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 10 / 11 / Server 2019 Standard / Server 2022 Standard
- Linux
  Ubuntu 18.04 / 20.04,
  openSUSE 15.0, SUSE Linux Enterprise Server 15
- macOS 11.0 (Big Sur) / 12.0 (Monterey)

Mindestens die folgenden VDI[1] Kombinationen sind möglich:

- Windows 2019 Terminal Server
  mit Windows 10 Clients
- Windows 2022 Terminal Server
  mit Windows 11 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 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

Einige Funktionen benötigen Netzzugriff.

2.4.1 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/ . Diese Funktion wird nur auf Anforderung des Benutzers zum Abruf der Lizenzdatei verwendet.

2.4.2 Update-Info Abfrage

In der Standard-Konfiguration kontaktiert SLCC den intarsys-Server http://service.intarsys.de/ und informiert den Benutzer, ob Aktualisierungen für SLCC vorliegen. Diese Funktion ist abschaltbar. Die Aktualisierung muss manuell erfolgen. Dazu muss der Rechner, auf dem die Anwendung installiert wird, via *http* (Port 80) Zugang haben zum intarsys-Server http://service.intarsys.de/ haben.

2.4.3 Signaturen/Zertifikate validieren

Für das Validieren von Signaturen und Zertifikaten ist der Zugriff auf unterschiedliche Internet Dienste erforderlich.

2.4.3.1 OCSP Dienst

Die optionale Gültigkeitsprüfung von Zertifikaten per Online-Statusabfrage (OCSP) benötigt einen Zugang zum OCSP-Dienst des jeweiligen Zertifizierungsdienstleisters.
Diese sind verfügbar über das Protokoll *http* (***Port 80***). Die OCSP-Antworten sind signiert und werden vor Verwendung in SLCC geprüft.

2.4.3.2 Sperrlisten Dienst (CRL)

Die optionale Gültigkeitsprüfung von Zertifikaten per Sperrliste (CRL) benötigt einen Zugang zum CRL-Service des Zertifizierungsdienstleisters. Die zugenhörige Adresse ist entweder in SLCC konfiguriert oder über das zu prüfende Zertifkat zu ermitteln. 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. Sperrlisten sind signiert und werden vor Verwendung in SLCC geprüft.

2.4.3.3 EU-Vertrauenslisten (TL[2] und LOTL[3])

Für die Validierung von Signaturen werden Vertrauenslisten benötigt. Die Anwendung wird mit bei Erstellung der Software gültigen 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. Die TL sind signiert. Vor Verwendung in SLCC wird die Signatur geprüft. Die EU-Vertrauenslisten werden hauptsächlich via *https* (**Port 443**), in Einzelfällen auch *http* (**Port 80**) von unterschiedlichen Adressen[4] geladen.

2.4.3.4 intarsys-Vertrauensliste (intarsys TL)

Die intarsys TL stellt analog zu den EU-Vertrauenslisten Wurzel- und Zwischenzertifikate des nicht von der eIDAS abgedeckten Raumes zur Verfügung. intarsys stellt darüber z. B. Zertifikate der ZertES-PKI (Schweiz) und einiger fortgschrittenen Vertrauensdienste zur Verfügung. Die intarsys TL ist ebenfalls signiert. Vor Verwendung in SLCC wird die Signatur geprüft. Sie wird via *https* (**Port 443**) über die URL https://service.intarsys.de/tl/intarsys.xml abgerufen.

2.4.4 Signaturen erstellen

2.4.4.1 Fernsignaturen

Bei Signatur über einen Fernsignaturdienstleister muss Zugriff auf dessen Services bestehen. Informationen dazu finden Sie in den Service-Dokumentationen der jeweiligen Anbieter.

2.4.4.2 Zertifikate prüfen und LTV-Fähigkeit

SLCC kann so konfiguriert werden, dass beim Erstellen einer Signatur vorab das Signaturzertifikat auf Gültigkeit geprüft wird oder zum Zwecke einer LTV-Signatur Validierungsinformationen in die Signatur eingebettet werden. In diesen Fällen sind die in Kap. 2.4.3 genannten Zugänge ebenfalls erforderlich.

