

Eine detaillierte Anleitung

## Wie löse ich meine Zertifikatslizenz auf [www.swissign.net](http://www.swissign.net) ein?

Diese Anleitung beschreibt die einzelnen Schritte zur Erlangung eines Zertifikates. Typischerweise haben Sie von Ihrer Einkaufsstelle oder Ihrem Reseller einen Lizenzcode erhalten. Diesen können Sie nun in einen Zertifikatsantrag umwandeln, um das endgültige Zertifikat zu erlangen.

Loggen Sie sich auf [www.swissign.net](http://www.swissign.net) ein. Gegebenenfalls haben Sie auch einen passenden Link hierzu per E-Mail von Ihrem Einkauf / Reseller erhalten.

### Antragstellung des Zertifikates mit der Zertifikatslizenz auf [www.swissign.net](http://www.swissign.net)

Auf der technischen Plattform [swissign.net](http://swissign.net) haben Sie drei Möglichkeiten:

- «Weiter ohne Konto»: Dabei machen Sie keine Angaben im Feld Benutzername oder Passwort. Diese Version wählen Sie, wenn Sie nur ein einzelnes Zertifikat beziehen und dieses nicht auf [swissign.net](http://swissign.net), sondern auf Ihrem eigenen Rechner verwalten. Für eine Ungültigkeitserklärung müssen Sie sich unbedingt den Ungültigkeitscode während der Zertifikatsbestellung merken.
- «Anmelden» (im Menü links): Hiermit legen Sie ein Konto auf der technischen Plattform [swissign.net](http://swissign.net) an, das völlig unabhängig ist vom Einkaufskonto im Webshop [www.swissign.com](http://www.swissign.com). Insbesondere für Organisationen mit mehreren Zertifikaten wird hier eine bequeme Möglichkeit geboten, die Zertifikate für die eigene Organisation zu verwalten, ggfs. nochmals bereitzustellen etc. Aber auch Einzelzertifikate können hier bequem angesehen, heruntergeladen und revoziert werden.
- «Login»: Falls Sie schon ein Konto angelegt haben.

### Was ist ein Konto?

Ein Konto repräsentiert einen Benutzer oder eine Gruppe von Benutzern, die sich durch Benutzername/Passwort oder mittels Zertifikat anmelden können. Ein Konto umfasst Kontakt-Informationen, speziell die E-Mail-Adresse für Benachrichtigungen und optional eine Telefonnummer. Die Information kann vom Konteninhaber verändert werden. Jede Zertifikatsanforderung unter Benutzung dieses Kontos wird diesem Konto zugeordnet. Damit müssen die Konteninformationen nicht jeder Zertifikatsanforderung einzeln zugeordnet werden.

### Nutzung ohne Benutzerkonto

Einfache Benutzerkonten sind hauptsächlich für Kunden sinnvoll, die im Webshop Zertifikate bestellen, und mittels Benutzerkonto alle Zertifikate im Überblick haben möchten, die sie zuvor erworben haben. Webshop-Nutzer, die nur ein Zertifikat bestellt haben, können generell auch ohne Benutzerkonto fortfahren («Weiter ohne Konto»). Sie haben so aber keine Möglichkeit mehr, Informationen über Ihr Zertifikat abzurufen. Benutzer ohne Konto brauchen für die Beantragung eines Zertifikates zwingend einen Lizenzcode, den sie z.B. zuvor im Webshop erworben haben.

