

## **Zertifikatsplattform swissign.net**

### Bedienungsanleitung

Glattbrugg, Dezember 2014

## Inhaltsverzeichnis

1.	Einleitung	4
1.1	SwissSign	4
1.2	Ziel und Zweck dieses Dokumentes	4
1.3	Aufbau dieses Dokumentes	4
1.4	Voraussetzungen für die Nutzung von swissign.net	4
2.	PKI – Prozesse und Rollen	4
3.	Bedienkonzept	6
3.1	Konten	6
3.2	Zertifikatslizenz	6
3.3	Aufbau der Benutzeroberfläche	7
3.4	Start und Login auf www.swissign.net	8
3.5	Umgang mit Benutzerkonten	9
3.6	Kontoverwaltung	11
4.	Öffnen einer csv/Excel Datei bei Lizenzbeantragung	13
5.	Beantragung von Zertifikaten	13
5.1	Anfordern von SSL Zertifikaten	15
5.2	Persönliche Zertifikate (S/MIME)	19
5.3	Weitere Zertifikatstypen: z. B. Code Signing Zertifikat	20
5.4	Organisationszertifikat für HSM	21
5.5	Organisationszertifikat (auf smart card mit USB Leser)	22
5.6	Eingabe und Überprüfung eines CSR	22
5.7	Zurückziehen von Zertifikatsanträgen	24
5.8	Genehmigungs-Prozess	25
5.9	Erneuerungs-Prozess	25
5.10	Ungültigkeitsprozess (Revokation)	25
6.	Management von Zertifikaten	27
6.1	Wahl der Rechte	27
6.2	Suche von Zertifikaten	27
6.3	Anzeige der Ergebnisse	28
6.4	Attribute/Abrufbarkeit anzeigen/ändern, Download, Übertragung von Zertifikaten	29
6.5	Antragsformular nochmals erzeugen	30
6.6	Neues Zusenden der E-Mail zum Eigentumsnachweis	31
6.7	Eigentumsnachweis durchführen	32
7.	Freigabe des Zertifikatsantrages – Einreichen des Formulars	33
8.	Vollmachten	35
9.	Herunterladen des ausgestellten Zertifikates	35

10.	E-Mail-Benachrichtigungen	36
10.1	E-Mail-Verkehr bei Zertifikatsanforderung durch Requester	36
11.	Root und Zwischen-Zertifikate importieren	37
12.	Support Kontakt	38
13.	Typische Probleme	38
14.	Index	41

## 1. Einleitung

### 1.1 SwissSign

Die SwissSign AG ist eine international anerkannte Herausgeberin von digitalen Zertifikaten.

Die Zertifikatsplattform swissign.net dient der Ausstellung und Verwaltung von SwissSign Zertifikaten. Der Vorteil bei der Nutzung der Plattform liegt sowohl im Wegfall des Aufbaues und des Betriebes einer eigenen Zertifizierungsstelle als auch in der Qualität der bezogenen Zertifikate bezüglich der Verbreitung in den Wurzelzertifikatsverzeichnissen (Root Stores) und deren Compliance zu den entsprechenden internationalen Standards.

Auf swissign.net können Kunden Zertifikate beantragen («Request») und für ungültig erklären lassen («Revoke»), sowie Zertifikate und gängige Zertifikatsanträge suchen und verwalten.

### 1.2 Ziel und Zweck dieses Dokumentes

Dieses Dokument zeigt im Detail auf, wie mit swissign.net Zertifikate verwaltet werden können: Beantragung, Verwaltung und Revokation.

### 1.3 Aufbau dieses Dokumentes

Die Struktur dieses Dokumentes folgt den klassischen Prozessen, die bei privaten Schlüsselverwaltungen (PKI = Private Key Infrastructure) üblich sind. Diese PKI-Prozesse und deren Rollen werden in einem Grundlagenkapitel dargestellt.

Durch den Index am Ende dieser Bedienungsanleitung lassen sich schnell Antworten auf Fragen finden. Die Anleitung verwendet Querverweise, durch Auswahl der Kapitelnummern im Text können Sie schnell verbundene, relevante Inhalte finden. Die Screenshots in dieser Anleitung wurden mit dem Internet Explorer 9 erstellt, in anderen Browsern kann es zu Abweichungen der Darstellung kommen.

### 1.4 Voraussetzungen für die Nutzung von swissign.net

Eine beliebige Person, die Empfänger eines signierten Dokumentes ist oder sich an einer Webseite anmeldet, wird «Relaying Party» genannt und muss sich auf den Inhalt des Zertifikates verlassen können. Sie vertraut also dem Certificate Service Provider. Infolge dieser Kette des Vertrauens unterzeichnet der Kunde den AGBs, wo er sich den Regeln des Certificate Service Providers unterwirft und seine besondere Verantwortung und Sorgfalt im Umgang und in der Ausstellung von Zertifikaten dokumentiert. Die Regeln des Certificate Service Providers sind in der Zertifizierungspolitik und Zertifizierungspraktiken CP/CPS ([www.swissign.com/cpcps](http://www.swissign.com/cpcps)) im Detail beschrieben.

## 2. PKI – Prozesse und Rollen

Zertifikate haben zwei zentrale Aufgaben, so sind sie einmal ein Container für den öffentlichen Schlüssel und andererseits verbinden sie den öffentlichen Schlüssel mit dem Zertifi-

katsinhaber/Schlüsselinhaber. Die Aufgabe eines Certificate Service Providers ist es, diese Verbindung als unabhängiger Dritter auf dem Niveau gemäss CP/CPS zu bestätigen und zu garantieren. Damit das gewährleistet werden kann, benötigt er folgende Services, Tätigkeiten und Rollen:

#### **Registration Service (Antragstellungsdienst)**

- Zertifikatsantragstellung durch den Antragssteller
- Zertifikatsantragsprüfung durch den Registrierungsstellenverantwortlichen (RAO = Registration Authority Officer) oder nachfolgend RA-Administrator genannt.
- Freigabe des Zertifikatsantrags durch den RA-Administrator (RAO)

#### **Certificate Generation Service (Generierungsdienst für Zertifikate)**

- Erzeugung des Zertifikates

#### **Revocation Service (Dienst zur Ungültigkeitserklärung)**

- Online-Ungültigkeitserklärung durch den Zertifikatsinhaber
- Offline-Ungültigkeitserklärung durch den RA-Administrator (RAO)

#### **Dissemination Services (Verbreitung der Informationen)**

- CP/CPS
- OCSP (Online Certificate Status Protocol) – Online Status über die Gültigkeit von Zertifikaten
- CRL (Certificate Revocation List) – Ungültigkeitslisten (offline) von Zertifikaten
- LDAP (Light Weight Address Directory)

Sofern keine Managed PKI im Einsatz ist, übernimmt grundsätzlich SwissSign die Rolle des RA-Administrators.

Die folgende Tabelle gibt einen Überblick der Tätigkeiten und deren Abbildung in der swissign.net Plattform:

<b>Tätigkeit</b>	<b>Rolle/Wer</b>	<b>Unterstützung auf swissign.net</b>
Zertifikatsantrag	Antragsteller/Systemadministratoren	GUI
Freigabe	RA-Administrator	SwissSign / Silver Zertifikate durch Eigentumsnachweis E-Mail
Ausstellung/Erzeugung	-	CA
Installation	Antragsteller/Systemadministratoren	E-Mail mit Download Link

Ungültig erklären	Antragsteller/Systemadministrator, RA-Administrator	GUI
Erneuerung	Antragsteller/Systemadministrator, RA-Administrator	Warn-E-Mail 10 Tage und 30 Tage vor Ablauf
Suchen/Verwalten	Antragsteller/Systemadministrator	GUI

### 3. Bedienkonzept

Die Benutzeroberfläche ist nativ ohne Nutzung einer speziellen Software für die Benutzeroberfläche geschrieben. Das dient dem Ziel der Sicherheit, da die Nutzung fremder, nicht bekannter Softwarepakete auch immer ein Sicherheitsrisiko bedeutet. Insofern wird die Verwendung von Graphiken und Symbolen in der Benutzeroberfläche minimiert.

#### 3.1 Konten

Konten (Accounts) dienen der Verwaltung von Zertifikaten auf Stufe der Anforderer (Requestoren) respektive Anforderer-Gruppe (Requestor-Gruppe) und wurden in früheren Releases der SwissSign Plattform auch Profile genannt.

Ein Konto repräsentiert einen Benutzer oder eine Gruppe von Benutzern, die sich durch Benutzername/Passwort oder mittels Zertifikat anmelden können. Konten können durch jeden Benutzer selbst angelegt werden, um danach eine Lizenz aus dem Shop einzulösen.

Ein Konto umfasst Kontaktinformationen, speziell die E-Mail-Adresse für Benachrichtigungen und optional eine Telefonnummer. Die Information kann vom Konteninhaber verändert werden.

Der Anforderer kann Zertifikatsanforderungen im Rahmen der für ihn bezogenen Lizenz für einen bestimmten Zertifikatstyp stellen. Die Lizenz lässt automatisch nur die Bestellung eines bestimmten Zertifikatstyps zu. Jede Zertifikatsanforderung unter Benutzung dieses Kontos wird diesem Konto zugeordnet. Damit müssen die Kontoinformationen (wie z. B. die Adresse für E-Mail Benachrichtigungen) nicht jeder Zertifikatsanforderung einzeln zugeordnet werden. Jede einzelne Zertifikatsanforderung wird über einen Workflow zu den entsprechenden RA-Administratoren bei SwissSign weitergeleitet, welche diese Anforderung prüfen und bewilligen müssen.

**Achtung:** Das Konto zur Einlösung der Lizenz auf swissign.net hat nichts mit den Benutzerkonten zu tun, die ggfs. im Webshop [www.swissign.com](http://www.swissign.com) angelegt wurden.

#### 3.2 Zertifikatslizenz

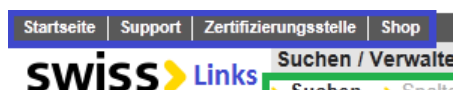
Eine Zertifikatslizenz ist ein Code, der es dem Benutzer erlaubt ein entsprechendes Zertifikat anzufordern. Der Lizenzcode kann typischerweise im SwissSign Webshop erworben werden.

## 3.3 Aufbau der Benutzeroberfläche

Die Benutzeroberfläche ist in folgende Bereiche unterteilt:

- Header-Bereich: Allgemeine Informationen und Sprachauswahl
- Hauptmenü
- Menüzeile
- Arbeitsbereich

Die Benutzeroberfläche ist in folgende Bereiche unterteilt, auf die im nachfolgenden Text referenziert wird:



Oben links gibt es mehrere Schaltflächen, die mit Links verbunden sind:

- Startseite: Durch Betätigen dieser Schaltfläche kommt man immer wie-der auf die Startseite der Benutzeroberfläche zurück.
- Support: Ein Link zum Helpdesk
- Zertifizierungsstelle: Hier gelangt man zu allgemeinen Informationen über SwissSign und zu weiteren Links z. B. zur CP/CPS und den Zertifikaten der Root und Issuing (Intermediate) CA.
- Shop : Hier gelangt man zum Webshop von SwissSign.

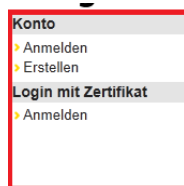
Besonderheit: Der Anwender kann durch eine Schaltfläche ganz oben rechts diese Leiste komplett (inklusive Logo) ausblenden, um eine grössere Arbeitsfläche zu haben.



## Sprachumschaltung

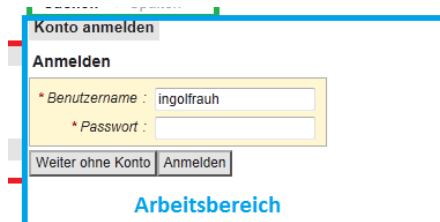
Oben rechts kann jederzeit die Sprache geändert werden.

- DE : Benutzeroberfläche in Deutsch
- EN : Benutzeroberfläche in Englisch



## Hauptmenü

Links befindet sich das Hauptmenü. Unterhalb der einzelnen Untermenü-Überschriften sind Aktionen anwählbar.



Über die Menüpunkte im Hauptmenü wird der Applikationsablauf im Arbeitsbereich gesteuert.



