel-, Stapel- und Komfortsignaturen mit einer SSEE zu erstellen, die über einen direkt am Arbeitsplatzrechner angeschlossenen Kartenleser kontaktiert wird.

Das Produkt erstellt im aktuellen Zustand keine automatischen Massensignaturen.

Das Produkt prüft im aktuellen Zustand keine Signaturen.

Signaturapplet: Einzel- und Stapelsignatur erstellen

Der Prozess zur Erstellung einer Signatur läuft grundsätzlich folgendermaßen ab:

Eine Webanwendung versorgt über das Applet-API das SLCS Signaturapplet mit Aufrufparametern und den zu signierenden Daten und startet es in der JVM eines Browsers am Client.

Das Signaturapplet weist den Anwender darauf hin, eine SSEE in den am Client angeschlossenen Kartenleser zu stecken und zeigt die Zertifikatsdaten der gesteckten SSEE an. So weist das Produkt den Anwender vor Beginn des Signaturprozesses eindeutig darauf hin, dass er im Begriff ist, eine qualifizierte Signatur zu erstellen. Das Produkt macht kenntlich, mit welcher Identität der Anwender signiert. Bei Bedarf kann sich

der Anwender die zu signierenden Daten anzeigen lassen. Dazu bietet das Signaturapplet *Trusted Viewer* für Dokumente vom Typ PDF, Text und XML an. Zusätzlich kann der Benutzer das Signaturapplet via GUI auffordert, die Daten zur Anzeige an die Anwendung weiterzuleiten, die im Browser dem Typ der Daten zugeordnet ist.

Sobald der Anwender den Signaturauftrag via GUI freigibt, berechnet das Signaturapplet den Hashwert des Dokuments bzw. übergibt den bereits berechneten Hashwert via PC/SC-Schnittstelle über den lokal angeschlossenen Kartenleser an die gesteckte SSEE. Diese signiert den Hashwert und meldet die signierten Daten zurück an das Signaturapplet, welches konfigurierbar eines der folgenden Signaturformate erstellt:

- 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 Kartenleser zu autorisieren.

Bei der Erzeugung einer qualifizierten elektronischen Signatur ist die Verwendung dieser Kartenleser sowie die Eingabe der PIN über die Tastatureinheit der Kartenleser zwingend erforderlich.

Komponenten des Produktes haben keine Kenntnis der PIN und speichern diese nicht für eine spätere Verwendung zwischen.

Um sicherzustellen, dass die SSEE tatsächlich die übergebenen Daten signiert hat, entschlüsselt das Signaturapplet die signierten Daten und verifiziert den resultierenden Hashwert mit dem zur Signatur übergebenen Hashwert. Stellt das Signaturapplet einen Fehler fest, informiert es den Anwender mit einer Fehlermeldung per Oberfläche.

Das Signaturapplet übergibt das Signaturergebnis zur Weiterverarbeitung an die Webanwendung.

Signaturapplet: Komfortsignatur erstellen

Die Komfortsignatur erlaubt es, nach erstmaliger Eingabe der Signatur-PIN solange Signaturprozesse durchführen zu lassen bis

- die SSEE gezogen wird,
- ein definierbares Zeitintervall abgelaufen ist,
- eine definierbare Anzahl von Signaturen erreicht ist.

Der Prozess zur Erstellung einer Komfortsignatur unterscheidet sich in folgenden Punkten vom Standardprozess:

- Steht die Komponente SLCC RDS zur Verfügung und ist eine Signaturkarte gesteckt, zeigt das Signaturapplet diese Komponente als mögliches Signaturgerät an.
- Wird dieses Signaturgerät ausgewählt, wird der erste Signaturauftrag analog zur Einzelsignatur an SLCC RDS übertragen. SLCC RDS zeigt die Identifikationsdaten des Signaturauftrags an. Der Kartenleser fordert zur Eingabe der Signatur-PIN auf. Nachdem der Benutzer die Signatur-PIN eingegeben hat, erfolgt der Signaturprozess analog zur Einzelsignatur mit dem Unterschied, dass die SSEE nach Abschluss der Signatur offen bleibt.
- Weitere Signaturprozesse erfolgen in gleicher Weise nach vorheriger Anzeige des Signaturauftrags, ohne dass die Signatur-PIN erneut eingegeben werden muss.
- Die SSEE wird geschlossen durch die o.g. Ereignisse. Danach muss für einen erneuten Signaturvorgang die Signatur-PIN erneut eingegeben werden.
- Es wird eine Multisignatur-taugliche SSEE eingesetzt.

