

# SwissSign CA

SwissSign AG

Handbuch für RA-Operatoren

**Copyright © 2012-2022, libC Technologies SA. Alle Rechte vorbehalten.**

Die Programme (die sowohl die Software als auch die Dokumentation umfassen) enthalten geschützte Informationen von libC Technologies SA und SwissSign AG; Sie werden im Rahmen einer Lizenzvereinbarung bereitgestellt, die Nutzungs- und Offenlegungsbeschränkungen enthält, und sind ausserdem durch Urheberrechte, Patente und andere Gesetze zum Schutz geistigen und gewerblichen Eigentums geschützt. Reverse Engineering, Disassemblierung oder Dekompilierung der Programme ist untersagt.

Diese Programmdokumentation darf ausschliesslich zur Unterstützung der Bereitstellung der Programme und nicht für andere Zwecke verwendet werden. Die in diesem Dokument enthaltenen Informationen können jederzeit und ohne Vorankündigung geändert werden. Bitte teilen Sie uns Probleme in Bezug auf diese Dokumentation schriftlich mit. Die SwissSign AG übernimmt keine Garantie für die Fehlerfreiheit dieses Dokuments. Sofern nicht ausdrücklich in Ihrer Lizenzvereinbarung gestattet, darf kein Bestandteil der Programme ohne die ausdrückliche, schriftliche Genehmigung der SwissSign AG in irgendeiner Form oder mit irgendwelchen Mitteln, elektronisch oder mechanisch, für irgendeinen Zweck vervielfältigt oder übertragen werden.

**Revision**

<b>Rev.</b>	<b>Datum</b>	<b>Wer</b>	<b>Kommentar</b>
1.0	23.03.2022	SwissSign AG	Ursprüngliches Dokument
1.1	13.07.2022	SwissSign AG	Aktualisierung Screenshots
1.2	06.10.2022	SwissSign AG	Abschnitte aktualisiert, um den aktuellen Stand der CA widerzuspiegeln

Akronym	Bedeutung
<b>ACME</b>	Automatic Certificate Management Environment
<b>Administrator</b>	Nutzer, der über die Admin-Rechte für die Admin-Benutzeroberfläche verfügt.
<b>AIA</b>	Zugriff auf Zertifizierungsstelleninfos
<b>AKI</b>	Zertifizierungsstelleninfo
<b>ARL</b>	Zertifizierungsstellen-Sperrliste
<b>BC</b>	Zertifikateinschränkung
<b>CA</b>	Zertifizierungsstelle
<b>CAA</b>	Certification Authority Authorization Rule
<b>CAO</b>	Nutzer, der über die Admin-Rechte für die Operator-Benutzeroberfläche verfügt.
<b>CDP</b>	CRL-Verteilungspunkt
<b>Client</b>	Ein Client ist eine logische Gruppierung der unterschiedlichen PKIs, welche für einen bestimmten Bereich erstellt werden können.
<b>CMC</b>	Certificate Management über CMS (Cryptographic Message Syntax)
<b>CNG</b>	Microsofts CryptoAPI der nächsten Generation
<b>CMP</b>	Certificate Management Protocol
<b>CP</b>	Zertifikatsrichtlinie
<b>CPS</b>	Zertifikatverwendungserklärung
<b>CRL</b>	Zertifikatssperrliste
<b>CSR</b>	Zertifikatsignaturanforderung Ein base64-codiertes PKCS#10 (siehe PKCS#10) einschliesslich Anfangs- und Endbaken
<b>CT</b>	Certificate Transparency
<b>DC</b>	Domain Controller
<b>DIT</b>	Directory Information Tree (LDAP)
<b>DSS</b>	Document Signer Service
<b>EKU</b>	erweiterte Schlüsselverwendung
<b>KU</b>	Schlüsselverwendung
<b>IIS</b>	Microsoft Internet Information Server
<b>LDAP</b>	Lightweight Directory Access Protocol
<b>MAP</b>	Microsoft Application Policies
<b>MCT</b>	Microsoft-Zertifikatvorlage
<b>MSCA</b>	Microsoft Certification Authority
<b>NC</b>	Namenseinschränkung
<b>OCSP</b>	Online Certificate Status-Protokoll
<b>PKCS#10</b>	Eine Zertifikatsanfrage im Binärformat (siehe CSR)
<b>PKCS#12</b>	Eine Datenstruktur, welche normalerweise eine Zertifikatkette sowie den privaten Schlüssel) des entsprechenden untergeordneten Zertifikats enthält. Diese Datei wird mit einer PIN verschlüsselt.
<b>QCv2</b>	Qualified Statement v2
<b>RA-Operator</b>	Ein RA-Operator kann Zertifikate ausstellen, widerrufen, wiederherstellen oder erneuern.
<b>RP</b>	Vertrauende Seite (OIDC)
<b>SAN</b>	alternativer Antragstellername
<b>SKI</b>	Schlüsselkennung des Antragstellers

