TLS-Client-Zertifikat erstellen

Inhaltsverzeichnis

Was ist ein TLS-Zertifikat und wofür wird es benötigt?

Das TLS-Zertifikat (**T**ransport **L**ayer **S**ecurity, deutsch: Transportschichtsicherheit) ist auch unter dem Namen SSL (**S**ecure **S**ockets **L**ayer) bekannt. TLS ist die technische Weiterentwicklung des SSL-Protokolls. Daten und Informationen sollen über gesicherte Verbindungen ausgetauscht werden, damit diese nicht von unbefugten Dritten mitgelesen werden können. Dies ist vor allem dann wichtig, wenn Daten über das Web verschickt werden. Eine der wichtigsten Möglichkeiten den Datenaustausch abzusichern ist der Einsatz eines Zertifikats. Das hier genutzte **TLS-(Client)-Zertifikat** enthält Identifizierungsinformationen, mit denen Sie sich gegenüber einem bestimmten Server „ausweisen" können.

Unsere Software *Sign Live! CC* nutzt dieses Zertifikat für die **Fernsignatur** mit dem „**All-in-Signingservice (AIS)**" der Swisscom. Für den Signaturvorgang werden dabei ausschließlich die Hash-Werte (Fingerprint) der Dokumente oder Dateien an den Fernsignaturdienst übergeben. Die effektiv lesbaren Dateien und Dokumente verlassen die Systemumgebung Ihres Unternehmens nicht. Der Vertrauensdiensteanbieter hat also keine Einsicht in die zu signierenden Dateien und Dokumente und kann auf den Inhalt keine Rückschlüsse ziehen.

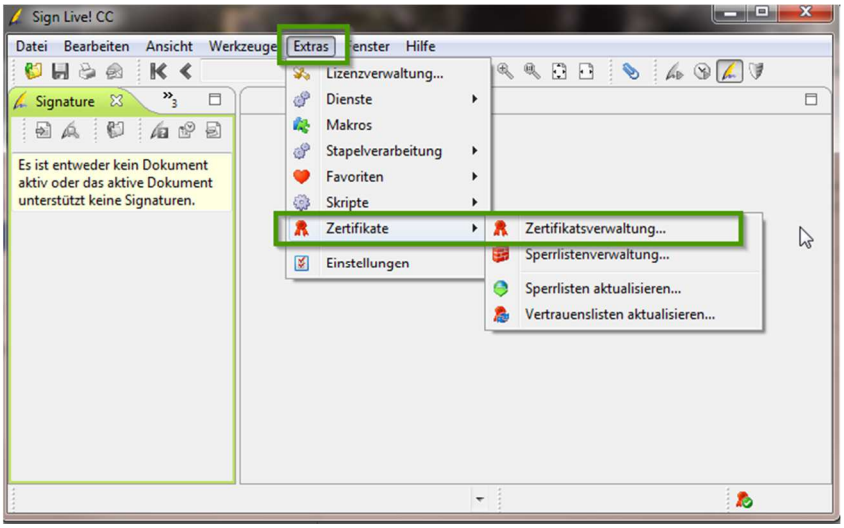
Dieses Tutorial unterstützt Sie bei der Erstellung des Zertifikats.

Voraussetzungen

- Sie sind bei der Swisscom als Nutzer für AIS registriert und die entsprechenden Unterlagen der Swisscom liegen Ihnen vor.
- Sie haben *Sign Live! CC* installiert (https://www.intarsys.de/download).

So erstellen Sie ein TLS-Zertifikat mit *Sign Live! CC*

Starten Sie *Sign Live! CC* und öffnen Sie die Zertifikatsverwaltung über Menüpunkt ***Extras > Zertifikate***.

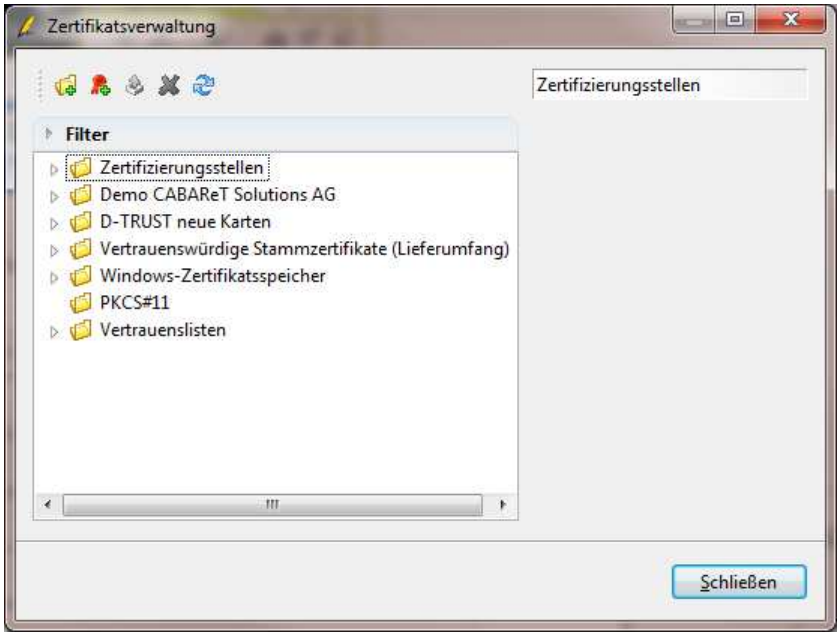


Zum Öffnen der Zertifikatsverwaltung wählen Sie Menüpunkt

Extras > Zertifikate > Zertifikatsverwaltung...