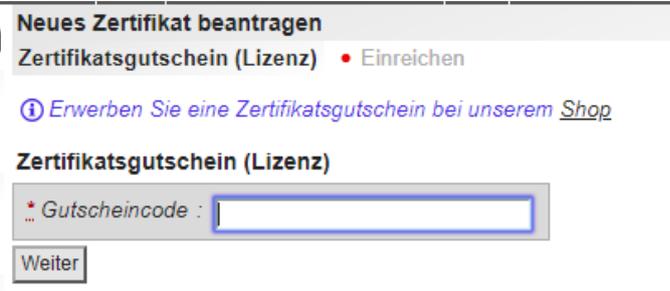
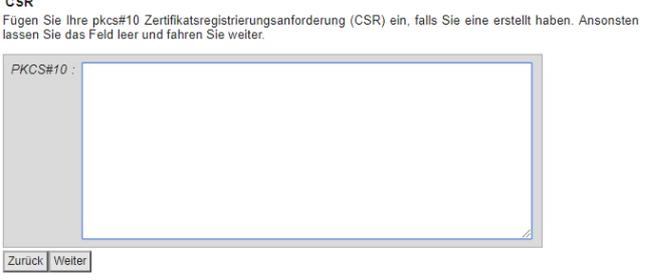
## Erstellen eines Benutzerkontos

<p>Als Webshop-Nutzer kann man erstmalig ein Konto erstellen, falls man nicht ohne Konto fortfahren will. Hierzu wählt man im Hauptmenü links den Punkt «Erstellen» unter «Konto» aus.</p>	
<p>Es werden anschliessend in der Hauptansicht Kontodaten abgefragt, hierunter den Benutzernamen und das Passwort unter dem man sich zukünftig beim Konto einwählen will. Dem Konto wird auch eine E-Mail-Adresse hinterlegt, die für zukünftige Zertifikatsanträge als Standard E-Mail-Adresse genutzt wird, um auf einen etwaigen Ablauf des Zertifikates hinzuweisen. Auch die bevorzugte Sprache der Benutzeroberfläche und des E-Mail-Kommunikation kann man anwählen. Mit der Schaltfläche «Konto erstellen» wird das Konto erstellt.</p>	
<p>Das System berücksichtigt bei der Wahl von Passwörtern deren Sicherheit. Die Sicherheit wird mit einem Algorithmus geprüft und bei der Eingabe angezeigt. Wird ein unsicheres Passwort gewählt, so erfordert dies eine gesonderte Bestätigung nach der Eingabe, dass man wirklich mit diesem unsicheren Passwort fortfahren will.</p>	

## Anfordern von Zertifikaten

Benutzer müssen im Besitz eines Lizenzcodes sein, um Zertifikate anzufordern. Dieser wurde zuvor im Shop erworben. Ein Lizenzcode berechtigt einen Benutzer dazu, eine bestimmte Anzahl Zertifikate anzufordern – in der Regel ein einziges Zertifikat. Ein Lizenzcode bestimmt ein Produkt, worüber eine Anforderung gestellt werden kann.

<p>Bei Beantragung als Benutzer mit Konto ist ein Login notwendig. Für die Beantragung mit Lizenzcode ist das Anlegen eines Kontos optional und somit kein Login notwendig. Es kann in diesem Fall mit «Weiter ohne Konto» fortgefahren werden.</p> <p>Benutzerkonten müssen vorgängig durch den Nutzer angelegt sein.</p>	
<p>Sofern man bereits mit einem anderen Konto eingeloggt ist, kann es Sinn machen, sich zunächst über das Hauptmenü abzumelden und dann an einem Konto anzumelden, mit dem man Zertifikate beantragen kann. Oder man erstellt eine neues Konto über den Menüpunkt «Erstellen».</p>	

