

# TSL-Zertifikat für AIS erstellen

## Kurzanleitung

### Inhaltsverzeichnis

1	Ziel .....	2
2	Hintergrund .....	2
3	Allgemeine Hinweise .....	2
4	Methode: Sign Live! CC Desktop-Anwendung.....	2
4.1	SLCC installieren.....	2
4.2	TLS-Zertifikat/Schlüssel erzeugen und exportieren .....	3
5	Methode: OpenSSL.....	11
6	Methode: 90-Tage-Demo-Zertifikat verwenden .....	12

## 1 Ziel

Für die Verwendung des Swisscom AIS-Service mit *Sign Live! cloud suite gears* (fortan: *SLcs gears*) ist die Erstellung eines SSL/TLS-Zugangszertifikats (fortan: TLS<sup>1</sup>-Zertifikat) notwendig. Dieses Dokument stellt Methoden vor, wie diese ohne weitere Anleitung zu erstellen sind.

Spezielle Voraussetzungen sind nicht erforderlich.

## 2 Hintergrund

Vorgabe der Swisscom für die Kommunikation zwischen Teilnehmerapplikation (*SLcs gears*) und Signing Service AIS ist TLS-Verschlüsselung auf Basis eines nach Vorgabe erzeugten TLS-Zertifikats und des zugehörigen privaten Schlüssels.

## 3 Allgemeine Hinweise

Je nach Signaturservice werden weitere Anforderungen an die Aufbewahrung des Zertifikats/privaten Schlüssels und des zugehörigen Kennworts gestellt. Detaillierte Vorgaben sind dem jeweiligen Antrag bzw. der zum Antrag gehörenden Annahmeerklärung zu entnehmen.

Sinnvoll ist immer, Zertifikat/privaten Schlüssel direkt auf dem Signaturserver zu erstellen und das zugehörige Kennwort getrennt davon in einem Kennwortspeicher aufzubewahren.

## 4 Methode: Sign Live! CC Desktop-Anwendung

Diese Methode ist vollständig GUI-unterstützt und bietet die geringsten Einstiegshürden. Folgende Schritte sind durchzuführen:

1. *Sign Live! CC* (SLCC) gemäß Anleitung installieren (Lizenz ist nicht erforderlich).
2. TLS-Zertifikat/Schlüssel erzeugen und exportieren.

### 4.1 SLCC installieren

Laden Sie SLCC von der intarsys Homepage herunter

[https://www.intarsys.de/dl\\_slcc](https://www.intarsys.de/dl_slcc)

unter installieren und starten Sie die Anwendung gemäß Vorgabe.

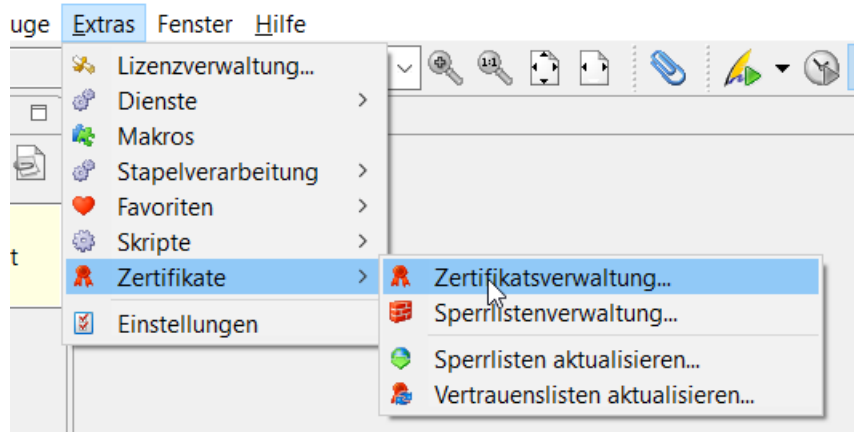
---


<sup>1</sup> TLS (*transport layer security*) ist die modernere Form von SSL (*secure socket layer*)

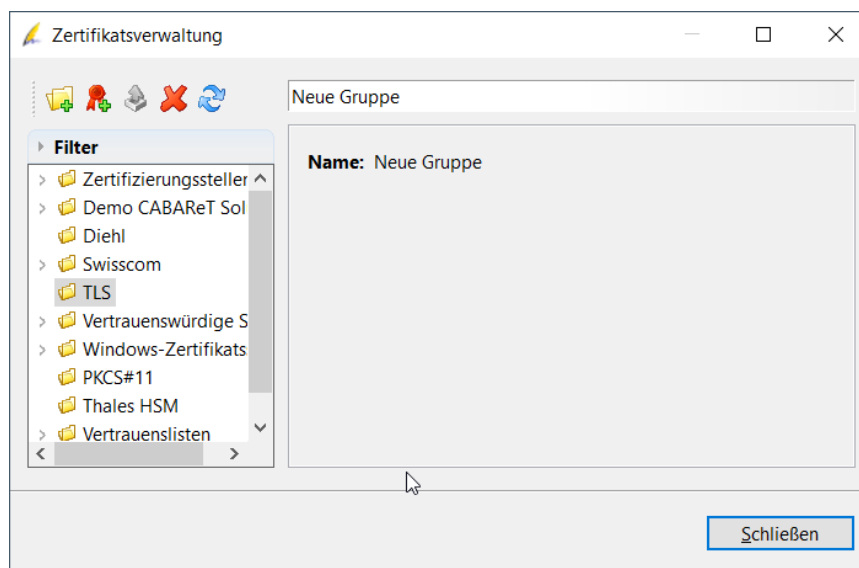
## 4.2 TLS-Zertifikat/Schlüssel erzeugen und exportieren