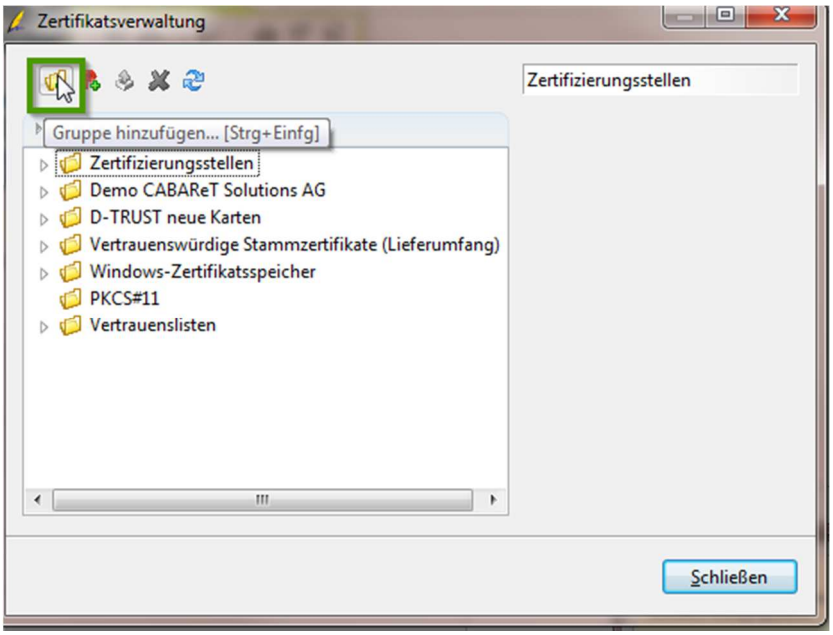
Neue Gruppe in der Zertifikatsverwaltung erstellen

Es öffnet sich das Fenster der Zertifikatsverwaltung. Hier sind die bereits vorhandenen Zertifikate **in verschiedenen Gruppen** hinterlegt.
Der überwiegende Teil der Zertifikate ist im Lieferumfang *Sign Live! CC* enthalten.



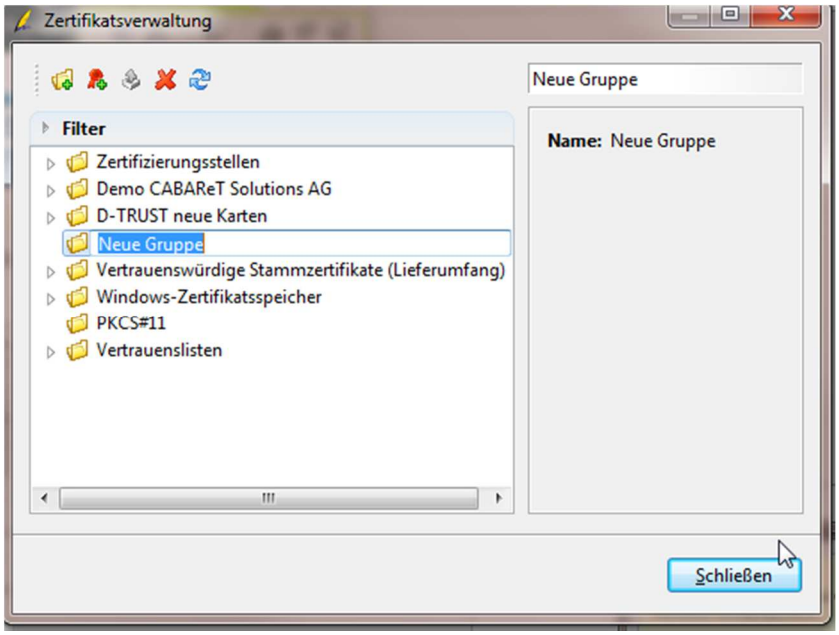
Selbstverständlich können Sie das neue Zertifikat in eine der vorhandenen Gruppen ablegen. Zur besseren Übersicht empfehlen wir das Anlegen einer neuen Gruppe.

Zur Erstellung einer neuen Gruppe klicken Sie auf das Ordner-Symbol in der Symbolleiste.



