Sign Live! CC
Automation mit Signaturkarten
Installationshinweise

Projekt:	
erstellt von:	Jörg Steinbach
erstellt am:	12.07.2018
Version:	1.3
letzte Änderung:	05.05.2021

Historie

Version	Autor	Änderungen
1.0	jst	initial
1.1	jst	Ergänzungen: Kartenleser, Sicherheit
1.2	jst	Tabelle USB Device Server
1.3	jst	besondere Hinweise ergänzt

1 Einführung

Beim Einsatz von Signaturkarten[1] in serverbasierten Prozessen stellen sich immer die folgenden Fragen:

Kartenleser-Frage: Wie schließe ich den Kartenleser an den Server an?

PIN-Frage: Wer läuft ins Rechenzentrum und gibt die PIN ein?

Im Rechenzentrumsbetrieb gibt es unterschiedliche Gründe, einen Kartenleser nicht direkt an den Rechner anzuschließen bzw. anschließen zu können:

- Signaturdienst soll auf einer Server-Farm betrieben werden. Die VM, auf der der Dienst betrieben wird, kann nicht einem dedizierten Rechner zugeordnet werden.
- Kartenleser finden im Rack keinen Platz mehr / sollen physikalisch an anderer Stelle, evtl. sogar außerhalb des Rechenzentrums platziert werden, damit z. B. der Administrator nicht ins Rechenzentrum laufen muss.
- Administrator kann 2:00 Uhr morgens keine PIN am Kartenleser eingeben, wenn Rechner neu gestartet wird.
- Einige Reiner SCT Kartenlesers verlangen nach Neustart des Kartenlesers (z. B. bedingt durch Stromunterbrechung) das Ziehen/Stecken der gesteckten Karte. Ohne diesen Prozess kann keine Verbindung zur Karte aufgebaut werden.

Dieses Handbuch stellt im Kapitel 2 ein Konzept vor, welches diese Frage mit maximalem Administrationskomfort beantwortet, und fasst in den Kapiteln 3-6 die nötigen Administrationshinweise zusammen.

Im Kontext von Signaturkarten ist maximaler Administrationskomfort immer mit einer Reduzierung von Sicherheit verbunden. Der Leser möge anhand der in Kapitel 7 gelieferten Informationen selbst entscheiden, welche Kompromissformel er für seinen Betrieb findet.

2 Konzept

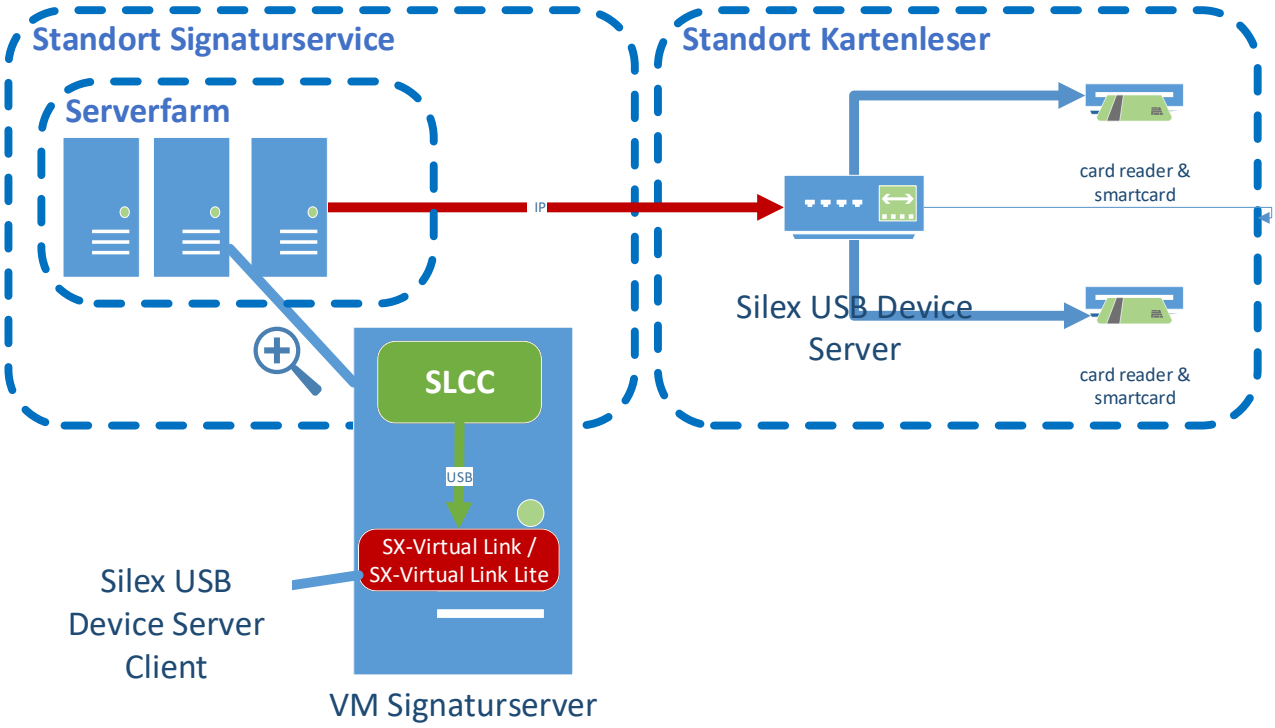
Auf Basis von USB Device Servern und den Konfigurationsmöglichkeiten, in Sign Live! CC PINs zu speichern, können wir die gestellten Fragen mit einfachen Mitteln beantworten.

USB Device Server stellen an sie angeschlossene USB-Geräte im Netzwerk zur Verfügung. Über die auf einem Rechner installierte Client-Software der USB Device Server können diese Rechner auf die angebotenen USB-Geräte in der gleichen Form zugreifen, wie wenn sie lokal angeschlossen wären. Somit ist die Kommunikation zwischen ihrer Signatursoftware und den Signaturkarten an jedem netzwerktechnisch erreichbaren Ort in ihrem Unternehmen möglich.

Sign Live! CC bietet die Möglichkeit, PINs für Smartcards via Kartenleser/GUI einzugeben und bei Bedarf in verschlüsselter Form dauerhaft zu speichern. Somit ist es möglich, Kartenleser sowohl fernzusteuern, als auch z. B. nach Server-Neustarts automatisiert PINs einzugeben.

[1] Der Begriff „Signaturkarte“ wird synonym für Signaturerstellungseinheit verwendet und bezeichnet somit Signatur- und Siegelkarten.

Z. Zt. setzen wir vorwiegend USB Device Server der Firma Silex (DS-510, DS-600) ein, weil sich diese in unseren Kundenprojekten bewährt und wir damit Knowhow aufgebaut haben. Die folgende Beschreibung bezieht sich daher auf diese Geräte. Andere Geräte sollten in ähnlicher Weise funktionieren.



3 Kartenleser

Damit SLCC auf eine Signaturkarte zugreifen kann, benötigt es einen Kartenleser und den zum Kartenleser passenden Treiber.

1. Bitte installieren Sie den Kartenlesertreiber nach Vorgabe des Herstellers auf dem Signaturserver.
2. Bitte installieren Sie auf dem Signaturserver eine Software für Fernwartung, die weder das RDP- noch das ICA-Protokoll verwendet (z. B. VNC).
   Hintergrund:
   Beide Protokolle stellen korrekt die via USB am Server angeschlossenen Geräte zur Verfügung (s. Windows Geräte-Manager). Jedoch macht das für die Kommunikation zur Karte notwendige PC/SC-Protokoll Probleme, sofern Programme die das PC/SC-Protokoll verwenden unter dem gleichen Benutzer laufen, wie der RDP-/ICA-Benutzer. Dies führt dazu, dass weder SLCC noch der CyberJack-Geräte-Manager Zugriff auf Kartenleser/Signaturkarte haben.
   D. h. für die Installation der Software ist ein anderes Fernwartungsprotokoll notwendig (z. B. VNC). Die Überwachung des Servers ist via RDP/ICA möglich, sofern der sich anmeldende Benutzer nicht der gleiche ist, unter dem auf die Karten zugegriffen wird.