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] TL: Trusted List – Nationale Liste der Vertrauensdienste
[3] LOTL: List of Trusted Lists – EU TL, sie verweist auf die nationalen TL
[4] je EU-Land mind. eine Adresse

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)	eHBA G2.0 eHBA G2.1 Siegelkarte D-TRUST Card 4.4 D-TRUST Card - Einzelsignatur (4.1) D-TRUST Card - Multicard 100 (4.1) - Stapelsignatur bis 100 Dokumente D-TRUST Card - Multicard (4.1) – Massensignatur 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 E/S E/M E E/S E/S/M E/M E E/S E/S/M
Deutsches Gesundheitsnetz (DGN)	DGN SprintCard DGN BusinessCard	E E/S
medisign	Elektronischer Arztausweis (eHBA) (bis Ausstelldatum 2021) Elektronischer Zahnarztausweis (eHBA/eZAA) (bis Ausstelldatum 2021) Elektronischer Psychotherapeutenausweis (ePTA) (bis 2021) Elektronischer Ausweis für Zahnärzte (ZOD) (bis Ausstelldatum 2021) Elektronischer Arztausweis (eHBA 2.1)	E
TeleSec	TeleSec Signature Card 2.0 TeleSec Signature Card 2.0	E E/S/M
SHC	Heilberufsausweis (eHBA) Generation 2.1	E/S
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-2100
Kobil KAAN Advanced
Omnikey CardMan Trust CM 3621
Omnikey CardMan Trust CM 3821
Reiner SCT cyberJack e-com plus
Reiner SCT cyberJack secoder
Reiner SCT cyberJack RFID komfort
Reiner SCT cyberJack one
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
Cherry TC 1100

Weitere Kartenleser der Klasse 1 auf Anfrage.

3.4 Getestete Kombinationen am Arbeitsplatz unter Windows 10 und 11

Kartenleser										
Handelsname	**Treiber**	**BNotK**	**D-Trust**	**D-Trust eHBA G2**	**DGN**	**medisign**	**medisign eHAB 2.1**	**TeleSec**	**SHC eHBA 2.1**	**SwissSign**
Cherry SmartBoard xx44[13]	HID Global V 1.2.24.27	√	√	√	√	√	√	√	√	√
Cherry SmartTerminal ST-2100	Cherry SmartCard Package V3.3 Build 9	√	√	√	√	√	√	√	√	√
Cherry KC 1000 SC	HID Global V 1.0.5.152	√	√	√	√	√	√	√	√	√
Cherry TC 1100[2]	Cherry SmartCard Package V3.3 Build 9	√	√	√	√	√	√	√	√	√
Kobil KAAN Advanced	KOBIL Kartenleser Treiber v2.3.08081	√	√[3]	x	√	√	x	√	x	√
Omnikey CardMan Trust CM3821[4]		√	√[5]	x	√	√	x	√	x	√
Reiner SCT cyberJack e-com plus[65]	cyberJack Base Components 7.8.10	√	√	x	√	√	x	√	x	√
Reiner SCT cyberJack secoder[7]		√	√	x	√	√	x	√	x	√
Reiner SCT cyberJack RFID komfort[8]		√	√	√	√	√	√	√	√	√
Reiner SCT cyberJack one[9]		√	√	√	√	√	√	√	√	√
SCM Microsystems SPR532	SCM Microsystems V 4.54.0.0	√	√	√	√	√	√	√	√	√

[1] Der Kartenleser unterstützt keine sichere PIN-Eingabe
[2] Der Kartenleser unterstützt keine sichere PIN-Eingabe
[3] Der Kartenleser unterstützt keine D-Trust Signaturkarten der Serie 4.x.
[4] Der Kartenleser funktioniert für einzelne Signaturen einwandfrei. Eine sichere PIN-Eingabe wird nicht unterstützt.
[5] Der Kartenleser unterstützt keine D-Trust Signaturkarten der Serie 4.x.
[6] Der Kartenleser kann nur PIN's mit max. 15 Ziffern verarbeiten
[7] Der Kartenleser kann nur PIN's mit max. 15 Ziffern verarbeiten
[8] Der Kartenleser kann nur PIN's mit max. 15 Ziffern verarbeiten
[9] Der Kartenleser kann nur PIN's mit max. 15 Ziffern verarbeiten