## Inhalt

1	SwissSign CA .....	6
1.1	Standards.....	7
2	Einleitung .....	8
3	RA-Benutzeroberfläche.....	10
3.1	Login mit SwissID.....	10
3.1.1	Onboarding auf SwissID.....	10
3.2	Hauptmenü .....	11
3.3	Dashboard .....	12
3.3.1	Ablaufende Zertifikate .....	12
3.4	Ausstellung .....	13
3.4.1	Zertifikatsrichtlinien.....	14
3.4.2	Ausstellung PKCS#10.....	15
3.4.3	Ausstellung PKCS#12.....	17
3.4.4	Zusätzliche Informationen für die Registrierung .....	18
3.4.5	Zusätzliche E-Mails über Erneuerungen .....	18
3.4.6	Veröffentlichung des Zertifikats .....	19
3.5	Bestellungen und Zertifikate.....	20
3.5.1	Bestelldetails des Zertifikats.....	23
3.5.2	Zertifikat revozieren.....	26
3.5.3	Zertifikat veröffentlichen .....	27
3.5.4	Informationen zum Zertifikat.....	28
3.6	ACME.....	31
3.7	Domänenüberprüfung (Domain-Validierung) .....	32
3.7.1	DNS Vor-Validierung .....	32
3.7.2	Ausstehende Validierung von Zertifikatsbestellungen.....	34
3.8	Konto.....	35
3.8.1	Kontodaten.....	35
3.8.2	Berechtigungen .....	36
3.8.3	Service-API-Schlüssel.....	37
4	RA API.....	38
4.1	Rollen und Berechtigungen.....	38
4.2	Service-API-Schlüssel.....	38
4.2.1	API-Schlüssel-Rollover.....	38
4.3	Authentifizierung .....	38
4.3.1	Erstellung von JWTs .....	39
4.3.2	HTTP-Anforderung.....	39
5	CMC.....	39

## 1 SwissSign CA

SwissSign CA baut auf SwissPKI™ von LibC auf. Dabei handelt es sich um eine Certificate Authority Software (kurz CA-Software), die eine robuste, hardwarebasierte, zentralisierte Schlüsselverwaltung in Kombination mit starker Kryptographie bietet, um Geschäftsprozesse zu schützen.

Die Lösung deckt den gesamten Lifecycle der kryptografischen Schlüsselverwaltung, die online Hardware-zu-Hardware Schlüsselverteilung, manipulationssichere Audits sowie Nutzungsprotokolle für die Compliance zu Standards, sowie den gesamten Zertifikat- und Schlüsselverwaltung-Lifecycle ab.

SwissSign CA ist ein funktionsreicher, vollständig integrierter Public Key Infrastruktur-Service, mit dem Sie die Sicherheit Ihres Unternehmens erhöhen. Unsere Managed PKI Services bieten alle notwendigen vorkonfigurierten Funktionen und Dienste, mit denen Sie Ihre digitale Sicherheit sicher, einfach und schnell erhöhen.

Mit SwissSign CA halten Sie Ihre Zertifikate auf dem neuesten Stand und behalten immer den vollen Überblick.

## 1.1 Standards

SwissSign CA unterstützt die Ausstellung und Verwaltung von öffentlich vertrauenswürdigen und qualifizierten Zertifikaten. Für die Implementierung gelten die folgenden Standards und Spezifikationen:

- ✓ Das "Certificate Issuing and Management Components Protection Profile" definiert die Anforderungen für Komponenten, welche Zertifikate mit einem öffentlichen Schlüssel ausstellen, widerrufen und verwalten, wie beispielsweise X.509-Zertifikate. Die Anforderungen sind in den Common Criteria (CC) festgelegt.
- ✓ ETSI-Standards für die Ausstellung von qualifizierten Zertifikaten, die den Anforderungen der Verordnung entsprechen
- ✓ ETSI-Standards für die Ausstellung von Website-Zertifikaten, die den Anforderungen der Dokumente des CA/Browser-Forums entsprechen
- ✓ ETSI Other Trust Services mit Zeitstempeln und CAs, die neben qualifizierten Zertifikaten auch andere Zertifikate ausstellen
- ✓ Grundlegende Richtlinien für das ForumCA/Browser Forum, Erweiterte Validierungsrichtlinien und Sicherheitsanforderungen für Netzwerke und Zertifikatssysteme (CT-Log, DNS-Besitzerprüfungen und CAA-Checks)
- ✓ Schweizerisches Gesetz über elektronische Signaturen und Zertifikate ZertES
- ✓ X.509v3
- ✓ PKIX RFCs

## 2 Einleitung

Die RA-Benutzeroberfläche ist die Benutzerschnittstelle für die Ausstellung von Zertifikaten und deren Lifecycle-Management.

In Ihrer Rolle als Operator (RA-Operator) haben Sie Zugriff auf die RA-Benutzeroberfläche.

Als RA-Operator sind Sie autorisiert, PKI-Tasks für einen oder mehrere Clients auszuführen. Ein Client bezeichnet ein Unternehmen oder eine Organisation, die über eine Vereinbarung mit SwissSign verfügt.

Als RA-Operator sind Sie dafür verantwortlich, Anfragen für digitale Zertifikate anzunehmen und Personen, Unternehmen oder Systeme zu authentifizieren, welche eine Anfrage für ein bestimmtes Zertifikat stellen.

Die Ihrem Benutzerkonto zugewiesene RA-Operator-Rolle ist an bestimmte Berechtigungen gekoppelt.