Durch das Verwenden von HTTPS zwischen Signaturapplet und SLCC RDS und einem eindeutigen Token, welches nur den Teilkomponenten Signaturapplet und SLCC RDS bekannt ist, ist sichergestellt, dass keine andere Komponente Kontakt zur SSEE aufbauen kann.

Die Teilkomponenten Signaturapplet, SLCC RDS, Kartenleser und SSEE werden auf dem gleichen Rechner betrieben. SLCC RDS wird so konfiguriert, dass nur lokale Signaturanforderungen angenommen werden.

Beim Verlassen des Arbeitsplatzes muss der Benutzer die SSEE aus dem Signatursystem entfernen.

Bridge Signaturkomponente: Einzel- und Stapelsignatur erstellen

Der Prozess zur Erstellung einer Signatur mit der Bridge Signaturkomponente läuft grundsätzlich in der gleichen Weise ab wie im Szenario „Signaturapplet: Einzel- und Stapelsignatur erstellen“. Der Unterschied besteht darin, dass die Bridge Signaturkomponente nicht in der Browser-JVM sondern in einer separaten JVM gestartet wird und dass dadurch bedingt die Signaturaufforderung der Web-Anwendung nicht innerhalb des Browsers abläuft sondern zu der *externen* Bridge Signaturkomponente erfolgt. Die Sicherheit dieser Verbindung ist dadurch gewährleistet, dass HTTPS und zusätzlich ein eindeutiges Token verwendet wird, welches nur der Web Anwendung und der Bridge Signaturkomponente bekannt ist. Zudem werden Browser, Bridge Signaturkomponente, Kartenleser und SSEE auf dem gleichen Rechner betrieben. Die Bridge Signaturkomponente wird so konfiguriert, dass nur lokale Signaturanforderungen angenommen werden.

Bridge Signaturkomponente: Komfortsignatur erstellen

Da die Bridge Signaturkomponente selbstständig in der Lage ist, eine Verbindung über mehr als eine Signatur hinweg zur SSEE aufrechtzuerhalten, ist die Komponente SLCC RDS in diesem Szenario nicht notwendig. Lediglich der initiale Signaturaufruf an die Bridge Signaturkomponente muss so parametrisiert sein, dass die SSEE nach der Signatur offen bleibt. Weitere Signaturanforderungen werden dann ohne erneute Eingabe der PIN erfüllt solange, bis eine o. g. Ende-Bedingungen erfüllt ist.

3.4.2 Manipulationen des Produkts erkennbar machen

PRÜFUNG DES INSTALLATIONSPAKETS

Das Installationspaket ist mit dem zum intarsys Code Signing Zertifikat gehörigen Signaturschlüssel signiert. Die zugehörige Signaturdatei wird mit dem Installationspaket ausgeliefert. Der Administrator kann die Signatur prüfen mit einer handelsüblichen Signaturanwendungskomponente, z. B. *Sign Live! CC validate* (http://www.intarsys.de/produkte/sign-live/cc-validate).

PRÜFUNG DER INSTALLATION SERVERSEITIG

Die Integritätsprüfung der bestehenden Installation erfolgt über bitweisen Dateivergleich mit einem als integer geprüften und anschließend entpackten Installationspaket.