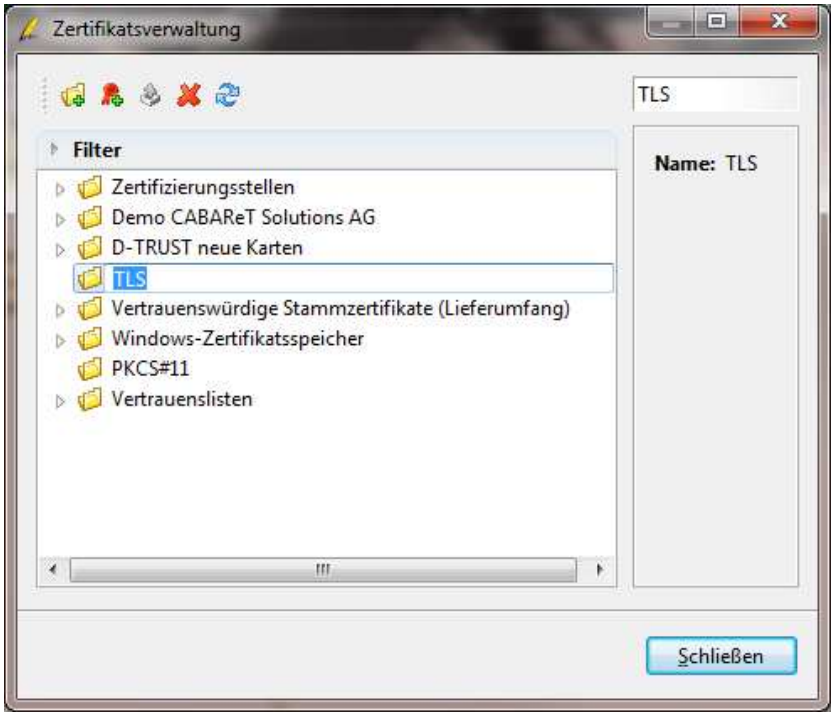
Alternativ können Sie eine neue Gruppe auch mit der Tastenkombination [Strg + Einfg] erstellen.

Es wird automatisch eine Gruppe mit dem Namen ***Neue Gruppe*** angelegt. Solange der Text markiert ist kann er überschrieben werden.



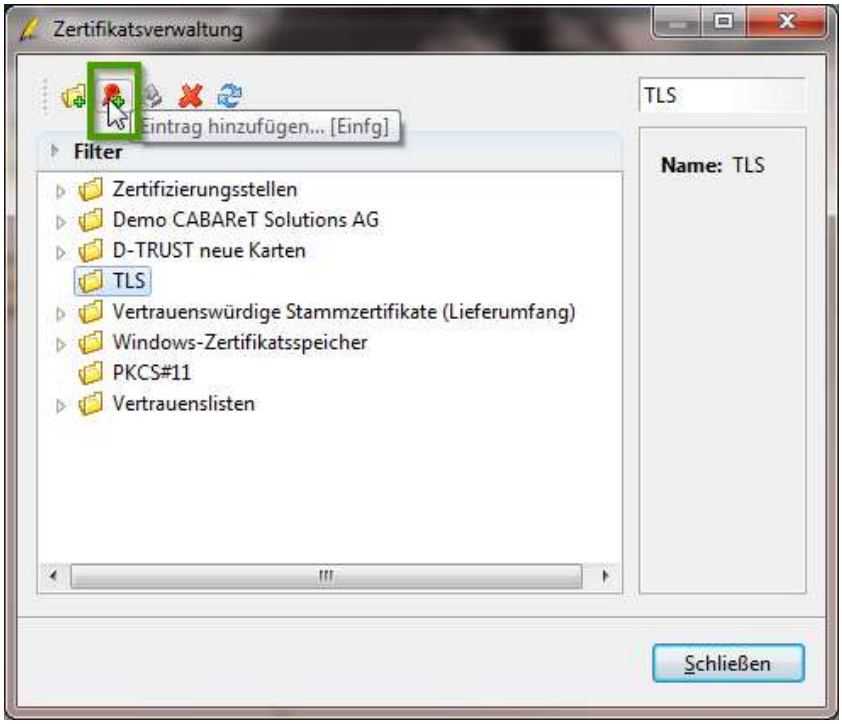
Über das Kontextmenü oder die Taste [F2] kann der Name bei Bedarf geändert werden.

Nennen Sie die neue Gruppe zum Beispiel „TLS“.



Zertifikat erstellen

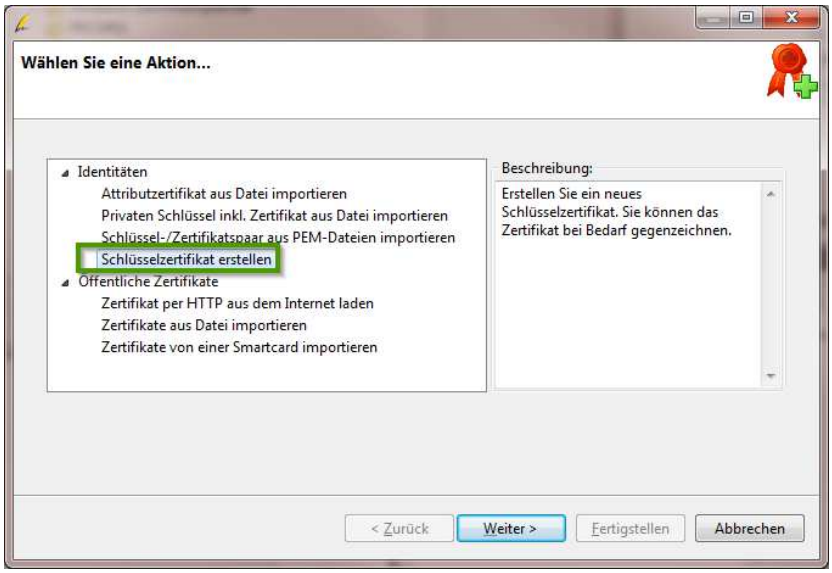
Um ein Zertifikat hinzuzufügen wählen Sie das zweite Symbol.