<p>Ein Konto bietet folgende Vorteile:</p> <ul style="list-style-type: none"> <li>• Kontodaten (E-Mail-Adresse, Spracheinstellung) werden direkt übernommen und bei der Erstellung eines Zertifikates als Attribute dem Zertifikat beigelegt. 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.</li> <li>• Nach denen mit einem Konto angeforderten Zertifikaten kann gezielt durch Anwendung eines Filters gesucht werden. Mehrere Zertifikate können damit einfach verwaltet werden. Zertifikate können auch zurückgezogen werden oder nochmals heruntergeladen werden.</li> </ul>	
<p>Um Zertifikate neu zu beantragen ist im Hauptmenü links unter Oberpunkt «Zertifikate» der Unterpunkt «Neu» zu wählen.</p>	
<p>Wenn Sie einen Cutscheincode im Shop erworben haben, geben Sie diesen unter «Lizenzcode» ein.</p> <p>Im nächsten Schritt bekommen Sie das mit diesem Lizenzcode verbundene Produkt angezeigt.</p>	
<p>In der Hauptansicht muss nun die Teilnehmervereinbarung Zertifikatsdienstleistungen gelesen und bestätigt werden. Hierzu die Schaltfläche «Ich akzeptiere diese Bedingungen» wählen.</p>	
<p>Optional: Zertifikatsregistrierungsanforderung, in Englisch «Certificate Signing Request» (CSR), eingeben. Für den Benutzer besteht die Möglichkeit, dass er sich extern mit eigenen Tools (certtool.exe oder OpenSSL) ein Schlüsselpaar erzeugt 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.</p> <p>Sollte der Benutzer sich dafür entscheiden, von SwissSign die Schlüssel generieren zu lassen, so</p>	

ist das Feld unter PKCS#10 leer zu lassen und nur die Schaltfläche «Weiter» zu betätigen.

**Achtung:** Dieses Verfahren ist für SSL Zertifikate nicht zulässig. Für SSL Zertifikate muss zwingend ein CSR eingereicht werden.

## 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 wiederherstellen. 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.

**Achtung:** Dieses Verfahren ist für SSL Zertifikate nicht zulässig. Für SSL Zertifikate muss zwingend ein

Das von SwissSign generierte Schlüsselpaar verbleibt auf der Plattform und kann im Falle von persönlichen Zertifikaten jederzeit neu unter Verwendung des Passwortes heruntergeladen werden.

## Hinweis

Für die von SwissSign generierten Schlüssel sind 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.

## Anfordern von SSL Zertifikaten

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

In der Hauptansicht ist zunächst die Identität ausfüllen: Zunächst muss dem Zertifikat ein Domänenname vergeben werden, der später auch im Subject des Zertifikates steht. Ort, ggfs. Kanton/Bundesland und Staat mit dem Hauptsitz der Organisation sind in den nachfolgenden Feldern einzugeben. Bei Silver Zertifikaten ist nur der Eintrag des Domännennamens verpflichtend. Danach ist die Schaltfläche «Weiter» zu betätigen.

Bitte stellen Sie sicher, dass eine etwaige eingegebene E-Mail-Adresse bereits existiert.

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

**SSL Gold Certificate**

• Zertifikatsgutschein (Lizenz) • Gültigkeit • Teilnehmerbedingungen • CSR **Attrib**

**Attribute**

\* Domäne :   
Voll qualifizierter Domänenname Ihres Servers.  
 Beispiel: www.company.com

Details zur Organisation 1 :

Details zur Organisation 2 :

Details zur Organisation 3 :

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

\* Ortschaft :

Kanton/Bundesland :   
Erforderlich (ausser nicht anwendbar)

\* Land :