Hinweise

- **Signaturkarte Ziehen/Stecken bei Reiner SCT Kartenleser**
  Nach Neustart des Kartenlesers (bedingt durch Stromunterbrechung) verlangen einige Reiner SCT Kartenleser das Ziehen/Stecken bereits eingesteckter Signaturkarten.
  Workaround:
  Betreiben Sie Reiner SCT Kartenleser über eine USB Device Server. Dieser hält die Verbindung zum Kartenleser aufrecht, so dass das Ziehen/Stecken nur dann notwendig wird, wenn die Stromversorgung des USB Device Servers unterbrochen wird.

4 Signaturkarten

Signaturkarten enthalten ein oder meistens mehrere Zertifikate. Um mit diesen Zertifikaten zu signieren, müssen Sie

1. die PINs der Zertifikate initialisieren. Hierzu stellt der Kartenausgeber Software zur Verfügung. In den meisten Fällen können Sie dies auch mit SLCC unter der Menüoption Werkzeuge>Smartcard Werkzeuge>PIN Management durchführen.
2. die Karte dem Kartenausgeber zurückmelden, damit dieser die Karte für Sie freischaltet.

Zu beiden Punkten haben Sie zusammen mit der Signaturkarte detaillierte Informationen vom Kartenausgeber erhalten.

Wichtige Hinweise!

- Sie benötigen eine Siegel-/Signaturkarte mit Massensignaturfunktion (mit einer PIN-Eingabe beliebig viele Signaturen erstellen).
- Wenn Sie die PIN für ein Zertifikat 3 x hintereinander falsch eingeben, wird das betreffende Zertifikat auf dieser Karte gesperrt und ist nicht mehr verwendbar[2]. Wenn Sie nur 1 x oder 2 x die PIN falsch eingegeben haben, können und sollten Sie den Fehlerzähler zurücksetzen, indem Sie die PIN einmal korrekt eingeben.

Tipps

- Initialisieren Sie zu Beginn **alle** Zertifikate der Karte und bewahren Sie die PINs an einem sicheren Ort auf.
- Wenn Sie mehrere Karten mit automatischer PIN Eingabe betreiben, ist es sinnvoll, dass die verwendeten Zertifikate die gleiche PIN erhalten, um Fehleingaben zu vermeiden.

5 Sign Live! CC

Im Folgenden finden Sie als Kurzanleitung die für dieses Konzept wichtigen Punkte zur Installation/Konfiguration von Sign Live! CC. Die vollständige Dokumentation finden Sie im SLCC-

[2] bei Telesec-Karten besteht die Möglichkeit, die PIN über eine andere PIN zu reaktivieren

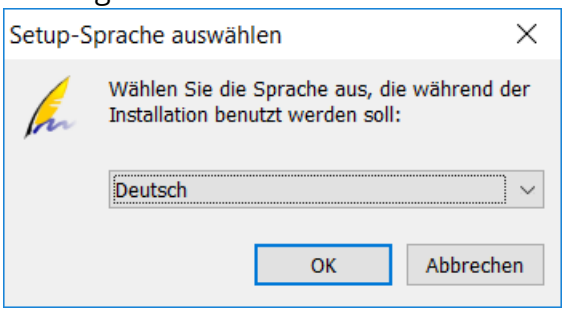
Installationsverzeichnis unter <SLCC_INSTALL>\doc bzw. über die Hilfe-Funktion in der gestarteten Software.

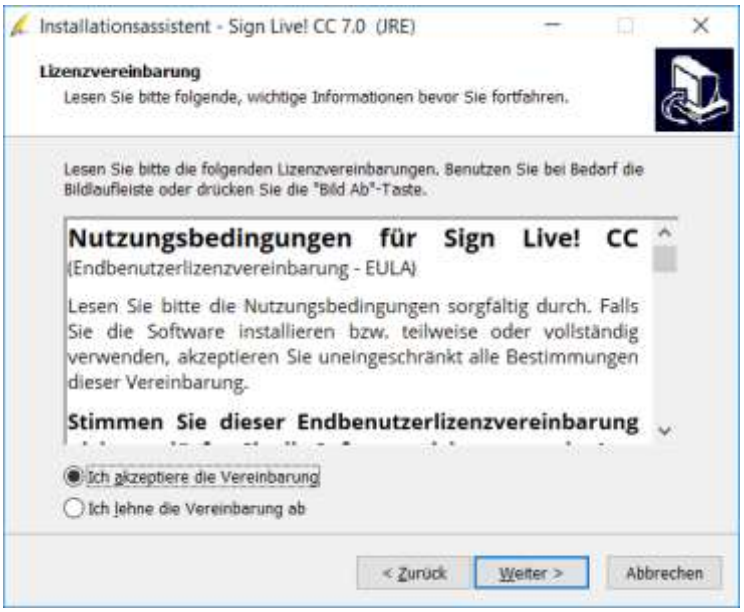
5.1 SLCC installieren

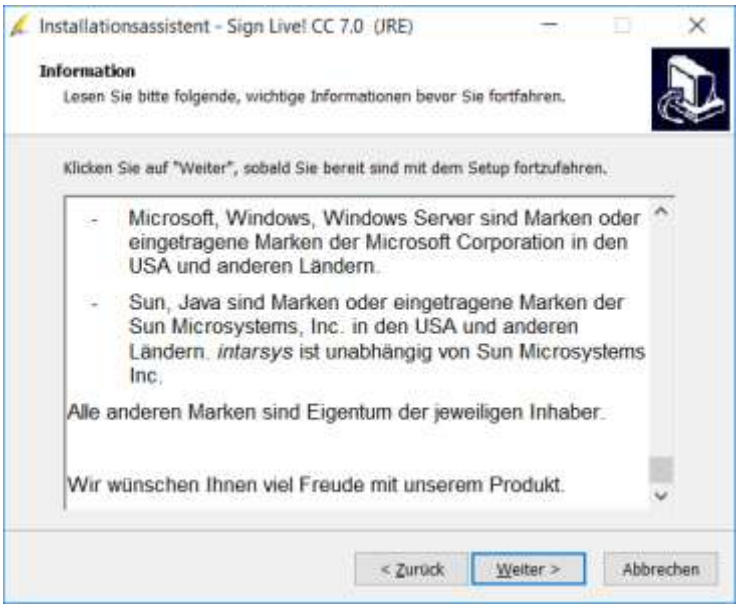
Laden Sie den jeweils aktuellen SLCC-Installer von der intarsys Hompage herunter: https://www.intarsys.de/versionshinweise.

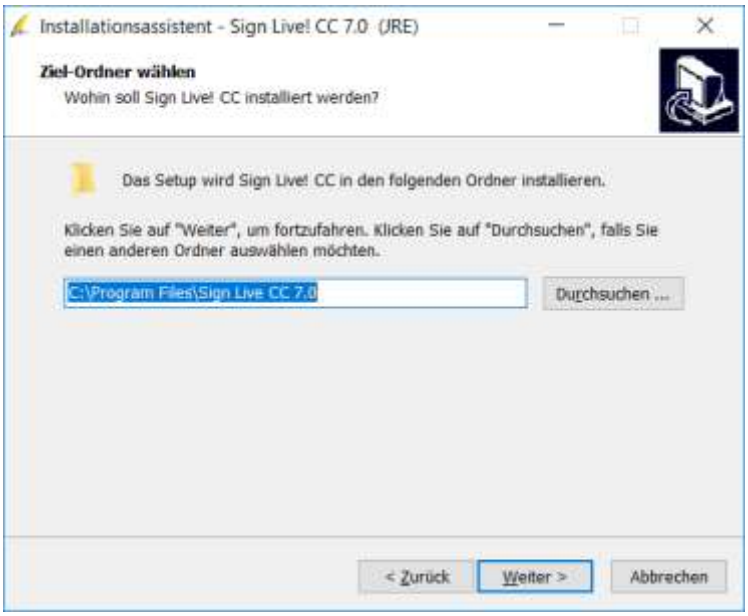
Gehen Sie nun bitte folgendermaßen vor:

1. Starten Sie den Installer mit Administrationsrechten und führen Sie ihn mit Default-Einstellungen durch:

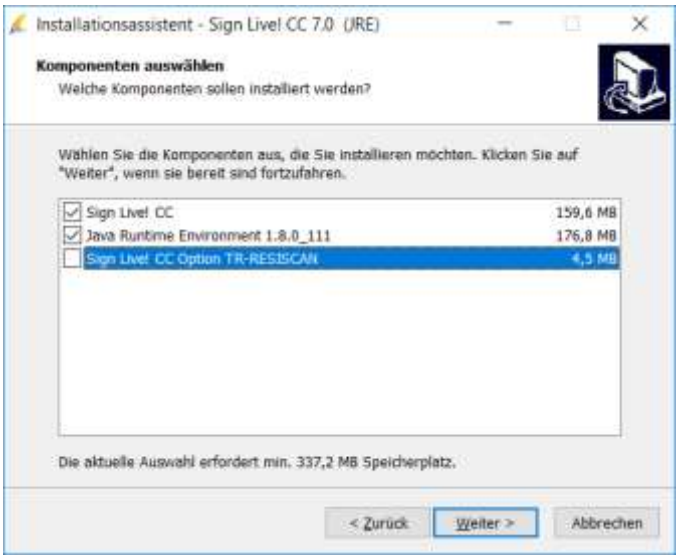


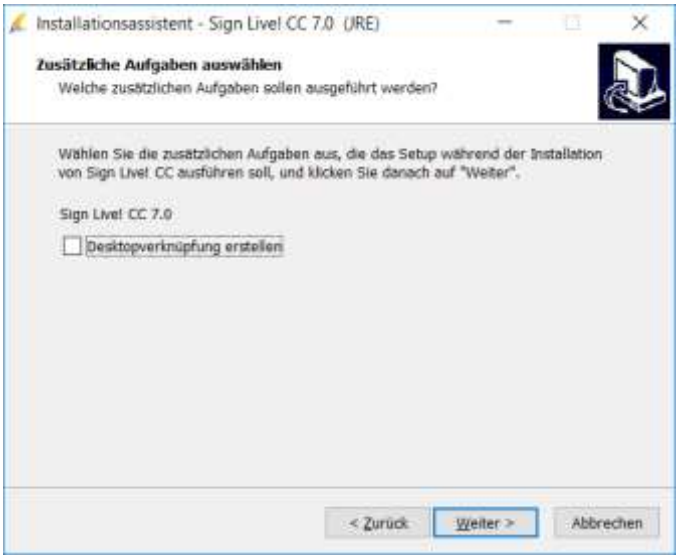


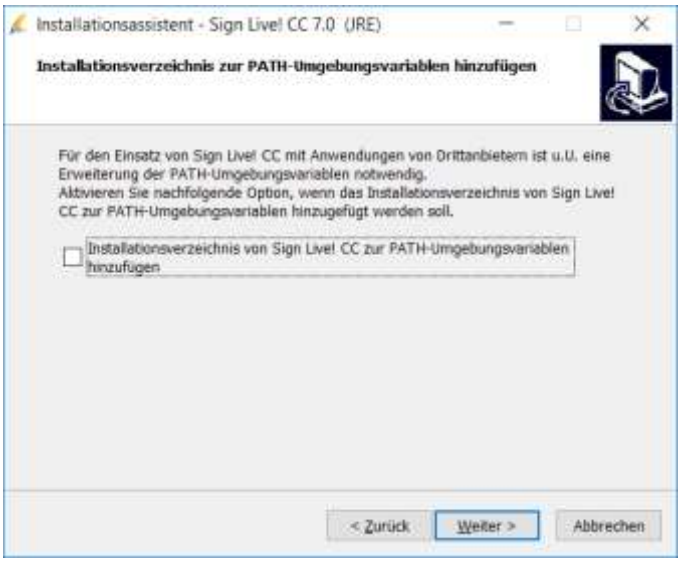


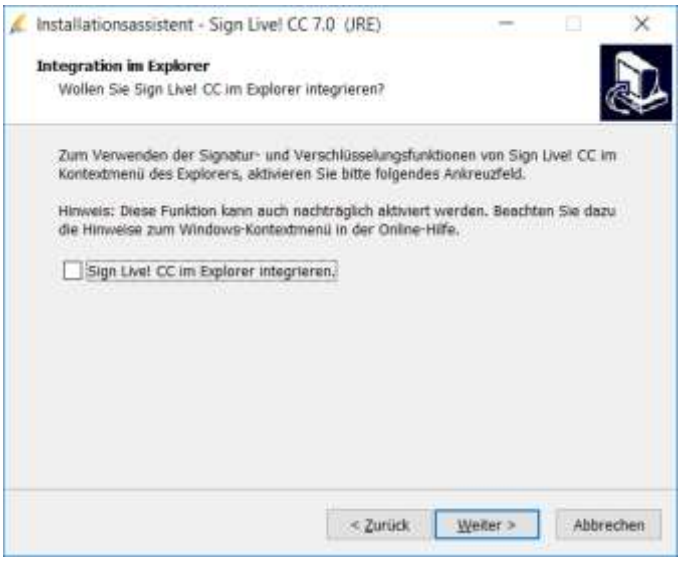


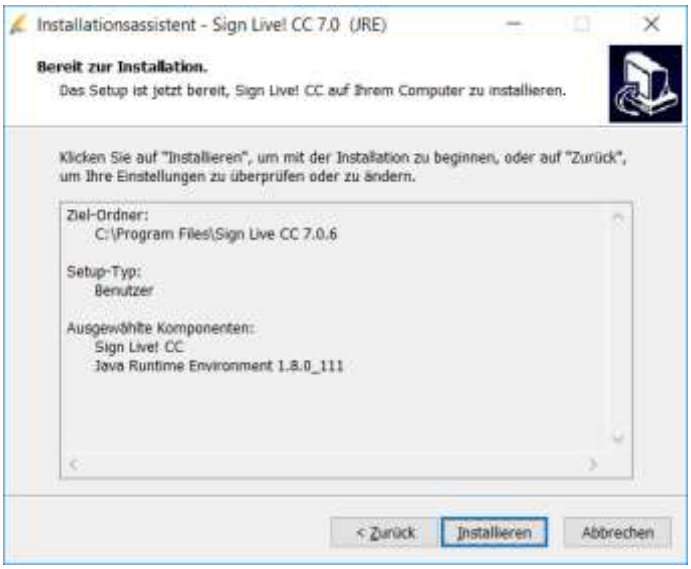
Die Option TR-RESISCAN benötigen Sie nicht:


Installationsassistent - Sign Live! CC 7.0 (JRE)
Komponenten auswählen
Welche Komponenten sollen installiert werden?
Wählen Sie die Komponenten aus, die Sie installieren möchten. Klicken Sie auf "Weiter", wenn sie bereit sind fortzufahren.
Sign Live! CC 159,6 MB
Java Runtime Environment 1.8.0_111 176,8 MB
Sign Live! CC Option TR-RESISCAN 4,5 MB
Die aktuelle Auswahl erfordert min. 337,2 MB Speicherplatz.
< Zurück
Weiter >
Abbrechen


Installationsassistent - Sign Live! CC 7.0 (JRE)
Zusätzliche Aufgaben auswählen
Welche zusätzlichen Aufgaben sollen ausgeführt werden?
Wählen Sie die zusätzlichen Aufgaben aus, die das Setup während der Installation von Sign Live! CC ausführen soll, und klicken Sie danach auf "Weiter".
Sign Live! CC 7.0
Desktopverknüpfung erstellen
< Zurück
Weiter >
Abbrechen


Installationsassistent - Sign Live! CC 7.0 (JRE)
Installationsverzeichnis zur PATH-Umgebungsvariablen hinzufügen
Für den Einsatz von Sign Live! CC mit Anwendungen von Drittanbietern ist u.U. eine Erweiterung der PATH-Umgebungsvariablen notwendig.
Aktivieren Sie nachfolgende Option, wenn das Installationsverzeichnis von Sign Live! CC zur PATH-Umgebungsvariablen hinzugefügt werden soll.
Installationsverzeichnis von Sign Live! CC zur PATH-Umgebungsvariablen hinzufügen
< Zurück
Weiter >
Abbrechen





SLCC ist nun im gewünschten Verzeichnis <SLCC_INSTALL> installiert.
Das Profilverzeichnis <SLCC_PROFILE>, in dem SLCC Konfigurations- und Log-Dateien ablegt, liegt versionsabhängig z. B. unter C:\ProgramData\.SignLiveCC_7.0

2. Ohne Lizenzdatei ist der Betrieb eines SLCC-Dienstcontainers nicht möglich. Installieren Sie die vom Hersteller gelieferte(n) Lizenzdatei(en) im Verzeichnis <SLCC_PROFILE>\licenses und starten Sie die Software neu, um die Lizenzdateien zu aktivieren.
3. optional: Um das Profilverzeichnisses an einer anderen Stelle abzulegen, verschieben Sie bitte das aktuelle Profilverzeichnis an die gewünschte Stelle und machen dies SLCC bekannt über die Konfigurationsdatei <SLCC_INSTALL>\config\service.config.
4. **Wichtig!** Verwenden Sie zum Konfigurieren von SLCC für den Betrieb als Windows-Dienst immer den GUI-Modus über die Verknüpfung „Sign Live! CC 7.0 Service Administrator“, niemals einen anderen Link oder direkt den Programmaufruf *SignLiveCC.exe* ohne Parameter. Andernfalls verwenden Windows Dienst und GUI Variante unterschiedliche Konfigurationsverzeichnisse.