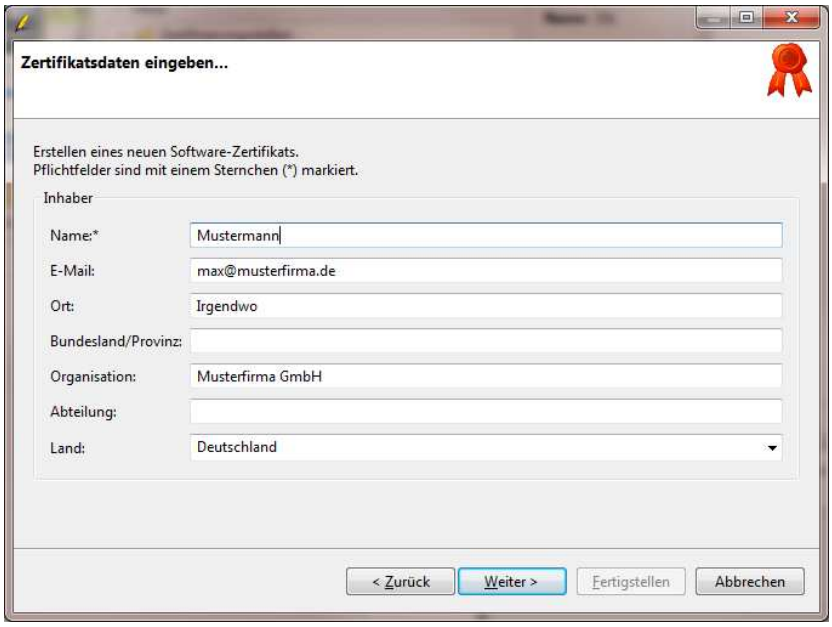
Fügen Sie über das zweite Symbol oder die Taste [Einfg] ein neues Zertifikat hinzu.

Das nächste Fenster öffnet sich automatisch.

Wählen Sie im Bereich ***Identitäten*** den Eintrag ***Schlüsselzertifikat erstellen*** und klicken Sie [Weiter >].



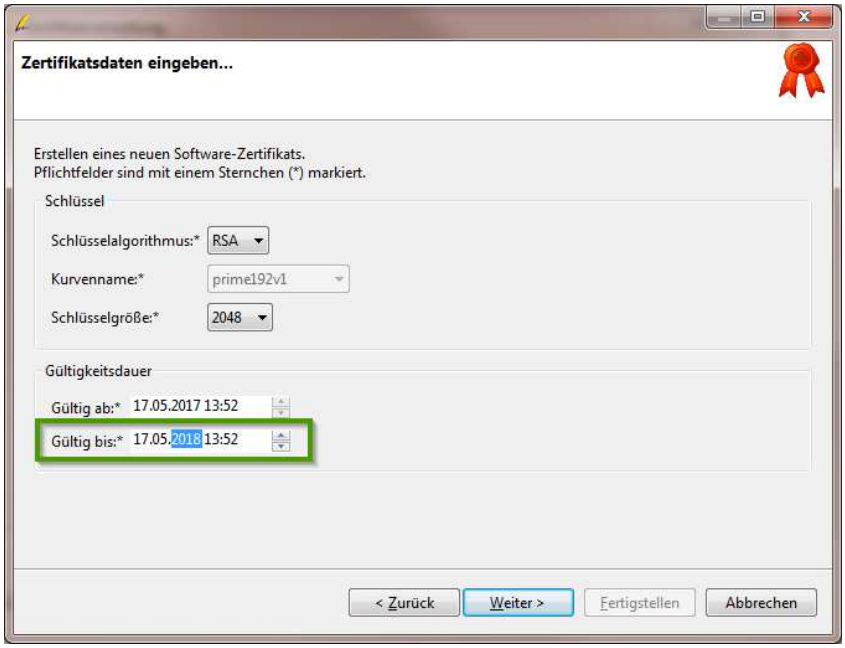
Im nächsten Fenster geben Sie die Zertifikatsdaten ein und [Weiter >].



Mit den Daten die Sie hier eintragen, weisen Sie sich gegenüber dem Server aus.

Der Eintrag im Pflichtfeld „Name“ ist frei wählbar. Hier geben Sie dem Zertifikat einen Namen.

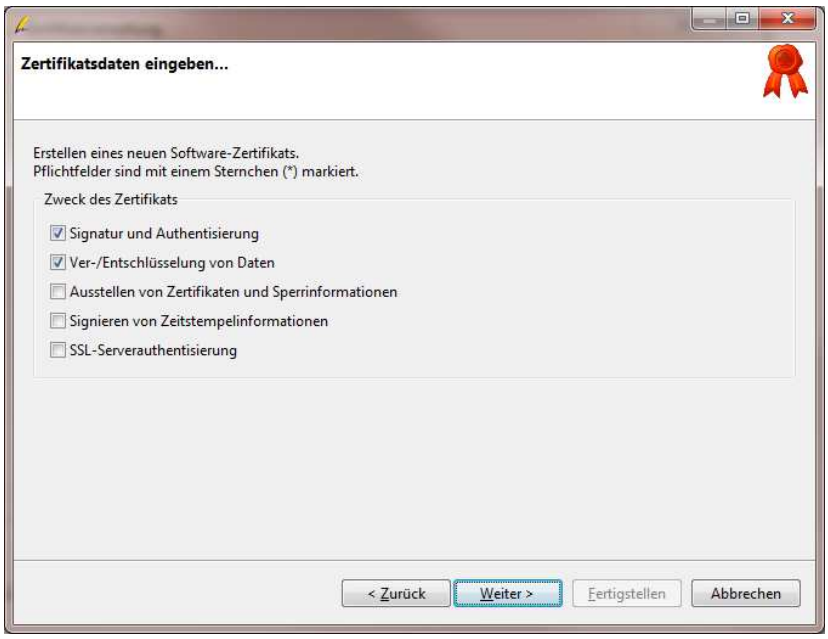
Prüfen Sie im nächsten Fenster die Eingaben und **passen Sie die Laufzeit** an.
Dann[Weiter >].