3.5 Getestete Kombinationen unter Windows Server 2019 Standard und 2022 Standard

Kartenleser							
Handelsname	**Treiber**	**BNotK**	**D-Trust**	**DGN**	**medisign**	**TeleSec**	**SwissSign**
Cherry SmartTerminal ST-2000	Cherry Smart Card Setup V3.3	√	√	√	√	√	√
Cherry TC 1100[1]		√	√	√	√	√	√
Reiner SCT cyberJack e-com plus[2]	cyberJack Base Components 7.8.10	√	√	√	√	√	√
Reiner SCT cyberJack one[3]		√	√	√	√	√	√
Reiner SCT cyberJack RFID komfort[4]		√	√	√	√	√	√

[1] Der Kartenleser unterstützt keine sichere PIN-Eingabe
[2] Der Kartenleser kann nur PIN's mit max. 15 Ziffern verarbeiten
[3] Der Kartenleser kann nur PIN's mit max. 15 Ziffern verarbeiten
[4] Der Kartenleser kann nur PIN's mit max. 15 Ziffern verarbeiten

3.6 Getestete Kombinationen unter Linux: Ubuntu 18.04 und 20.04

Kartenleser										
Handelsname	*Treiber*	*BNotK*	*D-Trust 3.x*	*D-Trust ab 4.x*	*D-Trust eHBA*	*DGN*	*medisign*	*medisign eHBA 2.1*	*TeleSec*	*SwissSign*
Cherry SmartTerminal ST-2100	libccid v1.4.31-1 (Ubuntu 20.04)	√	√	√	√	√	√	√	√	√
Cherry TC 1100[1]	libpcsclite1 v1.8.26-3 (Ubuntu 20.04)	√	√	√	√	√	√	√	√	√
Kobil KAAN Advanced	libccid v1.4.29-1 (Ubuntu 18.04)	√	√[2]	x	x	√	√	x	√	√
	libpcsclite1 v1.8.23-1 (Ubuntu 18.04)									
Omnikey CardMan Trust CM3821[3]		√	√[4][5]	x	x	√	√	x	√	√
Reiner SCT cyberJack e-com plus[6]	pcsc-cyberjack6 v3.99.5final.sp13	√	√	x	x	√	√	x	√	√
Reiner SCT cyberJack secoder[7]		√	√	x	x	√	√	x	√	√
Reiner SCT cyberJack RFID komfort[8]		√	√	√	√	√	√	√	√	√
Reiner SCT cyberJack one[9]		√	√	√	√	√	√	√	√	√

[1] Der Kartenleser untersützt keine sichere PIN-Eingabe
[2] Der Kartenleser unterstützt keine D-Trust Signaturkarten der Serie 4.x.
[3] Der Kartenleser funktioniert für qualifizierte Signaturen einwandfrei. Fortgeschrittene Signatur, Authentisierung und Verschlüsselung werden nicht unterstützt.
[4] Der Kartenleser unterstützt keine D-Trust Signaturkarten der Serie 4.x.
[5] Neuere Signaturkarten des Herstellers werden nicht unterstützt.
[6] Der Kartenleser kann nur PIN's mit max. 15 Ziffern verarbeiten
[7] Der Kartenleser kann nur PIN's mit max. 15 Ziffern verarbeiten
[8] Der Kartenleser kann nur PIN's mit max. 15 Ziffern verarbeiten
[9] 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 3.x**	**D-Trust ab 4.x**	**D-Trust eHBA**	**DGN**	**medisign**	**medisign eHBA 2.1**	**TeleSec**	**SwissSign**
Cherry SmartTerminal ST-2100	libccid v1.4.31-1	√	√	√	√	√	√	√	√	√
Cherry TC 1100[1]		√	√	√	√	√	√	√	√	√
Kobil KAAN Advanced	libccid v1.4.31-1	√	√[2]	x	x	√	√	x	√	√
Omnikey CardMan Trust CM3821[3]	libccid v1.4.31-1	√	√[4][5]	x	x	√	√	x	√	√
Reiner SCT cyberJack e-com plus[6]	pcsc-cyberjack v3.99.5final.sp13	√	√	x	x	√	√	x	√	√
Reiner SCT cyberJack secoder[7]		√	√	x	x	√	√	x	√	√
Reiner SCT cyberJack RFID komfort[8]		√	√	√	√	√	√	√	√	√
Reiner SCT cyberJack one[9]		√	√	√	√	√	√	√	√	√