Je nach gewähltem Menü im Hauptmenü gibt es einen Workflow oder Ablauf bzw. mehrere parallele Aktionen, die möglich sind. Um den Arbeitsbereich entsprechend anzusteuern, kann auf die Schaltflächen der Menüzeile oberhalb des Arbeitsbereichs geklickt werden.

### 3.4 Start und Login auf www.swissign.net

Benutzer, die vom Shop direkt bereits die Lizenz einlösen, können überlegen, ob sie die Lizenz mit einem Konto oder ohne Konto einlösen wollen.

Die Errichtung eines Kontos hat mehrere Vorteile:

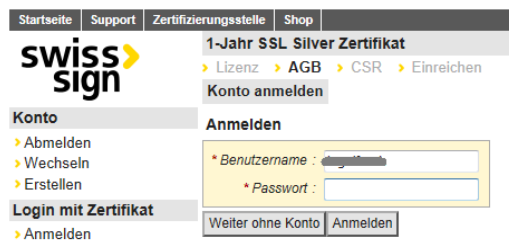
- Verwaltung mehrerer Zertifikate einfacher (Reports, Übersichten etc.)
- Revokation (Zurückziehen) von Zertifikaten ist einfacher
- Zentraler Ort zum Herunterladen von Zertifikaten



Benutzer, die mittels Lizenzcode eine Zertifikatslizenz einlösen wollen, werden auf swissign.net folgenden Bildschirm sehen:

Sie können nun fortfahren ohne Konto («Weiter ohne Konto»), mit Anmeldung («Anmelden») oder mit der Erzeugung eines Kontos im

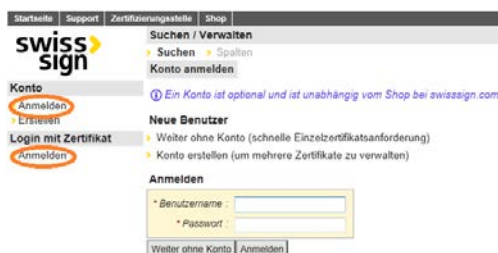




Hauptmenü links («Konto-Erstellen»).

Sofern Sie diesem Link nicht gefolgt sind, können Sie die Plattform mit

[www.swissign.net](http://www.swissign.net) aufrufen.

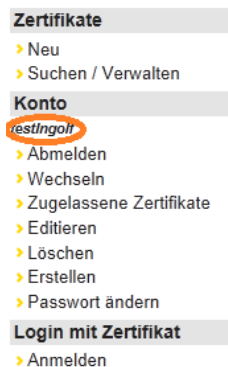


Generell gibt zwei Optionen um sich anzumelden:

- Login mit Zertifikat: Diese Option steht nur Managed PKI Kunden der SwissSign zur Verfügung.
- Login mit Kontoname und Passwort

Es ist immer möglich als bereits eingeloggter Benutzer eine andere Rolle einzunehmen und sich mit einem dementsprechenden Konto einzuloggen.

Sobald man im Konto eingeloggt ist, wird der Kontoname unterhalb der Menüzeile «Konto» kursiv und fett gedruckt angezeigt.

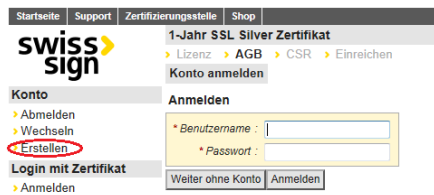


## Hinweise:

- Es ist darauf zu achten, dass man nur mit einem Konto angemeldet ist. Mit «Abmelden» können Sie sich aus dem entsprechenden Konto ausloggen.
- Beim Login wird ein Profil-Session-Cookie (signiert) gesetzt. Dieser ist 30 Minuten gültig.
- Sollten Sie Ihr Passwort vergessen haben, so wenden Sie sich an den Support.

## 3.5 Umgang mit Benutzerkonten

### 3.5.1 Anlegen eines Kontos



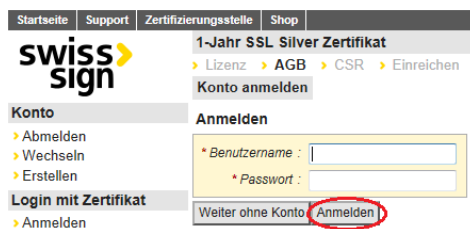
Ein Zertifikatsanforderer kann ein Konto erstellen, sofern dieses noch nicht existiert. Er wählt hierfür im Hauptmenü «Konto» den Menüpunkt «Erstellen».



Der Benutzer wird nun aufgefordert, Attribute zu seinem Konto anzulegen:

Hierzu gehört eine E-Mail-Adresse, die für alle Benachrichtigungen zu den Zertifikaten genutzt wird, die unter diesem Konto beantragt wurden, unabhängig von der E-Mail Adresse, die in einem Zertifikat selber enthalten ist. Die bevorzugte Sprache legt die Sprache für die E-Mail-Benachrichtigungen und die Sprache der Benutzeroberfläche nach dem Login fest. Eine Telefonnummer kann optional eingegeben werden und erleichtert die Arbeit des Supports.

### 3.5.2 Anmelden am Konto



Ein Zertifikatsanforderer kann sich in seinem zuvor eingerichteten Konto anmelden. Er muss als Benutzername seinen gewählten Kontonamen und als Passwort sein Passwort eingeben. Anschliessend muss er den Knopf «Anmelden» betätigen.

### 3.6 Kontoverwaltung

Als Benutzer hat man die Möglichkeit im Nachhinein sein Konto zu verwalten.

**Konto**  
 testingolf

- > Abmelden
- > Wechseln
- > Editieren
- > Löschen
- > Erstellen
- > Passwort ändern

Im Hauptmenü hat man unter dem Menüpunkt «Konto» folgende Möglichkeiten, sein Konto zu verwalten:

Mit «Abmelden» kann man sich komplett aus der Anwendung abmelden und ist praktisch ein Benutzer ohne Konto der Webseite. Benutzer ohne Konto können z. B. immer noch öffentlich publizierte Zertifikate suchen und anzeigen lassen.

**Konto anmelden**

**Anmelden**

\* Benutzername :

\* Passwort :

Weiter mit testingolf

Mit «Wechseln» kann man in ein anderes Konto wechseln, indem man sich an diesem anmeldet.

**Konto editieren**

**Konto testingolf editieren**

① Die Kontoangaben werden nicht an Dritte weitergegeben.  
 ② Die Kontoangaben werden **nicht** in Zertifikate übernommen, die unter diesem Konto angefordert werden.

\* E-Mail Adresse :

Telefonnummer(n) :

Optionaler Freitext

Bevorzugte Sprache :  English  Deutsch

Anforderer für : SwissSign Email Validation RA

**Suchen**

Mit «Editieren» kann man die Attribute des Kontos verändern, z. B. die E-Mail-Adresse oder Telefonnummer.

Mit «Löschen» kann das bereits vorhandene Konto wieder gelöscht werden. Achtung: Das jeweilige Konto wird sofort gelöscht.

**Konto erstellen**

**Konto registrieren**

① Die Kontoangaben werden nicht an Dritte weitergegeben.  
 ② Die Kontoangaben werden **nicht** in Zertifikate übernommen, die unter diesem Konto angefordert werden.

\* Benutzername :

\* Passwort :

\* Passwort wiederholen :

\* E-Mail Adresse :

Telefonnummer(n) :

Optionaler Freitext

Bevorzugte Sprache :  English  Deutsch

Mit «Erstellen» kann ein weiteres Konto erstellt werden. Es läuft analog zum erstmaligen Erstellen des Kontos. In diesem Falle muss der Benutzername, das Passwort und eine E-Mail Adresse eingegeben werden, die für alle Benachrichtigungen zu den Zertifikaten genutzt wird, die unter diesem Konto beantragt wurden, unabhängig von der E-Mail Adresse, die in einem Zertifikat selber enthalten ist. Die bevorzugte Sprache legt die Sprache für die E-Mail Benachrichtigungen und die Sprache der Benutzeroberfläche nach dem Login fest.

## Passwort ändern

### Passwort von Konto testIngolf ändern

\* Passwort :

\* Passwort wiederholen :

Abbrechen Passwort ändern

Mit «Passwort ändern » ändert man das Passwort zu einem vorhandene Konto.

**Hinweis:** Bei Beantragung von Zertifikaten werden die Angaben aus dem Konto für Benachrichtigungen zu dem jeweiligen Request verwendet. Das heisst die E-Mail-Adresse und das Zertifikat werden automatisch mit dem Profil verknüpft, sofern der Beantragende das nicht explizit ändert.

Es ist auch möglich, den Zugang zum Konto auf einen zertifikatsbasierten Zugang umzustellen. Hierfür gibt es den Menüeintrag «Zugelassene Zertifikate ». Danach können Sie dann direkt sich in das Konto einloggen ohne Nutzung von Username und Passwort. Bitte beachten Sie, dass Sie für den zertifikatsbasierten Zugang ein persönliches Zertifikat benötigen, welches das sichere Login in seiner Schlüsselverwendung zulässt. Zum Beispiel kann hierfür das SwissSign Gold Personal ID Zertifikat genutzt werden.

## Zertifikate

- > Neu
- > Suchen / Verwalten

## Konto

### Requestor\_ce1

- > Abmelden
- > Wechseln
- > Zugelassene Zertifikate**
- > Editieren
- > Löschen
- > Erstellen
- > Passwort ändern

### Verfügbare Konten

- > CE
- Requestor\_ce1

## Auswertungen

### Zertifikate

#### Zugelassene Zertifikate

Zertifikate, die zum passwortlosen Logon ins Konto Requestor\_ce1 zugelassen sind

Entfernen	Subjekt	Alternativer Name des Subjekts
	/CN=pseudo: CEMO_RAO_CE/Email=corneilia.enske@swissign.com	email=corneilia.enske@swissign.com, o=OFFN:corneilia

#### Zertifikat zur Verwendung von Konto Requestor\_ce1 berechtigen

\* Schlüsselidentifikator / Zertifikatsidentifikator:

Zertifikat autorisieren

Zertifikate

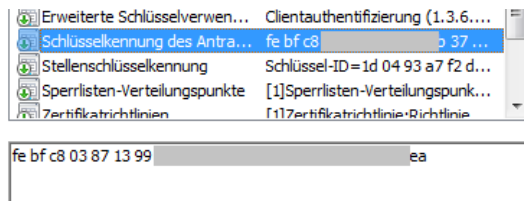
Zurück zu Zertifikate

Wählen Sie zunächst den Menüpunkt «Zugelassene Zertifikate».

Der Tab «Zugelassene Zertifikate» zeigt alle Zertifikate an, sofern diese schon mit einem Konto verbunden sind.

Ein neues Zertifikat kann über das Eingabefeld «Schlüssel-Identifikator» eingegeben werden. Hier ist die ID des Zertifikates einzugeben.

Mit der Schaltfläche «Entfernen» kann auch ein Zertifikat wieder einem Konto entzogen werden. Der Benutzer muss sich dann wieder mit Benutzername/Passwort einloggen.



Den Schlüssel-Identifikator können Sie aus der Standardzertifikatsanzeige Ihres Betriebssystems entnehmen.

#### 4. Öffnen einer csv /Excel Datei bei Lizenzbeantragung

Sofern Sie von Ihrem Reseller einen Link erhalten haben und diesen anklicken, oder im Shop auf das Schlüsselsymbol anklicken, kann es passieren, dass Sie einen Download einer «certificates.csv» Datei angeboten bekommen.

In diesem Fall wurde ein Lizenzschlüssel im Link verwendet, der bereits in ein gültiges Zertifikat eingelöst wurde.



Die wesentlichen Daten des bereits ausgestellten Zertifikats werden in Excel angezeigt:

	A	B	C	D	E	F
1	Status	Läuft ab	Subjekt	Alternativer Name	Anforderungsidentifikator	Konto
2	valid	10/10/2019 19:33	/CN=Email: [redacted]	email: [redacted]	9E27BF0C-1B0E-474E-B01C49D4A...	[redacted]

#### 5. Beantragung von Zertifikaten

Jede Zertifikatsanforderung basiert auf einen Lizenzcode und den Zertifikatstypen, die mit diesem Lizenzcode verbunden sind.

Lizenzen können im SwissSign Webshop gekauft. Eine Lizenz berechtigt einen Benutzer dazu, eine bestimmte Anzahl Zertifikate anzufordern – in der Regel ein einziges Zertifikat. Eine Lizenz bestimmt ein Produkt, worüber eine Anforderung gestellt werden kann.