Zurück **Weiter**

<p>Neu kann der Kunde auswählen ob er sein Zertifikat als precert oder OCSP Stapling erstellen will.</p> <p>precert: Keine Änderung am Server nötig, damit ab Chrome 68 das Zertifikat richtig angezeigt wird. Hier sind CT Lists im Zertifikat hinterlegt anhand von welchen die Validierung durchgeführt wird.</p> <p>OCSP Stapling: Es ist eine Änderung am Server nötig – OCSP Stapling muss aktiviert werden. Der Vorteil daran ist, dass der Zugriff für den Kunden schneller ist.</p>	<p><b>SSL Gold Certificate</b></p> <ul style="list-style-type: none"> <li>• Zertifikatsgutschein (Lizenz)</li> <li>• Gültigkeit</li> <li>• Teilnehmerbedingungen</li> <li>• CSR</li> <li>• Attribute</li> </ul> <p><b>CT logs</b></p> <p>CT-Log Projekt dient der Überprüfung von Zertifikatsausstellungen. Die Logs, die sämtliche aller Zertifizierungsstellen weltweit auflisten, sind offen. Somit kann jeder Ausstellungen für überwachen und Falschausstellungen erkennen.</p> <p>Zertifizierungsstellen können Zertifikate bereits während der Antragsphase auflisten (sogen: oder erst nach Genehmigung und Ausstellung. Mit einem Precertificate wird die Loginform als x509v3 Zertifikatsweiterung (Signed Certificate Stamp (SCT)) eingetragen und kann v direkt erkannt werden. Im Falle eines Eintrages nach Ausstellung, wird die Log-Information Gültigkeitsabfrage mittels „OCSP Stapling“ übermittelt. Letzteres Verfahren ist eleganter, Betrieb auch einstellen können und das Zertifikat immer mit einer Ersatzloginformation für versorgt wird. Allerdings wird OCSP Stapling noch nicht von allen Webservern unterstützt folgende Webserver OCSP Stapling:</p> <ul style="list-style-type: none"> <li>• Apache &gt; 2.2.3</li> <li>• Nginx &gt; 1.3.7</li> <li>• Microsoft IIS Windows Server &gt; 2008</li> <li>• HA Proxy &gt; 1.5.0</li> <li>• LiteSpeed Web Server &gt; 4.2.4</li> <li>• F5 Networks BIG-IP &gt; 11.6.0</li> </ul> <p>Achtung: Alle ab dem 30. April 2018 ausgestellten Zertifikate werden in Google ( vertrauenswürdig angezeigt, falls CT-Log Informationen zu diesem Zertifikat verfügbar sind OCSP Stapling nicht unterstützen, wählen Sie bitte die Option „pre-certificate“.</p> <p><b>CT log method</b> <input type="radio"/> pre-certificate <input type="radio"/> stapling</p> <p>Zurück Weiter</p>
<p>Sofern Sie mit Konto eingeloggt sind, können Sie Ihre Konto Angaben über den menüpunkt «Editieren» anpassen.</p>	
<p>Im letzten Schritt muss ein Passwort eingegeben werden. Dieses kann SwissSign nicht zurücksetzen, es ist also wichtig, sich dieses gut zu merken.</p>	<p><b>⚠ Aus Sicherheitsgründen ist SwissSign nicht in der Lage, verlorene Schlüsselpasswörter wiederherzustellen. Für deren sichere Aufbewahrung ist ausschliesslich der Benutzer verantwortlich.</b></p> <p>* Passwort : <input type="password"/></p> <p>* Passwort wiederholen : <input type="password"/></p> <p>Zurück Zertifikat anfordern</p>
<p>Jetzt kann das Zertifikat angefordert werden. Alle Zertifikatsdaten werden nochmals angezeigt. Sind eventuell Fehler vorhanden, können die vorherigen Schritte in der Menüzeile oben nochmals angewählt werden und die Daten können angepasst werden. Sollten die Daten eines von Ihnen eingegebenen CSRs fehlerhaft sein, können Sie diese Daten auch bequem über die Ansteuerung des Menüs «Attribute» in der Menüzeile oben editieren.</p>	

Im Falle von Gold Zertifikaten haben Sie nun einen gesonderten Antrag auszudrucken, auszufüllen und mit den notwendigen Dokumenten an das SwissSign Fulfillment Center zu senden:

**SwissSign AG, Fulfillment Center, Sägereistrasse 5 , 8152 Glattbrugg**

## Hinweis

Achten Sie bei der Einreichung eines Zertifikatsantrages für Gold Zertifikate darauf, dass

- Gehörige Unterschriften gemäss (Handels-) Register für die Organisation unterzeichnen. Bei Unterschrift zu zweien, sind zwei Unterschriften notwendig!
- Die Domäne Validierung ist erfolgreich abgeschlossen

Alle unterschreibenden Personen eine Kopie ihrer ID oder Pass beilegen, der sowohl das Foto als auch die Unterschrift zeigt.

