

# 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](mailto:support@intarsys.de)

internet: [www.intarsys.de](http://www.intarsys.de)

Alle genannten Warenzeichen sind Eigentum der jeweiligen Rechtsträger und werden als solche anerkannt.

© intarsys AG 2021

# Inhaltsverzeichnis

<b><u>1</u></b>	<b><u>Übersicht .....</u></b>	<b><u>3</u></b>
<b><u>2</u></b>	<b><u>Systemvoraussetzungen.....</u></b>	<b><u>3</u></b>
2.1	Betriebssysteme.....	3
2.2	Hardware .....	4
2.3	Software .....	4
2.3.1	Java .....	4
2.4	Netzzugang .....	4
2.4.1	Online-Aktivierung des Lizenzschlüssels .....	4
2.4.2	Update-Info Abfrage .....	4
2.4.3	Signaturen/Zertifikate validieren .....	4
2.4.3.1	OCSP Dienst .....	4
2.4.3.2	Sperrlisten Dienst (CRL) .....	5
2.4.3.3	EU-Vertrauenslisten (TL und LOTL).....	5
2.4.3.4	intarsys-Vertrauensliste (intarsys TL) .....	5
2.4.4	Signaturen erstellen .....	5
2.4.4.1	Fernsignaturen.....	5
2.4.4.2	Zertifikate prüfen und LTV-Fähigkeit.....	5
2.5	Signaturerstellung mit lokaler Signaturerstellungseinheit .....	5
2.5.1	Signaturkarten .....	6
2.5.2	Kartenleser .....	6
2.6	Signaturerstellung mit Signaturserver .....	6
2.7	Signaturerstellung über Fernsignatordienst .....	6
<b><u>3</u></b>	<b><u>Tabellen .....</u></b>	<b><u>7</u></b>
3.1	Signaturerstellungseinheiten.....	7
3.2	Unterstützte Kartenleser Klasse 2/3.....	9
3.3	Unterstützte Kartenleser Klasse 1 .....	10
3.4	Getestete Kombinationen am Arbeitsplatz unter Windows 7 und 10 10	
3.5	Getestete Kombinationen unter Windows Server 2016 Standard und 2019 Standard .....	11
3.6	Getestete Kombinationen unter Linux: Ubuntu 18.04 und 20.04....	13
3.7	Getestete Kombinationen unter Linux: OpenSUSE 15-0.....	14
3.8	Getestete Kombinationen unter Mac OS X 10.14.6, 10.15.....	15

# 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 erstellt 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 elektronische 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 2016 Standard / Server 2019 Standard
- Linux  
Ubuntu 18.04 / 20.04,  
openSUSE 15.0, SUSE Linux Enterprise Server 15
- Mac OS X 10.15 (Catalina) / 11.0 (Big Sur)

Mindestens die folgenden VDI<sup>1</sup> Kombinationen sind möglich:

- Windows 2019 Terminal Server  
mit Windows 7 Clients
- Windows 2019 Terminal Server  
mit Windows 10 Clients

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

---

<sup>1</sup> Virtual Desktop Infrastructure

## 2.2 Hardware

### PROZESSOR

Intel Pentium 1 GHz oder gleichwertiger Prozessor

### FREIER HAUPTSPICHER

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 zugehörige Adresse ist entweder in SLCC konfiguriert oder über das zu prüfende Zertifikat 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<sup>2</sup> und LOTL<sup>3</sup>)

Für die Validierung von Signaturen werden Vertrauenslisten benötigt. Die Anwendung wird mit bei Erstellung der Software gültigen Standardsatz der Vertrauenslisten ausgeliefert. Da die Vertrauenslisten jedoch in regelmäßigen Abständen durch die jeweiligen Herausgeber ergänzt werden, empfiehlt sich die regelmäßige Aktualisierung der Vertrauenslisten 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<sup>4</sup> 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 fortgeschrittenen 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 Fernsignatordienstleister 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.