**Konto anmelden**

**Anmelden**

\* Benutzername :

\* Passwort :

Weiter ohne Konto | Anmelden

Es wird grundsätzlich beim Zertifikatsantrag die Verwendung eines Kontos empfohlen. Bei diesem muss man sich anmelden.

- Kontodaten (E-Mail-Adresse, Spracheinstellung) werden direkt übernommen und bei der Erstellung eines Zertifikates als Attribute dem Zertifikat beigefügt. Dabei handelt es sich nicht um Daten, die im Zertifikat enthalten sind, aber z. B. zugeordnete Daten, wie z. B. die E-Mail-Adresse, an die Ablaufnotifikationen bezüglich dieses Zertifikates gehen.

Nach denen mit einem Konto angeforderten Zertifikaten kann gezielt gesucht werden.

Um Zertifikate neu zu beantragen ist im Hauptmenü links unter Oberpunkt «Zertifikate» der Unterpunkt «Neu» zu wählen.



Der im Shop erworbene Lizenzcode ist unter «Lizenzcode» einzutragen.

Im Arbeitsbereich muss nun die AGB gelesen und bestätigt werden. Hierzu die Schaltfläche «Ich akzeptiere diese Bedingungen» wählen. Durch Anwahl des Wortes «Aufklappen» kann der gesamte Text der AGB gelesen werden.

Optional: Zertifikatsregistrierungsanforderung (CSR = Certificate Signing Request) eingeben. Benutzer können sich extern mit eigenen Tools (z. B. certtool.exe oder OpenSSL) ein Schlüsselpaar erzeugen und nur für den öffentlichen Schlüssel ein Zertifikat anfordert. Diese Anforderung geschieht mittels eines sogenannten CSR, den diese Tools automatisch generieren. Der vom externen Tool generierte CSR Text im PKCS#10 Format ist in das nachfolgende Feld einzugeben und die Schaltfläche «Weiter» zu wählen. Ein typischer Signing Request ist nebenstehend zu sehen.

Sollte der Benutzer sich dafür entscheiden, von

SwissSign die Schlüssel generieren zu lassen, so ist das Feld unter PKCS#10 leer zu lassen und nur die Schaltfläche «Weiter» zu betätigen.

**Hinweis:** Alternativ kann der Benutzer auch SwissSign damit beauftragen für ihn den privaten und öffentlichen Schlüssel zu generieren. Bei der Generierung des privaten Schlüssels wird dieser sofort mit einem Passwort, welches der Benutzer eingibt, verschlüsselt. SwissSign kennt dieses Passwort nicht und kann dieses auch nicht wieder herstellen. Es ist daher sorgfältig aufzubewahren. Im Falle eines Verlustes sind alle mit diesem Schlüssel verschlüsselten Daten nicht mehr lesbar und können nicht mehr weiterverwendet werden.

Das von SwissSign generierte SSL Schlüsselpaar bleibt für kurze Zeit (3 Monate) auf der Plattform. Schlüsselpaare für S/MIME Personenzertifikate bleiben während ihrer Laufzeit auf der Plattform und können jederzeit neu unter Verwendung des Passwortes heruntergeladen werden.

Die nachfolgenden Schritte unterscheiden sich jetzt von Zertifikat zu Zertifikat. Daher werden nach den Zertifikatstypen die Unterkapitel getrennt.

## 5.1 Anfordern von SSL Zertifikaten

Nachfolgend ist der typische Ablauf bei der Bestellung von SSL Gold Zertifikaten beschrieben.

1-Jahr SSL Gold Zertifikat

Lizenz > AGB > CSR > **Attribute** > Kontakt > Einreichen

**Attribute**

\* Domäne :   
Voll qualifizierter Domänenname (FQDN) Ihres Servers.  
Beispiel: www.swissign.com

E-Mail :

Organisation :   
Einschliesslich Rechtsform, wie amtlich registriert.  
Beispiel: SwissSign AG, Google Inc.

Organisationseinheit :

Ortschaft :

Kanton/Bundesland :

Erforderlich, wenn Organisation definiert (ausser nicht anwendbar)

Land :

Zurück | Weiter

Im Arbeitsbereich ist zunächst die Identität auszufüllen: Zunächst muss dem Zertifikat ein Domänenname vergeben werden, der später auch im Subject des Zertifikates steht. Die Organisation, Ort, ggfs. Kanton/Bundesland und Staat mit dem Hauptsitz der Organisation kann bei z. B. Goldzertifikaten ebenfalls eingegeben werden. Bei Silver Zertifikaten ist nur der Eintrag des Domänennamens verpflichtend.

Danach ist die Schaltfläche «Weiter» zu betätigen.

Alle Pflichtfelder sind immer mit einem (\*) gekennzeichnet.

Sofern Sie via Konto eingeloggt sind, erhalten Sie nicht mehr die gezeigte Kontakt-Ansicht. In diesem Fall wird als Kontakt der in den Kontoeinstellungen hinterlegte Kontaktdatenatz genommen. Wollen Sie dennoch diesen expli-

**2-Jahre SSL Gold Zertifikat**

Lizenz > AGB > CSR > Attribute **Kontakt** Einreichen

**Kontakt**  
Adresse, wo Sie Benachrichtigungen zu diesem Antrag erhalten möchten.

\* E-Mail Adresse :   
Überschreibt die obige vordefinierte E-Mail Adresse

Telefonnummer(n) :

Bevorzugte Sprache :  Deutsch (Profil)  
 English  
 Deutsch

zeit anpassen, müssen Sie in der Menüzeile oben den Punkt «Kontakt» wählen. Die hier eingegebenen Kontaktdaten überschreiben dann die im Konto hinterlegten Daten – aber nur für das hier angeforderte Zertifikat.

Benutzer ohne Kontologin kommen automatisch auf diese Kontaktseite und füllen die Daten E-Mail-Adresse und bevorzugte Sprache aus. Die E-Mail-Einstellungen wirken sich z. B. auf Hinweis-E-Mails zum baldigen Ablauf von Zertifikaten aus.

Anschliessend ist die Schaltfläche «Weiter» zu betätigen.

**1-Jahr SSL Gold Zertifikat**

Lizenz > AGB > CSR > Attribute > Kontakt > **Zertifikatsanfragen**

**Zertifikatsanfragen**

ID	Produkt	Status	Datum
1	1-Jahr SSL Gold Zertifikat	Abgeschlossen	2014-05-09 13:45:54

**Schlüsselgenerierung**  
Die angegebene Schlüssellänge ist mit einem Passwort geschützt, das Sie rechtzeitig weiterleiten.  
Für die Schlüsselgenerierung ist ein Passwort erforderlich, das die Länge, den Zeichensatz und die Komplexität erfüllt.  
Für diesen Schritt ist die Verwendung eines sicheren Schlüssels erforderlich.

Jetzt kann das Zertifikat angefordert werden. Alle Zertifikatsdaten werden nochmals angezeigt. Sind eventuell Fehler vorhanden, können die vorherigen Menüs in der Menüzeile oben nochmals angewählt werden und die Daten können angepasst werden. Auch wenn Sie Ihre Daten mittels CSR eingegeben haben können Sie hiermit nochmals Ihre Daten anpassen. Im Falle einer Schlüsselgenerierung durch SwissSign (kein CSR wurde eingegeben) ist im Passwortfeld ein sicherer Schlüssel für den Transfer des Passwortes einzugeben. Anschliessend ist die Schaltfläche «Zertifikat anfordern» anzuwählen.

Im Falle von Gold und Gold EV Zertifikaten werden Sie nun gebeten, ein Registrierungsformular auszudrucken und unterzeichnen zu lassen. Hierin sind die Organisation und die Domänenzugehörigkeit zu bestätigen.

**SSL Demo Certificate with Organization**

Lizenz > AGB > CSR > Attribute **Kontakt** Einreichen

**Einreichen**

Lizenz  
Produkt: SSL Demo Certificate with Organization  
Lizenzcode:

AGB  
AGB: gold 2.0 2014-05-09 13:45:54

CSR

Attribute  
Domäne:   
E-Mail:  
Organisation: MPKI Test Demo AG

Sollten Sie Ihr Zertifikat mit Hilfe eines CSR beantragt haben und die dort verwendeten Namen enthalten einen Umlaut, so können Sie im orangenen Feld unter «Einreichen» sehen, ob der Umlaut richtig interpretiert wurde. Sollte das nicht der Fall sein, können Sie den Umlautwert korrigieren:

Gehen Sie wieder in der Menüleiste zurück auf das Menü «Attribute».



**SSL Demo Certificate with Organization**

[Lizenz](#) > [AGB](#) > [CSR](#) > **Attribute** > [Kontakt](#) > [Einreichen](#)

**Attribute**

\* Domäne :  |    
Voll qualifizierter Domänenname (FQDN) Ihres Servers.  
 Beispiel: www.swissign.com

E-Mail :

\* Organisation : MPKI Test Demo AG  
Einschliesslich Rechtsform, wie amtlich registriert.  
 Beispiel: SwissSign AG, Google Inc.

Organisationseinheit :

Ortschaft :

Kanton/Bundesland :

Erforderlich, wenn Organisation definiert (ausser nicht anwendbar)

Kanton/Bundesland :  Anwendbar  Nicht anwendbar

Land : Schweiz - CH

Die von Ihnen im CSR dargestellten Attribute wurden jetzt den Feldern zugeordnet und können editiert werden. Mit «Weiter» kommen Sie dann wieder zu der zuletzt angezeigten «Einreichen» Anzeige.

Hintergrundinformation hierzu: Umlaute werden in Zertifikaten nach UTF-8 Codierung behandelt ([www.utf8-zeichentabelle.de/unicode-utf8-table.pl?start=128&number=128&names=-&utf8=string-literal](http://www.utf8-zeichentabelle.de/unicode-utf8-table.pl?start=128&number=128&names=-&utf8=string-literal)). So wird z. B. ein Firmenname «Test und Söhne» wie folgt im Hintergrund codiert: «Test und S\c3\xb6hne». Die Weboberfläche macht das bequem im Hintergrund, bei CSR Eingaben kann es aber immer wieder zu Fehler kommen, je nach Qualität des CSR Tools.

**Hinweis:** Der Organisationsname im Zertifikat sollte in derselben Art und Weise geschrieben werden wie im Handelsregisterauszug. Auch eventuelle Organisationsformen sollten mit derselben Abkürzung verwendet werden wie im Handelsregisterauszug (z. B. «AG»).

Ein SSL Silver Zertifikat wird ähnlich wie oben beantragt:

**1-Jahr SSL Silver Zertifikat**

[Lizenz](#) > [AGB](#) > [CSR](#) > **Domäne** > [Inhaber](#) > [Kontakt](#) > [Einreichen](#)

**Domäne**

\* Domäne :

Voll qualifizierter Domänenname (FQDN) Ihres Servers.  
 Beispiel: www.swissign.com

Im Arbeitsbereich ist nur der Domänenname einzugeben. Es muss ein voll qualifizierter Domänenname sein und kein interner Domänenname oder eine IP-Adresse.

Alle Pflichtfelder sind immer mit einem (\*) gekennzeichnet.

**1-Jahr SSL Silver Zertifikat**

[Lizenz](#) > [AGB](#) > [CSR](#) > [Domäne](#) > **Inhaber** > [Kontakt](#) > [Einreichen](#)

**Inhaber**

E-Mail Adresse, mit der die Registrierungsstelle sicherstellen kann, dass Sie der rechtmässige Inhaber von mydomain.com sind.

\* Validerung e-Mail-Adresse :

admin@mydomain.com  
 administrator@mydomain.com  
 postmaster@mydomain.com  
 webmaster@mydomain.com

Sie müssen nun die Inhaberschaft bzw. die Zugriffskontrolle auf diese Domäne zeigen. Hierzu wird Ihnen eine E-Mail an ein von Ihnen wahlweise angegebenes E-Mail-Konto, das mit dieser Domäne verbunden ist, versendet.

Der weitere Ablauf ist dann wie beim SSL Gold Zertifikat oben.