Gehen Sie folgendermaßen vor:

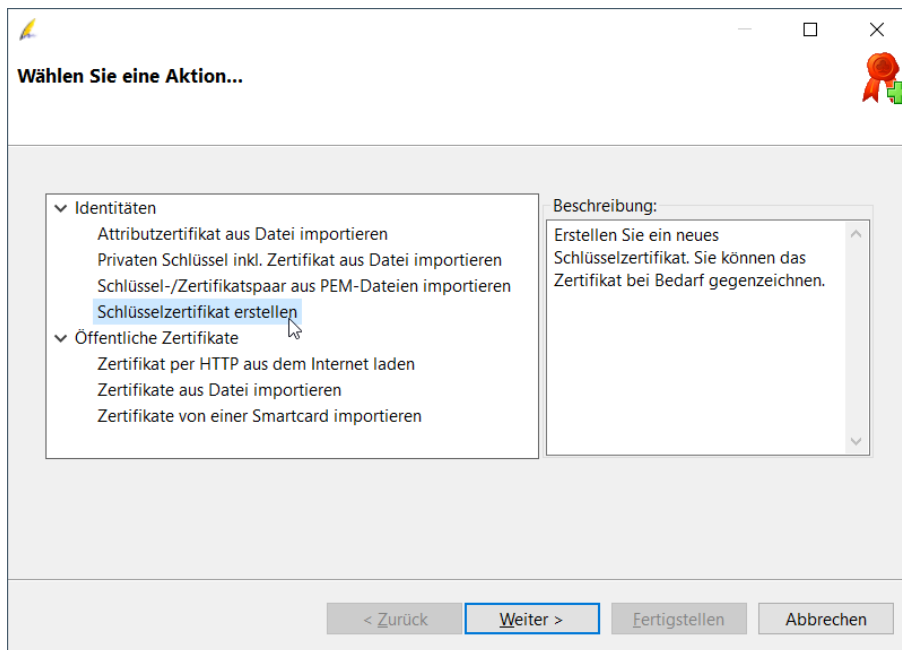
1. Öffnen Sie in *Sign Live! CC* die Zertifikatsverwaltung



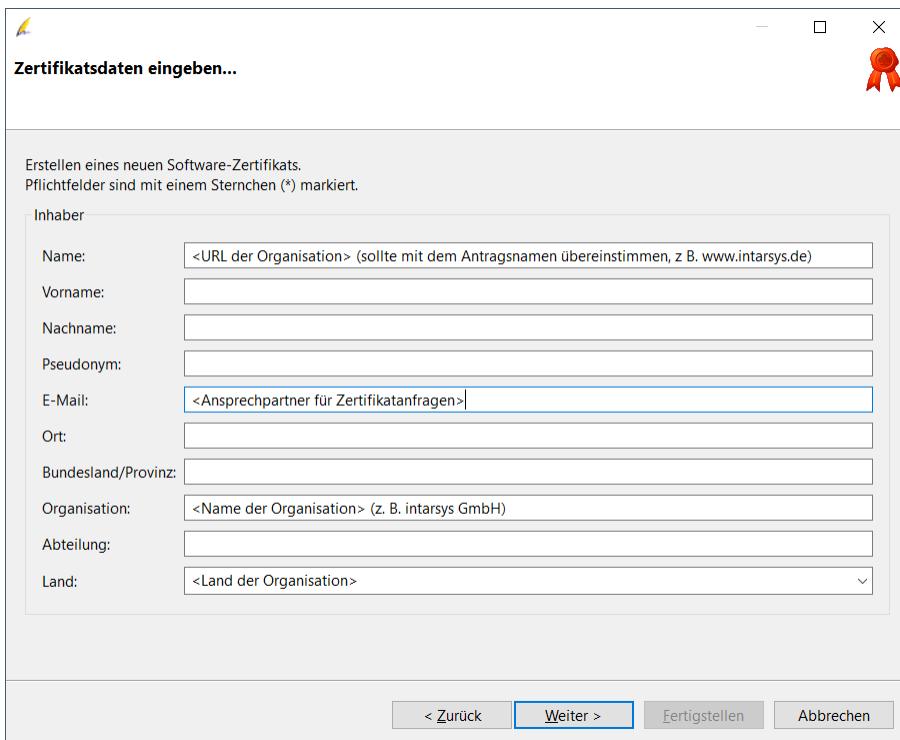
2. Erstellen Sie über  eine neue Zertifikatsgruppe, z. B. „TLS“



3. Erstellen Sie über  ein neues Schlüsselzertifikat



#### 4. Erfassen Sie über **Weiter** die Zertifikatsdaten



Erstellen eines neuen Software-Zertifikats.  
Pflichtfelder sind mit einem Sternchen (\*) markiert.