PRÜFUNG DER SIGNATURKOMPONENTE CLIENTSEITIG

Die *cloud suite*-Komponenten sind mit dem zum intarsys Code Signing Zertifikat gehörigen Signaturschlüssel signiert. Bei Start der Anwendung überprüft die Java-Laufzeitumgebung die Signatur und zeigt dem Anwender das Ergebnis der Prüfung und das Code Signing Zertifikat an. Somit kann sich der Anwender von der Authentizität und der Integrität der verwendeten Komponenten überzeugen.

Der Anwender erkennt über den Info-Dialog der *cloud suite*-Komponenten Name und Version der Komponente. Das Signaturapplet zeigt über den Kommunikationsstatus zusätzlich an, ob die umfassende HTML-Seite und Code-Basis des Applets via HTTPS geladen wurde.

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
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.*	Diese gesetzlichen Anforderungen werden folgendermaßen umgesetzt: Die *cloud suite*-Komponenten zeigen vor der Signatur Informationen an, die erkennen lassen, dass der Anwender im Begriff ist, eine qualifizierte Signatur zu erstellen, und welchem Signaturschlüssel-Inhaber die zu erstellende Signatur zuzuordnen ist. Bei Bedarf kann sich der Benutzer die Inhalte des Zertifikats detailliert anzeigen lassen. Die Webanwendung, in die die *cloud suite*-Komponente eingebettet ist, soll durch den Ablauf deutlich machen, auf welche Daten sich die zu erstellende Signatur bezieht. Bei Bedarf kann sich der Benutzer vor Erstellung der Signatur die zu signierenden Daten vollständig anzeigen lassen. Dazu verwendet der Benutzer entweder die zur *cloud suite*-Komponente gehörigen *Trusted Viewer* für die Datentypen PDF, Text und XML oder fordert die *cloud suite*-Komponente auf, die Daten der Anwendung zur Anzeige zu übergeben, die der Browser/das Betriebssystem, in dem die *cloud suite*-Komponente betrieben wird, dem Datentyp zuordnet.
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.*	Das Produkt implementiert die Funktion zur Überprüfung signierter Dateien nicht.
Satz 3 *Signaturanwendungskomponenten müssen nach Bedarf auch den Inhalt der zu signierenden oder signierten Daten*	Diese gesetzlichen Anforderungen werden folgendermaßen umgesetzt: Die Webanwendung, in die *cloud suite*-Komponente eingebettet ist, soll durch den

§ 17 Abs. 2 SigG	abgedeckt durch
hinreichend erkennen lassen. Die Signaturschlüssel-Inhaber sollen solche Signaturanwendungskomponenten einsetzen oder andere geeignete Maßnahmen zur Sicherheit qualifizierter elektronischer Signaturen treffen.	Ablauf deutlich machen, auf welche Daten sich die zu erstellende Signatur bezieht. Bei Bedarf kann sich der Benutzer vor Erstellung der Signatur die zu signierenden Daten vollständig anzeigen lassen. Dazu verwendet der Benutzer entweder die zur *cloud suite*-Komponente gehörigen *Trusted Viewer* für die Datentypen PDF, Text und XML oder fordert die *cloud suite*-Komponente auf, die Daten der Anwendung zur Anzeige zu übergeben, die der Browser/das Betriebssystem, in dem die *cloud suite*-Komponente betrieben wird, dem Datentyp zuordnet.