## Validierung der Zertifikatsangaben

File Bearbeiten Ansicht Navigation Nachricht Extras Hilfe

Von ca@swissign.com

Betreff: Neue SwissSign Silver Zertifikat Anforderung D9421E36A2B1A04DF318C755C20C37

An [Redacted]

Sehr geehrte Kundin  
Sehr geehrter Kunde

Folgende Zertifikatsanforderung wurde soeben bei SwissSign eingereicht:  
/CN=Email:[Redacted]online.de/OU=Email Validated Only (ema[Redacted]online.de)

Als rechtmässiger Inhaber der E-Mail Adresse [Redacted]@online.de können Sie diese Anforderung selbst genehmigen. Um die Anforderung jetzt zu genehmigen, öffnen Sie bitte folgenden Link in Ihrem Browser:

<https://swissign.net/cgi-bin/request/approve?auth=3BC6DF785603E96AD34F1FABBC808AE70B2AC96B&id=D9421E36A2B1A04DF318C755C20C37>

Um die Zertifikatsanforderung zu annullieren, verwenden Sie folgenden Link:

[https://swissign.net/cgi-bin/request/cancel?auth=5955D5DF8DBB7661063472C487E3A2F04965F5DB&license=9F3C8C494683C590\\_LMYmub](https://swissign.net/cgi-bin/request/cancel?auth=5955D5DF8DBB7661063472C487E3A2F04965F5DB&license=9F3C8C494683C590_LMYmub)

Falls Sie vermuten, dass jemand versucht, Ihre E-Mail Adresse [Redacted]@online.de zu missbrauchen, kontaktieren Sie uns bitte unter [registration@swissign.com](mailto:registration@swissign.com). Weitere Kontaktmöglichkeiten finden Sie unter <http://swissign.com/contact>.

Mit freundlichen Grüßen,  
Ihr SwissSign Team

Bei Silver Zertifikaten – wie hier im Beispiel – wird lediglich die Existenz der E-Mail-Adresse oder der Domäne getestet. Das dauert nur Sekunden bis Minuten: Sie erhalten von uns eine E-Mail an die im Zertifikat geschützte E-Mail-Adresse und bestätigen diese durch Klick auf den Genehmigungslink, um die Zertifikatsanforderung freizugeben. Sie werden daraufhin auf die Freigabeseite der Zertifikatsanforderung geleitet.

Startseite Support Zertifizierungsstelle Shop Zertifikat für ungültig erklären Help

SwissSign Zertifikate Suchen / Verwalten

Suchen Spalten

Zertifikate

- Neu
- Suchen / Verwalten

Konto

festjoskoe

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

Login mit Zertifikat

- Anmelden

Genehmigung bestätigen

Zu genehmigende Anforderung

Status	Gültig von	Läuft ab	Subjekt	Alternativer Name
hängig	--	--	/CN=joseph.koenig@swissign.com/Email=joseph.koenig@swissign.com	email:joseph.koenig@swissign.com

Genehmigung bestätigen

\* Anforderungsidentifikator :

Genehmigungscode :

Abbrechen Genehmigung bestätigen

Suchen

Zurück zu Suchen

Mit «Ja» bestätigen Sie die Freigabe. Es folgt noch ein letzter Check vom Fulfillment Center:

Startseite | Support | Zertifizierungsstelle | Shop | Zertifikat für ungültig erklären | Help