Die Zertifikatsdaten im oberen Bereich sollten automatisch wie dargestellt eingetragen sein und nicht geändert werden.

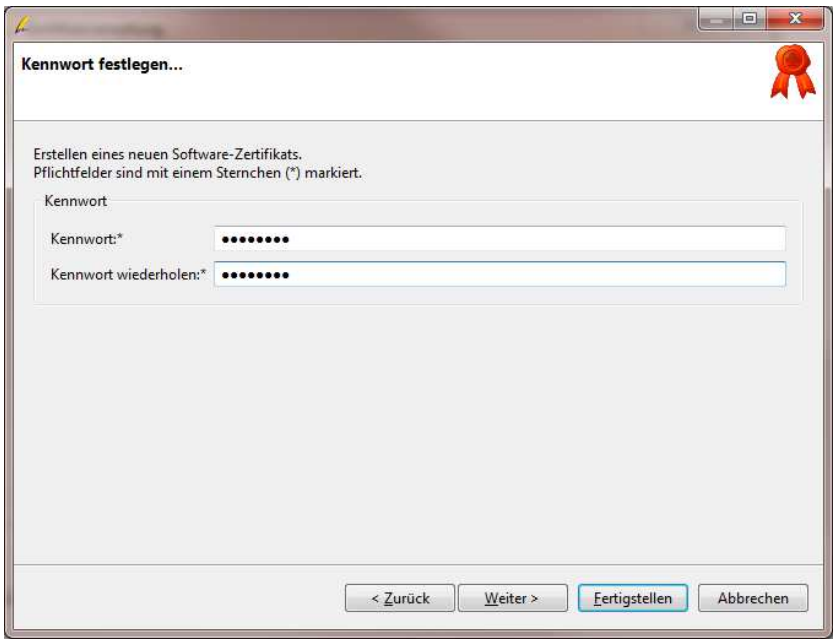
Die Laufzeit des Zertifikats können Sie selbst bestimmen. Sie sollte **mindestens** 1 Jahr betragen.

Definieren Sie den Zweck des Zertifikats und [Weiter >].



Bitte belassen Sie die Einstellungen so, da es sonst zu Fehlermeldungen kommen kann.

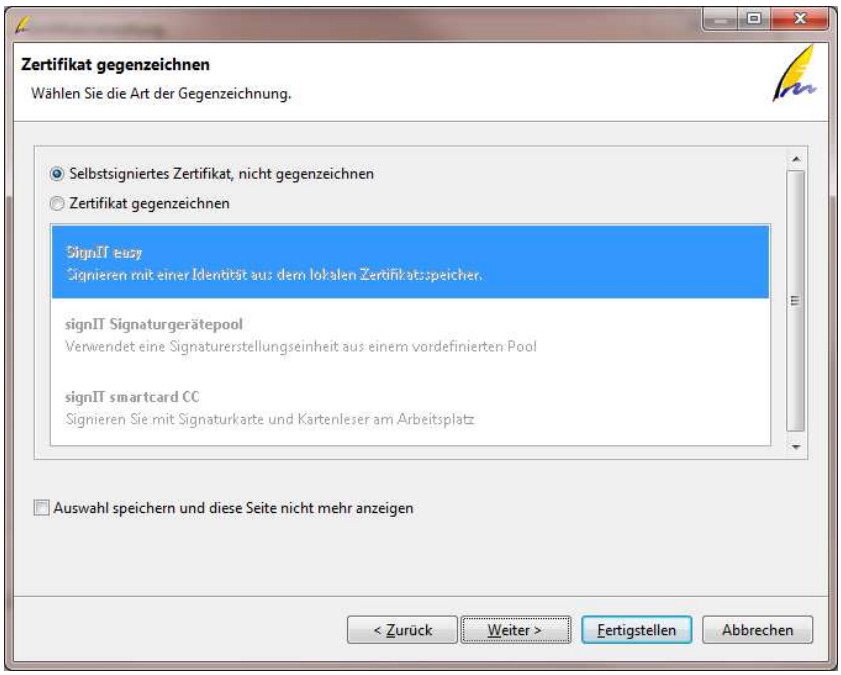
In diesem Fenster definieren Sie das **Kennwort** für das Zertifikat.



Wir empfehlen ein Kennwort mit **mindestens 8 Zeichen**. Dabei sollten Sie auch Sonderzeichen und Zahlen verwenden.