Wichtig! Aktivieren Sie niemals gleichzeitig SLCC im GUI-Modus und den SLCC Windows-Dienst, da beide das gleiche Verzeichnis <SLCC_PROFILE> verwenden.

5.2 SLCC als Windows Dienst installieren

Voraussetzung ist, dass Sign Live! CC bereits installiert ist.

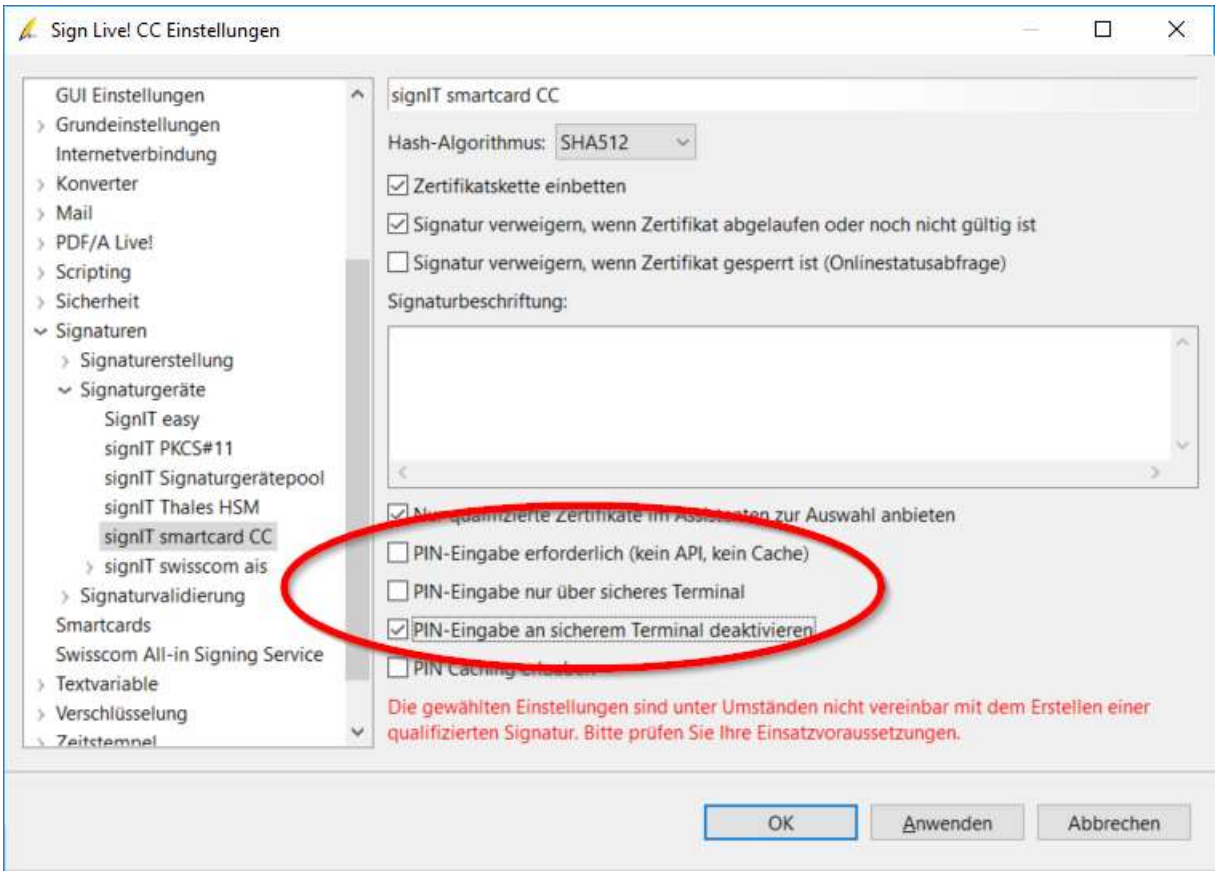
Gehen Sie nun bitte folgendermaßen vor:

1. Starten Sie die Kommandodatei <SLCC_INSTALL>\bin\SignLiveCC_service_install.bat mit Administrationsrechten.
2. Bei Bedarf können Sie nun inder Windows Dienstverwaltung die Eigenschaften des Dienstes anpassen bzw. den Dienst steuern.
   Alternativ können Sie den Dienst auch über die Kommandodateien <SLCC_INSTALL>\bin\SignLiveCC_service_start.bat etc. steuern.
   Sie benötigen dazu ebenfalls Administrationsrechte. Dies können Sie auch bequem in den Eigenschaften der Verknüpfung hinterlegen:

5.3 Entfernte PIN-Eingabe

Entfernte PIN-Eingabe bedeutet, dass die PIN der Signaturkarte nicht am Kartenleser, sondern über das GUI von SLCC eingegeben wird. Dazu müssen Sie die Sicherheitsmechanismen von SLCC deaktivieren:

1. Starten Sie SLCC im GUI-Modus über die Verknüpfung „Sign Live! CC 7.0 Service Administrator“.
2. Nehmen Sie dazu unter Extras>Einstellungen folgende Einstellungen vor:



Nun ist die sicher PIN-Eingabe deaktiviert und Sie können bei der nächsten PIN-Abfrage die PIN über das GUI eingeben.