<sup>2</sup> TL: Trusted List – Nationale Liste der Vertrauensdienste

<sup>3</sup> LOTL: List of Trusted Lists – EU TL, sie verweist auf die nationalen TL

<sup>4</sup> 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 elektronischen 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 Vertrauensdiensteanbieter 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 <sup>1</sup>
Bundesnotarkammer (BNotK)	Bundesnotarkammer Signaturkarte 100 Bundesnotarkammer Signaturkarte unlimited	E/S E/S/M
Bundesdruckerei (D-Trust)	eHBA G2 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/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

<sup>1</sup> E=Einzelsignaturkarte S=Stapelsignaturkarte M=Massensignaturkarte

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

Weitere Signaturkarten auf Anfrage oder generisch über PKCS#11 Schnittstelle

### 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 KAAAN Advanced
Omniquey CardMan Trust CM 3621
Omniquey CardMan Trust CM 3821
Reiner SCT cyberJack e-com
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 7 und 10

Kartenleser								
Handelsname	Treiber	BNotK	D-Trust	D-Trust eHBA G2	DGN	medisign	TeleSec	SwissSign
Cherry SmartBoard xx44 <sup>13</sup>	HID Global V 1.2.24.27	✓	✓	✗	✓	✓	✓	✓
Cherry SmartTerminal ST-2000	Cherry SmartCard Package V3.3 Build 9	✓	✓	✗	✓	✓	✓	✓
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 <sup>2</sup>	Cherry SmartCard Package V3.3 Build 9	✓	✓	✗	✓	✓	✓	✓
Kobil KAAAN Advanced	KOBIL Kartenleser Treiber v2.3.08081	✓	✓ <sup>3</sup>	✗	✓	✓	✓	✓
Omnikey CardMan Trust CM3621 <sup>4</sup>	HID Global V 1.2.24.27	✓	✓ <sup>5</sup>	✗	✓	✓	✓	✓

<sup>1</sup> Der Kartenleser unterstützt keine sichere PIN-Eingabe

<sup>2</sup> Der Kartenleser unterstützt keine sichere PIN-Eingabe

<sup>3</sup> Der Kartenleser unterstützt keine D-Trust Signaturkarten der Serie 4.x.

<sup>4</sup> Der Kartenleser funktioniert für einzelne Signaturen einwandfrei. Eine sichere PIN-Eingabe wird nicht unterstützt.

<sup>5</sup> Der Kartenleser unterstützt keine D-Trust Signaturkarten der Serie 4.x.

Omniquey CardMan Trust CM3821 <sup>1</sup>		✓	✓ <sup>2</sup>	✗	✓	✓	✓	✓
Reiner SCT cyberJack e-com <sup>3</sup>	Cyber Jack Base Components 7.8.6	✓	✓	✗	✓	✓	✓	✓
Reiner SCT cyberJack e-com plus <sup>45</sup>		✓	✓	✗	✓	✓	✓	✓
Reiner SCT cyberJack secoder <sup>5</sup>		✓	✓	✗	✓	✓	✓	✓
Reiner SCT cyberJack RFID komfort <sup>6</sup>		✓	✓	✓	✓	✓	✓	✓
Reiner SCT cyberJack one <sup>7</sup>		✓	✓	✓	✓	✓	✓	✓
SCM Microsystems SPR532	SCM Microsystems V 4.54.0.0	✓	✓	✗	✓	✓	✓	✓

### 3.5 Getestete Kombinationen unter Windows Server 2016 Standard und 2019 Standard

Kartenleser							
Handelsname	Treiber	BNotK	D-Trust	DGN	medisign	TeleSec	SwissSign
		Cherry SmartTerminal ST-2000	Cherry Smart Card Setup V3.3	✓	✓	✓	✓
Cherry TC 1100 <sup>8</sup>	✓	✓		✓	✓	✓	✓

<sup>1</sup> Der Kartenleser funktioniert für einzelne Signaturen einwandfrei. Eine sichere PIN-Eingabe wird nicht unterstützt.

<sup>2</sup> Der Kartenleser unterstützt keine D-Trust Signaturkarten der Serie 4.x.

<sup>3</sup> Der Kartenleser kann nur PIN's mit max. 15 Ziffern verarbeiten

<sup>4</sup> Der Kartenleser kann nur PIN's mit max. 15 Ziffern verarbeiten

<sup>5</sup> Der Kartenleser kann nur PIN's mit max. 15 Ziffern verarbeiten

<sup>6</sup> Der Kartenleser kann nur PIN's mit max. 15 Ziffern verarbeiten

<sup>7</sup> Der Kartenleser kann nur PIN's mit max. 15 Ziffern verarbeiten

<sup>8</sup> Der Kartenleser unterstützt keine sichere PIN-Eingabe

Omniquey CardMan Trust CM3821 <sup>1</sup>	HID Global Synch-API 3.0.1.11	✓	✓ <sup>2</sup>	✓	✓	✓	✓
Reiner SCT cyberJack e-com plus <sup>3</sup>	cyberJack Base Components 7.8.6	✓	✓	✓	✓	✓	✓
Reiner SCT cyberJack secoder <sup>4</sup>		✓	✓	✓	✓	✓	✓
Reiner SCT cyberJack RFID komfort <sup>5</sup>		✓	✓	✓	✓	✓	✓

<sup>1</sup> Der Kartenleser funktioniert für einzelne Signaturen einwandfrei. Eine sichere PIN-Eingabe wird nicht unterstützt.