Ein Multi-Domain Zertifikat erlaubt den Eintrag von bis zu zwanzig zusätzlichen Domänen zu einer Hauptdomäne:

**Identität**

\* Domäne :

Voll qualifizierter Domänenname (FQDN) Ihres Servers.  
Beispiel: www.swissign.com

Weitere Domänen :

E-Mail :

\* Organisation :

Die Anzahl der Domänen , die zusätzlich zur Hauptdomäne in das Zertifikat aufgenommen werden soll, muss gewählt werden.

**Identität**

\* Domäne :

Voll qualifizierter Domänenname (FQDN) Ihres Servers.  
Beispiel: www.swissign.com

Weitere Domänen :

\* Domäne :

\* Domäne :

\* Domäne :

E-Mail :

Nach der Auswahl werden die Eingabefelder sofort angezeigt und können entsprechend ausgefüllt werden. Hinweis: Es ist absolut notwendig, dass die Organisation auch im Besitz dieser Domänen ist oder eine Vollmacht des Besitzers vorliegt.

Der weitere Ablauf ist dann wie oben beschrieben.

Bei einem SSL EV Gold Zertifikat gilt es noch einige Besonderheiten zu beachten. Im Rahmen der Zertifikatsantragstellung werden noch besondere Angaben abgefragt:

**1-year EV SSL Multidomain Gold Certificate**

Lizenz > AGB > CSR > Identität > Wirtschaftskategorie

**Wirtschaftskategorie**

Private Organisation  
Unternehmen, welche in einem staatlich verordneten oder kommissionierten Paragrafenregister eingetragen sind  
Organisation des öffentlichen Sektors  
Die legale Existenz dieser Organisation wird durch eine staatliche Stelle auf Ebene des Bundes oder des Kantons / des Bundeslandes bestätigt.  
Unternehmerische Einheit  
Unternehmen, welche nicht als "Private Organisation" bezeichnet werden können, sollen diese Tätigkeitsform wählen. Zum Beispiel: Gewerbe/Panorama  
Jahresumsatz > Einzelfirma  
Nicht-kommerzielle Tätigkeit  
Organisationen, welche nicht in eine dieser Kategorien passen, wählen diese Tätigkeitsform

Eine ausführliche Erläuterung der verschiedenen Organisationsformen finden Sie im Dokument [EV SSL Certificate Guidelines](#)

wirtschaftskategorie

Zurück Weiter

Nach Angabe der Zertifikatsdaten wird noch die Wirtschaftskategorie überprüft. Diese muss mit den Einträgen im Handelsregister oder sonstigem Register übereinstimmen.

**1-year EV SSL Multidomain Gold Certificate**

Lizenz > AGB > CSR > Identität > Wirtschaftskategorie **Registrierungsstaat**

**Registrierungsstaat**

Geben Sie das Land des Amtes, bei dem Ihre Organisation registriert wurde.

\* Registrierungsstaat :

Zurück Weiter

Auch der Staat (Registrierungsstaat ) und ggfs. Kanton/Provinz/Bundesland oder Ortschaft, bei der die Organisation registriert wurde, muss angegeben werden.

**1-year EV SSL Multidomain Gold Certificate**

Lizenz > AGB > CSR > Identität > Wirtschaftskategorie > Registrierungsstaat **Registrierungskanton/-bundesland/-ortschaft**

**Registrierungskanton/-bundesland/-ortschaft**

Registrierungskanton/-bundesland :

Leer lassen, falls das Amt seine Tätigkeit auf Staatsebene ausübt

Zurück Weiter

**1-year EV SSL Multidomain Gold Certificate**

Lizenz > AGB > CSR > Identität > Wirtschaftskategorie > Registrierungsstaat > **Registrierungskanton/-bundesland/-ortschaft** > **Registrierungsnummer** > Kontakt > Einreichen

**Registrierungsnummer**

Bitte geben Sie die Registrierungsnummer (z.B. Handelsregister-Nr. in der Schweiz) ein, die Ihrer Organisation vom zuständigen öffentlichen Amt Ihrer Region zugewiesen wurde.

\* Registrierungsnummer :

Zurück Weiter

Die entsprechende Registrierungsnummer ist ebenfalls einzutragen. Bitte beachten Sie, dass hier in der Schweiz die neue UID einzutragen ist.

Der weitere Ablauf ist dann wie oben beschrieben.

**Hinweis:** Es sind für die von SwissSign generierten Schlüssel sichere Passwörter zu verwenden. Unsichere Passwörter (z. B. zu geringe Länge) müssen explizit bestätigt werden. Passwörter sind sicher aufzubewahren und dürfen nicht verloren gehen. SwissSign kennt diese Passwörter nicht und kann diese im Falle eines Verlustes auch nicht wiederherstellen. Das Zertifikat und die damit verschlüsselten Daten sind dann verloren. Private Schlüssel von SSL Zertifikaten werden nach kurzer Zeit ebenfalls gelöscht, diese sind rechtzeitig vom SwissSign System herunterzuladen.

## 5.2 Persönliche Zertifikate (S/MIME)

Nachfolgend wird die Vorgehensweise bei Personenzertifikaten beschrieben:

**1-Jahr Personal Gold Zertifikat mit Organisationseintrag**  
 > Lizenz > AGB > CSR **Attribute** > Kontakt > Einreichen

**Attribute**  
 Sie können Ihren richtigen Namen oder ein Pseudonym eingeben.

Vorname(n) Nachname(n) :   
Buchstabiert wie im Ausweis

Pseudonym :   
Nur dann eingeben, wenn das Feld Vorname Nachname leer bleibt.

\* E-Mail :

Organisation :   
Einschliesslich Rechtsform, wie amtlich registriert.  
 Beispiel: SwissSign AG, Google Inc.

Organisationseinheit :

Land :

Zurück Weiter

Hier sind die Attribute für das Personenzertifikat einzugeben. Alle erforderlichen Felder sind mit einem Stern (\*) gekennzeichnet. Bei Gold Zertifikaten werden Vor-/Nachnamen eingegeben. Auch die Verwendung eines Pseudonyms ist gestattet, dann muss das Feld Vor-/Nachname freigelassen werden. Es ist darauf zu achten, die Namen so zu verwenden, wie sie auch in der eigenen ID/Reisepass geschrieben werden. Bei Silver Zertifikaten ist nur die Eingabe der E-Mail-Adresse notwendig. Diese muss bei Anforderung des Zertifikates aber bereits existent sein. Gold Zertifikate mit Organisationseintrag werden hier mit der Organisation spezifiziert. Danach ist die Schaltfläche «Weiter» zu betätigen.

Pseudonyme können für anonyme Mailboxen oder Gruppen-Accounts genutzt werden. Wichtig ist, dass es einen Verantwortlichen für dieses Zertifikat dann gibt. Namen, die in das Pseudonym Feld eingegeben werden, werden mit dem String «pseudo:» im Zertifikat dargestellt, z. B. wird das Pseudonym «Sales-Mailbox» als «pseudo: Sales-Mailbox» dargestellt.

**1-Jahr Personal Gold Zertifikat mit Organisationseintrag**  
 > Lizenz > AGB > CSR > Attribute **Kontakt** > Einreichen

**Kontakt**  
 Adresse, wo Sie Benachrichtigungen zu diesem Antrag erhalten möchten.

E-Mail Adresse :   
Überschreibt die oben vordefinierte E-Mail Adresse (optional)

Telefonnummer(n) :

Bevorzugte Sprache :  Deutsch (Konto)  
 English  
 Deutsch

Zurück Weiter

Sofern Sie mit einem Konto eingeloggt sind, erhalten Sie nicht mehr die gezeigte Kontaktansicht. In diesem Fall wird als Kontakt die in den Kontoeinstellungen hinterlegten Daten genommen. Wollen Sie dennoch diese explizit anpassen, müssen Sie in der Menüzeile oben den Punkt «Kontakt» wählen. Die hier eingegebenen Kontaktdaten überschreiben dann die im Profil hinterlegten Daten – aber nur für das

hier angeforderte Zertifikat.

Benutzer ohne Kontologin kommen automatisch auf diese Kontaktseite und füllen die Daten E-Mail-Adresse und bevorzugte Sprache aus. Die E-Mail-Konfiguration wirkt sich z. B. auf Hinweis-E-Mails zum Ablauf von Zertifikaten aus.

Anschliessend ist die Schaltfläche «Weiter» zu betätigen.

**1-Jahr Personal Gold Zertifikat mit Organisationseintrag**

[Lizenz](#) > [AGB](#) > [CSR](#) > [Attribute](#) > [Kontakt](#) **Einreichen**

---

**Einreichen**

> Lizenz  
*Produkt:* 1-Jahr Personal Gold Zertifikat mit Organisationseintrag  
*Lizenzcode:*

---

> AGB  
*AGB:* gold 2.0 2014-01-23 12:16:14

---

> CSR

> Attribute  
*Vorname(n) Nachname(n):* Ingolf Rauh  
*Pseudonym:*  
*E-Mail:* ingolf.rauh@swissign.com  
*Organisation:*  
*Organisationseinheit:*  
*Land:* undefiniert

---

> Kontakt  
*E-Mail Adresse:* ingolf.rauh@swissign.com (Konto)  
*Telefonnummer(n):*  
*Bevorzugte Sprache:* Deutsch (Konto)

---

**Zertifikatsangaben**

Subjekt DN	CN	Ingolf Rauh
	emailAddress	ingolf.rauh@swissign.com
Alternativer Name des Subjekts	email	ingolf.rauh@swissign.com

**Schlüsselerzeugung**  
 Der erzeugte Schlüssel wird mit einem Passwort geschützt, das Sie nachfolgender selber wählen.

*⚠ Aus Sicherheitsgründen ist SwissSign nicht in der Lage, verlorene Schlüsselpasswörter wiederherzustellen. Für deren sichere Aufbewahrung ist ausschliesslich der Benutzer verantwortlich.*

\* Passwort :

\* Passwort wiederholen :

Jetzt kann das Zertifikat angefordert werden. Alle Zertifikatsdaten werden nochmals angezeigt. Sind eventuell Fehler vorhanden, können die vorherigen Menüs in der Menüzeile oben nochmals angewählt und die Daten können angepasst werden. Andernfalls ist im Falle einer Schlüsselgenerierung durch SwissSign im Passwortfeld ein sicherer Schlüssel für den Transfer des Passwortes einzugeben. Anschliessend ist die Schaltfläche «Zertifikat anfordern» anzuwählen.

Im Falle von Gold Zertifikaten, werden die Benutzer gebeten, ein Antragsformular auszu-drucken und unterzeichnen zu lassen. Hierin sind die Organisation und die Domänenzugehörigkeit zu bestätigen.

**Hinweis:** Es sind für die von SwissSign generierten Schlüssel sichere Passwörter zu verwenden. Unsichere Passwörter (z. B. zu geringe Länge) müssen explizit bestätigt werden. Passwörter sind gehörig aufzubewahren und dürfen nicht verloren gehen. SwissSign kennt diese Passwörter nicht und kann diese im Falle eines Verlustes auch nicht wiederherstellen. Das Zertifikat und die damit verschlüsselten Daten sind dann verloren.

### 5.3 Weitere Zertifikatstypen: z. B. Code Signing Zertifikat

**1-Jahr Code Signing Zertifikat** EN DE MA

› Lizenz › AGB › CSR **Attribute** › Kontakt › Einreichen

**Attribute**

E-Mail :

Organisationseinheit :

\* Organisation :   
Einschliesslich Rechtsform, wie amtlich registriert.  
Beispiel: Unternehmen AG, Company Inc.

Ortschaft :

Kanton/Bundesland :

\* Land :

Zurück Weiter

Das Ausfüllen erfolgt analog zu den obigen Beispielen. Beim Code Signing Zertifikat muss mindestens die Organisationsbezeichnung und das Land angegeben werden.

## 5.4 Organisationszertifikat für HSM

Im Falle eines Organisationszertifikat es für eine HSM müssen Sie verpflichtend einen CSR eingeben.

**1-Jahr Organisation Platinum Zertifikat für HSM**

› Lizenz › AGB **CSR** › Einreichen

**CSR**

Fügen Sie Ihre pkcs#10 Zertifikatsregistrierungsanforderung (CSR) ein.

\* PKCS#10 :

Zurück Weiter

Die weiteren Schritte laufen dann analog wie oben.