Ihre Rolle ist einem oder mehreren Clients zugewiesen. Deshalb kann SwissSign Ihnen ggf. auf Clientbasis unterschiedliche Berechtigungen zuweisen. So können Sie möglicherweise sowohl die Berechtigung zur Ausstellung als auch zum Widerruf von Zertifikaten für Client A, aber nur die Berechtigung zur Ausstellung von Zertifikaten für Client B erteilen.

Ein RA-Operator verfügt über die folgenden Berechtigungen:

- ✓ Nach Zertifikaten und Zertifikatsbestellungen suchen und Zertifikate in verschiedenen Formaten wie PEM, DER oder PKCS#7 herunterladen.
- ✓ Zertifikate ausstellen
- ✓ Zertifikate widerrufen
- ✓ Zertifikate veröffentlichen/die Veröffentlichung aufheben (sofern diese Option für das betreffende Zertifikatsprodukt aktiviert ist)
- ✓ Metadaten von Zertifikaten wie Erinnerungs-E-Mails oder Zertifikatskommentare aktualisieren
- ✓ Suche nach ACME-Tokens, ihrem Status und den zugehörigen Domainnamen
- ✓ Domainnamen für die Ausstellung von SSL-Zertifikaten vorab validieren
- ✓ Ihre API-Schlüssel verwalten. API-Schlüssel werden in Verbindung mit der REST-API zur Automatisierung Ihrer Registrierungsprozesse verwendet

Als RA-Operator haben Sie Zugriff auf alle Zertifikate von anderen RA-Operatoren, die demselben Client zugewiesen wurden, sowie auf Zertifikate, die von automatischen Protokoll-Handlern über Protokolle wie ACME, CMC oder OpenAPI (RESTful RA API) ausgestellt wurden.

Das Ausstellen oder Widerrufen von Zertifikaten über die RA-Benutzeroberfläche ist ein manueller Prozess, während die zuvor erwähnten Protokolle vollständig automatisiert sind. Abhängig von der Produkt- und Protokollkonfiguration des Clients der PKI, finden Sie auch Zertifikate, die nicht von Ihnen ausgestellt oder widerrufen wurden.

SwissSign CA unterstützt mehrere automatisierte sowie nicht automatisierte Protokolle zur Registrierung. Dabei handelt es sich um die folgenden Protokolle:



<b>Protokoll</b>	<b>Beschreibung</b>
<b>RA- Benutzeroberfläche</b>	Manuelle Ausstellung von Zertifikaten und die Lebenszyklusmanagement (dieses Dokument)
<b>RA API</b>	OpenAPI v3-Spezifikation zur Automatisierung und Integration Ihrer MPKI in Ihre Dienste.
<b>ACME</b>	RFC8555 ACME HTTPS-Dienst freigegeben für Clients. Sie können jede Client-Software verwenden, die diesem Standard entspricht. Allerdings empfehlen wir Ihnen folgende getestete Client-Software zu verwenden: <ul style="list-style-type: none"><li>- Certbot ACME Client von Red Hat Enterprise Linux oder</li><li>- ACMESharp für Microsoft-Plattformen</li></ul>
<b>CMC</b>	Zertifikatsverwaltung über CMS (Cryptographic Message Syntax) nach RFC 5272

### 3 RA-Benutzeroberfläche

Als RA-Operator erhalten Sie Zugriff auf die folgenden Bereiche der RA-Benutzeroberfläche:

Bereich	Beschreibung
<b>Dashboard</b>	Übersichtsseite, die das Folgende anzeigt: <ul style="list-style-type: none"> <li>- Alle Zertifikate, die in 'd' Tagen ablaufen</li> </ul>
<b>Ausstellung</b>	Eine durchsuchbare Liste aller Zertifikatsprodukte, die Sie für ausgewählte Client(s) ausstellen können
<b>Bestellungen und Zertifikate</b>	Eine durchsuchbare Liste aller ausgestellten Zertifikate und Zertifikatsbestellungen
<b>ACME</b>	Eine durchsuchbare Liste aller angeforderten ACME-Token, Domainnamen und des zugehörigen Status.  Dieser Abschnitt ist nur verfügbar, wenn Sie über Zertifikatsprodukte verfügen, die mit einem Client verbunden sind, der Zertifikate über das ACME-Protokoll ausstellen kann.  <b>HINWEIS:</b> ACME wird nur dann angezeigt, wenn das Protokoll für die Ausstellung von Zertifikaten angewendet wird.
<b>Domain-Validierung</b>	Eine durchsuchbare Liste von vorab validierten Domainnamen.
<b>Konto</b>	Ihre Kontoinformationen und -einstellungen  Ausserdem finden Sie hier das Servicekonto für den automatisierten Zugriff über die RA API.

#### 3.1 Login mit SwissID

Der RA-Operator loggt sich mit der SwissID in den MPKI-Service auf SwissSign CA ein.