§ 15 Abs. 2 SigV	abgedeckt durch
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 und*	zu a) Die Geheimhaltung des Signaturschlüssels wird durch den ausschließlichen Einsatz von sicheren Kartenlesern der Klasse II/III und SSEE zur Erstellung von elektronischen, qualifizierten Signaturen sichergestellt. zu b) Die Webanwendung, die mit der *cloud suite*-Komponente kommuniziert, und die *cloud suite*-Komponente selbst führen den Benutzer via GUI in der Form, dass er zur Erstellung einer qualifizierten, elektronischen Signatur die Signatur-PIN über einen sicheren Kartenleser der Klasse II/III eingibt. Die Webanwendung, die mit der *cloud suite*-Komponente kommuniziert, die *cloud suite*-Komponente selbst und deren Kommunikation untereinander sind so konzipiert, dass jeder Signierende ausschließlich die Daten signiert, die ihm zuvor angezeigt wurden. Der Umfang der Daten kann weder erweitert noch vermindert werden. Dies bezieht sich sowohl auf Einzel- wie auch auf Stapelsignaturen. Im Falle der Komfortsignatur (die einmalige Eingabe einer PIN öffnet die SSEE für eine Signatursession, in der mehrere Signaturvorgänge durchgeführt werden) sorgen die Sicherheitsmechanismen der Bridge Signaturkomponente bzw. der Teilkomponente SLCC RDS dafür, dass ausschließlich Signaturaufträge, die zuvor dem Benutzer angezeigt wurden, durchgeführt werden. Der Benutzer kann durch Ziehen der SSEE die Signatursession beenden. Zusätzlich endet die Signatursession automatisch bei Erreichen einer zuvor definierten Signaturanzahl oder eines zuvor definierten Zeitintervalls.

§ 15 Abs. 2 SigV	abgedeckt durch
	zu c) Die Webanwendung, die mit der *cloud suite*-Komponente kommuniziert, und die *cloud suite*-Komponente selbst informieren den Benutzer eindeutig, dass die Erzeugung einer Signatur initiiert wird. (s. auch Kap. 3.4.1)
2. bei der Prüfung einer qualifizierten elektronischen Signatur *a) die Korrektheit der Signatur zuverlässig geprüft und zutreffend angezeigt wird und* *b) eindeutig erkennbar wird, ob die nachgeprüften qualifizierten Zertifikate im jeweiligen Zertifikat-Verzeichnis zum angegebenen Zeitpunkt vorhanden und nicht gesperrt waren.*	Das Produkt implementiert die Funktion zur Überprüfung signierter Dateien nicht.

§ 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 Signaturanwendungskomponente werden umgesetzt durch - eine durch den Administrator zu prüfende Signatur des Installationspakets (vor der Installation) - einen durch den Administrator durchzuführenden, bitweisen Dateivergleich mit einem vertrauenswürdig entpackten Installationspaket (nach erfolgter Installation in regelmäßigen Abständen) - die durch den Benutzer durchzuführende Signatur-Prüfung der via JNLP geladenen Komponenten während des Betriebs Die Auflagen zum Betrieb des Produktes weisen auf diese Maßnahmen hin.

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

Anforderungen	abgedeckt durch
a) Abgelaufene Algorithmen: 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	Das Produkt umfasst keine Funktion zur Validierung von qualifizierten Signaturen und muss daher keine Prüfergebnisse darstellen und damit auch keine Aussagen zu abgelaufenen Algorithmen treffen.

Anforderungen	abgedeckt durch
Wissenschaft und Technik entspricht, und 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. Unspezifische Aussagen zu abgelaufenen Algorithmen sind nicht zulässig.	
b) Nicht implementierte Algorithmen: 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. Unspezifische Aussagen zu nicht implementierten Algorithmen sind nicht zulässig.	Das Produkt umfasst keine Funktion zur Validierung von qualifizierten Signaturen und muss daher keine Prüfergebnisse darstellen und damit auch keine Aussagen zu nicht implementierten Algorithmen treffen.
c) Qualifizierte Zeitstempel: 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. 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. Unspezifische Aussagen zu qualifizierten Zeitstempeln sind nicht zulässig.	Das Produkt kann bei entsprechender Konfiguration Daten mit einem Qualifizierten Zeitstempel nach §2 Nr. 14 SigG versehen, führt jedoch keine Validierung des Zeitstempels durch. 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 wird in eine Webanwendung integriert. Serverseitig wird es unter einem J2EE-konformen Anwendungsserver gehostet, clientseitig in einer durch einen Webbrowser (Signaturapplet) bzw. einer separaten JVM (Bridge Signaturkomponente) betrieben. Die jeweiligen Einsatzumgebungen für Server und Client müssen den nachfolgend beschriebenen Anforderungen genügen.

