Systemvoraussetzungen

Datenblatt zu Sign Live! CC 7.1

Kritik, Kommentare & Korrekturen

Wir sind ständig bemüht, unsere Dokumentation zu optimieren und Ihren Bedürfnissen anzupassen. Ihre Anregungen sind uns dabei eine wertvolle Hilfe. Sie erreichen uns über folgende Kontaktmöglichkeiten:

e-mail: support@intarsys.de
internet: www.intarsys.de

Inhaltsverzeichnis

1 Übersicht

Dieses Dokument gibt Ihnen eine Übersicht der Systemvoraussetzungen, die für den Betrieb von Sign Live! CC und seinen Varianten erforderlich sind. Sign Live! CC erstellt elektronische Signaturen in vielfältiger Weise.

Insbesondere erstellt Sign Live! CC fortgeschrittene/qualifizierte elektronische Signaturen und fortgeschrittene/qualifizierte elektronische Siegel. Diese können über Kartenleser lokal oder entfernt über Signaturserver angeschlossene Signaturerstellungseinheiten (z. B. Signaturkarte, HSM) und ebenso mittels Fernsignaturservices erstelllt werden. Gleiches gilt auch für die Erstellung von Zeitstempeln.

Da hinsichtlich der Systemvoraussetzungen kein Unterschied zwischen einer elektronischen Signatur und einem elektronischen Siegel besteht, werden wir im Weiteren den Begriff elektronsiche Signatur für beides verwenden.

Die hier angegebenen Kombinationen von Betriebssystem, Chipkartenleser und Signaturkarten, sind die vom Hersteller getesteten. Es ist zu erwarten, dass weitere Kombinationen ohne Änderung der Software ebenfalls funktionstüchtig sind. Für den Einsatz solcher Kombinationen übernimmt der Betreiber die Verantwortung. Setzen Sie sich mit uns in Verbindung, wenn Sie Informationen zu weiteren Kombinationen benötigen.

2 Systemvoraussetzungen

Im Folgenden sind die hard- und softwareseitig zu erfüllenden Anforderungen aufgeführt. Weitere organisatorisch/technisch zu erfüllende Anforderungen entnehmen Sie bitte der mit dem Produkt ausgelieferten Dokumentation (Menüoption „Hilfe > Hilfe“).

2.1 Betriebssysteme

Sign Live! CC kann unter folgenden Betriebssystemen eingesetzt werden:

- Windows 7 / 8.1 / 10 / Server 2012 R2 / Server 2016 Standard
- Linux
  Ubuntu 16.04 / 18.04,
  openSUSE 15.0, SUSE Linux Enterprise Server 15
- Mac OS X 10.13 / 10.14

Mindestens die folgenden VDI[1] Kombinationen sind möglich:

- Windows 2016 Terminal Server
  mit Windows 7 Clients
- Windows 2016 Terminal Server
  mit Ubuntu 16.04 / 18.04 Clients

Die verwendbaren Karten-/Kartenleserkombinationen entsprechen denen des Client Betriebssystems. Detaillierte Installationshinweise erhalten Sie über den Hersteller. Weitere VDI-Kombinationen auf Anfrage.

[1] Virtual Desktop Infrastructure

2.2 Hardware

PROZESSOR

Intel Pentium 1 GHz oder gleichwertiger Prozessor

FREIER HAUPTSPEICHER

Minimum 256 MB, empfohlen 512 MB

FREIER FESTPLATTENSPEICHER

Sign Live! CC: ca. 200 MB,
zusätzlich 150 MB zum Entpacken der Installationsdateien

MONITORAUFLÖSUNG

Minimum 800 x 600, empfohlen 1024 x 768

2.3 Software

2.3.1 Java

Die Anwendung benötigt eine JVM Version 11. Ein Java Runtime Environment Version 11 ist in allen Installationsmedien vorhanden.

2.4 Netzzugang

2.4.1 Funktion: Integrität der Anwendung prüfen

Die Integrität der Anwendung wird über das auf der intarsys Homepage verfügbare Applet Installation Verifier geprüft. Dazu ist der Internetzugang über das Protokoll *http* (Port 80) notwendig.

2.4.2 Funktion: Validieren von Signaturen/Zertifikaten

2.4.2.1 Online-Aktivierung des Lizenzschlüssels

Für die bequeme Online-Aktivierung der Anwendung muss der Rechner, auf dem die Anwendung installiert wird, via *http* (Port 80) Zugang haben zum intarsys-Server http://service.intarsys.de/ .