**Inhaber**

Name:

Vorname:

Nachname:

Pseudonym:

E-Mail:

Ort:

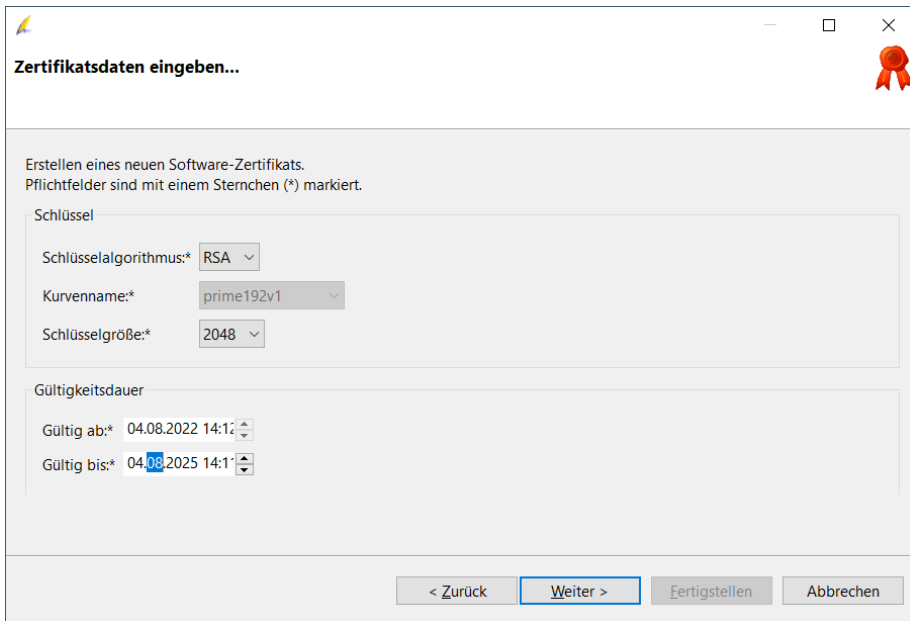
Bundesland/Provinz:

Organisation:

Abteilung:

Land:

#### 5. Erfassen Sie über **Weiter** die technischen Zertifikatsparameter



**Zertifikatsdaten eingeben...**

Erstellen eines neuen Software-Zertifikats.  
Pflichtfelder sind mit einem Sternchen (\*) markiert.

Schlüssel

Schlüsselalgorithmus\* RSA

Kurvenname\* prime192v1

Schlüsselgröße\* 2048

Gültigkeitsdauer

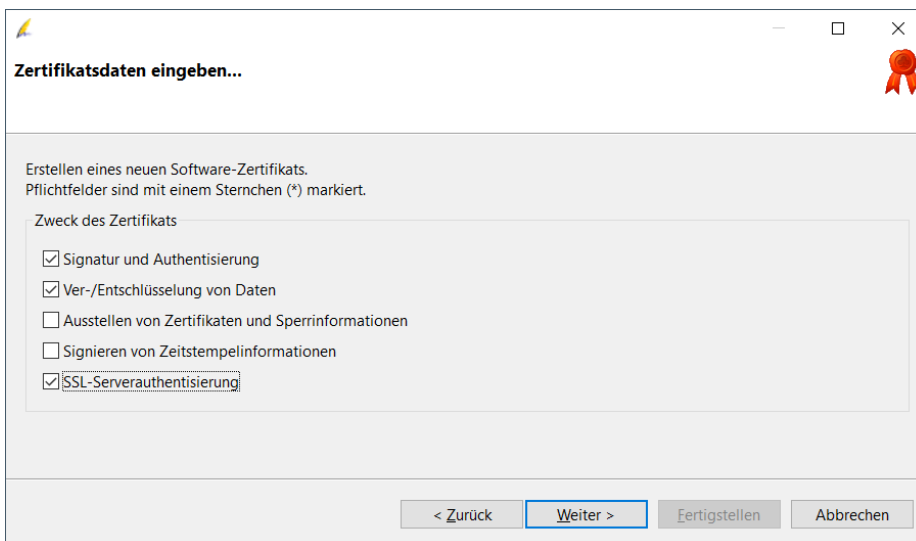
Gültig ab\* 04.08.2022 14:12

Gültig bis\* 04.08.2025 14:12

< Zurück Weiter > Fertigstellen Abbrechen

Achten Sie insbesondere darauf, dass die Zertifikatslaufzeit 3 Jahre nicht überschreitet!

6. Definieren Sie über **Weiter** die Verwendungszwecke des Zertifikats



**Zertifikatsdaten eingeben...**

Erstellen eines neuen Software-Zertifikats.  
Pflichtfelder sind mit einem Sternchen (\*) markiert.

Zweck des Zertifikats

Signatur und Authentisierung

Ver-/Entschlüsselung von Daten

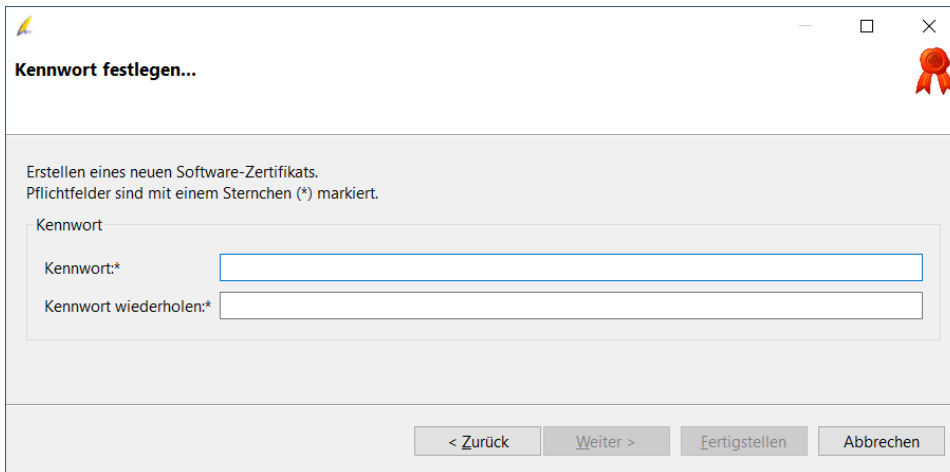
Ausstellen von Zertifikaten und Sperrinformationen

Signieren von Zeitstempelinformationen

SSL-Serverauthentisierung

< Zurück Weiter > Fertigstellen Abbrechen

## 7. Definieren Sie ein Kennwort



**Kennwort festlegen...**

Erstellen eines neuen Software-Zertifikats.  
Pflichtfelder sind mit einem Sternchen (\*) markiert.