## 5.5 Organisationszertifikat (auf Smartcard mit USB Leser)

Im Falle eines Organisationszertifikates auf Smartcard mit USB Leser verbleiben Sie auf der Plattform swissign.com und füllen direkt alle Zertifikatsdetails aus:

**NOTICE**  
Das Formular wird nicht per eMail verschickt werden (Admin mode ist 'on')

Art des Zertifikats 1-Jahr Organisationszertifikat  
 Laufzeit 1 Jahr(e)  
 Lesegerät Mit USB Reader

Füllen Sie bitte die folgenden Felder aus und drücken Sie danach auf "Weiter".

Die mit einem \* bezeichneten Felder müssen zwingend ausgefüllt werden.

Die Angaben, die im Zertifikat eingetragen und von uns geprüft werden, sind gelb hinterlegt.

Beachten Sie vor allem bei den Feldern Vorname und Nachname die Hilfestellungen indem Sie mit der Maus über das blaue Informationszeichen fahren.

**Antragsdaten**

Anrede\*

Vorname\*

Nachnamen\*

Name der Organisation\*

Details zur Organisation, Teil 1

Details zur Organisation, Teil 2

Land\*

Standortkanton\*

Ort\*

E-Mail Adresse\*

E-Mail Adresse bestätigen\*

Third Party Services  Ja

Nachdem Sie den Lizenzlink angeklickt haben werden Sie auf folgende Formularseite umgeleitet. Sie müssen hier Ihre Anrede, Vorname, Name, Namen der Organisation (bitte selbe Schreibweise und Organisationsform wie im Handelsregister nutzen), das Land (Hauptsitz der Organisation), Kanton/Provinz und Ort eingeben.

Bitte geben Sie auch eine E-Mail-Adresse ein. Bitte beachten Sie, dass diese E-Mail-Adresse auch für Benachrichtigungen über das Zertifikat verwendet wird und nicht die im Konto unter swissign.net angegebene E-Mail-Adresse. Diese wird nicht genutzt. Alle gelb unterlegten Eingabefelder werden auch als Inhalt für das Zertifikat später genutzt.

Falls Sie einen Signaturservice als Dritter für eine Organisation erbringen, markieren Sie bitte das Feld »Third Party Services«.

**Lieferadresse (privat oder geschäftlich)**

Firma

Vorname\*

Nachname\*

Adresse 1\*

Adresse 2

PLZ und Ort\*

Land

Telefonnummer\*

Korrespondenzsprache

**Alternative Kundeninformation**  
(Falls zusätzlich zu Ihnen noch eine weitere Person über den Antragsverlauf informiert werden soll)

Alternativer Kontakt

Die Lieferadresse wird für die Kommunikation genutzt. Sie kann von der obigen Adresse abweichen, sofern Sie z. B. Drittanbieter eines Signaturservices sind.

## 5.6 Eingabe und Überprüfung eines CSR

Bei Verwendung eines CSRs werden die CSR Eingaben automatisch geprüft gegen die Regeln von SwissSign, die Lizenz/Produkttypbedingungen und die Vorschriften der CP/CPS.

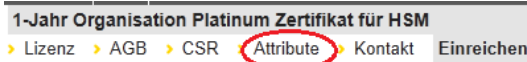


Falls der CSR gegen diese Regeln verstösst, werden Änderungsvorschläge für diesen CSR angezeigt. Diese müssen akzeptiert werden. Es ist zu beachten, dass die Zertifikatsausstellung nur auf den geänderten Zertifikatsdetails beruhen kann und letztendlich nach den Attributen geschieht, die auf der letzten Seite bei der Zertifikatsanforderung angezeigt werden.

Bitte wählen Sie «Zur Kenntnis genommen» und klicken Sie dann auf »Weiter«.



Häufig ergibt sich bei der CSR Eingabe auch das Problem, dass Sonderzeichen nicht richtig dargestellt werden.



Sofern das der Fall ist, wählen Sie in der oberen Menüleiste den Menüpunkt «Attribute».



Sie können nun den Sonderzeichenfehler verbessern/editieren.

1-Jahr Organisation Platinum Zertifikat für HSM

Lizenz > AGB > CSR > Attribute > Kontakt Einreichen

**Einreichen**

Lizenz  
Lizenzcode: 4A102BAE4B450250\_NrNCruk

AGB  
AGB: platinum 2.0 2014-12-29 14:32:11

CSR  
PKCS#10: MIIC4TCCAckCAQAwZax...  
Übersprungene Attribute: Zur Kenntnis genommen

Attribute  
E-Mail: hans.mustermann@abc.com  
Organisationseinheit: defaultValue  
Organisation: ABC AG  
Ortschaft: Zürich  
Kanton/Bundesland: Zürich  
Land: Schweiz - CH

Kontakt  
E-Mail-Adresse: [hans.mustermann@swissign.ch](mailto:hans.mustermann@swissign.ch) (Konto)  
Telefonnummer(n):  
Bevorzugte Sprache: Deutsch (Konto)

Zertifikatsangaben

Subjekt DN	CN	ABC AG
	emailAddress	hans.mustermann@abc.com
	OU	defaultValue
	O	ABC AG
	L	Zürich
	ST	Zürich
	C	CH
Alternativer Name des Subjekts	email	hans.mustermann@abc.com

Zurück Zertifikat anfordern

Die Seite unter «Einreichen» zeigt nun die endgültigen Zertifikatswerte an, die in den Zertifikatsantrag fließen werden.

## 5.7 Zurückziehen von Zertifikatsanträgen

Zertifikatsanträge, die z. B. versehentlich gestellt wurden, können – solange sie nicht genehmigt wurden – zurückgezogen werden. Die Lizenz bleibt dann erhalten. Hierfür ist der Antrag zunächst einmal zu suchen oder alternativ ist die bereits verbrauchte Lizenz nochmals einzugeben, um zu der Suche weitergeleitet zu werden.

### Zertifikate

- > Neu
- > Suchen / Verwalten

Im Hauptmenü wird der Menüpunkt «Suchen/Verwalten» angewählt.

Suchen / Verwalten

Suchen > Spalten

Suchen

Text suchen:

Lizenz:

Konto:  <beliebig>  Ingolfrauh

Gültig von:  Zeitspanne Beispiel: 2010-01, 2010-05

Läuft ab:  Zeitspanne Beispiel: 2010-01, 2010-05

Status:  pending  approved  rejected  cancelled  valid  revoked  expired

Öffentliche Zertifikate:  Ausblenden  Einblenden

Seitengröße:  10

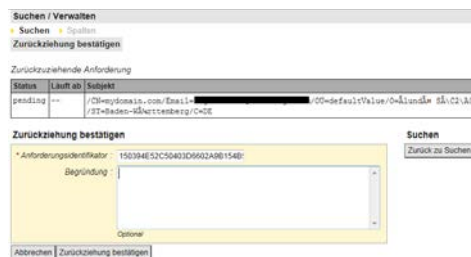
Suchen

Gibt man im Suchfeld keine weiteren Suchkriterien an, so werden alle eigenen beantragten Zertifikate angezeigt. Sie können aber im Lizenzfeld auch den Lizenzcode eingeben.

Attribute	Zurückziehen	pending	--	/CN= /OU= -1723
-----------	--------------	---------	----	-----------------------

Nun kann man das Zertifikat heraussuchen und den Schaltknopf «Zurückziehen» drücken.





Im nachfolgenden Fenster müssen die Gründe für eine Zurückziehung eingegeben werden (als Freitext).

Danach ist die Zurückziehung zu bestätigen.

✓ Anforderung 150394E52C50403D6602A9B154B578 zurückgezogen

Sie erhalten daraufhin eine Bestätigung (auch per E-Mail).

## 5.8 Genehmigungs-Prozess

Die Zertifikatsanträge werden anschliessend vom RA-Operator der SwissSign genehmigt. Die Voraussetzungen für das Genehmigungsverfahren sind weiter unten beschrieben.

## 5.9 Erneuerungs-Prozess

Sobald ein Zertifikat abläuft, muss dieses erneuert werden. Hierzu ist ein neuer Zertifikatsantrag nach oben beschriebenen Ablauf zu stellen. Es gibt (noch) keine Erneuerungsfunktion, die die Werte bereits ausgestellter Zertifikate übernimmt für die Beantragung des neuen Zertifikates. Es empfiehlt sich das neue Zertifikat bereits 2-3 Wochen zuvor auszustellen und mit dem auslaufenden Zertifikat parallel laufen zu lassen.

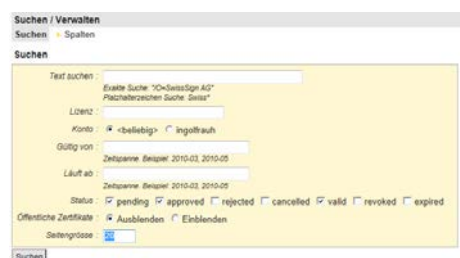
## 5.10 Ungültigkeitsprozess (Revokation)

Der Anforderer kann selber Zertifikate für ungültig erklären, sogenannte «revozieren». Hierfür loggt er sich unter seinem Login ein und sucht das entsprechende Zertifikat.

### Zertifikate

- Neu
- Suchen / Verwalten

Im Hauptmenü wird der Menüpunkt «Suchen/Verwalten» angewählt.



Gibt man im Suchfeld keine weiteren Suchkriterien an, so werden alle eigenen beantragten Zertifikate angezeigt.

<< Anfang < Zurück Weiter > >> Ende csv Export St		
Herunterladen / Attribute Für ungültig erklären	Status > >>	Läuft ab << < > >>
	valid	2015-02-03 15:05:23

Nun kann man das Zertifikat herausuchen und den Schaltknopf «Für ungültig erklären» drücken.

Ungültigkeitserklärung ist unumkehrlich

Für ungültig zu erklärendes Zertifikat

Status	Läuft ab	Subjekt	Alternativer Name
valid	2015-02-03 15:05:23	/CN=gned01.DLTTI/Email=	email=

- Sie können sich nicht mehr authentifizieren
- Sie können nicht mehr digital unterschreiben
- Dritte können keine Dokumente mehr für Sie verschlüsseln
- Entschlüsselung ist immer noch möglich

Ungültigkeitserklärung bestätigen

\* Zertifikatsidentifikator: 05B4305565A2ADC0724E494B7D

\* Begründung

- keine Angaben
- kompromittierter Schlüssel
- Subjektinformation geändert
- Ersetzt
- Ende der Benutzung
- Berechtigung entzogen

Kommentar:

Suchen  
Zurück zu Suchen

Abbrechen Ungültigkeitserklärung bestätigen

Im nachfolgenden Fenster müssen die Gründe für eine Ungültigkeitserklärung eingegeben werden:

- Keine Angaben
- Kompromittierter Schlüssel: Der private Schlüssel wurde gestohlen bzw. es besteht die Gefahr, dass er gestohlen wurde.
- Subject-Information geändert, z. B. Änderung des Firmennamens, oder Nachnamens.
- Ersetzt: Das Zertifikat wurde durch ein anderes ersetzt.
- Ende der Benutzung: Das Zertifikat wird nicht mehr weiter benötigt, z. B. Austritt eines Mitarbeitenden aus dem Unternehmen.
- Berechtigung entzogen, z. B. aufgrund von nicht bezahlten Zertifikatslizenzen.

Optional kann auch ein Kommentar abgegeben werden.

**Hinweis:** Eine abgegebene Ungültigkeitserklärung kann nicht mehr revidiert werden. Das Zertifikat wird als ungültig markiert in allen Listen (CRL) oder Diensten (OCSP), die bei einer Zertifikatsgültigkeitsanfrage herangezogen werden.

## 6. Management von Zertifikaten

### 6.1 Wahl der Rechte

Je nach gewählter Benutzerrolle können Zertifikate verwaltet werden. Auch ein Benutzer ohne Login hat z. B. Möglichkeiten, öffentliche Zertifikate zu suchen. Die folgende Übersicht zeigt die Möglichkeiten:

#### Rechte

Ohne Login

#### Möglichkeiten

- Suche öffentlicher Zertifikate
- Anzeige der Ergebnisse
- Zertifikatsattribute anzeigen
- Herunterladen bestimmter Zertifikate

Login als Benutzer, der kein Administrator ist

- Suche von Zertifikaten
- Anzeige der Ergebnisse
- Zertifikatsattribute anzeigen
- Herunterladen bestimmter Zertifikate, sofern er Anforderer-Rolle hat.
- Änderung von Attributen eigener Zertifikate
- Herunterladen der für einen selbst generierten Schlüssel mit Passwort

### 6.2 Suche von Zertifikaten



Im Hauptmenü wird unter dem Label «Zertifikate» der Menüpunkt «Suchen/Verwalten» gewählt.