2.4.2.2 Zugang zu aktuellen EU-Vertrauenslisten (LOTL)

Für die Validierung von Signaturen werden Vertrauenslisten benötigt. Die Anwendung wird mit einem Standardsatz der Vertrauenlisten ausgeliefert. Da die Vertrauenlisten jedoch in regelmäßigen Abständen durch die jeweilgen Herausgeber ergänzt werden, empfiehlt sich die regelmäßige Aktualisierung der Vertrauenlisten aus der Anwendung heraus.

Standardmäßig benötigt die Anwendung Zugang zu diesen Vertrauenlisten über die Protokolle *http* (***Port 80***) und *https* (***Port 443***).

2.4.2.3 Zugang zu aktuellen Sperrlisten

Für die Validierung von Signaturen muss das signierende Zertifikat hinsichtlich Sperreinträgen geprüft werden. Hierfür benötigt die Anwendung aktuelle Sperrlisten, die über entsprechende Dienste der Zertifizierungsdienstleister bereitgestellt werden.

Standardmäßig benötigt die Anwendung Zugang zu diesen Diensten über die Protokolle *http* (***Port 80***) und *ldap* (***Port 389***). Alternativ können Sperrlisten auch über einen Dateiserver zur Verfügung gestellt werden.

2.4.2.4 Zugang zu OCSP Diensten

Die optionale Gültigkeitsprüfung von Zertifikaten per Online-Statusabfrage (OCSP) benötigt einen Zugang zu den entsprechenden OCSP-Diensten der Zertifizierungsdienstleister. Diese sind verfügbar über das Protokoll *http* (***Port 80***).

2.5 Signaturerstellung mit lokaler Signaturerstellungseinheit

Für die Erstellung einer fortgeschrittenen/qualifizierten Signatur mit lokaler Signaturerstellungseinheit sind eine geeignete Signaturkarte und ein geeigneter Kartenleser erforderlich.

2.5.1 Signaturkarten

Die Tabelle „Signaturerstellungseinheiten“ gibt einen Überblick über die mit Sign Live! CC getesteten Signaturkarten. Über die Homepage der Bundesnetzagentur finden Sie weitere Details zu den Signaturkarten. In Abhängigkeit vom Kartenleser und der betriebssystemspezifischen Treibersituation sind bestimmte Kombinationen für die Erstellung einer qualifizierten Signatur nicht verwendbar. Prüfen Sie deshalb auch die jeweilige Tabelle für betriebssystemspezifische Kombinationen von Kartenleser und Signaturkarte.

Beachten Sie, dass Sie nach der seit 1.7.2016 in Deutschland gültigen eIDAS-Verordnung zur Erstellung einer qualifizierten elektronsichen Signatur eine qualifizierte Signaturerstellungseinheit benötigen.

2.5.2 Kartenleser

Die Tabelle „Unterstützte Kartenleser Klasse 2/3“ gibt einen Überblick über die mit Sign Live! CC getesteten Kartenleser. Über die Homepage der Bundesnetzagentur finden Sie weitere Details zu den Kartenlesern. In Abhängigkeit von Signaturkarte und der betriebssystemspezifischen Treibersituation sind bestimmte Kombinationen für die Erstellung einer qualifizierten Signatur nicht verwendbar. Prüfen Sie deshalb auch die jeweilige Tabelle für betriebssystemspezifische Kombinationen von Kartenleser und Signaturkarte.

2.6 Signaturerstellung mit Signaturserver

Für die Erstellung einer qualifizierten Signatur mit dem Signaturserver secunet multisign Enterprise der secunet Security Network AG muss ein solcher per Intra- oder Internet verfügbar sein.

2.7 Signaturerstellung über Fernsignaturdienst

Aktuell unterstützt Sign Live! CC die Fernsignatur über die Vertrauensdiensteanbeiter Bundesdruckerei (D-Trust) und Swisscom. Für die Nutzung dieses Service sind separate Verträge mit den jeweiligen VDA's abzuschliessen und die Zugangsdaten in Sign Live! CC zu konfigurieren.