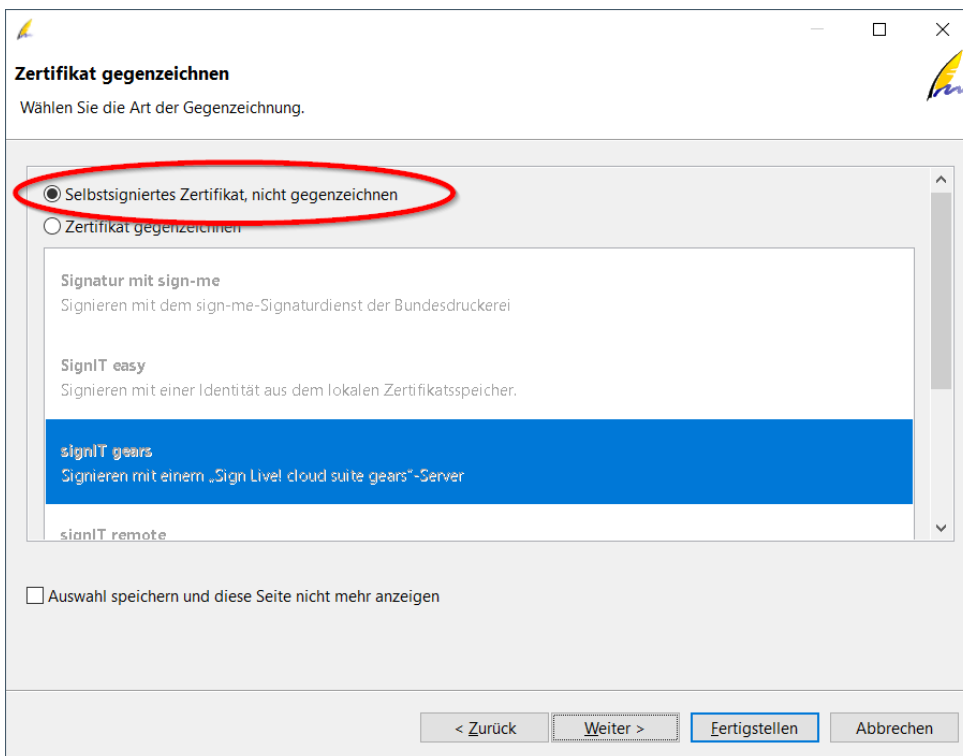
Kennwort

Kennwort:\*

Kennwort wiederholen:\*

< Zurück Weiter > Fertigstellen Abbrechen

## 8. Wählen Sie selbstsigniertes Zertifikat



**Zertifikat gegenzeichnen**

Wählen Sie die Art der Gegenzeichnung.

Selbstsigniertes Zertifikat, nicht gegenzeichnen

Zertifikat gegenzeichnen

Signatur mit sign-me  
Signieren mit dem sign-me-Signatordienst der Bundesdruckerei

SignIT easy  
Signieren mit einer Identität aus dem lokalen Zertifikatsspeicher.

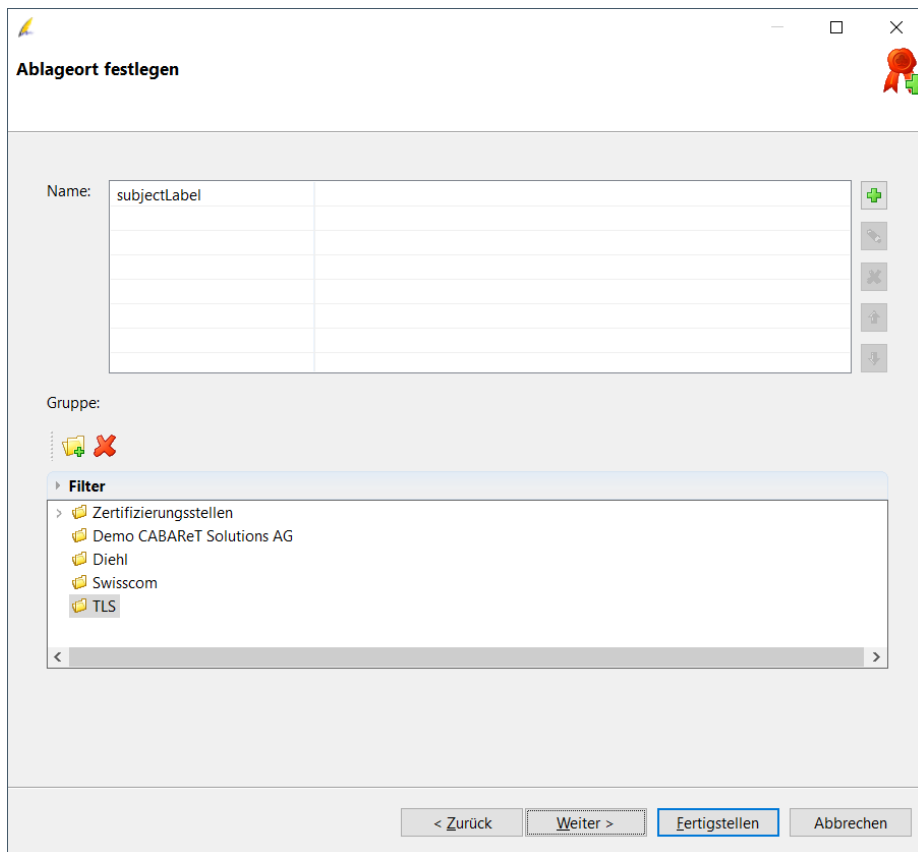
**signIT gears**  
Signieren mit einem „Sign Level cloud suite gears“-Server