##### 3.1.1 Onboarding auf SwissID

Bei SwissID handelt es sich um ein sicheres Login von SwissSign. Für das Onboarding auf SwissID folgen Sie den Anweisungen unter folgendem Link:

<https://www.swissign.com/support/dokumentationen/ra-operator-onboarding>

**WICHTIG:** RA-Operatoren verwenden zur Identifizierung bitte dieselbe E-Mail-Adresse, die sie auf dem Bestellformular für ihren MPKI-Service angegeben haben, oder die E-Mail-Adresse, unter der sie bereits zuvor von SwissSign in ihrer Funktion als RA-Operator des MPKI-Service von SwissSign kontaktiert wurden.

## 3.2 Hauptmenü

Die RA-Benutzeroberfläche bietet Ihnen über das Hauptmenü Zugriff auf die verschiedenen Bereiche der Anwendung:



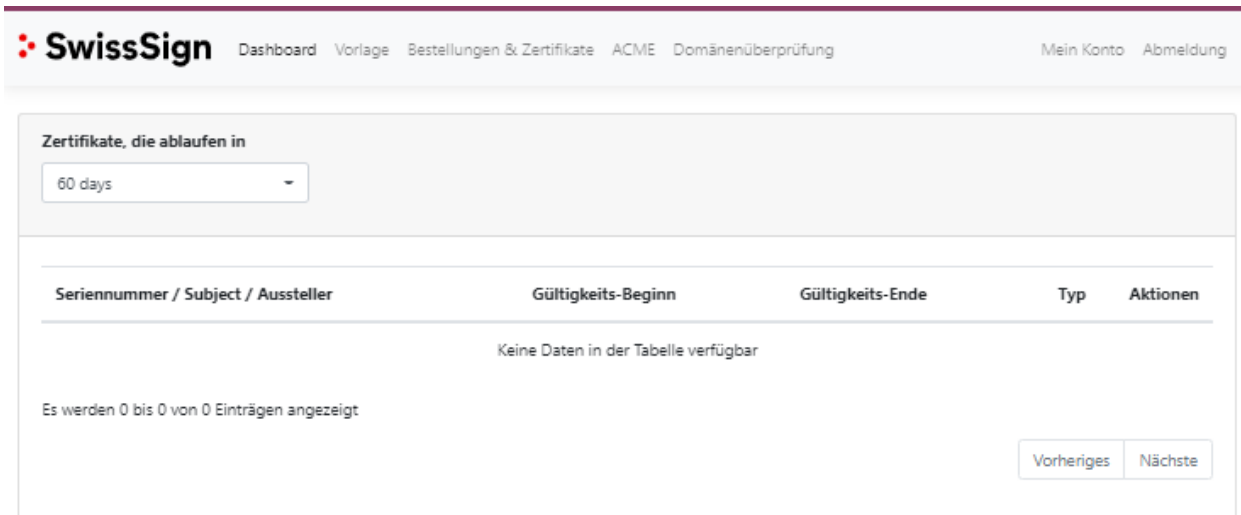
- Für den Zugriff auf das Dashboard siehe Kapitel 3.3 *Dashboard*
- Für den Zugriff auf die Zertifikatsausstellung siehe Kapitel 3.4 *Issuance*
- Für den Zugriff auf Bestellungen und Zertifikate siehe Kapitel 3.5 *Orders and Certificates*
- Für den Zugriff auf die ACME-Token siehe Kapitel 3.6 *ACME*
- Für den Zugriff auf das DNS siehe Kapitel 3.7 *DNS*
- Für den Zugriff auf das Konto siehe Kapitel 3.8 *Account*

### 3.3 Dashboard

Wenn Sie sich bei der RA-Benutzeroberfläche anmelden, landen Sie automatisch auf dem Dashboard. Dort haben Sie Zugriff auf eine Liste mit den bald ablaufenden Zertifikaten.

#### 3.3.1 Ablaufende Zertifikate

In der Tabelle für ablaufende Zertifikate finden Sie eine Liste von Zertifikaten, die demnächst ablaufen. Verwenden Sie das Dropdown-Menü oberhalb des Bereichs, um die Liste zu filtern.



**Zertifikate, die ablaufen in**

60 days

Seriennummer / Subject / Aussteller	Gültigkeits-Beginn	Gültigkeits-Ende	Typ	Aktionen
Keine Daten in der Tabelle verfügbar				

Es werden 0 bis 0 von 0 Einträgen angezeigt

Vorheriges Nächstes

Spalte	Beschreibung
<b>Serien#</b>	Die Seriennummer des Zertifikats
<b>Antragsteller</b>	Definierter Name (DN) des Antragstellers des Zertifikats
<b>Aussteller</b>	Antragsteller-DN der ausstellenden CA
<b>Typ</b>	Zeigt den Zertifikatstyp an: <ul style="list-style-type: none"> <li>- Externes Zertifikat (aus der aktuellen MPKI importiert)</li> <li>-</li> </ul>
<b>Aktionen</b>	<ol style="list-style-type: none"> <li>1. Links zur Detailseite des Zertifikats bearbeiten</li> <li>2. Das Zertifikat im PEM-Format herunterladen</li> <li>3. Eine Veröffentlichungsanfrage senden (nur verfügbar, wenn für das Zertifikat die Option LDAP-Veröffentlichung aktiviert ist. Nur für S/MIME-Zertifikate verfügbar.)</li> </ol>

### 3.4 Ausstellung

Über das Menü "Ausstellung" haben Sie Zugriff auf die Liste der Zertifikatsprodukte (Richtlinieninstanzen), die für die Ausstellung von Zertifikaten zur Verfügung stehen. Über die Felder "Suche" und "Clients" oberhalb der Tabelle können Sie diese Liste filtern.