In dem Arbeitsbereich kann jetzt nach einem Lizenzschlüssel oder alternativ nach einem Text gesucht werden, der ein Zertifikat enthält. Das Platzhalterzeichen «\*» kann verwendet werden. Der Suchstring sollte immer Anführungszeichen als erstes und letztes Zeichen haben.

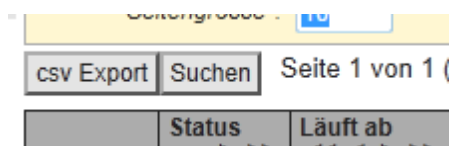
Je nach Rolle können auch mehr Suchattribute zur Verfügung gestellt werden, z. B. der Status der Zertifikate oder Zertifikatsanträge (z. B. «pending»).

Die Anzahl der Ergebnisse ist auf die unter «Seitengrösse» eingestellte Anzahl von Zertifikaten begrenzt. Die Anzahl kann angepasst werden.

Ohne Eingabe von Suchkriterien werden die eigenen Zertifikate angezeigt.

## Hinweise:

- Die Anpassung der Anzahl der Ergebnisse (Seitengrösse) auf grosse Zahlenwerte kann zu langen Abfragezeiten führen. Will man die Ergebnisse später exportieren (z. B. in Excel), werden immer nur die angezeigten Ergebnisse exportiert. Gegebenenfalls empfiehlt es sich dann, die Anzahl der an-gezeigten Ergebnisse so hochzusetzen, dass alle Ergebnisdatensätze angezeigt werden. Diese können dann alle in Excel exportiert werden.
- Die Suche nach öffentlichen Zertifikaten ist immer auf die Anzeige von 20 Zertifikaten beschränkt und kann nur mit einem Filter (z. B. Texteingabe) durchgeführt werden.



Ausgegebene Datensätze können unter «csv Export » exportiert werden und z. B. nach Excel importiert werden.

## 6.3 Anzeige der Ergebnisse

Die Anzeige einzelner Attribute zu einem Zertifikat kann bequem gesteuert und festgelegt werden:



Sofern Sie nicht bereits im «Suchen/Verwalten» Menü sind, wählen Sie dieses im Hauptmenü unter «Zertifikate», Menüpunkt «Suchen/Verwalten».

In der Menüleiste oben wählen Sie den Menü Tab «Spalten».

Suchen / Verwalten

Suchen Spalten

Spalten

Gültig von	> >>	Einblenden
Status	<< < > >>	Ausblenden
Läuft ab	<< < > >>	Ausblenden
Subjekt	<< < > >>	Ausblenden
Alternativer Name	<< < > >>	Ausblenden
Zertifikatsidentifikator	<< < > >>	Einblenden
Anforderungsidentifikator	<< < > >>	Einblenden
Schlüsselidentifikator	<< < > >>	Einblenden

Sie sehen nun eine Tabelle von Attributen jeweils rechts versehen mit einer Schaltfläche «Einblenden» oder «Ausblenden».

Diejenigen Attribute, die derzeit in der Ergebnistabelle der Suche angezeigt werden, sind grau hinterlegt und markiert. Die anderen möglichen Attributwerte sind weiss hinterlegt und nicht markiert.

Suchen / Verwalten

Suchen Spalten

Spalten

Gültig von	> >>	Einblenden
Status	<< < > >>	Ausblenden
Läuft ab	<< < > >>	Ausblenden
Subjekt	<< < > >>	Ausblenden
Alternativer Name	<< < > >>	Ausblenden
Zertifikatsidentifikator	<< < > >>	Einblenden

Attributspalten in der Ergebnisliste können nun durch die Betätigung des Schalters «Einblenden» oder «Ausblenden» ein- bzw. ausgeschaltet werden.

Suchen / Verwalten

Suchen Spalten

Spalten

Gültig von	> >>	Einblenden
Status	<< < > >>	Ausblenden
Läuft ab	<< < > >>	Ausblenden
Subjekt	<< < > >>	Ausblenden
Alternativer Name	<< < > >>	Ausblenden
Zertifikatsidentifikator	<< < > >>	Einblenden
Anforderungsidentifikator	<< < > >>	Einblenden
Schlüsselidentifikator	<< < > >>	Einblenden

Über die Pfeiltasten «<<» oder «>>» können Spalten in der Ergebnistabelle um eine Position nach links oder rechts verrückt werden, analog auch in der Attributs List oben.

Mit den Doppelpfeiltasten «<<<» bzw. «>>>» kann gezielt eine Spalte an das linke oder rechte Ende der Tabelle bewegt werden.

**Hinweis:** Alle Zertifikate mit Abrufbarkeit «Public Download» können von beliebigen Benutzern (auch ohne Konto) angezeigt und ohne privaten Schlüssel heruntergeladen werden. Andere Zertifikate sind für unberechtigte Benutzer nicht sichtbar.

## 6.4 Attribute/Abrufbarkeit anzeigen/ändern, Download, Übertragung von Zertifikaten

Seite 1 von 1 (Datei)

csv Export Suchen

	Status	Läuft ab
	> >>	<< <
Zurückziehen	pending	--
Attribute		
Zurückziehen	pending	--
Attribute		
Zurückziehen	pending	--
Attribute		

Man kann im Nachhinein einige Attribute, die mit dem Zertifikat verknüpft sind, ändern. Hierfür ist in der Ergebnisliste zunächst die Schaltfläche «Attribute» anzuwählen.

**Attribute**

\* Anforderungsidentifikator : B148E07424F071B804B59B807EB

Abrufbarkeit :

Konto :  swissign.ag  Requestor\_ce1  CE  testIngolf  <none>

Alt. E-Mail :

Alt. Sprache :  English  Deutsch  <account>

Alt. Telefonnummer :

**Änderungsnachweis**

Geändert am	Status	Konto	Abrufbarkeit	Geändert von
2014-01-24 17:22:05	Pending	Requestor_ce1	private	/CN=Requestor: TNT RA0, TNT01F, RA0

Anschliessend können im Arbeitsbereich unter «Attribute » Einstellungen vorgenommen werden:

- Die E-Mail für die Notifikation 10 oder 30 Tage vor dem Zertifikatsablauf kann für dieses Zertifikat unter «Alt. E-Mail » angepasst werden, auch die dazugehörige Sprache unter «Alt. Sprache » (Alternative Sprache).
- Die Abrufbarkeit des Zertifikates auf dem swissign.net Zertifikatsverzeichnis kann über eine Auswahlliste geändert werden.

Sind mehrere Konten vorhanden, so kann das Zertifikat auch einem anderen Konto hierüber zugeordnet werden. Die entsprechende Checkbox für das Konto ist dann anzuwählen.

Abrufbarkeit :

Konto :

Alt. E-Mail :

Konto: cornelia.enke@tech.swissign.com

Die Abrufbarkeit kann auf drei Werte angepasst werden:

- Privat
- Öffentlich prüfbar
- Öffentlich zugänglich

Im Falle von «privat» wird auf swissign.net Ihr Zertifikat nicht für aussenstehende Benutzer angezeigt. Im Falle von «öffentlich prüfbar» kann Ihr Zertifikat nur für andere auf Gültigkeit geprüft werden. Bei «öffentlich zugänglich» sind alle Details Ihres Zertifikats für jedermann im Falle über die Suche sichtbar.

Alt. E-Mail :

Profil:

Alt. Sprache :  Eng

Profil:

Alt. Telefonnummer :

Änderungsnachweis

Alle Änderungen sind mit der Betätigung der Schaltfläche «Ändern» abzuschliessen.

## 6.5 Antragsformular / Registrierungsformular nochmals erzeugen

Sofern Sie ein Zertifikat der Stufe Gold beantragt haben, wurde als letzter Schritt das Download des Antragsformulars und Ausdruck angeboten. Sollte dieses verloren gegangen sein,

kann über die oben beschriebene Suche der Zertifikatsantrag nochmals gesucht werden und das Antragsformular nochmals aufgerufen werden.

	Status	Läuft ab
Zurückziehen <b>Attribute</b>	pending	--
Zurückziehen Attribute	pending	--
Zurückziehen Attribute	pending	--

Suchen Sie Ihren Zertifikatsantrag wie oben beschrieben und betätigen dann den Attribute Knopf.

### Genehmigung

Registrierungsdokument : [gold\\_multi\\_ucc\\_new](#)

Im Falle eines Gold Zertifikates wird Ihnen der Link zum Download des Antragsformulars nochmals angeboten:

## 6.6 Neues Zusenden der E-Mail zum Eigentumsnachweis

Im Falle von Silver SSL oder Personal Silver ID Zertifikaten wird Ihnen mit dem Zertifikatsantrag eine E-Mail zum Eigentumsnachweis an die bezeichnete E-Mail-Adresse zugesendet. Damit wird überprüft, ob Sie Eigentümer der genannten E-Mail-Adresse sind und Zugriff darauf haben.

Sollte diese E-Mail nicht angekommen sein (z. B. weil Sie die E-Mail erst aufgesetzt haben nachdem der Zertifikatsantrag versendet wurde), kann es notwendig sein, diese E-Mail nochmals neu zu versenden.

	Status	Läuft ab
Zurückziehen <b>Attribute</b>	pending	--
Zurückziehen Attribute	pending	--
Zurückziehen Attribute	pending	--

Suchen Sie Ihren Zertifikatsantrag wie oben beschrieben und betätigen dann den Attribute Knopf. Sie sehen den Bereich «Genehmigung».

### Genehmigung

- \* E-Mail :
- admin@swissign.com
  - administrator@swissign.com
  - hostmaster@swissign.com
  - postmaster@swissign.com
  - webmaster@swissign.com

E-Mail zum Eigentumsnachweis senden

Im Falle eines SSL Zertifikates können Sie nun nochmals die E-Mail-Adresse auswählen und neu zusenden lassen.

## Genehmigung

E-Mail : [ingolf.rauh@swissign.com](mailto:ingolf.rauh@swissign.com)

E-Mail zum Eigentumsnachweis senden

Im Falle eines Personal ID Zertifikates besteht nur die Möglichkeit die E-Mail nochmals an die im Zertifikat bezeichnete E-Mail-Adresse zu versenden.

### 6.7 Eigentumsnachweis durchführen

Im Falle von Silver SSL oder Personal Silver ID Zertifikaten haben Sie ein E-Mail erhalten mit einem Link mit dem Sie den Eigentumsnachweis der bezeichneten Domäne oder E-Mail-Adresse durchführen können.

Von:  ca@signdemo.com  
An:  [REDACTED]@PS  
Cc:  
Betreff: Neue SwissSign Silver Zertifikat Anforderung 13450AEA[REDACTED]C39  
Signiert von: ca@signdemo.com

Gesendet: Mo 29.12.2014

Sehr geehrte Kundin  
Sehr geehrter Kunde

Folgende Zertifikatsanforderung wurde soeben bei SwissSign eingereicht:  
/CN=Email: [ingolf.rauh@swissign.com](mailto:ingolf.rauh@swissign.com) OU=Email Validated Only (email:ingolf.rauh@swissign.com)

Als rechtmässiger Inhaber der E-Mail Adresse [ingolf.rauh@swissign.com](mailto:ingolf.rauh@swissign.com) können Sie diese Anforderung selbst genehmigen. Um die Anforderung jetzt zu genehmigen, öffnen Sie bitte folgenden Link in Ihrem Browser:

[https://swiss.signdemo.com/cgi-bin/request/approve?auth=65647A1BF5466D32E8F0\[REDACTED\]5&id=13450AEA1\[REDACTED\]ED](https://swiss.signdemo.com/cgi-bin/request/approve?auth=65647A1BF5466D32E8F0[REDACTED]5&id=13450AEA1[REDACTED]ED)

Um die Zertifikatsanforderung zu annullieren, verwenden Sie folgenden Link:

Sie haben in dem E-Mail 2 Links:

- Einen Link zum Zurückziehen des Zertifikatsantrages (die Lizenz ist dann wieder frei für einen neuen Zertifikatsantrag)
- Einen Link für die Autorisierung des Zugriffs auf die bezeichnete (E-Mail-)Domäne:





The screenshot shows the SwissSign user interface. At the top, there is a navigation bar with links for 'Startseite', 'Support', 'Vertrauen', 'swissign.com', and language options 'DE' and 'EN'. Below this is the SwissSign logo and a decorative banner with keys and the text 'S E CHF'. The main content area is divided into two columns. The left column contains a sidebar menu with options like 'Zertifikate', 'Konto', and 'Swiss Sign CA'. The right column is titled 'Zertifikatsanforderung genehmigen' and contains the text: 'Sie sind dabei, die folgende Zertifikatsanforderung zu genehmigen:'. Below this is a table with columns for 'Status', 'Seriennummer', and 'Subjekt DN (Alternativer Name des Subjekts)'. The table shows a pending request with a status of 'Pending since Mon Dec 29 15:11:42 2014', a serial number '13450AEA...', and a subject DN containing an email address. Below the table, there is a question 'Wollen Sie diese Zertifikatsanforderung jetzt genehmigen?' with 'Ja' and 'Nein' buttons.