signIT remote

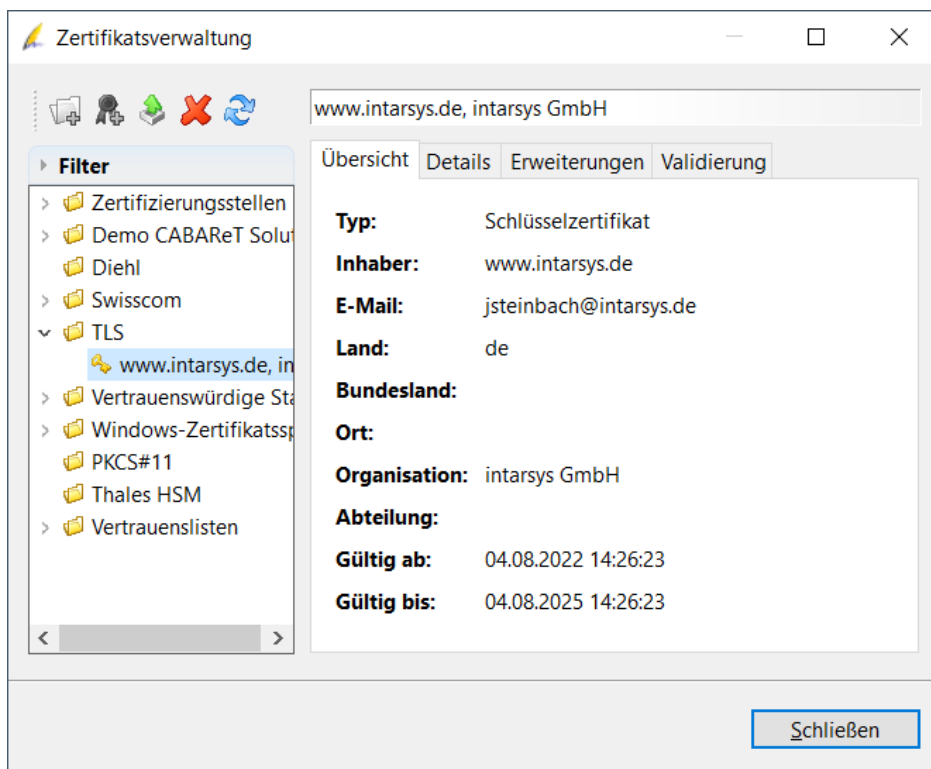
Auswahl speichern und diese Seite nicht mehr anzeigen

< Zurück Weiter > Fertigstellen Abbrechen

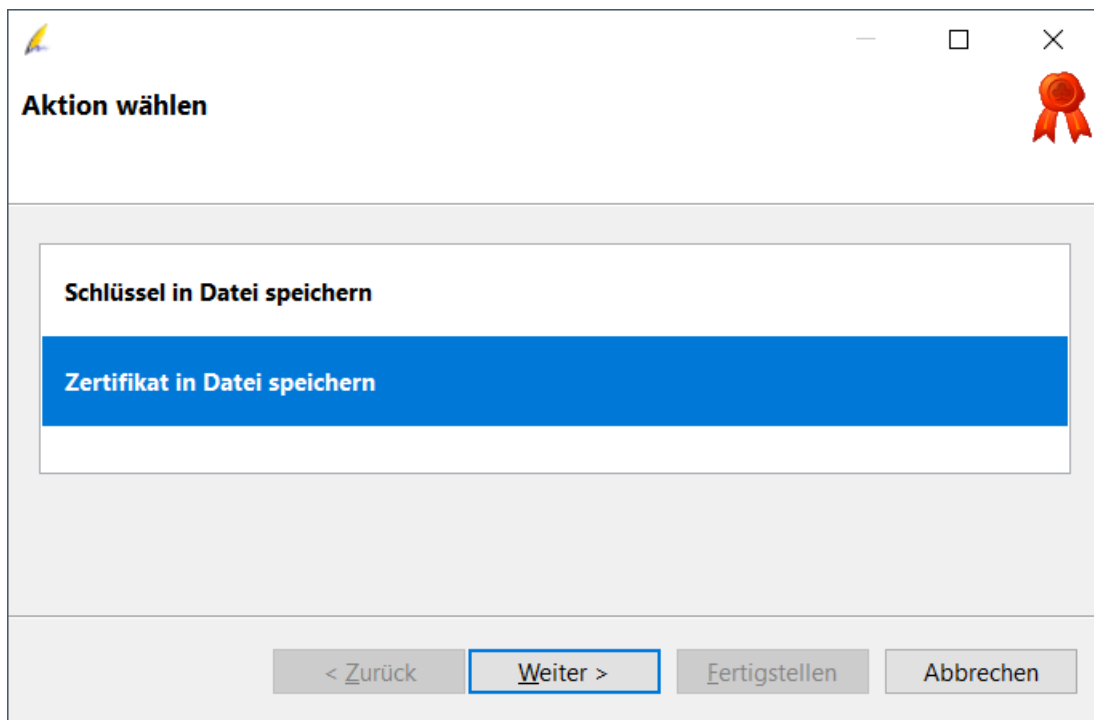
## 9. ... und legen Sie das Zertifikat mit **Fertigstellen** in der gewünschten Gruppe ab (die Markierung des Zertifikats als „vertrauenswürdig“ ist nicht erforderlich)