**SwissSign** [Dashboard](#) [Vorlage](#) [Bestellungen & Zertifikate](#) [ACME](#) [Domänenüberprüfung](#)
[Mein Konto](#) [Abmeldung](#)

---

**Suchen**

**Klienten**

CA	Klient	Policy Name	Typ	Auth.	Sources	Aktionen
<input type="checkbox"/> SwissSign RSA SMIME LCP ICA 2022 - 1 - STAG	MPKI0000104 - SwissSign AG	SwissSign Personal S/MIME E-Mail ID Silver	General			<a href="#">+</a>
<input type="checkbox"/> SwissSign RSA SMIME NCP extended ICA 2022 - 1 - STAG	MPKI0000104 - SwissSign AG	SwissSign Pro S/MIME E-Mail ID Gold	General			<a href="#">+</a>
<input type="checkbox"/> SwissSign RSA SMIME NCP extended ICA 2022 - 1 - STAG	MPKI0000104 - SwissSign AG	SwissSign Pro S/MIME E-Mail ID Gold RSASSA-PSS	General			<a href="#">+</a>
<input type="checkbox"/> SwissSign RSA SMIME NCP ICA 2022 - 1 STAG	MPKI0000104 - SwissSign AG	SwissSign Pro S/MIME E-Mail ID Gold with Auth	General			<a href="#">+</a>

Spalte	Beschreibung
<b>CA</b>	Die CA, die das Zertifikatsprodukt ausstellt
<b>Client</b>	Der dem Zertifikat zugeordnete Client (möglicherweise verfügen Sie über die Berechtigung, Zertifikate für mehrere Clients zu verwalten. Verwenden Sie das Client-Dropdown-Menü, um die verfügbaren Clients zu filtern)
<b>Richtlinienname</b>	Der Name des Zertifikatsprodukt
<b>Typ</b>	Der Produkttyp des Zertifikats (bei der Ausgabe durch RA-Operator immer als <i>Allgemein</i> angezeigt)
<b>Auth</b>	Zeigt ein Häkchen an, wenn der Richtlinieninstanz eine Autorisierungsregel zugeordnet wurde.
<b>Quellen</b>	Zeigt ein Häkchen an, wenn die Ausstellung über vorausgefüllte Datenquellen (DB und/oder LDAP) erfolgte. Bei vordefinierten Datenquellen wird die Ausstellung von Zertifikaten auf verfügbare Datensätze beschränkt, die in der/den Datenquelle(n) gefunden wurden
<b>Aktionen</b>	Ausstellen des Zertifikats leitet auf die Seite zur Ausstellung eines Zertifikats weiter.

### 3.4.1 Zertifikatsrichtlinien

Die Ausstellung eines Zertifikats erfolgt durch das Vervollständigen der Richtliniendetails auf der Seite für die Ausstellung von Zertifikaten. Welche Felder Sie ausfüllen, hängt von einer Reihe von Parametern ab:

- Felder, die zwar sichtbar, aber nicht editierbar sind, werden ausgegraut. Diese Werte werden von SwissSign festgelegt und können von Ihnen nicht überschrieben werden.
- Einige Richtlinienfelder werden möglicherweise nicht angezeigt, sind aber dennoch Teil des ausgestellten Zertifikats
- Richtlinienfelder, die bearbeitet werden können und sichtbar sind, können Sie ausfüllen oder bearbeiten. Es gibt obligatorische und optionale Felder. Obligatorische Felder sind mit einem "\*" gekennzeichnet
- Die Art der Schlüsselerzeugung (PKCS#10, PKCS#12).

Wenn die Richtlinien PKCS#10 erfordern, müssen Sie eine CSR bereitstellen, die mit den in der Richtlinie definierten Parametern für die Schlüsselerzeugung übereinstimmt. Bitte beachten Sie, dass Sie eine CSR mit einer Schlüsselpaargröße bereitstellen können, die grösser ist als der in den Richtlinien definierte Wert. Das Schlüsselpaar muss zu dem definierten Algorithmus passen. Beim Kopieren/Einfügen einer CSR werden für alle bearbeitbaren Werte die in der Anfrage enthaltenen Werte im Formular vorausgefüllt.

Wenn die Richtlinie die Generierung von PKCS#12-Schlüsseln erfordert, generiert SwissSign ein Schlüsselpaar für Sie und informiert die Zertifikatempfänger über den Download des Zertifikats einschliesslich des Schlüsselpaars für PKCS#12

- Die in der Richtlinienvorlage aktivierten Module
- Die der Richtlinieninstanz zugeordneten Regeln