Die Zertifikatsanforderung müssen Sie durch Klicken auf «Ja» genehmigen. Sie erhalten dann eine E-Mail mit dem Downloadlink zum Zertifikat.

## 7. Freigabe des Zertifikatsantrages – Einreichen des Formulars

Silver SSL oder Personal Silver ID Zertifikate werden normalerweise sofort nach Bestätigung des Zugriffs auf die im Zertifikat genannte Domäne ausgestellt. Im Fall von Gold, Gold EV und Organisationszertifikatsanträgen bietet die Plattform den Download eines PDF oder https Formulars zum Ausdruck an, welches dann entsprechend unterschrieben werden muss. Das Dokument ist bereits mit den zuvor eingegebenen Zertifikatsdetails ausgefüllt.

Folgende Information muss noch eingetragen werden:

- Autorisierung des Zertifikatsanforderer : hier füllen Sie den Namen, das Unterschriftsdatum und den Unterschriftsort desjenigen aus, der zuvor auch die Daten für den Zertifikatsantrag auf der Plattform eingegeben hat. Dieser hat dann hier auch zu unterschreiben.
- Autorisierung der Organisation (damit des Antragstellers): hier füllen Sie den Namen, das Unterschriftsdatum und den Unterschriftsort derjenigen Verantwortlichen oder desjenigen Verantwortlichen der Organisation aus, die auch im Handelsregister oder ähnlichen Organisationsdokumenten eingetragen sind. Diese Person(en) müssen dann hier auch unterzeichnen. Sofern eine Unterschrift zu zweien zwingend im Organisationsdokument vorgeschrieben ist, müssen hier auch zwei Organisationsverantwortliche unterschreiben.
- Autorisierung der Domäne (Domänenvollmacht): Falls das Zertifikat einen Domänennamen erwähnt, so hat der Eigentümer der Domäne hier zu unterzeichnen. Bitte füllen Sie den Namen, Unterschriftsdatum und Unterschriftsort des Eigentümers aus, auch wenn dieser gleichlautend wie der Verantwortliche der Organisation ist. Bitte lassen Sie auch

in diesem Fall hier unterzeichnen. Ansonsten kann der Domäneneigentümer über die Datenbank [whois.com](http://whois.com) oder [gwhois.org](http://gwhois.org) zum Beispiel ermittelt werden. Es sollte darauf geachtet werden, dass der Domänenunterzeichner in diesen Verzeichnissen auch gelistet ist.

Sofern die Organisation im Handelsregister aufgeführt ist, muss ein Handelsregisterauszug nicht mehr länger beigefügt werden. Falls die Organisation nicht im Handelsregister aufgeführt ist, sollte die Existenz Organisation anderweitig nachgewiesen werden. Bitte kontaktieren Sie hierfür im Zweifelsfalle das Helpdesk. Auf jeden Fall hilfreich sind Dokumente wie diese:

- Eine Kopie des Briefes der Offiziellen Steuerbehörde, welches den Eintrag der Umsatzsteuer-ID nachweist.
- Ein offizielles Register, was Ihre Organisation aufführt.
- Ein Bestätigungsschreiben der übergeordneten Verwaltungseinheit bei staatlichen Stellen und Verwaltungen.

Im Falle von EV Zertifikaten muss SwissSign die Organisation in einem öffentlichen Telefonbuch oder Branchenverzeichnis mit Adresse auffinden können, um die Adresse zu verifizieren. Falls die Firma noch nicht länger als 3 Jahre existiert, benötigen wir auch ein Bestätigungsschreiben der Bank über die Geschäftstätigkeit.

Von allen Unterzeichnern muss eine Kopie des Passes oder einer ID Karte beigefügt werden, die neben den Personendaten auch das Lichtbild und die Unterschrift deutlich zeigt.

Anträge müssen an folgende Adresse postalisch eingereicht werden:

SwissSign AG  
Fulfillment Center  
Sternmatt 6  
Postfach 2259  
CH 6010 KRIENS 2

Falls Sie die Unterlagen mit Kurierdienst versenden wollen ist folgende zusätzliche Adressbezeichnung notwendig:

Swiss Post Solutions AG  
SwissSign  
4. Obergeschoss  
Sternmatt 6  
Postfach 2259 / 6010 Kriens 2  
CH-6010 Kriens

Sie können vorab bei eiligen Anträgen auch die Unterlagen zusätzlich elektronisch an [registration@swissign.com](mailto:registration@swissign.com) richten. Sollte nicht binnen 10 Tagen danach die gleichen Unterlagen postalisch eingegangen sein, wird ein eventuell aufgrund der elektronischen Zusendung ausgestellt Zertifikat wieder revoziert.

## 8. Vollmacht en

Gerade bei der Bestellung von vielen Zertifikaten bietet sich die Nutzung einer Vollmacht an, damit nicht immer alle Verantwortlichen jeden Zertifikatsantrag unterschreiben müssen.

Ein grundsätzliches Vollmachtsdokument dafür finden Sie in diesem Bereich; [www.swissign.com/de/support/bestell-und-antragsprozess](http://www.swissign.com/de/support/bestell-und-antragsprozess). Das Dokument selber lautet Kundenvertrag mit Vollmachten für Zertifikate Stufe Gold mit Organisationseintrag.

Sie können innerhalb des Dokumentes ankreuzen worauf sich die Vollmacht bezieht, z. B. nur auf die Domäne oder auf Domäne und Organisation.

Bitte geben Sie einen Hinweis auf dem Antragsformular, sofern eine Vollmacht bereits bei SwissSign vorliegen sollte. Am besten fügen Sie immer eine Kopie dieser Vollmacht ihren Anträgen bei.

## 9. Herunterladen des ausgestellten Zertifikates

Sofern das Zertifikat genehmigt wurde, werden Sie eine E-Mail erhalten, die Ihnen den Downloadlink Ihres Zertifikates anbietet. Durch Klick auf diesen Link werden Sie auf eine Seite bei swissign.net geleitet, wo sie ihr Zertifikat herunterladen können:

Suchen / Verwalten

[Suchen](#) > [Spalten](#)  
[Herunterladen / Attribute](#)

*Das Authentisierungscookie ist nicht mehr gültig*

**Zertifikat**

Alternativer Name	Zertifikatsidentifikator	Läuft ab
email: [redacted]	EC2FD [redacted] FA32E534	2015-12-29 16:31:19

**Zertifikat und privaten Schlüssel herunterladen (.p12, PKCS#12)**

\* Anzeigename :

\* Schlüsselpasswort :

\* Herunterladenscode : 9EC78B [redacted] 41EDD41B5261 [redacted]

**Details**

Version	v3
Seriennummer	00:ec: [redacted] 85:71:10:2c:ed:fa:32:e5:34

Standardmässig wird der Download im p12 Dateiformat angeboten, sofern der Schlüssel bei SwissSign generiert wurde. Andere Formate können heruntergeladen werden, falls Sie ihr Zertifikat nochmals suchen und die Downloadaktion aktivieren. Sie können herunterladen:

## Download certificate (without private key)

Format :  .cer  
 .crt  
 .pem  
 .p7c (certificate chain)  
 .pem (certificate chain)

Download

Das cer , crt oder pem Format, welche alle keinen privaten Schlüssel beinhalten oder das p7c bzw. pem Format, welches nicht nur das beantragte Zertifikat, sondern die komplette Zertifikatskette beinhaltet. Damit erhalten Sie auch das Issuing Zertifikat (herausgebende Zertifikat oder Zwischenzertifikat ) und das Root Zertifikat (Wurzelzertifikat ) von SwissSign.

Sofern Sie einen zertifikatsbasierten Zugang auf ihrem Webserver einrichten, ist es notwendig auch das herausgebende Zertifikat und das Wurzelzertifikat zu installieren, da sonst die Browser das Zertifikat nicht als vertrauenswürdig anzeigen.

Sollte der private Schlüssel von SwissSign erzeugt worden sein, so müssen die darauf basierten SSL Zertifikatsdateien (p12) zeitnah heruntergeladen werden, da diese von SwissSign nach kurzer Zeit (3 Monate spätestens) gelöscht werden. Persönliche Zertifikate (Personal ID) sind davon nicht betroffen.

## 10. E-Mail-Benachrichtigungen

### 10.1 E-Mail-Verkehr bei Zertifikatsanforderung durch Requester

Das System erzeugt zu bestimmten Ereignissen E-Mails, die an bestimmte Personen versendet werden. Mit der Anforderung des Zertifikates hat man festgelegt, wer der Empfänger der E-Mail eines Zertifikates ist:

- Das Zertifikat wurde unter einem bestimmten Konto angefordert: Die E-Mail, die diesem Konto zugeordnet ist, wird für alle Benachrichtigungen bezüglich dieses Zertifikates genutzt.
- Das Zertifikat wurde ohne Konto angefordert: Es wurde während der Anforderung die Kontaktdaten und damit auch die E-Mail-Adresse für Benachrichtigungen über dieses Zertifikat festgelegt.

Von diesen Regeln ausgenommen sind sogenannte «Proof of Possession» E-Mails – also E-Mails, die überprüfen, ob der Benutzer Zugriff und Kontrolle über eine bestimmte E-Mail-Adresse hat. Das geschieht bei Zertifikaten der Stufe Silver, die nicht im Rahmen einer Managed PKI freigeschaltet wurden, sondern deren Lizenz im Webshop gekauft wurde. Bei einem Personal Silver ID Zertifikat wird direkt diejenige E-Mail-Adresse adressiert, die im Zertifikat aufgenommen werden soll. Bei einem Silver SSL Zertifikat wird die bei Antragstellung angegebene E-Mail-Adresse adressiert.

**Hinweis:** Auch bei einer Anforderung aus einem Konto heraus, in dem man eingeloggt ist, kann man die Kontaktdaten, die mit dieser Anforderung verknüpft sind, explizit ändern. Das ist weiter oben beschrieben. Siehe Kapitel 4.1

**Achtung:** Zu unterscheiden sind die Benachrichtigungs-E-Mail von den E-Mails, die zur Verifikation einer E-Mail oder Domäne z. B. an die E-Mail-Adresse des Zertifikatinhabers versendet werden. Hierbei wird abweichend von allen Kontoeinstellungen oder Kontakteinstellungen immer die E-Mail-Adresse des Zertifikates genommen, bzw. der Administrator einer Domäne angeschrieben, falls es sich um ein SSL Zertifikat handelt. Es ist unbedingt darauf zu achten, dass diese E-Mail-Adresse bereits existent ist, wenn das Zertifikat beantragt wird.

Alle E-Mail-Nachrichten unterscheiden sich nach Zertifikatstyp.

Typischerweise gibt es folgende Ereignisse, die E-Mails auslösen. Alle E-Mails werden auch zusätzlich an den Administrator versendet.