[1] Der Kartenleser untersützt keine sichere PIN-Eingabe
[2] Der Kartenleser unterstützt keine D-Trust Signaturkarten der Serie 4.x.
[3] Der Kartenleser funktioniert für qualifizierte Signaturen einwandfrei. Fortgeschrittene Signatur, Authentisierung und Verschlüsselung werden nicht unterstützt.
[4] Neuere Signaturkarten des Herstellers werden nicht unterstützt.
[5] Der Kartenleser unterstützt keine D-Trust Signaturkarten der Serie 4.x.
[6] Der Kartenleser kann nur PIN's mit max. 15 Ziffern verarbeiten
[7] Der Kartenleser kann nur PIN's mit max. 15 Ziffern verarbeiten
[8] Der Kartenleser kann nur PIN's mit max. 15 Ziffern verarbeiten
[9] Der Kartenleser kann nur PIN's mit max. 15 Ziffern verarbeiten

3.8 Getestete Kombinationen unter Mac OS 11.0, 12.0

Kartenleser										
Handelsname	**Treiber**	**BNotK**	**D-Trust**	**D-Trust eHBA G2**	**DGN**	**medisign**	**medisign eHBA 2.1**	**TeleSec**	**SHC eHBA 2.1**	**SwissSign**
Cherry SmartBoard xx44[1]	ifd-ccid bundle v1.4.34	√	√	x	√	√	x	x	x	x
Cherry SmartTerminal ST-2100		√	√[2]	x	√	√	x	x	x	x
Cherry KC 1000 SC		√	√	x	√	√	x	x	x	x
Cherry TC 1100[3]		√	√	x	√	√	x	x	x	x
Kobil KAAN Advanced		√	√[4]	x	√	√	x	√	x	√
Omnikey CardMan Trust CM3821[5]		√	√[6]	x	x	x	x	x	x	x
Reiner SCT cyberJack e-com plus[7]	cyberJack v3.99.5finalSP15	√	√	x	√	√	x	√	x	√
Reiner SCT cyberJack secoder[8]		√	√	x	√	√	x	√	x	√
Reiner SCT cyberJack RFID komfort[9]		√	√	√	√	√	√	√	√	√
Reiner SCT cyberJack one[10]		√	√	x	√	√	√	√	√	√
SCM Microsystems SPR532	ifd-ccid bundle v1.4.34	√	√	x	√	√	x	√	x	√

[1] Der Kartenleser untersützt keine sichere PIN-Eingabe
[2] Bei einigen Signaturkarten des Herstellers wird die sichere PIN-Eingabe nicht unterstützt
[3] Der Kartenleser untersützt keine sichere PIN-Eingabe
[4] Der Kartenleser unterstützt keine D-Trust Signaturkarten der Serie 4.x.
[5] Der Kartenleser funktioniert für einzelne Signaturen einwandfrei. Eine sichere PIN-Eingabe wird nicht unterstützt.
[6] Der Kartenleser unterstützt keine D-Trust Signaturkarten der Serie 4.x.
[7] Der Kartenleser kann nur PIN's mit max. 15 Ziffern verarbeiten
[8] Der Kartenleser kann nur PIN's mit max. 15 Ziffern verarbeiten
[9] Der Kartenleser kann nur PIN's mit max. 15 Ziffern verarbeiten
[10] Der Kartenleser kann nur PIN's mit max. 15 Ziffern verarbeiten