### 3.4.2 Ausstellung PKCS#10

Wenn Sie für eine Richtlinie ausstellen, die PKCS#10 erfordert, müssen Sie eine PKCS#10 (CSR) generieren, indem Sie beispielsweise OpenSSL, Microsoft CNG oder ein anderes Generierungstool verwenden, das in der Lage ist, eine Base64-codierte PKCS#10-Anfrage zu erzeugen. Das Format eines PKCS#10 sieht wie folgt aus:

```
-----BEGIN CERTIFICATE REQUEST-----
```

```
MIIcQTCCAQECAQAwPzEdMBsGA1UECgwUbGliQyBUZWNobm9sb2dpZXMgU0ExETAP
```

```
[ausgeblendet]
```

```
H+aC3/oJkApfonUK5m7eFzDsrN/cMWFQUQ5xFNDCzGmqBdX4U/Ft+s323otQMTN6
```

```
nl6IHYxn7IGxyCIAVg
```

```
-----END CERTIFICATE REQUEST-----
```

Auf der Seite "Zertifikatsausstellung" wird, wie unten dargestellt, der Textbereich angezeigt, in den Sie die generierte PKCS#10-Anfrage einfügen:

## Zertifikat ausstellen | SwissSign Personal S/MIME E-Mail ID Silver

### ^ Schlüsselgenerierungsparameter

Schlüssel-Generierungsquelle	Schlüsseltyp und Mindestgröße	Zertifikatshash-Algorithmus
PKCS10	RSA 2048	sha256

PKCS#10 Request Data (PEM) / Certificate Signing Request (CSR)

Copy/Paste the PKCS#10 request

[^ Alles zusammenklappen](#)

Zurück

CSR validieren

Sobald die Anfrage eingefügt wurde, wird sie automatisch von der Benutzeroberfläche automatisch validiert. Wenn die Validierung erfolgreich ist, wird anschliessend der verbleibende Teil der vorausgefüllten Richtlinie angezeigt. Wenn die Validierung fehlschlägt, wird eine Fehlermeldung angezeigt.

## Zertifikat ausstellen | SwissSign Personal S/MIME E-Mail ID Silver

▼ Fehler

### ^ Schlüsselgenerierungsparameter

Schlüssel-Generierungsquelle	Schlüsseltyp und Mindestgröße	Zertifikatshash-Algorithmus
PKCS10	RSA 2048	sha256

PKCS#10 Request Data (PEM) / Certificate Signing Request (CSR)

```
-----BEGIN CERTIFICATE REQUEST-----  
MTCGyCCAXyCAQsQzE3MAUwGAIIBG0wEjEATBMBR0oMDEM2yXMuU3IubSR
```

### ^ Gegenstand Distinguished Name

Unused Subject Attributes from CSR: c=CH,o=SwissSign AG

Allgemeiner Name	Kodierung	Wert
Email	IAS String	
Common Name	UTF8 String	adrain.mueller@swissigntest.ch

\* required

### ^ Zertifikatsgültigkeit

Gültigkeit	Dauer
Days	365

### ^ Gegenstand alternativer Name

email required.

Email	
-------	--

Max. Einträge: 1 + Element hinzufügen

Email 1\*  ⓘ

email required.

### ^ Zusätzliche Registrierungsinformationen

Kommentar

Zusätzliche Verlängerungs-E-Mails

+ Erneuerungs-E-Mail hinzufügen

### ^ Geschäftsbedingungen

Ich bestätige die Annahme und Einhaltung der Bedingungen des [Subscriber Agreement](#) der SwissSign AG.

Please read and accept the terms and conditions

[^ Alles zusammenklappen](#)

Zurück

Zertifikat ausstellen



### 3.4.3 Ausstellung PKCS#12

Um ein Zertifikat mit serverseitiger Schlüsselgenerierung (PKCS#12) auszustellen, füllen Sie einfach alle obligatorischen, editierbaren Felder auf der Ausstellungsseite aus.

Hinweis: Bei der Schlüsselerzeugung mit PKCS#12 mit PIN muss der Endbenutzer vor der Schlüsselerzeugung die PKCS#12-Schutz-PIN angeben. Dies bedeutet, dass der private PKCS#12-Schlüssel nicht hinterlegt werden kann und daher nicht zum Download für andere Empfänger zur Wiederherstellung zur Verfügung steht. Eine E-Mail mit einem Link zum Setzen der PKCS#12-PIN wird an den Empfänger gesendet (E-Mail in der SAN-RFC822-Erweiterung des Zertifikats), damit dieser die Informationen vor der Generierung des Schlüsselpaars und der Ausstellung des zugehörigen Zertifikats bereitstellt. Außerdem werden die PKCS#12-Daten nach 3 Monaten aus der PKI-Datenbank gelöscht.

## Selbstbedienung

### Geben Sie einen Pin für Ihr PKCS#12-Schlüsselpaar an.

**Passwort für privaten Schlüssel definieren\***

Das neue Kennwort für den privaten Schlüssel

**Kennwort des privaten Schlüssels bestätigen\***

### 3.4.4 Zusätzliche Informationen für die Registrierung

Die zusätzlichen Registrierungsinformationen erfassen Metadaten über die Zertifikatsbestellung. Im Textbereich "Kommentar" können Sie weitere Kontext-Informationen bereitstellen. Diese Informationen werden zu der Zertifikatsbestellung hinzugefügt und können zu einem späteren Zeitpunkt von anderen RA-Operatoren eingesehen werden. Es können auch zu einem späteren Zeitpunkt Kommentare zu einer Zertifikatsbestellung hinzugefügt werden.