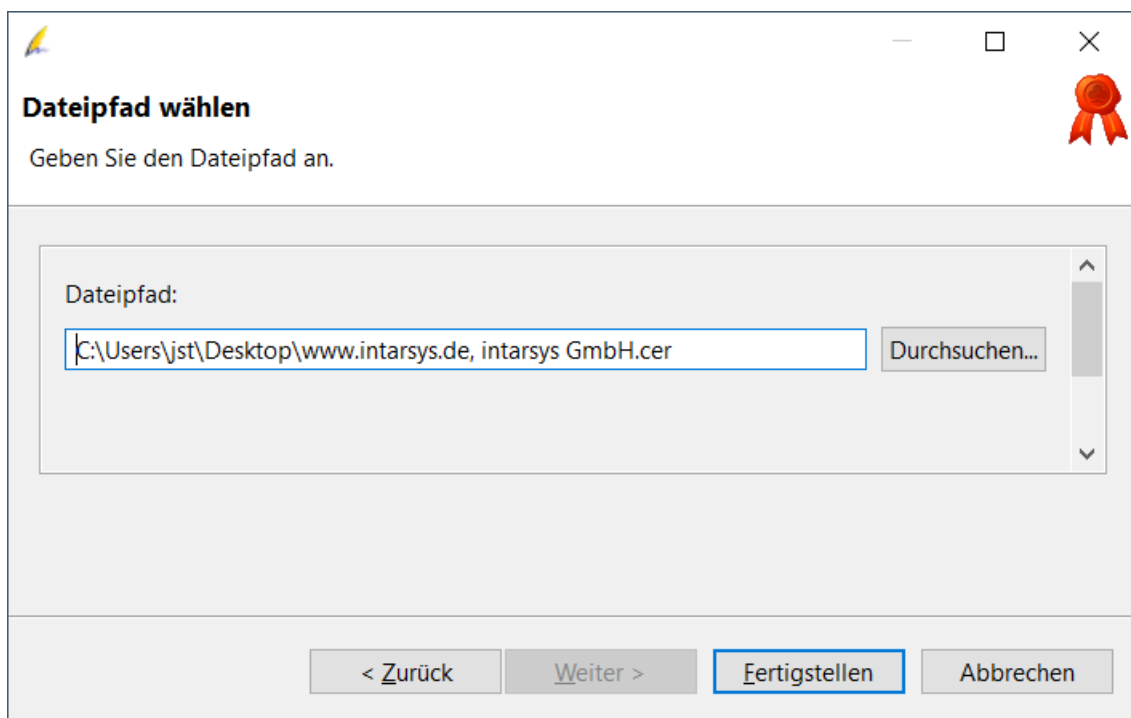
10. Das Ergebnis liegt nun in der *Sign Live! CC* Zertifikatsverwaltung:



11. Exportieren Sie das Zertifikat (\*.cer) über  und



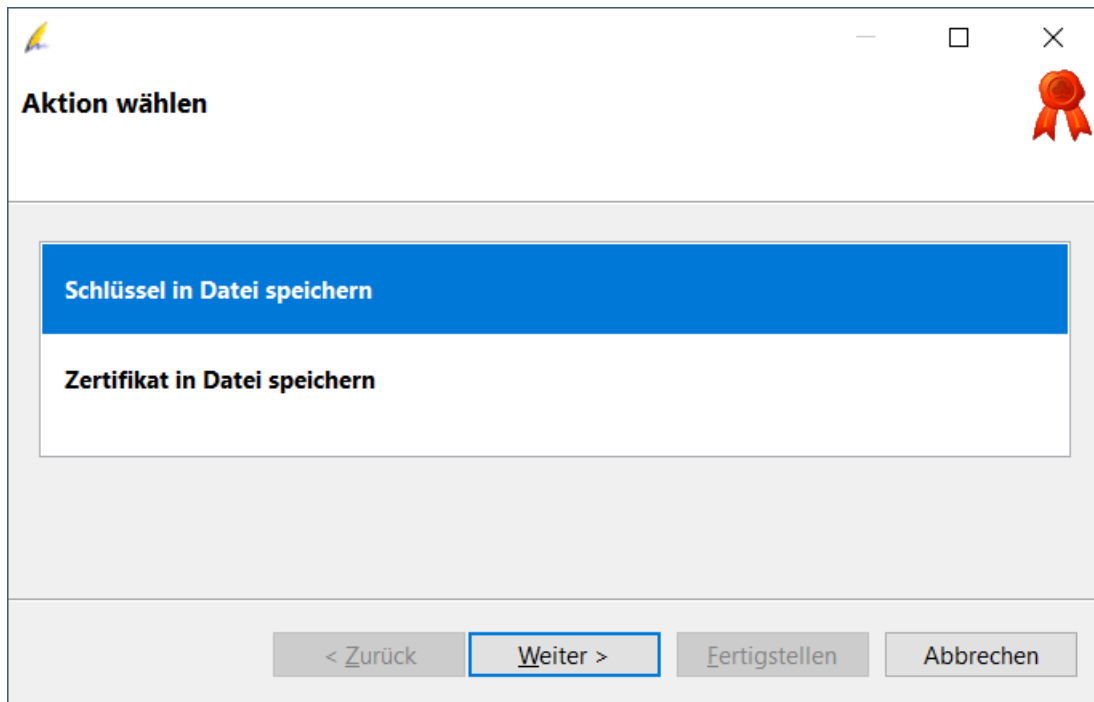
Den Pfad können Sie frei wählen



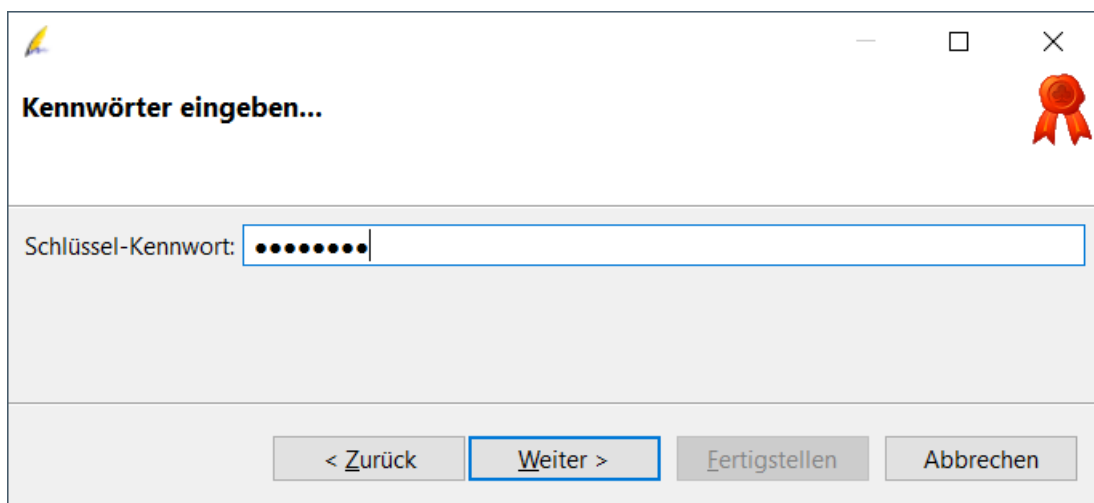
Mit **Fertigstellen** legt *Sign Live! CC* das Zertifikat an gewünschter Stelle ab.



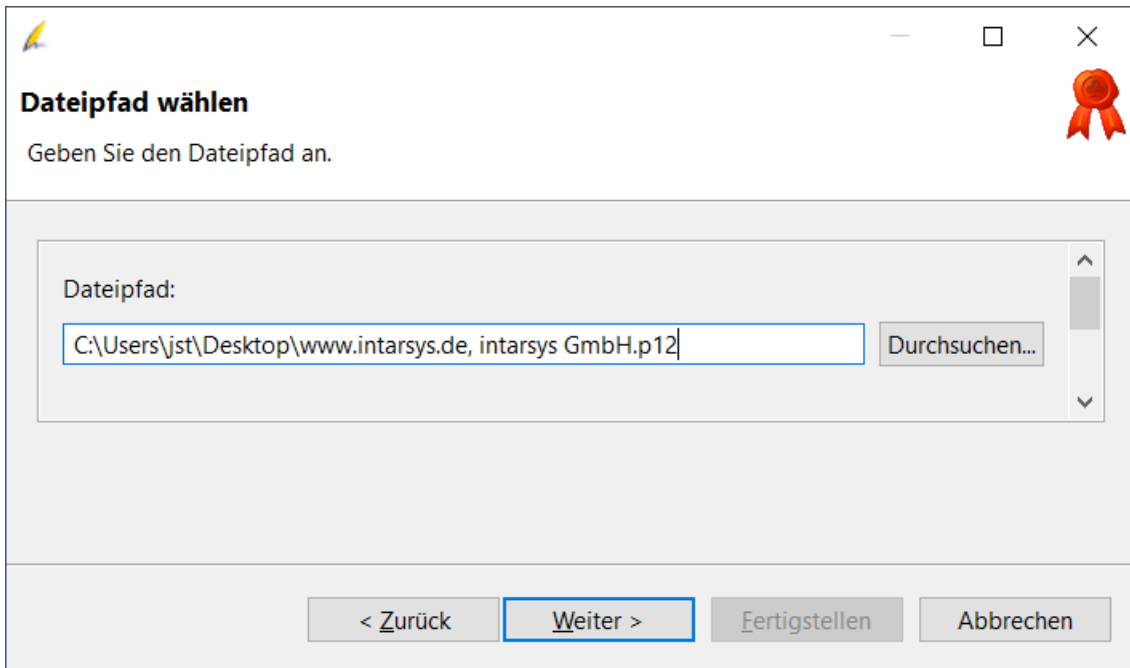
12. Exportieren Sie **zusätzlich** das Zertifikat mit Schlüssel (\*.p12) über  und