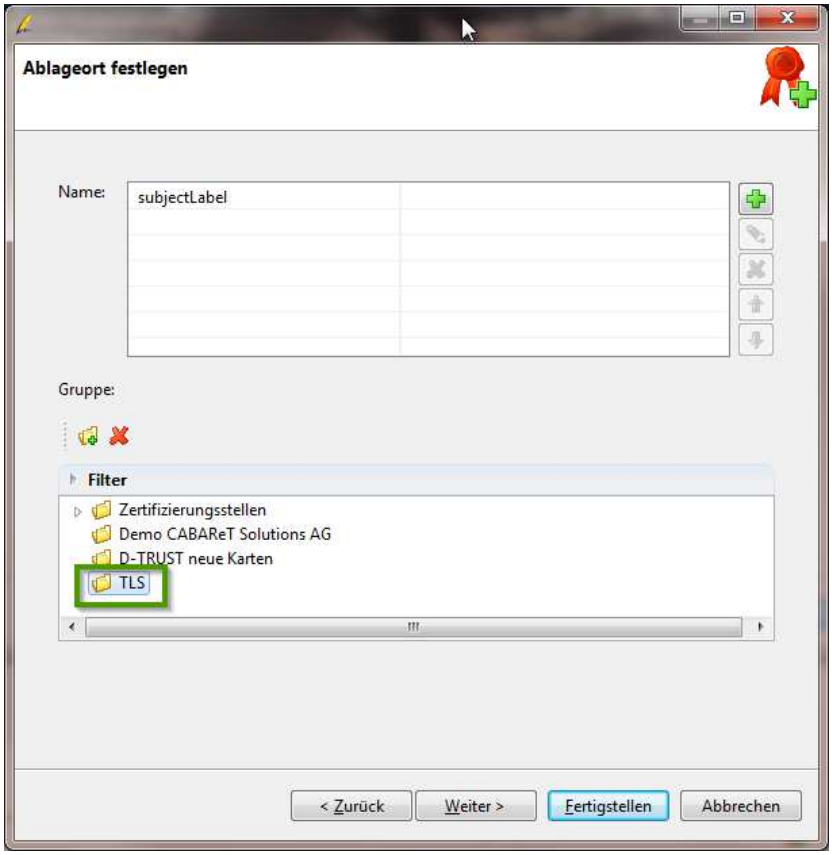
Notieren Sie sich das Kennwort und bewahren Sie diese Information an einem sicheren Ort auf.

Da das Zertifikat nicht gegengezeichnet werden muss, können Sie hier gleich auf den Button [Fertigstellen] klicken.
Mit [Weiter >] öffnet sich dieses Fenster …



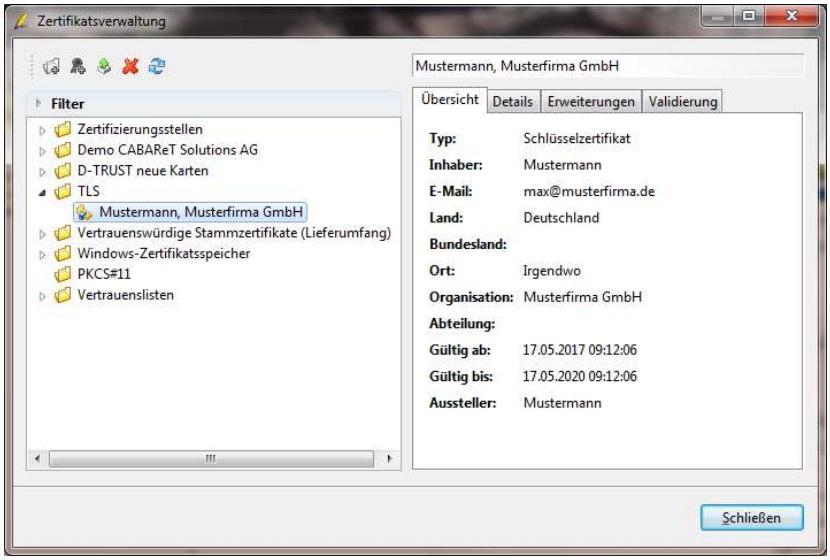
… um dann hier [Fertigstellen] zu drücken.

Als Ablageort für das Zertifikat wählen Sie die extra angelegte Gruppe und [Weiter >].



Sie können das Zertifikat als vertrauenswürdig markieren und [Fertigstellen].

Das Fertige Zertifikat wird nun in der Zertifikatsverwaltung mit allen Informationen angezeigt.