**SwissSign** Zertifikate Suchen / Verwalten

Suchen • Spalten

**Zertifikate**

- Neu ✓ 6E77B61DE3384384F42C6495F3820700F13778F9 genehmigt
- Suchen / Verwalten

**Konto**

Testjoskoe

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

**Login mit Zertifikat**

- Anmelden

**Suchen**

Text suchen :  x

Exakte Suche: \*O=SwissSign AG\*  
Platzhalterzeichen Suche: Swiss\*

Lizenz :

Konto :  <beliebig>  Testjoskoe

Contract ID :

Gültig von :   
Zeitspanne: Beispiel: 2010-03, 2010-05

Läuft ab :   
Zeitspanne: Beispiel: 2010-03, 2010-05

Status :  hängig  genehmigt  annulliert  zurückgewiesen  gültig  revoziert  abgelaufen  unvollständig  alle  keine

Öffentliche Zertifikate :  Ausblenden  Einblenden

Seitengrösse :

csv Export | Suchen | Seite 1 von 1 (Datensätze 1-1 von 1)

	Status >>	Gültig von << < > >>	Läuft ab << < > >>	Subjekt << < > >>	Alternativer Name << < > >>
Zurückziehen	genehmigt	--	--	/CN=joseph.koenig@swissign.com/Email=joseph.koenig@swissign.com	email:joseph.koenig@swissign.com
Attribute					

Im Falle eines Gold Zertifikates wird zunächst der schriftliche Antrag und die Dokumentation von SwissSign geprüft und von SwissSign freigegeben.

In der Übersicht nach der Erstellung der Anforderung sehen Sie den Zufallswert zur Domänenvalidierung sowie die Information, dass das Zertifikat erst endgültig bewilligt werden kann, wenn dieser Check durchgeführt ist.

## SSL Gold Certificate

✓ Sie haben folgende Zertifikatsanforderung erfolgreich eingereicht:

### Anforderungsangaben

Subjekt DN	CN	test.swstestsupport.ch
	O	SwsTestSupport
	L	Zürich
	ST	Zürich
	C	CH
Alternativer Name des Subjekts	DNS	test.swstestsupport.ch
	DNS	www.test.swstestsupport.ch
Anforderungsidentifikator		123606E9C7000D9FCD3B2D3D15C7E385C6DDE9BE
Schlüsselidentifikator		1C5110C7E6CDF7947FF378BE96DC13B810748646
Lizenzcode		bnJ8u5r6p8eLujm4qN
Ungültigerklärungscode		1A02420963577C080A36BE7533C695ED5A7875EA

① Bitte bewahren Sie die Lizenz- und Ungültigerklärungscode an einem sicheren Ort auf. Sollte Ihr privater Schlüssel verloren gehen oder gestohlen werden, brauchen Sie beide Codes, um Ihr Zertifikat für ungültig zu erklären.

① After printing and signing the [registration document](https://swissign.net:443/regdoc?lang=en&id=123606E9C7000D9FCD3B2D3D15C7E385C6DDE9BE) (<https://swissign.net:443/regdoc?lang=en&id=123606E9C7000D9FCD3B2D3D15C7E385C6DDE9BE>), please send it with the required documents to the following registration authority using regular mail:

- **SwissSign**

SwissSign AG  
Fulfillmentcenter  
Sternmatt 6  
Postfach 2259  
CH-6010 Kriens 2  
[registration@swissign.com](mailto:registration@swissign.com)  
+41 848 776655 (Telefon)

- **Zufallswert: «dN5VsMibPrXgKLNDkkldKwniAN3DCQJKV9czeP0u7l»**

Bitte beachten Sie, dass das Zertifikat erst endgültig bewilligt wird wenn die Domänen Prüfung erfolgreich durchgeführt worden ist. Bemerkung: Im Falle von Multidomain, nutzen Sie dasselbe Zufallswert für alle Domänen.