5.1.1 Einsatzumgebung Server

5.1.1.1 Anwendungsserver (J2EE)

Die *cloud suite*-Komponenten benötigen serverseitig einen J2EE-konformen Anwendungsserver. Getestet wurde das Produkt mit Tomcat 7.0 unter Windows 2008 Server.

Hardware und Betriebssystemanforderungen sind vom gewählten Anwendungsserver und der darin betriebenen Webanwendung abzuleiten.

5.1.1.2 Signaturanwendungskomponente Sign Live! CC

Soll das CloudSuite-API verwendet werden, benötigt die Webanwendung Zugriff auf die Signaturanwendungskomponente *Sign Live! CC* 7.0 in der Form, dass deren Code in den Prozessraum des Anwendungsserver geladen werden kann. Der Benutzer muss die Auflagen der zugehörigen Sicherheitsbestätigung/Herstellererklärung und die Installationshinweise des *Sign Live! CC cloud suite* Entwicklerhandbuchs berücksichtigen.

5.1.1.3 Java Runtime Environment (JRE)

Soll das CloudSuite-API verwendet werden, muss der Anwendungsserver mit einer JVM Version 1.7 oder 1.8 betrieben werden. Eine Java-Ablaufumgebung (JRE) ist ausreichend.

5.1.2 Einsatzumgebung Client

5.1.2.1 Hardware

PROZESSOR

Intel Pentium 1 GHz oder gleichwertiger Prozessor

FREIER HAUPTSPEICHER

Minimum 256 MB, empfohlen 512 MB

FREIER FESTPLATTENSPEICHER

25 MB notwendig

MONITORAUFLÖSUNG

Minimum 1024 x 768

5.1.2.2 Betriebssystem

Windows

- Windows 7
- Windows 8.1

- Windows 10

Linux

- Ubuntu 14.04, 16.04

Mac OS X

- Mac OS X 10.11, 10.12

5.1.2.3 Internet-Browser mit Java-Ablaufumgebung

Die Anwendung benötigt einen Internetbrowser mit integrierter Java-Ablaufumgebung (JRE) 1.8.0. Getestet wurden die folgenden Kombinationen:

- unter Linux (1.8.0_45):
  Firefox 50
- unter Mac OS X 10.10 (1.8.0_45):
  Firefox 50, Safari 8.0
- unter Mac OS X 10.11 (1.8.0_45):
  Firefox 50, Safari 9.0
- unter Windows (1.8.0_45):
  Firefox 50, Internet Explorer 10, 11

5.1.2.4 SSEE / Kartenleser

Zur Erstellung von qualifizierten Signaturen benötigt das Produkt einen an den Client-Rechner angeschlossenen Kartenleser gemäß Tabelle 5 Zusätzliche bestätigte Produkte - Kartenleser und eine SSEE gemäß Tabelle 4 Zusätzliche bestätigte Produkte – SSEE. Der Benutzer muss die Auflagen der zugehörigen Sicherheitsbestätigungen berücksichtigen.

5.1.2.5 Anwendungen zur Darstellung der zu signierenden Daten

Die zur Darstellung der zu signierenden Daten notwendigen Anwendungen müssen auf dem Client installiert und im verwendeten Browser/Betriebssystem für den jeweiligen Datentyp registriert sein.

5.1.2.6 Signaturanwendungskomponente Sign Live! CC remote device service

Falls der Benutzer Komfortsignaturen mit dem Signaturapplet erstellt (1 PIN-Eingabe für mehrere Signaturprozesse), muss die Signaturanwendungskomponente *Sign Live! CC* in der in Tabelle 3 angegebenen Version auf dem gleichen Rechner installiert werden, auf dem das Signaturapplet in Betrieb ist. Die SAK *Sign Live! CC* muss so konfiguriert werden, wie in der Anwenderdokumentation des Produktes *Sign Live! CC cloud suite* beschrieben. Zusätzlich muss der Benutzer die Auflagen der Herstellererklärung SAK *Sign Live! CC* berücksichtigen.