#### Textbereich für Kommentare

Der Textbereich ist immer aktiv, sodass Sie Kommentare zu Ihrem Zertifikat hinzuzufügen können. Diese Kommentare werden angezeigt, wenn Benutzer auf die Detailseite des Zertifikats navigieren.

#### ^ Zusätzliche Registrierungsinformationen

Kommentar

### 3.4.5 Zusätzliche E-Mails über Erneuerungen

Diese Option wird angezeigt, wenn der Richtlinieninstanz eine Erneuerungsregel zugewiesen ist. Alle E-Mail-Adressen in dieser Liste werden über eine Erneuerung benachrichtigt. Es kann sein, dass das von Ihnen ausgestellte Zertifikat keine E-Mail-Adresse im alternativen Antragstellernamen (RFC822) enthält. Verwenden Sie die Felder "Zusätzliche Erinnerungs-E-Mails", um Empfänger anzugeben, die Sie über die Zertifikatserneuerung informieren möchten. RA-Operatoren erhalten auf Anfrage Benachrichtigungen über die Erneuerung.

#### ^ Zusätzliche Registrierungsinformationen

Kommentar

Zusätzliche Verlängerungs-E-Mails

[+ Erneuerungs-E-Mail hinzufügen](#)

#### ^ Geschäftsbedingungen

Ich bestätige die Annahme und Einhaltung der Bedingungen des [Subscriber Agreement](#) der SwissSign AG.

[Please read and accept the terms and conditions](#)

[^ Alles zusammenklappen](#)

Zurück

Zertifikat ausstellen

### 3.4.6 Veröffentlichung des Zertifikats

Gilt nur für S/MIME-Zertifikate: Wenn die LDAP-Veröffentlichung des Zertifikats in der Zertifikatsrichtlinie aktiviert ist, können Sie die Veröffentlichung des ausgestellten Zertifikats im LDAP aktivieren oder deaktivieren. Die Informationen für den Zugriff auf das LDAP werden von SwissSign bereitgestellt. Wenn aktiviert, wird das ausgestellte Zertifikat im LDAP veröffentlicht und bei Widerruf wieder aus dem LDAP entfernt.

#### ^ Zertifikatsveröffentlichung

Zertifikat veröffentlichen

### 3.5 Bestellungen und Zertifikate

Jede Anfrage auf Ausstellung eines Zertifikats erzeugt eine Zertifikatsbestellung. Die Zertifikatsbestellung wird durch eine eindeutige Id in Form einer UUID mit dem Präfix 'ord-' identifiziert.

Beispiel: ord-4068d5fe-feab-4c15-a1f2-a0cdd9268320

Je nach Bearbeitungsstufe bei der Zertifikatserteilung wird die Zertifikatsbestellung in einen anderen Status gesetzt.

Bestellstatus des Zertifikats	Beschreibung	Verfügt über ein Zertifikat
<b>NEU</b>	Eine neue Zertifikatsbestellung wird erstellt und die Zertifikatsrichtlinie wird validiert (sowohl statisch als auch zur Laufzeit). Der Ausstellungsprozess beginnt.	nein
<b>PENDING_CSR_RENEWAL</b>	Bei der Zertifikatsbestellung handelt es sich um eine automatische Zertifikatserneuerung, für die eine Regel definiert ist. Der Empfänger des erneuerten Zertifikats muss eine CSR bereitstellen, damit die Verarbeitung fortgesetzt werden kann. Die Verarbeitungsaufgabe wird angehalten und in den Status WARTEN übertragen.	nein
<b>SCHLÜSSEL_VALIDIERUNG</b>	Das Schlüsselpaar wird validiert und optional generiert, wenn es sich bei der Zertifikatsrichtlinie um den Typ PKCS#12 handelt	nein
<b>TBS_GENERIEREN</b>	Die Strukturgenerierung des TBS („to-be-signed“) basierend auf der Richtlinie des Zertifikats. Mit Ausnahme der CT-Erweiterung ist diese Struktur unveränderlich.	nein
<b>VORAB_VALIDIERUNG</b>	Startet mehrere untergeordnete Aufträge, um den statischen Inhalt und die Laufzeitwerte erneut zu validieren, führt eine CAA-Prüfung durch (falls erforderlich), fährt mit der DNS-Eigentümerprüfung und/oder der E-Mail-Validierung des Endbenutzers (falls erforderlich) und dem Vor-Linting des TBS fort	nein
<b>VOR_AUSSTELLUNG</b>	Führt bei Bedarf den Pre-Cert-CT-Log-Eintrag aus	nein
<b>AUSSTELLUNG</b>	Das Zertifikat wird ausgestellt. Bei Bedarf wird die Poison Pill aus der CT-Protokollstruktur entfernt und die TBS-Struktur signiert, um das finale Zertifikat zu erstellen	ja
<b>NACH_VALIDIERUNG_</b>	Bei Bedarf wird ein Post-Linting durchgeführt und das CT-Protokoll veröffentlicht, sofern aktiviert.	ja
<b>FINALIZE_ISSUANCE</b>	Die Bestellabwicklung wird bereinigt und bei Bedarf werden Benachrichtigungen versendet. Eine Anfrage zur	ja