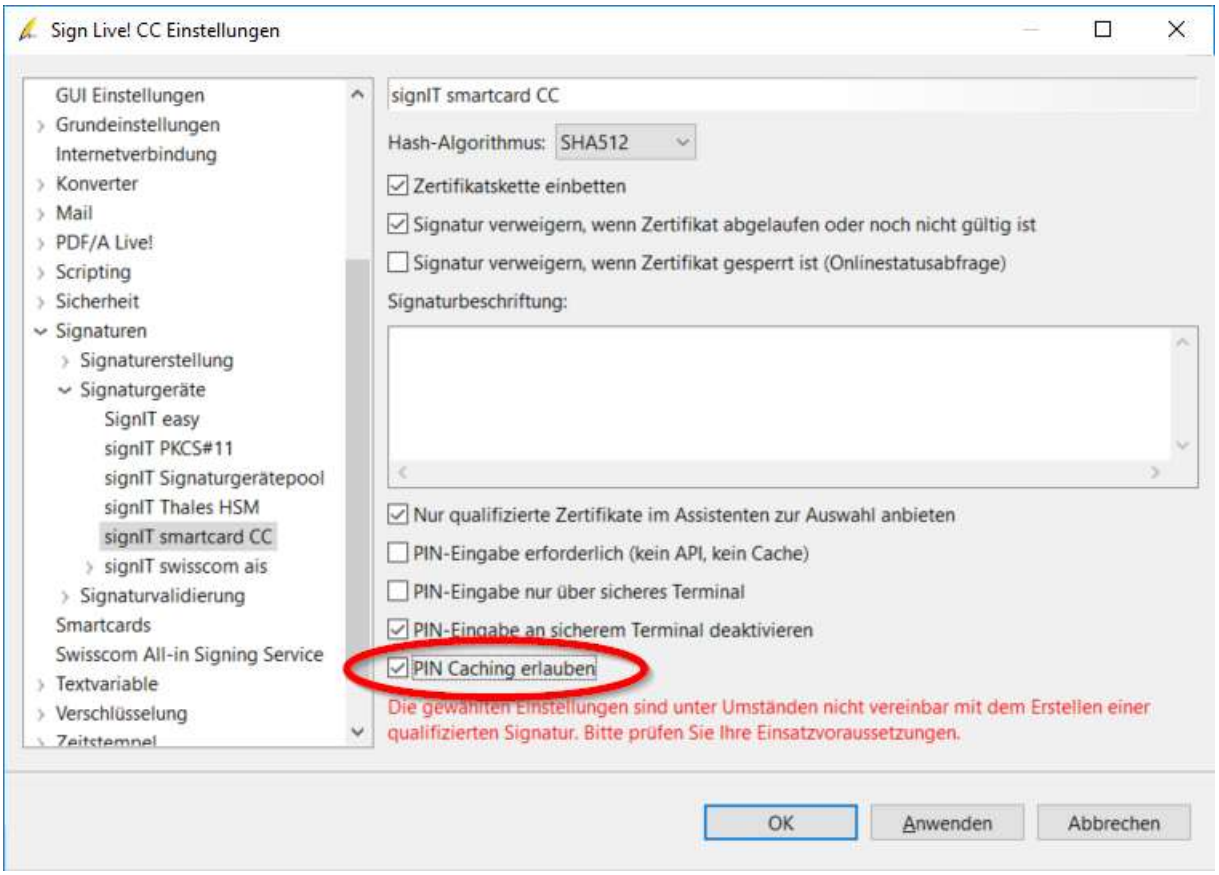
5.4 Automatische PIN-Eingabe

Automatische PIN-Eingabe bedeutet, dass SLCC die PIN der Signaturkarte in verschlüsselter Form verwaltet und bei PIN-Abfrage via Filtereinstellungen auswählt und automatisch ohne Benutzerinteraktion eingibt.

Vorsicht! Die definierten Einstellungen müssen korrekt sein. Die meisten Signaturkaten sperren nach dreimaliger Falscheingabe den Zugang zur Karte und müssen dann je nach Hersteller neu bestellt werden.

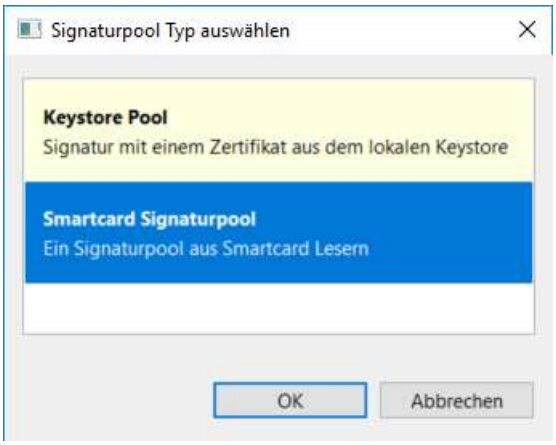
Für die automatische PIN-Eingabe gehen Sie bitte folgendermaßen vor: Dazu müssen Sie die Sicherheitsmechanismen von SLCC deaktivieren:

1. Starten Sie SLCC im GUI-Modus über die Verknüpfung „Sign Live! CC 7.0 Service Administrator“.
2. **PIN-Caching erlauben**
   Zunächst müssen Sie zusätzlich zur entfernten PIN-Eingabe das PIN-Caching erlauben. Nehmen Sie dazu unter Extras>Einstellungen folgende Einstellungen vor:

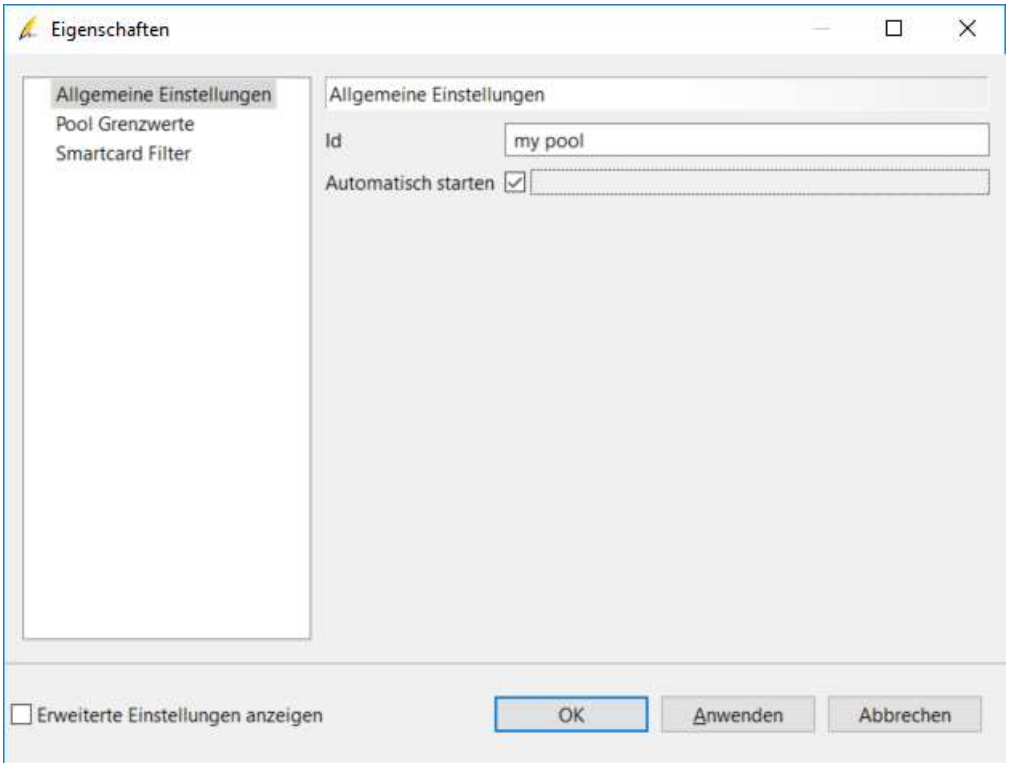


Nun ist das PIN-Caching erlaubt.

3. **Smartcard-Pool anlegen**
   Smartcards werden in SLCC über Smartcard-Pools angesprochen. Falls noch nicht vorhanden, legen Sie zunächst einen Smartcard Signaturpool für den Zugriff auf 1-N Karten an:
   Über Werkzeuge>Signaturfunktionen>Signaturpool Verwaltung öffnen Sie die Pool Verwaltung. Über ➕ legen Sie einen neuen Pool an. Wählen Sie Smartcard Signaturpool,



vergeben Sie einen Namen und setzen Sie auf jeden Fall die Option „Automatisch starten“:



Im Standardfall ist ein Pool für 1 Karte vorgesehen. Sollen mehr als 1 Karte eingesetzt werden, passen Sie die Pool Grenzwerte entsprechend an und erwerben Sie die dazu notwendige Lizenz.