Zudem muss der Benutzer eine massensignaturfähige SSEE verwenden.

5.2 Anbindung an ein Netzwerk

Für den Betrieb des Produktes sind Client und Server in der Regel über Netzwerk verbunden. Um zu gewährleisten, dass Server und Client nur für berechtigtes Personal erreichbar sind, sind die folgenden Auflagen zu berücksichtigen:

- Netzwerkverbindungen müssen durch die Installieren und geeignetes Konfigurieren einer Firewall und organisatorische Maßnahmen so abgesichert sein, dass Angriffe unterbunden bzw. erkannt werden.

- Das Produkt darf nur in Verbindung mit einem aktiven Virenscanner an ein Netzwerk angeschlossen werden, so dass auf dem Signaturrechner installierte, bösartige Programme erkannt werden können.
- Zugriffe vom Client auf den Server haben in gesicherter Form per HTTPS zu erfolgen. Der Betreiber muss mit Hilfe der im Entwicklerhandbuch gegebenen Informationen beurteilen, welche Form der Client-Authentisierung für das Einsatzszenario sinnvoll und notwendig ist.

Die in diesem Abschnitt gemachten Auflagen müssen eingehalten werden.

5.3 Auslieferung und Installation

5.3.1 Auslieferung

Das Produkt wird als Installationspaket im Format ZIP ausgeliefert. Es ist mit dem zum intarsys Code Signing Zertifikat gehörigen Signaturschlüssel (s. Kapitel 2.1) signiert. Der Hersteller liefert das Installationspaket dem Lizenznehmer per CD oder über die intarsys Homepage (http://www.intarsys.de) aus. Zusätzlich können Vertriebspartner der intarsys das Produkt in der gleichen Form ausliefern. Weitere Übertragungswege sind individuell vereinbar.

Das Installationspaket umfasst das Entwicklerhandbuch im Format PDF und alle für den Betrieb des Produktes notwendigen Dateien mit Ausnahme derer, die in den Einsatzvoraussetzungen genannt sind.

Der Lizenznehmer integriert die *cloud suite*-Komponenten in seine Webanwendung und stellt sie den Endanwendern per HTTPS zur Verfügung. Es ist die Aufgabe des Lizenznehmers, dem Endanwender Informationen zur sicheren Bedienung der *cloud suite*-Komponenten zur Verfügung zu stellen.

5.3.2 Installation

Der Administrator installiert das Produkt gemäß dem im mitgelieferten Entwicklerhandbuch beschriebenen Verfahren. Der Administrator muss entsprechende Voraussetzungen zur Bedienung eines Rechners besitzen.

ÜBERPRÜFUNG DER INTEGRITÄT DES INSTALLATIONSPAKETS

Der Administrator ist angehalten, vor der Installation die Integrität des zu verwendenden Installationspakets mit einer handelsüblichen Signaturanwendungskomponente wie z. B. *Sign Live! CC* (http://www.intarsys.de) zu prüfen.

ÜBERPRÜFUNG DER INTEGRITÄT DES INSTALLIERTEN PRODUKTES

Der Administrator ist angehalten, das bereits installierte Produkt regelmäßig zu prüfen, wie in Kapitel 3.4.2 beschrieben.

5.3.3 Auslieferung und Installation im Wartungsfall

Im Wartungsfall erhält der Administrator vom Hersteller ein weiteres Installationspaket im Format ZIP. Diese Dateien ersetzen die ursprünglich installierten Dateien vollständig. Nach abgeschlossener Nachinstallation soll der Administrator in jedem Fall die Integrität der Installation prüfen wie unter Kapitel 3.4.2 beschrieben.

Bei einem solchen Update verliert diese Herstellererklärung ihre Gültigkeit.