<sup>2</sup> Der Kartenleser unterstützt keine D-Trust Signaturkarten der Serie 4.x.

<sup>3</sup> Der Kartenleser kann nur PIN's mit max. 15 Ziffern verarbeiten

<sup>4</sup> Der Kartenleser kann nur PIN's mit max. 15 Ziffern verarbeiten

<sup>5</sup> Der Kartenleser kann nur PIN's mit max. 15 Ziffern verarbeiten

## 3.6 Getestete Kombinationen unter Linux: Ubuntu 18.04 und 20.04

Kartenleser		BNotK	D-Trust	DGN	medisign	TeleSec	SwissSign
Handelsname	Treiber						
Cherry SmartTerminal ST-2100	libccid v1.4.31-1	✓	✓	✓	✓	✓	✓
Cherry TC 1100 <sup>1</sup>	libccid v1.4.31-1	✓	✓	✓	✓	✓	✓
Kobil KAAAN Advanced	libccid v1.4.31-1	✓	✓ <sup>2</sup>	✓	✓	✓	✓
Omnikey CardMan Trust CM3821 <sup>3</sup>	libccid v1.4.31-1	✓	✓ <sup>45</sup>	✓	✓	✓	✓
Reiner SCT cyberJack e-com plus <sup>6</sup>	pcsc-cyberjack v3.99.5final.sp13	✓	✓	✓	✓	✓	✓
Reiner SCT cyberJack secoder <sup>7</sup>		✓	✓	✓	✓	✓	✓
Reiner SCT cyberJack RFID komfort <sup>8</sup>		✓	✓	✓	✓	✓	✓
Reiner SCT cyberJack one <sup>9</sup>		✓	✓	✓	✓	✓	✓

<sup>1</sup> Der Kartenleser unterstützt keine sichere PIN-Eingabe

<sup>2</sup> Der Kartenleser unterstützt keine D-Trust Signaturkarten der Serie 4.x.

<sup>3</sup> Der Kartenleser funktioniert für qualifizierte Signaturen einwandfrei. Fortgeschrittene Signatur, Authentisierung und Verschlüsselung werden nicht unterstützt.

<sup>4</sup> Der Kartenleser unterstützt keine D-Trust Signaturkarten der Serie 4.x.

<sup>5</sup> Neuere Signaturkarten des Herstellers werden nicht unterstützt.

<sup>6</sup> Der Kartenleser kann nur PIN's mit max. 15 Ziffern verarbeiten

<sup>7</sup> Der Kartenleser kann nur PIN's mit max. 15 Ziffern verarbeiten

<sup>8</sup> Der Kartenleser kann nur PIN's mit max. 15 Ziffern verarbeiten

<sup>9</sup> Der Kartenleser kann nur PIN's mit max. 15 Ziffern verarbeiten

## 3.7 Getestete Kombinationen unter Linux: OpenSUSE 15-0

Kartenleser		BNotK	D-Trust	DGN	medisign	TeleSec	SwissSign
Handelsname	Treiber						
Cherry SmartTerminal ST-2000	libccid v1.4.31-1	✓	✓	✓	✓	✓	✓
Cherry TC 1100 <sup>1</sup>		✓	✓	✓	✓	✓	✓
Kobil KAAAN Advanced	libccid v1.4.31-1	✓	✓ <sup>2</sup>	✓	✓	✓	✓
Omniquey CardMan Trust CM3821 <sup>3</sup>	libccid v1.4.31-1	✓	✓ <sup>45</sup>	✓	✓	✓	✓
Reiner SCT cyberJack e-com plus <sup>6</sup>	pcsc-cyberjack v3.99.5final.sp13-1	✓	✓	✓	✓	✓	✓
Reiner SCT cyberJack secoder <sup>7</sup>		✓	✓	✓	✓	✓	✓
Reiner SCT cyberJack RFID komfort <sup>8</sup>		✓	✓	✓	✓	✓	✓
Reiner SCT cyberJack one <sup>9</sup>		✓	✓	✓	✓	✓	✓

<sup>1</sup> Der Kartenleser unterstützt keine sichere PIN-Eingabe

<sup>2</sup> Der Kartenleser unterstützt keine D-Trust Signaturkarten der Serie 4.x.