Registrierungsdokument herunterladen

Seite drucken

## C) Domänen-Eintrag

Domänen	test.swstestsupport.ch www.test.swstestsupport.ch
Zufallswert	dN5VsMibPrXgKLNDkkdKwniAN3DCQJKV9czeP0u7I

Jede im Zertifikat eingetragene Domäne muss validiert werden, bevor das Zertifikat ausgestellt werden kann. Bitte tragen Sie das Zufallswert bei allen Domänen an einer der drei folgenden Stellen ein:

- entweder in einer Datei <https://test.swstestsupport.ch/.well-known/pki-validation/swissign-check.txt> ohne jegliche Zusätze eingefügt werden soll (keine Weiterleitungen sind zugelassen)
- oder in einem meta Tag einer HTML Datei unter <https://test.swstestsupport.ch/.well-known/pki-validation/swissign-check.htm> in der Form `<meta name="swissign-check" content="dN5VsMibPrXgKLNDkkdKwniAN3DCQJKV9czeP0u7I" />` (keine Weiterleitungen sind zugelassen)
- oder in einem TXT Eintrag des DNS records der Domäne: `swissign-check=dN5VsMibPrXgKLNDkkdKwniAN3DCQJKV9czeP0u7I`

Alle 3 Stellen werden durch das System automatisch geprüft. Die Prüfung muss innerhalb von 30 Tagen erfolgreich abgeschlossen werden. Nach erfolgreicher Prüfung sämtlicher im Zertifikat enthaltenen Domänen kann das Zertifikat freigegeben werden. Falls die Prüfung nach 30 Tagen nicht erfolgreich geprüft werden konnte, wird der Request zurückgewiesen.

## Herunterladen des Zertifikates auf [www.swissign.net](http://www.swissign.net)

An Ihre Kontaktadresse des Profils auf [swissign.net](http://www.swissign.net) haben Sie nach Freigabe durch das Fulfillment Center eine E-Mail erhalten. In dieser befindet sich auch der Downloadlink Ihres nun freigegebenen Zertifikates:

**Von:** <[ca@swissign.com](mailto:ca@swissign.com)>  
**Datum:** 5. November 2013 05:20:33 MEZ  
**An:** [REDACTED]@swissign.com  
**Kopie:** <[registration@swissign.com](mailto:registration@swissign.com)>  
**Betreff:** Ihre SwissSign Zertifikat Anforderung D9421E36A2B1A04DF318C755C20C37 wurde genehmigt  
**Antwort an:** SwissSign Certificate Authority <[ca@swissign.com](mailto:ca@swissign.com)>

Sehr geehrte Kundin  
Sehr geehrter Kunde

Ihre SwissSign Zertifikat Anforderung D9421E36A2B1A04DF318C755C20C37 mit folgendem Subjekt wurde genehmigt:  
/CN=Email:[REDACTED]@online.de/OU=Email Validated Only (email:[REDACTED]@online.de)

Um das neue SwissSign Zertifikat herunterzuladen und zu installieren, verwenden Sie bitte folgenden Link:  
<https://swissign.net/cgi-bin/id/download?auth=7F44946896031F30A5659C29C0971423F5344374&id=D9421E36A2B1A04DF318C755C20C37>

Dieser Link erlaubt es Ihnen, Ihr SwissSign Zertifikat zu einem späteren Zeitpunkt erneut herunterzuladen. Wir empfehlen Ihnen deshalb, eine Kopie dieser Nachricht aufzubewahren.

Mit freundlichen Grüßen,

Mit dem Downloadlink gelangen Sie auf die technische Plattform [swissign.net](http://www.swissign.net), auf der Sie das Zertifikat herunterladen können.