5.4 Auflagen für den Betrieb des Produktes

Als in eine Webanwendung integrierter Bestandteil wird das Produkt auf einem Server bereitgestellt und auf einem oder mehreren Clients verwendet. Sowohl Server als auch

Client müssen den Anforderungen entsprechen, die an einen geschützten Einsatzbereich[5] gestellt werden. Während des Betriebs sind im Einzelnen die folgenden Auflagen zur berücksichtigen. Die Allgemeinen Auflagen definieren Auflagen für Server und Client. Weitere Auflagen beziehen sich jeweils auf Server oder Client.

5.4.1 Allgemeine Auflagen

PERSONAL

Anwender und Administratoren der Anwendung müssen vertrauenswürdig sein. Sie kennen den Inhalt der zum Produkt gehörigen, mit dem Produkt ausgelieferten Dokumentation und berücksichtigen insbesondere die darin gegebenen Sicherheitshinweise. Es obliegt dem Betreiber, die notwendigen Informationen in geeigneter Form an geeigneter Stelle zur Verfügung zu stellen. Andere Personen dürfen keinen Zugriff auf das System haben.

ALGORITHMEN

Anwender 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.

AUFLAGEN ZUR SICHERHEIT DER IT-PLATTFORM UND APPLIKATIONEN

Die Integrität der Plattform und der eingesetzten zusätzlichen Softwareprodukte, wie z. B: Virenscanner, Firewall ist sicherzustellen. Sicherheitsupdates sind regelmäßig zu installieren.

Es ist sicherzustellen, dass die vom Produkt verwendeten Plattformen zum Installationszeitpunkt frei von Viren und Trojanern sind. Zusätzlich ist sicherzustellen, dass keine Schadsoftware eingespielt werden kann.

Es ist sicherzustellen, dass die verwendeten Kartenleser nicht bösartig manipuliert wurden.

AUFLAGEN ZUM SCHUTZ VOR MANUELLEM ZUGRIFF UNBEFUGTER

Die eingesetzten Rechner sind gegen manuellen Zugriff Unbefugter zu schützen. Dies kann z. B. durch eine Kombination aus softwaretechnischen Zugriffschutzmaßnahmen und Aufstellen in einem abschließbaren Raum geschehen.

AUFLAGEN ZUM SCHUTZ VOR ANGRIFFEN ÜBER DATENAUSTAUSCH PER DATENTRÄGER

Es ist sicherzustellen, dass Anwender/Administratoren die vollständige Kontrolle über eingelegte Speichermedien und Netzwerkfreigaben haben. Insbesondere muss sichergestellt sein, dass Dritte via Netzwerkfreigaben keine Möglichkeit haben, für den Signaturprozess verwendete Produkte zu manipulieren.

Werden Daten via Datenträger eingespielt, ist – z. B. mittels Virenscanner – sicherzustellen, dass keine Viren oder Trojaner eingespielt werden können.

AUFLAGEN ZUR SICHERHEITSADMINISTRATION DES BETRIEBS

Die eingesetzten Kartenleser und Rechner für Client und Server sind gegen unbefugte Benutzung zu sichern.

---

[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/media/archive/2648.pdf).

5.4.2 Auflagen für den Betrieb auf dem Server

Zusätzlich zu den allgemeinen Auflagen sind die folgenden Auflagen für den Betrieb des Produktes auf dem Server zu berücksichtigen:

KONFIGURATION

Der Administrator hat per Konfiguration sicherzustellen, dass das Herunterladen der *cloud suite*-Komponenten in gesicherter Form (HTTPS) erfolgt.

Die korrekte Verwendung der APIs kann von der Anwendung nicht überwacht werden. Der Administrator hat die aufrufende Anwendung und das Produkt mit Hilfe der mitgelieferten Dokumentation entsprechend zu konfigurieren und trägt selbst die Verantwortung dafür.

AUFLAGEN DER DRITTPRODUKTE

Die Auflagen, die die Signaturanwendungskomponente *Sign Live! CC* in der in Tabelle 3 angegebenen Version fordert, sind zu berücksichtigen.