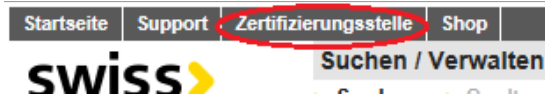
- Anforderung eines Zertifikates: Der Empfänger gemäss Kontoeinstellung oder Kontakteinstellung zum Zertifikat bekommt eine Bestätigungs-E-Mail. Er hat die Möglichkeit bei einem Webshop-Bezug des Zertifikates ggfs. ein notwendiges Antragsdokument herunterzuladen, welches ihm per Link angeboten wird. Er hat zusätzlich die Möglichkeit, die Anforderung wieder zurückzuziehen.
- Nach Genehmigung oder Zurückweisung des Zertifikates durch die Registrierungsstelle: Der Empfänger erhält an dieselbe Adresse wie bei der Anforderung eines Zertifikates ein E-Mail zugesendet. Ein Link in der E-Mail verweist direkt auf die Downloadseite des Zertifikates.
- 30 Tage vor Ablauf eines Zertifikates: 30 Tage vor Ablauf eines Zertifikates erhält der Empfänger an dieselbe Adresse wie bei der Anforderung eines Zertifikates eine E-Mail zugesendet, die ihn auf den Ablauf des Zertifikates hinweist.
- 10 Tage vor Ablauf eines Zertifikates: 10 Tage vor Ablauf eines Zertifikates wird der Benutzer erneut auf den Ablauf hingewiesen.
- Ungültigkeitserklärung: Bei einer Revozierung (Ungültigkeitserklärung) eines Zertifikates wird ebenfalls eine E-Mail ausgelöst, auch wenn der Benutzer selber diese Ungültigkeitserklärung durchgeführt hat.
- Zurückziehung eines Antrages: Wurde ein Zertifikatsantrag zurückgezogen, wird dieser Vorgang mit einer E-Mail bestätigt.

**Hinweis:** Hat sich die E-Mail-Adresse geändert und möchte man diese dem bereits ausgegebenen Zertifikat zuordnen, so ist das über eine Attributs-Änderung zum Zertifikat möglich. Siehe Kapitel 5.5.

## 11. Root und Zwischen-Zertifikate importieren

Root Zertifikate (Wurzelzertifikate) von SwissSign sind in allen wesentlichen Browsern und Betriebssystemen enthalten. Dennoch müssen diese insbesondere bei der Installation von SSL Zertifikaten bei Webservern oder Appliances händisch installiert werden. Am einfachsten ist es über den in Kapitel 8 beschriebenen Weg «Zertifikatskette herunterladen».

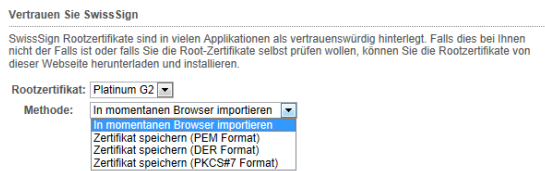
Möglich ist es aber auch über den direkten Link zu allen Root Zertifikaten von SwissSign:



Wählen Sie im Menü am oberen linken Bildschirmrand den Menüpunkt «Zertifizierungsstelle»



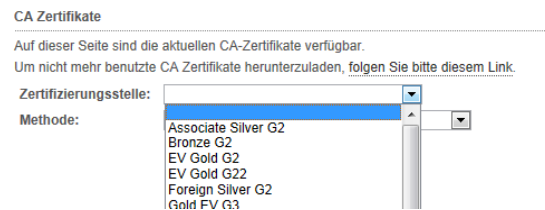
Ein neues Fenster öffnet sich und Sie erhalten links ein Hauptmenü angeboten. Zunächst können Sie die «Root Zertifikate importieren» anwählen.



Das entsprechende Root Zertifikat können Sie nun in verschiedenen Dateiformaten herunterladen oder in ihren momentanen Browser importieren.



Für die Zwischenzertifikate oder sogenannte Issuing Zertifikate wählen Sie den Menüpunkt «CA Zertifikate»



Auch hier können Sie zunächst das Zertifikat auswählen und in ihren Browser laden oder in verschiedenen Dateiformaten herunterladen.

## 12. Support Kontakt

Bei allen Fragen ist der Support über [www.swissign.com/de/support/kontaktformular](http://www.swissign.com/de/support/kontaktformular) oder [helpdesk@swissign.com](mailto:helpdesk@swissign.com) erreichbar oder kann über die Menüleiste oben angewählt werden.

## 13. Typische Probleme

Nachfolgend sind einige typische Problemstellungen und Lösungen beschrieben:

<p>Ich möchte die Schlüsselverwendung (key usage) anders belegen.</p>	<p>Abgesehen von den Zertifikatsinhalten, die in den Konfigurationsfeldern stehen (Domäne, Organisation, Ort, Kanton, Land, E-Mail, Name, Vorname, etc.) sind die restlichen Eigenschaften durch die Produktauswahl, z. B. Personal Silver ID gegeben. Diese sind im Shop beschrieben. Somit können diese Eigenschaften, worunter auch die Schlüsselverwendung fällt, nicht geändert werden. Änderungen im CSR werden ignoriert.</p>
<p>Mein SwissSign Zertifikat wird nicht als vertrauenswürdig angezeigt</p>	<p>Das passiert in der Regel immer dann, wenn bei einem SSL Zertifikat kein Zwischenzertifikat (Issuing Certificate) oder Wurzelzertifikat (Root Certificate) installiert wurde. Siehe Beschreibung oben. Achtung Adobe PDF Leser vertraut nur hardwaregebundenen Zertifikaten (SwissSign Stufe Platinum).</p>
<p>Mein Zertifikat soll öffentlich nicht auffindbar sein.</p>	<p>Gehen Sie unter Attribute und stellen die Abrufbarkeit auf «privat».</p>
<p>Mein privater Schlüssel wurde gestohlen oder ich habe ihn verloren</p>	<p>Sie sollten Ihr Zertifikat sofort revozieren. Suchen Sie das Zertifikat und betätigen den «Zurückziehen» Knopf.</p>
<p>Das Zertifikat entspricht nicht meinem Zertifikatsantrag</p>	<p>Wie weiter oben beschrieben kann es grundsätzlich eine Abweichung zwischen Ihrem CSR und dem Zertifikatsinhalt geben, da manche CSR Ausprägungen unterdrückt werden (z. B. key usage etc.). Sollte es dennoch eine nicht geklärte Abweichung geben, wenden Sie sich an den Support.</p>
<p>Mein Zertifikat läuft ab</p>	<p>Es gibt keine Verlängerungsmöglichkeit für Zertifikate. Sie müssen ein neues Zertifikat mit den gleichen Angaben beantragen.</p>
<p>Ich möchte mein Zertifikat zurückgeben</p>	<p>Grundsätzlich verbietet die AGB die Rückgabe von Zertifikaten. SwissSign nimmt aber aus Kulanz Zertifikate bis 1 Monat nach Ausstellung zurück und erstattet den Betrag. Danach werden Zertifikate nur noch gegen Gutschein für noch anteilige Restlaufzeit zurückgegeben. Sie müssen das</p>

	«retournierte» Zertifikat revozieren.
Suchfunktion zeigt fremde Zertifikate	Grundsätzlich werden bei einer generellen Suche auch fremde Zertifikate angezeigt, wie bei einem Telefonbuch auch Telefonnummern anderer Teilnehmer. Die Zertifikate dienen letztendlich zur Verschlüsselung von Kommunikationspartnern untereinander. Es werden nur Zertifikate angezeigt, die vom Besitzer in den begleitenden Eigenschaften (Attribute) des Zertifikates als «öffentlich zugänglich» markiert wurden.
Ich benötige das pfx Format	Das PFX Dateiformat ist das gleiche wie das p12 Dateiformat. Laden Sie das p12 Format herunter und benennen Sie die Datei um.
Ich muss meine Zertifikatsangaben im Nachhinein ändern.	Sofern der Antrag noch nicht genehmigt wurde, kann dieser über die Suche zurückgezogen werden. Sofern das Zertifikat bereits ausgestellt wurde, muss leider ein neues Zertifikat beantragt werden. Binnen eines Monats nach Ausstellung wird dabei der Betrag des alten Zertifikates aus Kulanz ersetzt, danach kann man einen Gutschein für die Restlaufzeit des Zertifikates erwerben.
Ich habe das E-Mail zum Eigentumsnachweis der Domäne nicht erhalten	Suchen Sie den Zertifikatsantrag und senden Sie sich über Attribute den Eigentumsnachweis nochmals neu zu wie oben beschrieben.
Ich muss mein Antragsformular nochmals ausdrucken.	Suchen Sie den Zertifikatsantrag und erzeugen Sie sich das Formular nochmals neu wie oben beschrieben.



## 14. Index

Ablauf 14  
Abmelden 11  
Abrufbarkeit 29  
AGB 4  
Allgemeine Geschäftsbedingungen 14  
Alt. E-Mail 29  
Alt. Sprache 29  
Anforderer  
Requester 27  
Anmelden 10  
anonyme Mailboxen 19  
Antragsformular 30  
Arbeitsbereich 7, 8  
Attribute 11, 14, 16, 19, 23, 28, 29  
Attributsänderung 37  
Aufklappen 14  
Ausblenden 28  
Autorisierung 33  
Berechtigung entzogen 26  
bevorzugte Sprache 11  
Bevorzugte Sprache 15  
CA Zertifikate 38  
cer 35  
Certificate Signing Request 14  
certificates.csv 13  
CodeSigning Zertifikat 20  
CP/CPS 4  
crt 35  
CSR 14, 16, 22  
Certificate Signing Request 14  
csv 13  
csv Export 28  
DE 7  
Domäne 17, 33  
Domänen 17, 18  
Domänenvollmacht 33  
Editieren 11  
Einblenden 28  
Einreichen 16  
E-Mail zum Eigentumsnachweis 31  
E-Mail-Adresse 11, 14, 15  
E-Mail-Benachrichtigungen 35  
EN 7  
Ende der Benutzung 26  
Entfernen 12  
Erneuerung 6  
Erneuerungs-Prozess 25  
Excel 13, 28  
Freigabe 5  
Für ungültig erklären 26  
Genehmigung 31  
Gruppenaccount 19  
Handelsregister 33  
Hauptmenü 7, 8  
Herunterladen 34  
issuing Zertifikat 35  
Kanton/Bundesland 15  
Kompromittierter Schlüssel 26  
Kontakt 15, 19  
Konto 9, 10, 11, 12, 14, 15, 19, 29  
LDAP 5  
Lizenz 8, 27  
Lizenzcode 14  
Login 27  
Login mit Zertifikat 9  
Löschen 11  
Menüzeile 7, 8  
Multi-Domain Zertifikat 17  
Neu 14  
OCSP 5, 26  
öffentlich 39  
Öffentlich prüfbar 30  
Öffentlich zugänglich 30  
öffentlichen Schlüssel 14  
Organisation 33  
Organisationszertifikat 21  
p12 35  
p7c 35  
Passwort 15, 18  
Passwort ändern 12  
pem 35  
Personenzertifikaten 19  
pfx 40  
PKCS#10 14  
PKI 4  
Privat 30  
Private Key Infrastructure  
PKI 4  
Profil 6  
Pseudonym 19  
Public download 29  
RA Administrator 5, 6  
Registrierungsformular 30  
Registrierungsformular 16  
Registrierungsnummer 18  
Registrierungsstaat 18  
relaying party 4  
Revokation 25  
Root Zertifikat 35  
Root Zertifikate 37

Rootzertifikate importieren 37  
Schlüsselidentifikator 12, 13  
Schlüsselverwendung 39  
Seitengrösse 27  
Shop 7  
Spalten 28  
Sprache 29  
SSL EV Gold Zertifikat 18  
SSL EV Zertifikate 33  
SSL Gold 15  
SSL Silver Zertifikat 17  
Suchen 27  
Suchen/Verwalten 6, 25, 28  
Sujektinformation geändert 26  
Support 7, 38  
Telefonnummer 11  
Text suchen 27  
Third Party Services 22  
Umlaute 16  
ungültig 25  
Ungültig erklären 5

UTF-8 16  
Verlängerungsmöglichkeit 39  
Verwalten 27  
Vollmacht 34  
Vorname  
Nachname 19  
Wechseln 11  
Wirtschaftskategorie 18  
Wurzelzertifikat 35  
Wurzelzertifikate 37  
Zertifikat anfordern 16, 20  
Zertifikatsablauf 29  
Zertifikatsanforderer 33  
Zertifikatsanforderung 32  
Zertifikatsantrag 5  
Zertifikatslizenz 6  
Zertifizierungsstelle 7, 37  
Zugelassene Zertifikate 12  
Zurückziehen 24  
Zurückziehen von Zertifikatsanträgen 24  
Zwischenzertifikat 35