3 Tabellen

3.1 Signaturerstellungseinheiten

Vertrauensdiensteanbieter	Handelsname der Signaturkarte(n)	Kartentyp[1]
Bundesnotarkammer (BNotK)	Bundesnotarkammer Signaturkarte 100 Bundesnotarkammer Signaturkarte unlimited	E/S E/S/M
Bundesdruckerei (D-Trust)	Siegelkarte D-TRUST Card 3.4 D-TRUST Card - Einzelsignatur (3.1) D-TRUST Card - Multicard 100 (3.1) - Stapelsignatur bis 100 Dokumente D-TRUST Card - Multicard (3.1) – Massensignatur	E/M E E/S E/S/M
Deutsches Gesundheitsnetz (DGN)	DGN SprintCard DGN BusinessCard	E E/S
medisign	Elektronischer Arztausweis (eHBA) Elektronischer Zahnarztausweis (eHBA/eZAA) Elektronischer Psychotherapeutenausweis (ePTA) Elektronischer Ausweis für Zahnärzte (ZOD)	E
TeleSec	TeleSec Signature Card 2.0 TeleSec Signature Card 2.0	E E/S/M

Vertrauensdiensteanbieter (CH)	Handelsname der Signaturkarte(n)	Kartentyp
SwissSign	SuisseID	E

Weitere Signaturkarten auf Anfrage oder generisch über PKCS#11 Schnittstelle

[1] E=Einzelsignaturkarte S=Stapelsignaturkarte M=Massensignaturkarte

3.2 Unterstützte Kartenleser Klasse 2/3

Hersteller und Handelsname des Kartenlesers
Cherry SmartBoard xx44
Cherry SmartTerminal ST-2000 (bereits abgekündigt)
Cherry SmartTerminal ST-2100
Kobil KAAN Advanced
Omnikey CardMan Trust CM 3621
Omnikey CardMan Trust CM 3821
Reiner SCT cyberJack e-com
Reiner SCT cyberJack e-com plus
Reiner SCT cyberJack secoder
Reiner SCT cyberJack RFID komfort
SCM Microsystems SPR532, V5.10

Weitere Kartenleser der Klassen 2/3 auf Anfrage.

3.3 Unterstützte Kartenleser Klasse 1

Hersteller und Handelsname des Kartenlesers
Cherry KC 1000 SC

Weitere Kartenleser der Klasse 1 auf Anfrage.

3.4 Getestete Kombinationen am Arbeitsplatz unter Windows 7 und 10

Kartenleser							
Handelsname	Treiber	BNotK	D-Trust	DGN	medisign	TeleSec	SwissSign
1Cherry SmartBoard xx44[1]	HID Global V 1.2.24.27	√	√	√	√	√	√
Cherry SmartTerminal ST-2000	SCM Microsystems V 4.54.0.0	√	√	√	√	√	√
Cherry SmartTerminal ST-2100	SCM Microsystems V 4.54.0.0	√	√	√	√	√	√
Cherry KC 1000 SC	HID Global V 1.0.5.152	√	√	√	√	√	√
Kobil KAAN Advanced	KOBIL Systems 2013.1.24.1	√	√	√	√	√	√
Omnikey CardMan Trust CM3621[1]	HID Global V 1.2.24.27	√	√	√	√	√	√
Omnikey CardMan Trust CM3821[1]		√	√	√	√	√	√
Reiner SCT cyberJack e-com[2]	Cyber Jack Base Components 7.7.2	√	√	√	√	√	√

[1] Der Kartenleser funktioniert für einzelne Signaturen einwandfrei. Bei Belastungstests kommt es vor, dass der Kartenleser die sichere PIN-Eingabe vorzeitig abbricht.

Reiner SCT cyberJack e-com plus[2]		√	√	√	√	√	√
Reiner SCT cyberJack secoder[2]		√	√	√	√	√	√
Reiner SCT cyberJack RFID komfort[1]		√	√	√	√	√	√
SCM Microsystems SPR532	SCM Microsystems V 4.54.0.0	√	√	√	√	√	√

3.5 Getestete Kombinationen unter Windows Server 2012 R2 und 2016 Standard

Kartenleser							
Handelsname	**Treiber**	**BNotK**	**D-Trust**	**DGN**	**medisign**	**TeleSec**	**SwissSign**
Cherry SmartTerminal ST-2000	Cherry Smart Card Setup V3.3	√	√	√	√	√	√
Kobil KAAN Advanced	Kobil Treiber V2.3	√	√	√	√	√	√
Omnikey CardMan Trust CM3821[2]	HID Global V 1.2.24.27	√	√	√	√	√	√
Reiner SCT cyberJack e-com plus[2]	cyberJack Base Components 7.7.2	√	√	√	√	√	√
Reiner SCT cyberJack secoder[2]		√	√	√	√	√	√
Reiner SCT cyberJack RFID komfort[3]		√	√	√	√	√	√

[1] Der Kartenleser kann nur PIN's mit max. 15 Ziffern verarbeiten
[2] Der Kartenleser funktioniert für einzelne Signaturen einwandfrei. Bei Belastungstests kommt es vor, dass der Kartenleser die sichere PIN-Eingabe vorzeitig abbricht.
[3] Der Kartenleser kann nur PIN's mit max. 15 Ziffern verarbeiten