5.4.3 Auflagen für den Betrieb auf dem Client

Zusätzlich zu den allgemeinen Auflagen sind die folgenden Auflagen für den Betrieb des Produktes auf dem Client zu berücksichtigen:

SYSTEMZEIT

Die Systemzeit muss korrekt eingestellt sein.

PRÜFUNG DER INTEGRITÄT DER TEILKOMPONENTE

Die *cloud suite*-Komponenten sind mit dem zum intarsys Code Signing Zertifikat gehörigen Signaturschlüssel signiert. Deren Laufzeitumgebung prüft die Signatur und zeigt bei Bedarf das zugehörige Zertifikat an. Der Anwender muss sich auf Basis dieser Hilfsmittel vor Verwenden der *cloud suite*-Komponenten von deren Authentizität und Integrität überzeugen.

VERFÜGBARKEIT ÜBER EINEN BEKANNTEN SERVER / GESICHERTE KOMMUNIKATION

Der Anwender hat sich durch die Anzeige des in der jeweiligen *cloud suite*-Komponente realisierten Kommunikationsstatus davon zu überzeugen, dass die Komponente via Intra- oder Internet von einem bekannten Server über ein gesichertes Kommunikationsprotokoll (HTTPS) geladen wird.

PRÜFUNG DES ZU SIGNIERENDEN DOKUMENTS

Der Anwender hat sich anhand der Beschreibung bzw. des Inhalts der zu signierenden Daten davon zu überzeugen, dass es sich tatsächlich um die Daten handelt, die er signieren möchte.

PRÜFUNG DES SIGNATURZERTIFIKATS

Der Anwender hat sich anhand der von der *cloud suite*-Komponente angezeigten Daten zu überzeugen, dass er mit seinem Zertifikat signiert.

PRÜFUNG DES KARTENLESERS

Der Anwender muss sicherstellen, dass er einen bestätigten, nicht manipulierten Kartenleser mit PIN-Pad zur PIN-Eingabe verwendet.

UMGANG MIT DER SSEE

Die PIN für die Verwendung der SSEE ist unbedingt vertraulich zu behandeln. Der Anwender hat dafür Sorge zu tragen, dass bei der PIN-Eingabe diese nicht ausgespäht werden kann.

AUFLAGEN DER DRITTPRODUKTE

Die durch Kartenleser und SSEE gegebenen Auflagen sind zu berücksichtigen.

Falls Komfortsignaturen in Verbindung mit dem Signaturapplet zum Einsatz kommen, müssen zusätzlich die durch die Signaturanwendungskomponente *Sign Live! CC* gegebenen Auflagen berücksichtigt werden. Insbesondere muss darauf geachtet werden, dass *Sign Live! CC* in der Rolle des *remote device service* nur lokale Aufrufe akzeptiert.

6 Algorithmen und zugehörige Parameter

Das Produkt verwendet zum Erstellen 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 auf den Internetseiten des Bundesanzeigers www.bundesanzeiger.de unter BAnz AT 01.02.2016 B5 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.

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

Tabelle 6 Hash-Algorithmen und deren Eignung gemäß BNetzA

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

Da das Produkt *Sign Live! CC cloud suite* optional das herstellererklärte Produkt *Sign Live! CC* in der in Tabelle 3 angegebenen Version verwendet, sind zusätzlich die an das verwendete Produkt gestellten Gültigkeitsbeschränkungen zu beachten.

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 zu der erklärten Version
   SLCS 7.0 Version 1.0
4. Testergebnisse zu der erklärten Version
   jeweils eine Testergebnistabelle je Testplan
   Erstellung: Dezember 2016
5. Sign Live! cloudsuite Developers Guide 7.0 als PDF Export
   (Version 1.0, 315 Seiten)

Das Entwicklerhandbuch wird im Format PDF mit dem Produkt ausgeliefert. Die Releasenotes ebenso.

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

Das zu meldende Produkt beinhaltet Teile des Produktes *Sign Live! CC 7.0*. Dieses 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 eingereicht.

Ende der Herstellererklärung