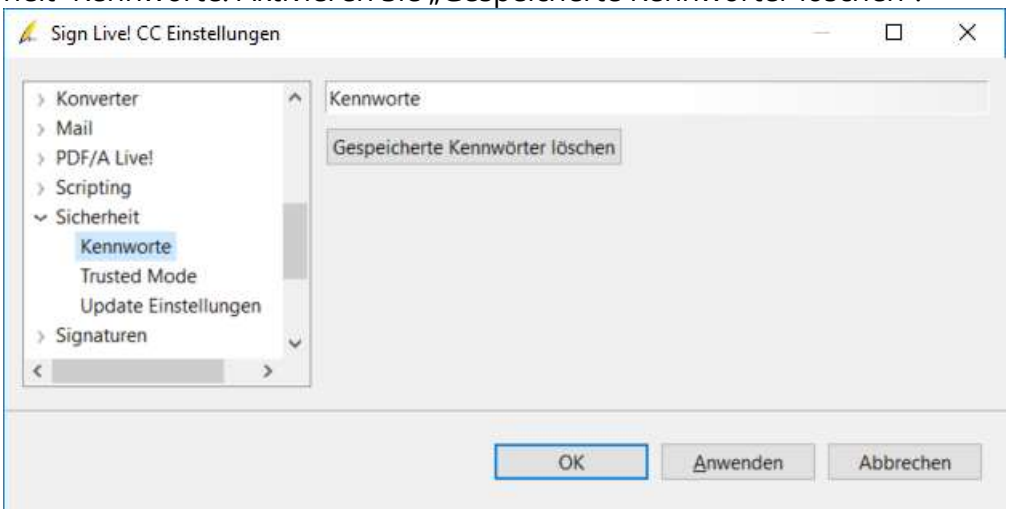
4. **Filter definieren**
   Über die Smartcard Filter eines Pools definieren Sie welche Zertifikate für diesen Pool sichtbar sein sollen. Die Attribute eines Filters sind UND-verknüpft, die Filter selbst sind ODER-verknüpft.
   Tipp:
   Die meisten Signaturkarten umfassen mehrere Zertifikate. Wählen Sie die Einstellung „Verbindliche Signaturzertifikate“, um ausschließlich qualifizierte Zertifikate zu selektieren. Wenn Sie unterschiedliche PINs für Ihre Signaturkarten vergeben haben, definieren Sie unbedingt eindeutige Filter für jede Signaturkarte, um automatisierte, falsche PIN-Eingaben zu vermeiden, was sehr schnell zur Unbrauchbarkeit der Karte führt.
5. **PIN registrieren**
   Nach Aktivieren der Schaltfläche „PIN hinterlegen“, sucht SLCC nach gemäß Filtereinstellungen verfügbaren Zertifikaten, zeigt sie nacheinander an und fragt für jedes die zugehörige PIN ab. Wenn Sie die PIN Eingabe ablehnen, wird beim nächsten Zertifikat fortgesetzt. Jede eingegebene PIN wird eineindeutig einem Zertifikat zugeordnet und gespeichert.

6. **PIN verwenden**
   Sobald nun eine Signaturaktion via Pool oder auch via Signaturassistent ausgelöst wird, versucht SLCC eine passende PIN zu ermitteln und verwendet diese auch sofort.

5.5 Gespeicherte PINs löschen

Zum Löschen gespeicherter PINs gehen Sie bitte folgendermaßen vor:

1. Starten Sie SLCC im GUI-Modus über die Verknüpfung „Sign Live! CC 7.0 Service Administrator“.
2. Öffnen Sie die Seite „Kennworte“ über die Menüoption Extras>Einstellungen>Sicherheit>Kennworte. Aktivieren Sie „Gespeicherte Kennwörter löschen“.



   Alle gespeicherten Kennwörter werden gelöscht.

6 Silex USB Device Server (SX Server)

Ein USB Device Server ist immer dann erforderlich, wenn der Kartenleser nicht direkt an den Server der Signatursoftware angeschlossen werden kann oder soll.

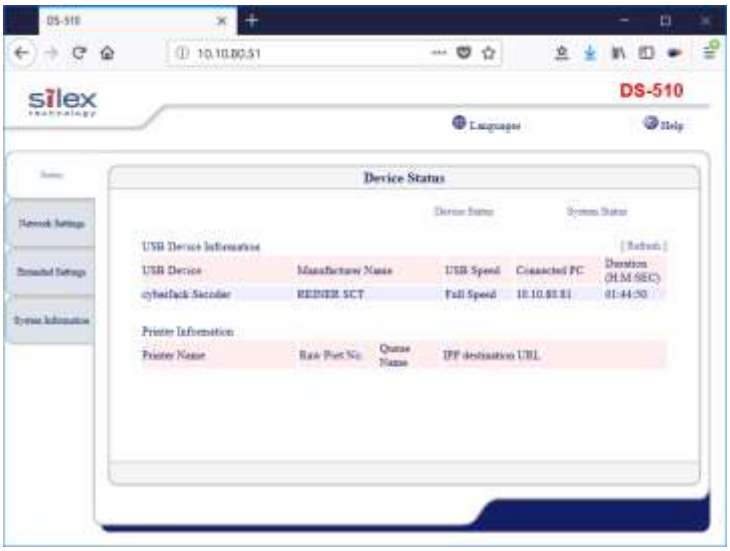
6.1 Server installieren/konfigurieren

Wichtiger Hinweis!

Die Verbindung zu den SX Servern wird immer über den Port 19540 hergestellt. Bitte sorgen Sie daher dafür, dass Port 19540 UDP und TCP nicht blockiert sind.

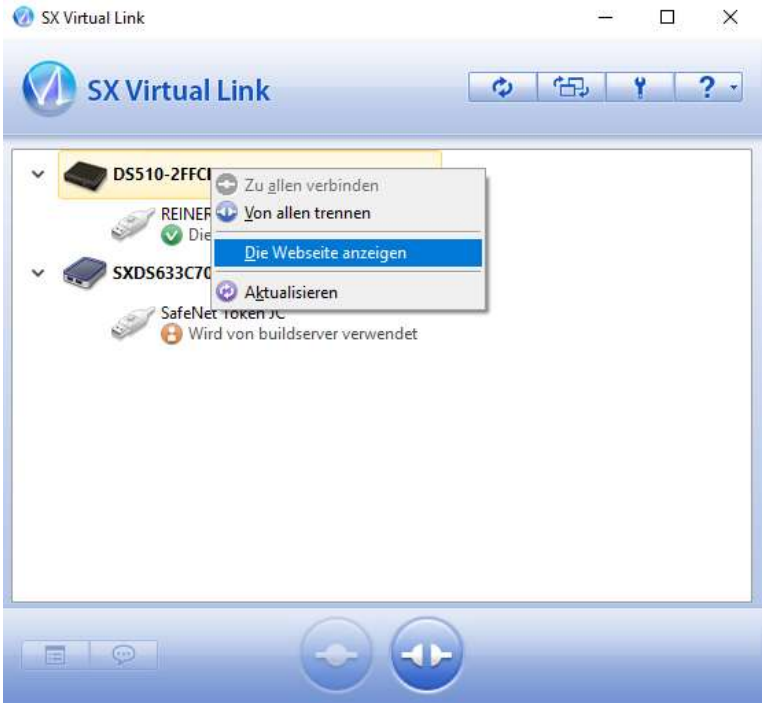
Folgender Ablauf hat sich bewährt:

1. Verbinden Sie den SX Server mit Ihrem Netzwerk und dann mit dem Stromnetz. Der USB Device Server registriert sich nun standardmäßig via DHCP im Netzwerk. An den SX Server via USB angeschlossene Gerätegeben sind fortan im Netzwerk verfügbar.
2. Der SX Server wird über eine SX Server Konfigurationsanwendung via Port 80 administriert. Dazu benötigen Sie seine IP, fortan <SX_HOST> genannt.
   Minimalistischer Ansatz: Ermitteln Sie die <SX_HOST> z. B. mit einen IP-Scanner wie „Angry IP Scanner“[3]. Geben Sie diese anschließend als URL http://<SX_HOST> im Browser ein und öffnen damit die SX Server Konfigurationsanwendung:



   Komfortabler Ansatz: Installieren und starten Sie die Silex Client Software **SX Virtual Link** (s. Kap. 6.2.1). Unter Optionen>Filter finden Sie die in ihrem Netzwerk verfügbaren SX Server und deren IP. Aktivieren Sie über das Kontextmenü des gewünschten SX Servers die Funktion „Die Webseite anzeigen“ (s. u.) und öffnen damit die SX Server Konfigurationsanwendung.

[3] ggfs. genügt auch die Kommandozeile arp -a



3. Folgende Konfigurationseinstellungen sind für den Server sinnvoll:
   - Ändern Sie das Default-Kennwort!!!
   (System Information>Password; der Initialzugang lautet („root“/““)
   - Definieren Sie bei Bedarf eine feste IP (Network Settings)
   - Definieren Sie bei Bedarf einen Filter für erlaubte Clients (Network Settings>Security)
   - Lassen Sie den ECO-Modus ausgeschaltet.