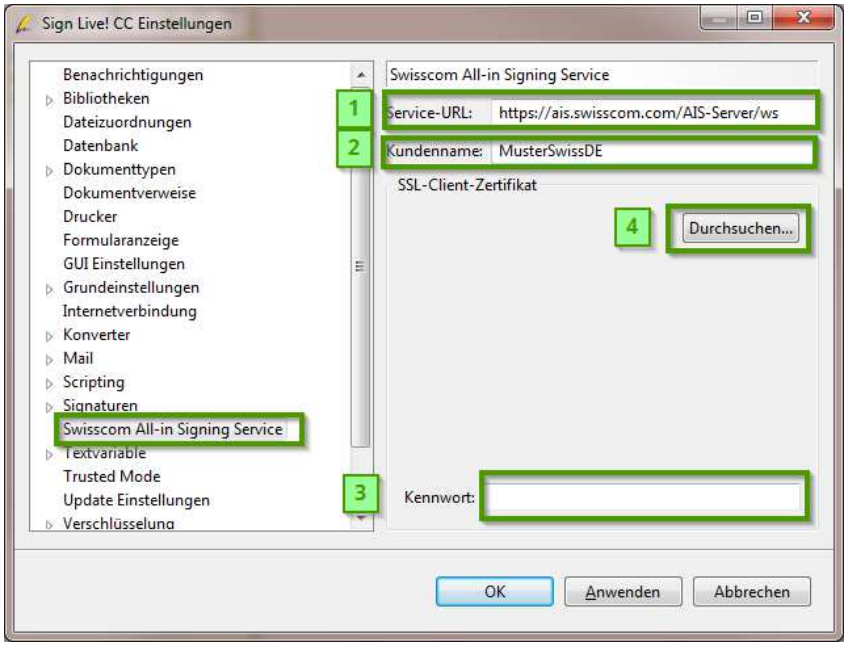
Mit [Schließen] beenden Sie den Vorgang.

All-in-Signing Service in *Sign Live! CC* einrichten

Nachdem nun das **TLS-Zertifikat** erstellt ist, kann es in *Sign Live! CC* eingebunden werden. Wählen Sie dazu dem Menüpunkt ***Extras > Einstellungen***. Folgendes Fenster öffnet sich.

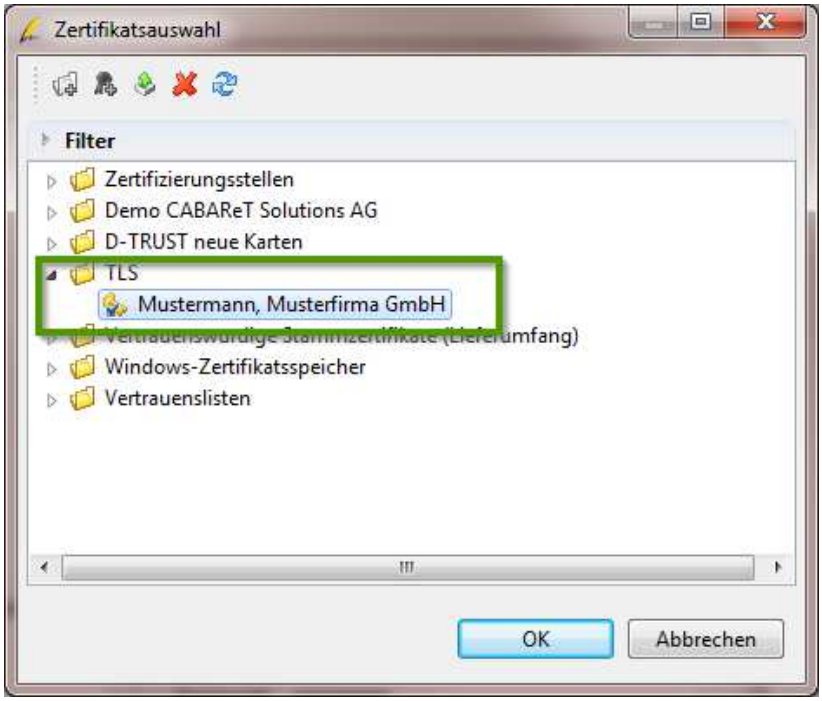
Klicken Sie im linken Fensterbereich auf „Swisscom All-in Signing Service“.
Im rechten Fenster sind folgende Einträge vorzunehmen bzw. zu prüfen.

1. Die Service-URL der Swisscom sollte bereits vorbelegt sein.
2. Kundenname ist der Name, **der von der Swisscom für Sie vergeben wurde**.
3. Tagen Sie als Kennwort das von Ihnen vergebene Kennwort für Ihr Zertifikat ein.
4. Klicken Sie auf [Durchsuchen …]



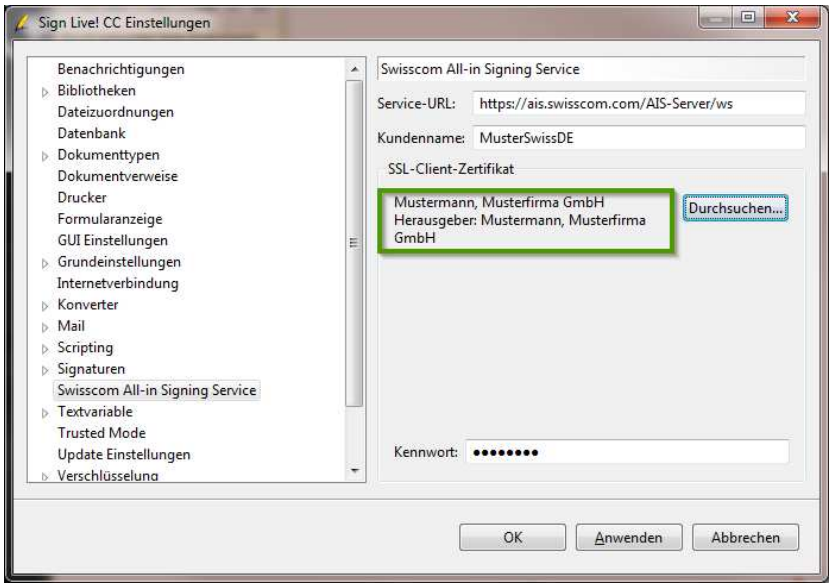
Mit [Durchsuchen…] stellen Sie die Verknüpfung zu Ihrem Zertifikat her.