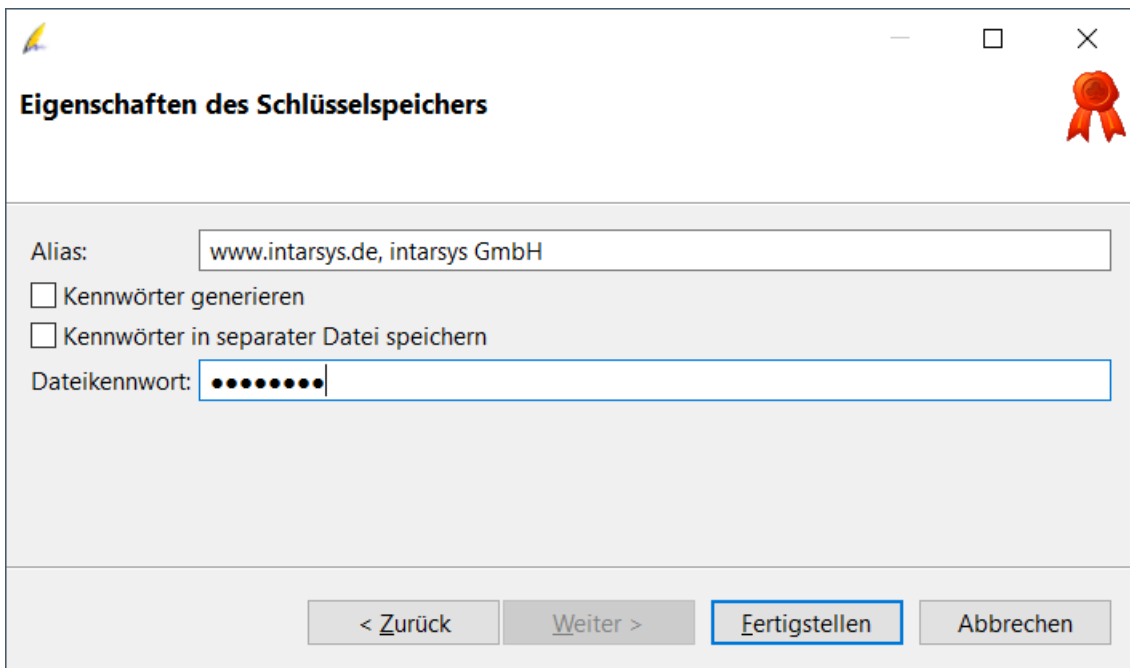
In diesem Fall müssen Sie zusätzlich ein Kennwort eingeben



Den Pfad können Sie frei wählen



Das Kennwort muss ein zweites Mal angegeben werden



Mit **Fertigstellen** legt SLCC das Zertifikat inklusive privatem Schlüssel an gewünschter Stelle ab.

### Wichtig!

Liefern Sie **nur das Zertifikat** (.cer) an die Swisscom aus, niemals den privaten Schlüssel! Das Zertifikat mit Schlüssel (.p12) verbleibt auf dem Server und wird von SLcs gears benötigt.

## 5 Methode: OpenSSL

Diese Methode setzt etwas Erfahrung mit OpenSSL<sup>2</sup> voraus.

Folgendes Skript dient im Kontext einer OpenSSL Installation auf Windows als Basisgerüst zur Erstellung eigener AIS-TLS-Zertifikate.

---

**create\_cert\_AIS-TLS.bat**

```
@echo off
echo.
echo run this command in a cmd shell started by start.bat
echo.

set "CN=www.intarsys.de"
set "ORGANISATION=AIS intarsys GmbH"
set "EMAILADDRESS=support@intarsys.de"
set "COUNTRY=DE"
set "PASSWORD=password"
set "OWNER=%CN%"

openssl req -x509 -sha512 -newkey rsa:2048 -days 1095 ^
-keyout "%OWNER%-privkey.pem" -passout pass:%PASSWORD% -out "%OWNER%-cert.pem" ^
-subj "/C=%COUNTRY%/O=%ORGANISATION%/CN=%CN%/emailAddress=%EMAILADDRESS%" ^
-addext "keyUsage=critical,digitalSignature,dataEncipherment,encipherOnly" ^
-addext "extendedKeyUsage=clientAuth" ^
-extensions v3_ca ^
-verbose

echo.
echo content (text) of %OWNER%-cert.pem
echo.
openssl x509 -in "%OWNER%-cert.pem" -text -noout

echo.
echo content (asn1) of %OWNER%-cert.pem
echo.
openssl asn1parse -i -in "%OWNER%-cert.pem" -dump

echo.
openssl x509 -in "%OWNER%-cert.pem" -outform pem -outform der -out %OWNER%.cer
echo.
echo %OWNER%.cer created
echo.

openssl pkcs12 -export -inkey "%OWNER%-privkey.pem" -in "%OWNER%-cert.pem" -out "%OWNER%.p12" ^
-passin pass:%PASSWORD% -passout pass:%PASSWORD%
echo.
echo %OWNER%.p12 created
echo.
```

---

<sup>2</sup> OpenSSL for Windows - <https://slproweb.com/products/Win32OpenSSL.html>

## 6 Methode: 90-Tage-Demo-Zertifikat verwenden

Diese Methode basiert darauf, eine bestehende Zertifikats-/Schlüsselkombination zu verwenden. Es bietet Ihnen jedoch nur den Zugang auf die Swisscom AIS-Demo-Instanz.

Melden Sie sich an der intarsys Homepage<sup>3</sup> an und laden Sie das jeweils aktuell gültige 90-Tage-Demo-Zertifikat ggfs. mit Konfiguration herunter:

[https://www.intarsys.de/download/SLcs-gears\\_demo-access-AIS](https://www.intarsys.de/download/SLcs-gears_demo-access-AIS)

Sollten Sie noch nicht für die intarsys Homepage registriert sein, kontaktieren Sie bitte Ihren Ansprechpartner.

---

<sup>3</sup> <https://www.intarsys.de/user/login>

Wir haben diese Kurzanleitung nach bestem Wissen erstellt.  
Sollten dennoch Fragen offen bleiben wenden Sie sich bitte an unseren Support, den Sie per E-Mail unter <mailto:support@intarsys.de> erreichen.