Startseite Support Zertifizierungsstelle Shop Zertifikat für ungültig erklären Help

## SwissSign Zertifikate Suchen / Verwalten

Suchen Spalten

Herunterladen / Attribute

**Zertifikat**

Status	Gültig von	Läuft ab	Subjekt	Alternativer Name	Zertifikatsidentifikator	Anforderung
gültig	2018-10-19 15:04:31	2019-10-19 15:04:31	/CN=Joseph.Koenig@swissign.com/Email=Joseph.Koenig@swissign.com	email:Joseph.Koenig@swissign.com	6E77B61DE3384384F42C6495F3820700F13778F9	6E77B61DE3384384F42C6495F3820700F13778F9

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

\* Anzeigenname : Joseph.Koenig@swissign.com

\* Schlüsselpasswort :

Herunterladen

**Zertifikat herunterladen (ohne privaten Schlüssel)**

Format :  cer  
 crt  
 pem  
 p7b (Zertifikatskette)  
 p7c (Zertifikatskette)  
 pem (Zertifikatskette)

Herunterladen

**Attribute**

\* Zertifikatsidentifikator : 6E77B61DE3384384F42C6495F3820700F13778F9

Abrufbarkeit : privat

Konto : Testjoskoe

Alt. E-Mail :

Konto: gmjoskoe.1@gmail.com

Alt. Sprache :  English  Deutsch  <Konto>

Konto: Deutsch

Notiz :

Abbrechen Speichern

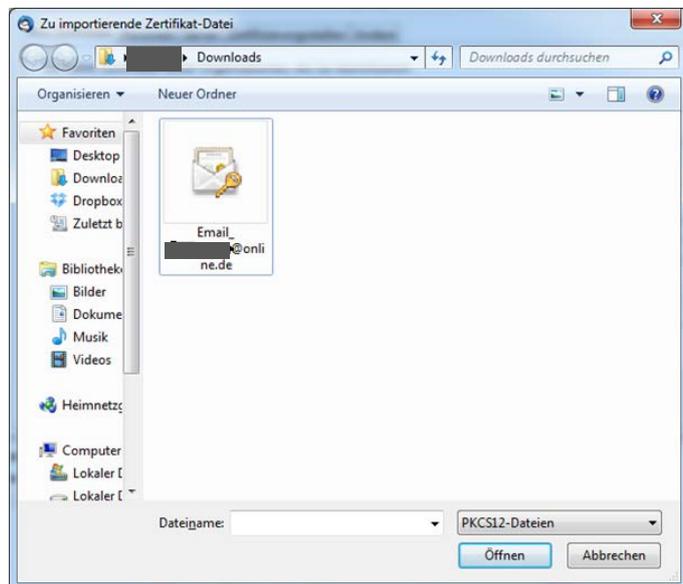
**Details**

Version	v3
Serial number	6e:77:b6:1d:e3:38:43:84:f4:2c:64:95:f3:82:07:00:f1:37:78:f9
Signaturalgo	RSA-SHA256
Aussteller DN	cn=SwissSign Personal Silver CA 2014 - G22, o=SwissSign AG, c=CH
Gültigkeit	2018-10-19 15:04:31, 2019-10-19 15:04:31
Subjekt DN	cn=Joseph.Koenig@swissign.com, emailAddress=Joseph.Koenig@swissign.com
Öffentlicher Schlüssel	RSA: #1 U.C.SEQUENCE {

Da wir in unserem Beispiel den privaten Schlüssel durch SwissSign haben erstellen lassen (Nicht mehr für SSL zulässig, in unserem Beispiel haben wir ein Email Zertifikat beantragt), empfiehlt sich die Kombination «privater Schlüssel + Zertifikat» mit dem von uns gewählten Passwort herunterzuladen. Das Format dieser Datei ist «.p12». Es kann aber auch das Zertifikat einzeln in beliebigem Format heruntergeladen werden.

## Installation auf Ihren Rechner

Die .p12 Datei kann beispielsweise unter Zertifikatsverwaltung direkt in den Mailclient installiert werden. Bei Windows reicht ein Doppelklick auf die Datei. Hier das Beispiel Thunderbird Mailclient:



Sollten Sie zum Ablauf noch Fragen haben oder Hilfe benötigen, steht unser Support Ihnen gerne zur Seite: [www.swissign.com/support](http://www.swissign.com/support).