6.2 Client installieren/konfigurieren

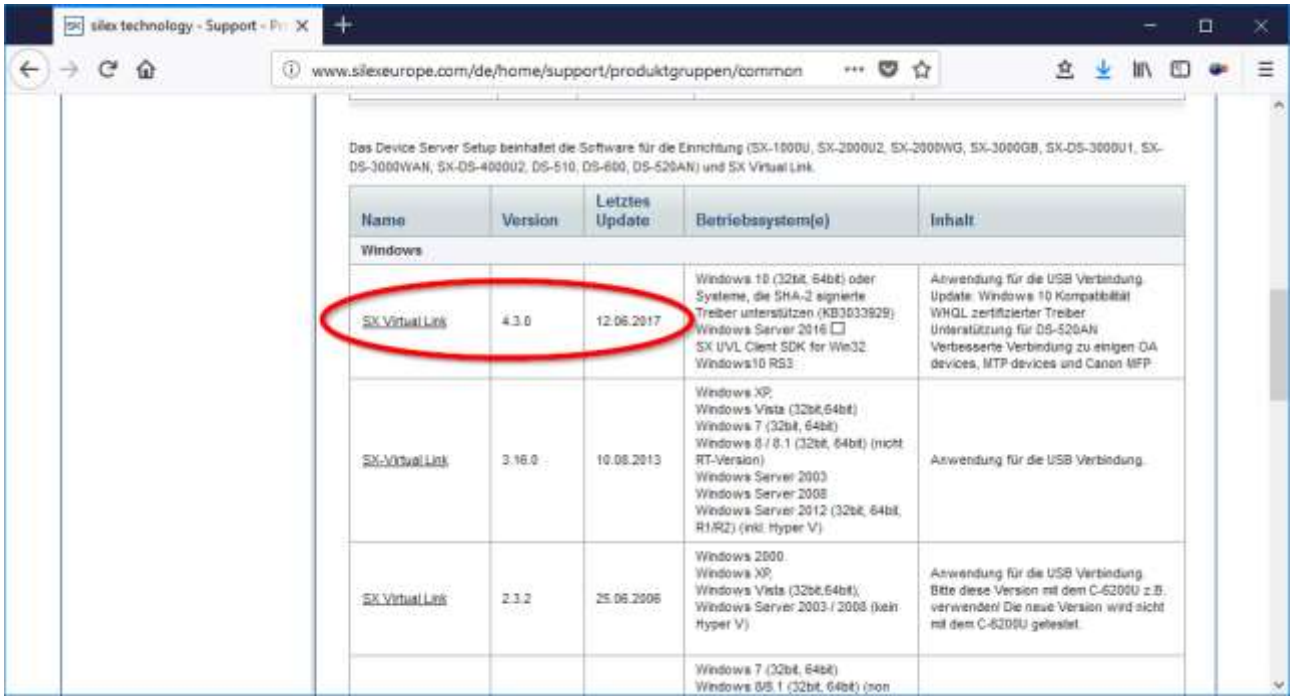
Nach Konfiguration des SX Servers müssen Sie nun den SX Client auf allen Systemen installieren, von denen aus auf die Kartenleser zugegriffen werden soll. Für den Fall, dass das Signatursystem mit manueller PIN-Eingabe arbeiten soll, ist **SX Virtual Link** als Client Software ausreichend (s. Kap. 6.2.1).

Wenn jedoch die PIN für die Kartenleser bei Systemstart vom Sign Live! CC Windows Dienst automatisch eingegeben werden soll, muss dafür gesorgt werden, dass die Verbindung zu den Kartenlesern zu diesem Zeitpunkt bereits aufgebaut ist. Dazu bedarf es einer Reihenfolgensteuerung von Sign Live! CC und der SX Client Software. In diesem Fall installieren Sie bitte die Software **SX Virtual Link Lite** (s. Kap. 6.2.2). In allen anderen Fällen können Sie darauf verzichten und die Steuerungsmöglichkeiten von SX Virtual Link verwenden.

6.2.1 SX Virtual Link installieren/konfigurieren

SX Virtual Link ermöglicht eine bequeme und übersichtliche Steuerung der Client-Komponente. Sie lässt sich automatisch bei Start von Windows starten und lässt die Definition von Reihenfolgebeziehung zu anderen Programmen, jedoch nicht zu Diensten zu. Details hierzu finden Sie in der zugehörigen Silex-Dokumentation.

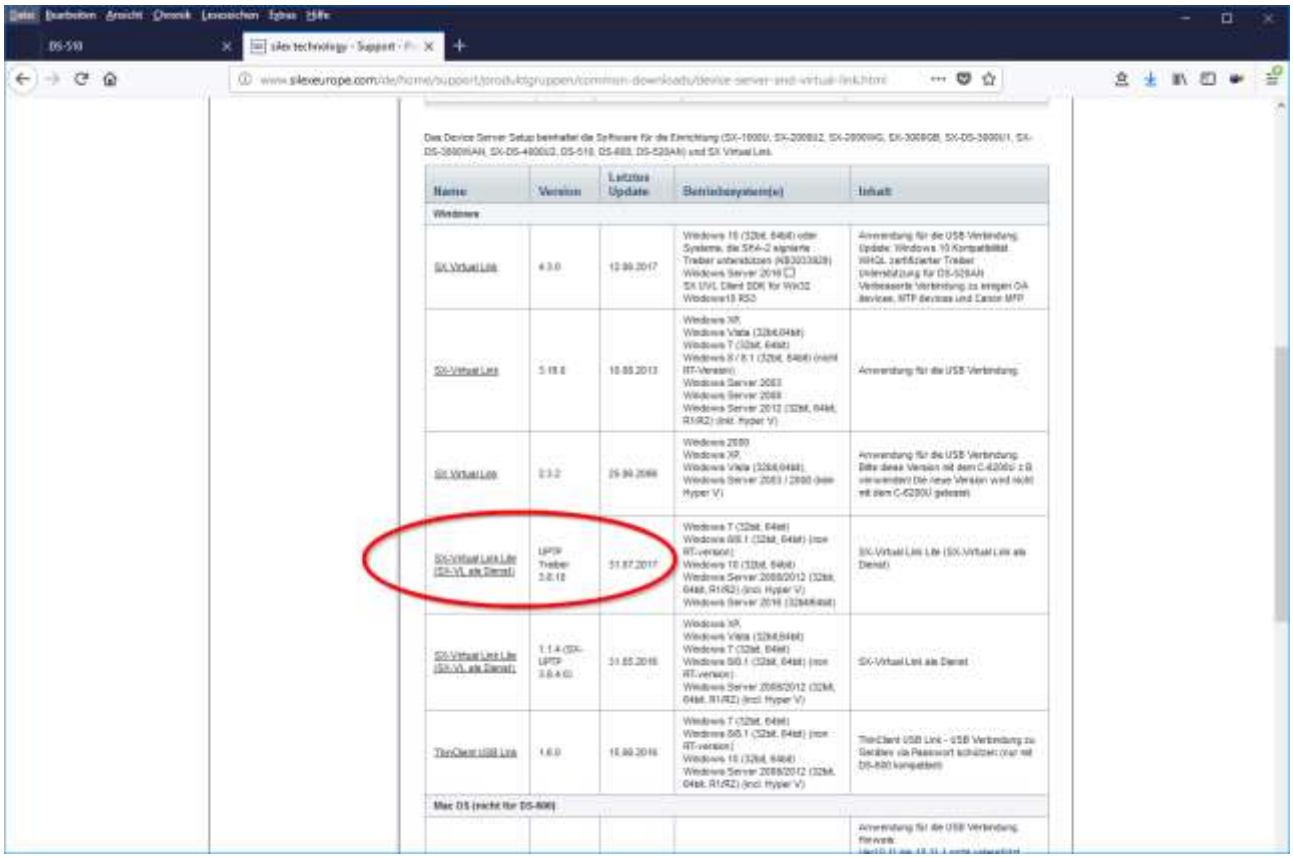
Laden Sie SX Virtual Link von der Silex Homepage[4] herunter und installieren Sie es durch Ausführen des Setups:



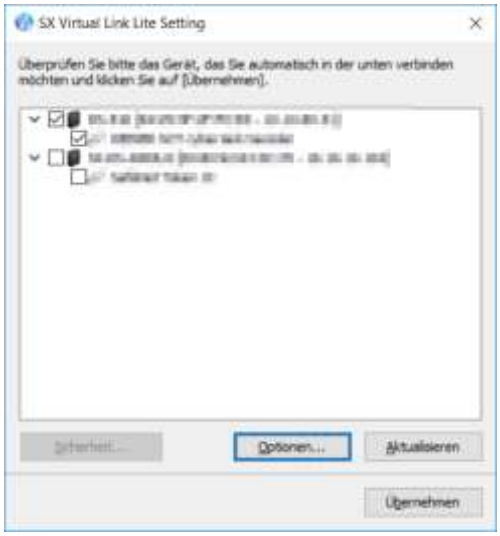
6.2.2 SX Virtual Link Lite installieren/konfigurieren

Laden Sie SX Virtual Link Lite von der Silex Homepage herunter und installieren Sie es durch Ausführen des Setups.