SCM Microsystems SPR532	SPR532 Installer V1.88	√	√	√	√	√	√

3.6 Getestete Kombinationen unter Linux: Ubuntu 16.04 und 18.04

Kartenleser							
Handelsname	**Treiber**	**BNotK**	**D-Trust**	**DGN**	**medisign**	**TeleSec**	**SwissSign**
Cherry SmartTerminal ST-2000	libccid v1.4.29-1	√	√	√	√	√	√
Cherry SmartTerminal ST-2100	libccid v1.4.29-1	√	√[1]	√	√	x	x
Kobil KAAN Advanced	libccid v1.4.29-1	√	√	√	√	√	√
Omnikey CardMan Trust CM3821[2]	libccid v1.4.29-1	√	√	√	√	√	√
Reiner SCT cyberJack e-com plus[2]	pcsc-cyberjack v3.99.5final.sp13	√	√	√	√	√	√
Reiner SCT cyberJack secoder[2]		√	√	√	√	√	√
Reiner SCT cyberJack RFID komfort[3]		√	√	√	√	√	√
SCM Microsystems SPR532	libccid v1.4.29-1	√	√	√	√	√	√

[1] Bei neueren Signaturkarten des Herstellers ist eine sichere PIN-Eingabe nicht möglich
[2] Der Kartenleser funktioniert für einzelne Signaturen einwandfrei. Bei Belastungstests kommt es vor, dass der Kartenleser die sichere PIN-Eingabe vorzeitig abbricht.
[3] Der Kartenleser kann nur PIN's mit max. 15 Ziffern verarbeiten

3.7 Getestete Kombinationen unter Linux: OpenSUSE 15-0

Kartenleser							
Handelsname	**Treiber**	**BNotK**	**D-Trust**	**DGN**	**medisign**	**TeleSec**	**SwissSign**
Cherry SmartTerminal ST-2000	libccid v1.4.29-1	√	√	√	√	√	√
Kobil KAAN Advanced	libccid v1.4.29-1	√	√	√	√	√	√
Omnikey CardMan Trust CM3821[1]	libccid v1.4.29-1	√	√	√	√	√	√
Reiner SCT cyberJack e-com plus[2]	pcsc-cyberjack v3.99.5final.sp13-1	√	√	√	√	√	√
Reiner SCT cyberJack secoder[2]		√	√	√	√	√	√
Reiner SCT cyberJack RFID komfort[2]		√	√	√	√	√	√
SCM Microsystems SPR332	libccid v1.4.29-1	√	√	√	√	√	√

[1] Der Kartenleser funktioniert für einzelne Signaturen einwandfrei. Bei Belastungstests kommt es vor, dass der Kartenleser die sichere PIN-Eingabe vorzeitig abbricht.
[2] Der Kartenleser kann nur PIN's mit max. 15 Ziffern verarbeiten

3.8 Getestete Kombinationen unter Mac OS X 10.14.3, 10.14.6

Kartenleser							
Handelsname	**Treiber**	**BNotK**	**D-Trust**	**DGN**	**medisign**	**TeleSec**	**SwissSign**
Cherry SmartBoard xx44[1]	IFD CCID Bundle v1.4.27	√	√	√	√	x	x
Cherry SmartTerminal ST-2000		√	√	√	√	x	x
Cherry SmartTerminal ST-2100		√	√[1]	√	√	x	x
Cherry KC 1000 SC		√	√	√	√	x	x
Kobil KAAN Advanced	IFD CCID Bundle v1.4.27	√	√	√	√	√	√
Omnikey CardMan Trust CM3621[2]	IFD CCID Bundle v1.4.27	√	√	x	x	x	x
Omnikey CardMan Trust CM3821[1]		√	√	x	x	x	x
Reiner SCT cyberJack e-com[2]	cyberJack v3.99.5finalSP13	√	√	√	√	√	√
Reiner SCT cyberJack e-com plus[2]		√	√	√	√	√	√
Reiner SCT cyberJack secoder[2]		√	√	√	√	√	√
Reiner SCT cyberJack RFID komfort[3]		√	√	√	√	√	√

[1] Bei einigen Signaturkarten des Herstellers wird die sichere PIN-Eingabe nicht unterstützt
[2] Der Kartenleser funktioniert für einzelne Signaturen einwandfrei. Bei Belastungstests kommt es vor, dass der Kartenleser die sichere PIN-Eingabe vorzeitig abbricht.
[3] Der Kartenleser kann nur PIN's mit max. 15 Ziffern verarbeiten

SCM Microsystems SPR532	IFD CCID Bundle v1.4.27	√	√	√	√	√	√