<sup>3</sup> Der Kartenleser funktioniert für qualifizierte Signaturen einwandfrei. Fortgeschrittene Signatur, Authentisierung und Verschlüsselung werden nicht unterstützt.

<sup>4</sup> Neuere Signaturkarten des Herstellers werden nicht unterstützt.

<sup>5</sup> Der Kartenleser unterstützt keine D-Trust Signaturkarten der Serie 4.x.

<sup>6</sup> Der Kartenleser kann nur PIN's mit max. 15 Ziffern verarbeiten

<sup>7</sup> Der Kartenleser kann nur PIN's mit max. 15 Ziffern verarbeiten

<sup>8</sup> Der Kartenleser kann nur PIN's mit max. 15 Ziffern verarbeiten

<sup>9</sup> Der Kartenleser kann nur PIN's mit max. 15 Ziffern verarbeiten

## 3.8 Getestete Kombinationen unter Mac OS X 10.15.6, 11.0

Kartenleser								
Handelsname	Treiber	BNotK	D-Trust	D-Trust eHBA G2	DGN	medisign	TeleSec	SwissSign
Cherry SmartBoard xx44 <sup>1</sup>	IFD CCID Bundle v1.4.32	✓	✓	✗	✓	✓	✗	✗
Cherry SmartTerminal ST-2000		✓	✓	✗	✓	✓	✗	✗
Cherry SmartTerminal ST-2100		✓	✓ <sup>2</sup>	✗	✓	✓	✗	✗
Cherry KC 1000 SC		✓	✓	✗	✓	✓	✗	✗
Cherry TC 1100 <sup>3</sup>		✓	✓	✗	✓	✓	✗	✗
Kobil KAAAN Advanced	IFD CCID Bundle v1.4.32	✓	✓ <sup>4</sup>	✗	✓	✓	✓	✓
Omniquey CardMan Trust CM3621 <sup>5</sup>	IFD CCID Bundle v1.4.32	✓	✓ <sup>6</sup>	✗	✗	✗	✗	✗
Omniquey CardMan Trust CM3821 <sup>7</sup>		✓	✓ <sup>8</sup>	✗	✗	✗	✗	✗

<sup>1</sup> Der Kartenleser unterstützt keine sichere PIN-Eingabe

<sup>2</sup> Bei einigen Signaturkarten des Herstellers wird die sichere PIN-Eingabe nicht unterstützt

<sup>3</sup> Der Kartenleser unterstützt keine sichere PIN-Eingabe

<sup>4</sup> Der Kartenleser unterstützt keine D-Trust Signaturkarten der Serie 4.x.

<sup>5</sup> Der Kartenleser funktioniert für einzelne Signaturen einwandfrei. Eine sichere PIN-Eingabe wird nicht unterstützt.

<sup>6</sup> Der Kartenleser unterstützt keine D-Trust Signaturkarten der Serie 4.x.

<sup>7</sup> Der Kartenleser funktioniert für einzelne Signaturen einwandfrei. Eine sichere PIN-Eingabe wird nicht unterstützt.

<sup>8</sup> Der Kartenleser unterstützt keine D-Trust Signaturkarten der Serie 4.x.

Reiner SCT cyberJack e-com <sup>1</sup>	cyberJack v3.99.5finalSP14	✓	✓	✗	✓	✓	✓	✓
Reiner SCT cyberJack e-com plus <sup>2</sup>		✓	✓	✗	✓	✓	✓	✓
Reiner SCT cyberJack secoder <sup>3</sup>		✓	✓	✗	✓	✓	✓	✓
Reiner SCT cyberJack RFID komfort <sup>4</sup>		✓	✓	✓	✓	✓	✓	✓
Reiner SCT cyberJack one <sup>5</sup>		✓	✓	✗	✓	✓	✓	✓
SCM Microsystems SPR532	IFD CCID Bundle v1.4.32	✓	✓	✗	✓	✓	✓	✓

<sup>1</sup> Der Kartenleser kann nur PIN's mit max. 15 Ziffern verarbeiten

<sup>2</sup> Der Kartenleser kann nur PIN's mit max. 15 Ziffern verarbeiten

<sup>3</sup> Der Kartenleser kann nur PIN's mit max. 15 Ziffern verarbeiten

<sup>4</sup> Der Kartenleser kann nur PIN's mit max. 15 Ziffern verarbeiten

<sup>5</sup> Der Kartenleser kann nur PIN's mit max. 15 Ziffern verarbeiten