Es öffnet sich das Fenster mit der Zertifikatsauswahl. Markieren Sie Ihr Zertifikat und bestätigen Sie die Eingabe mit [OK].



Eventuell müssen Sie die Gruppe TLS aufklappen um Zugriff auf Ihr Zertifikat zu haben.

Am Eintrag erkennen Sie, dass die Verknüpfung zum Zertifikat hergestellt wurde. Bitte bestätigen Sie mit [OK].



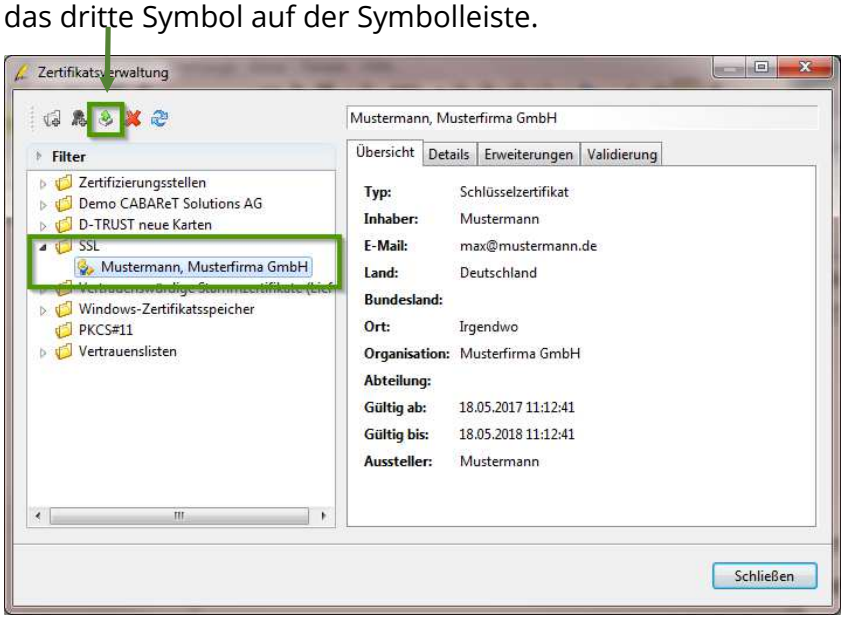
Zertifikat an Swisscom übermitteln

Nachdem nun das Zertifikat erstellt und die Daten in *Sign Live! CC* eingerichtet sind, muss das verwendetet Zertifikat exportiert und der Swisscom gemeldet werden.

Zertifikat exportieren

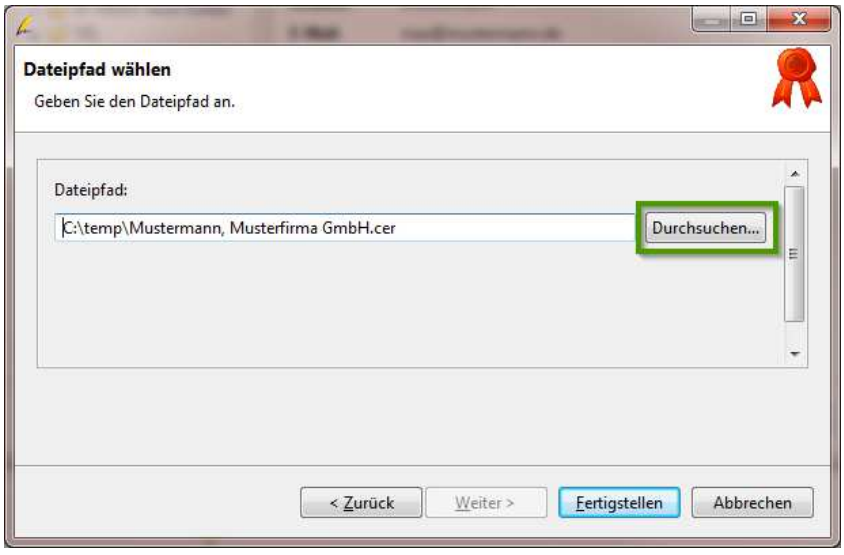
Öffnen Sie in *Sign Live! CC* die Zertifikatsverwaltung über das Menü ***Extras > Zertifikate > Zertifikatsverwaltung***.

Markieren Sie das von Ihnen erstellte Zertifikat und drücken Sie für den Export das dritte Symbol auf der Symbolleiste.



Es öffnet sich das Fenster „Aktion wählen“. Wählen Sie hier den Eintrag ***Zertifikat in Datei speichern*** und klicken Sie auf [Weiter].

Wählen Sie den Dateipfad, in den Sie das Zertifikat ablegen möchten und [Fertigstellen].



Mit Klick auf den Button [Durchsuchen] öffnet sich der Datei-explorer.

Übermitteln Sie das Zertifikat an Ihren Ansprechpartner bei der Swisscom, damit es dort eingespielt werden kann.

Nachdem die Swisscom Ihr Zertifikat eingespielt hat ist dies künftig Ihr digitaler „Ausweis“ bei der Swisscom.