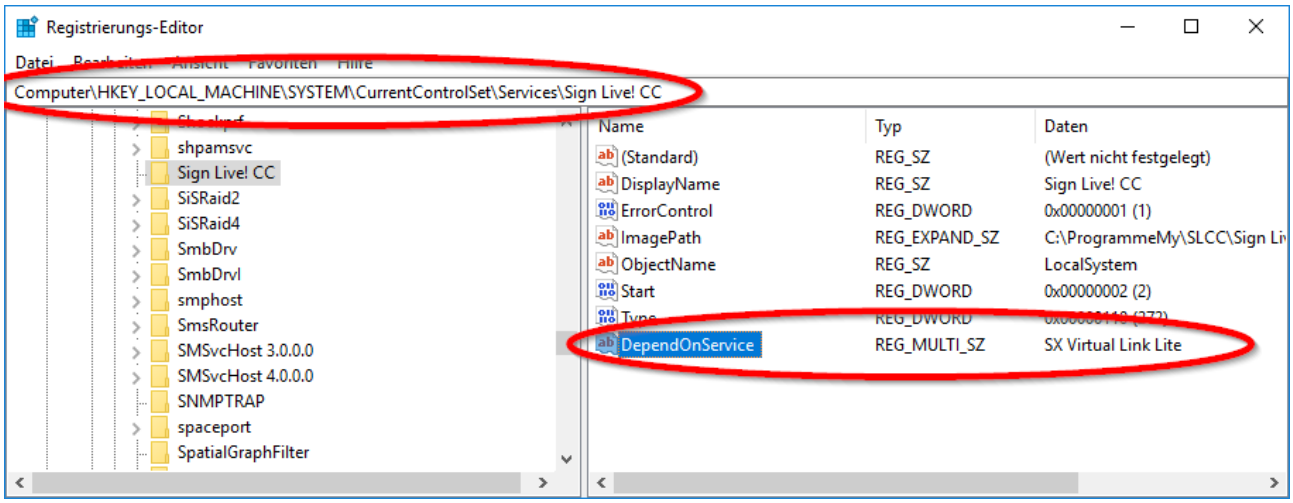
[4] http://www.silexeurope.com/de/home/support/produktgruppen/common-downloads/device-server-and-virtual-link.html



SX Virtual Link Lite installiert sich unter dem gleichen Namen als Windows-Service und startet automatisch. Die Konfiguration, mit welchem SX Server sich der Dienst verbinden soll, erfolgt über C:\Program Files\silex technology\SX Virtual Link Lite\Setting\SvlSetting.exe:



Damit Sign Live! CC erst dann startet, wenn SX Virtual Link Lite bereits eine Verbindung zur Karte aufgebaut hat, definieren Sie über den Windows Registrierungseditor (regedit) für Ihren Sign Live! CC – Windows Dienst die Abhängigkeit zu SX Virtual Link Lite durch folgenden Eintrag. Voraussetzung ist natürlich, dass der Sign Live! CC Windows Dienst bereits installiert ist.



Anschließend führen Sie bitte einen Neustart des Rechners durch.

6.3 Besondere Hinweise

Wichtige Hinweise zu Silex USB Device Servern finden Sie in den Silex FAQ unter http://www.silexeurope.com/de/home/support/faq/-usb-device-server.html .

6.3.1 USB Device Server in den Auslieferungszustand zurücksetzen

Unterbrechen Sie die Stromverbindung zu ihrem USB Device Server. Drücken Sie einen kleinen Druckknopf am Rande des Gerätes und halten Sie ihn gedrückt. Stellen Sie die Stromverbindung wieder her und lassen Sie den Druckknopf nach ca. 6 sek los.

Der USB Device Server ist nun auf den Initialzustand (*factory default)* zurückgesetzt. Die Zugangsdaten lauten wieder „root“/““.

6.3.2 USB-Hubs am USB Device Server

DS-510 und DS-600 können jeweils zwei USB-Geräte anschließen.

Mehr Geräte können über USB-Hubs an den USB Device Server angeschlossen werden, jedoch beschränkt auf eine (1) Hierarchieebene! Praxiserfahrungen zu diesem Szenario in Zusammenhang mit Kartenlesern haben wir noch nicht gesammelt.

6.3.3 Verbindung zu Kartenlesern geht sporadisch verloren

Windows meldet Kartenleser bei Inaktivität automatisch ab, wenn ein Timeout von 5 sec überschritten wird. SLCC sendet daher alle 4 sec ein *keep alive* Signal. Wenn dieses Signal z. B. bei Netzwerk-Problemen nicht rechtzeitig zum Kartenleser gelangt, kann daher die Verbindung zum Kartenleser verloren gehen.

Durch Hinzufügen/Setzen des Registry Keys HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Calais\TransactionTimeoutDelay kann der Default von 5 sec auf bis zu 60 sec hochgesetzt werden.

S. auch https://support.microsoft.com/en-us/help/2706168/applications-that-use-smart-card-authentication-stop-responding-on-a-c

7 Sicherheit

Welche zusätzlichen Risiken bestehen beim Betrieb eines USB Device Servers?

7.1 Angriffsszenario: Ausspähen der PIN / Mitlesen von Daten

7.1.1 Über Szenario ohne entfernte PIN-Eingabe

Über den USB Device Server wird zwischen Signaturserver und Signaturkarte eine „verlängernde" Umleitung via IP eingerichtet. Ohne entferne PIN-Eingabe werden zwischen Signaturserver und Signaturkarte weiterhin nur Hashwerte bzw. signierte Hashwerte ausgetauscht, also keine lesbaren Daten und auch keine PINs. Daher besteht in diesem Szenario kein größeres Risiko, ungewollt Daten preiszugeben, als beim direkten Anschließen des Kartenlesers an den Signaturserver.

7.1.2 Szenario mit entfernter PIN-Eingabe

Im Szenario entfernte PIN-Eingabe werden PINs der Signaturkarten über das Netzwerk übertragen. Wenn dieses Netzwerk nicht ausreichend sicher ist, sind diese PINs auf jeden Fall zu schützen. Andernfalls könnte der Angreifer die PIN erlauschen, die Signaturkarte entwenden und mit Karte und PIN „einkaufen gehen". D. h. in einem solchen Fall sollten ausschließlich USB Device Server eingesetzt werden, die eine Verschlüsselung der übertragenen Daten zwischen USB Device Server-Client und -Server zulassen.

Folgende Tabelle spiegelt den uns aus der Dokumentation der Geräte bekannten Funktionsumfang bzgl. Verschlüsselung der übertragenen Daten wieder[5]:

Hersteller	Typ	Verschlüsselung möglich
Silex	DS-510	nein
	DS-600	ja
SEH	myUTN-2500	ja

Tabelle 1 USB Device Server und Verschlüsselung

7.2 Angriffsszenario: Gesteckte Signaturkarte missbrauchen

Unabhängig von der entfernten PIN-Eingabe besteht das Risiko, dass ein Angreifer eine Verbindung zum Kartenleser aufbaut und mit der gesteckten Karte Signaturen erzeugt. Dazu muss zum einen die Karte „frei" (nicht gebunden in einer Session) sein und der Angreifer

[5] ohne Gewähr und Anspruch auf Vollständigkeit

muss die PIN der Karte kennen. Dieses Risiko kann durch Einschränkung der Kommunikation zwischen dem USB Device Server-Client und dem -Server vermindert werden (s. Kap. 6.1).

7.3 Formale Vorgaben

U. U. bestehen bei Signaturkarten formale Vorgaben, dass PINs nur über einen Klasse 2-Kartenleser (mit Tastatur) eingegeben werden dürfen. Für den Einsatz von Siegelkarten sind uns z. Zt. keine konkret formulierten Vorgaben bekannt. Der Leser möge selbst die Vorgaben der eingesetzten Komponenten prüfen und dann entscheiden.