	Veröffentlichung des Zertifikats wird versendet, falls diese Option aktiviert ist.	
<b>AUSGESTELLT</b>	Die Bestellabwicklung ist abgeschlossen und die Zertifikatsbestellung wird auf den Status AUSGESTELLT gesetzt.	ja
<b>WIDERRUFEN</b>	Die Zertifikatsbestellung wird widerrufen	ja
<b>FEHLGESCHLAGEN</b>	Bestellabwicklung fehlgeschlagen. Wenn ein Zertifikat ausgestellt wird und die Verarbeitung nach der ISSUE-Phase fehlschlägt, wird das Zertifikat widerrufen	–
<b>UNBEKANNT</b>	Undefinierter Status, die Bestellung ist verloren und wird vom Scheduler bereinigt. Falls vorhanden und gültig, kann dieser das Zertifikat optional widerrufen.	–

Die Seite Bestellungen und Zertifikate listet alle Zertifikate und Bestellungen auf, die Ihren Clients zugeordnet sind. Mit der Suchfunktion oben auf der Seite können Sie die Liste filtern.

**SwissSign** Dashboard Vorlage **Bestellungen & Zertifikate** ACME Domänenüberprüfung
Mein Konto Abmeldung

**Bestellung UUID**

**Seriennummer**

**Status**

**Mandant**






**CA**

**Attribut oder Wert**

**Datumsbereich**

Spalten ein-/ausblenden

ID	Status	Mandant	CA	Subject CN	Richtlinie	Gültigkeits-Beginn	Gültigkeits-Ende	Aktionen
<div style="display: flex; align-items: center;"> <div style="margin-right: 5px;"><small>ord</small></div> <div style="font-size: 0.8em;">ord-f1537de4-52e3-4253-bad4-0ba87164c842</div> </div> <div style="display: flex; align-items: center; margin-top: 2px;"> <div style="margin-right: 5px;"><small>ser</small></div> <div style="font-size: 0.8em;">08FDC6C2968145CE7446AA45E28C31DD1EC47A50</div> </div>	ISSUED	MPKI0000107 - SwissSign AG	SwissSign RSA TLS OV ICA 2022 - 1 - STAG	ov-rsa-tls-2022-valid-cert- demo.signdemo.com	SwissSign OV SSL Gold Single-Domain	08.07.2022	08.07.2023	<input type="button" value="i"/> <input type="button" value="🔄"/> <input type="button" value="📄"/> <input type="button" value="✉"/>
<div style="display: flex; align-items: center;"> <div style="margin-right: 5px;"><small>ord</small></div> <div style="font-size: 0.8em;">ord-5d20566b-5733-4c08-8f18-7620cad3ec62</div> </div> <div style="display: flex; align-items: center; margin-top: 2px;"> <div style="margin-right: 5px;"><small>ser</small></div> <div style="font-size: 0.8em;">-</div> </div>	FAILED	MPKI0000107 - SwissSign AG	SwissSign RSA TLS DV ICA 2022 - 1 - STAG		SwissSign DV SSL Silver Single-Domain	-	-	<input type="button" value="i"/>
<div style="display: flex; align-items: center;"> <div style="margin-right: 5px;"><small>ord</small></div> <div style="font-size: 0.8em;">ord-a0afa753-3f37-4af4-bd19-c29cd7824c90</div> </div> <div style="display: flex; align-items: center; margin-top: 2px;"> <div style="margin-right: 5px;"><small>ser</small></div> <div style="font-size: 0.8em;">28F44D98BC2D43C8BE89188DACF9CBAC189A9183</div> </div>	ISSUED	MPKI0000107 - SwissSign AG	SwissSign RSA TLS OV ICA 2022 - 1 - STAG	ov-rsa-tls-2022-expired-cert- demo.signdemo.com	SwissSign OV SSL Gold Single-Domain (1 day validity for demopages)	08.07.2022	09.07.2022	<input type="button" value="i"/> <input type="button" value="🔄"/> <input type="button" value="📄"/> <input type="button" value="✉"/>

Spalte	Beschreibung
<b>ID</b>	Enthält die Bestell-UUID und die Seriennummer des Zertifikats.
<b>Status</b>	Enthält den Status des Zertifikats.
<b>Client</b>	Enthält den Client, der zum Ausstellen dieses Zertifikats verwendet wurde.
<b>CA</b>	Enthält die Zertifizierungsstelle, die zum Ausstellen dieses Zertifikats verwendet wurde.
<b>Antragsteller-CN</b>	Enthält den allgemeinen Antragstellernamen des Zertifikats.
<b>Policy</b>	Enthält die Richtlinieninstanz (Zertifikatsprodukt), die zum Ausstellen dieses Zertifikats verwendet wurde.
<b>Start Validity</b>	Enthält das Startdatum der Zertifikatslaufzeit.
<b>End Validity</b>	Enthält das Enddatum der Zertifikatslaufzeit.
	Leitet Sie zur Seite der Zertifikatsbestellung weiter. Zeigt die Liste der Tasks an, die für die Zertifikatsbestellung ausgeführt wurden.
	Mit dieser Schaltfläche versenden Sie eine Anfrage zum Widerrufen eines Zertifikats.
	Mit dieser Schaltfläche versenden Sie eine Anfrage zur Veröffentlichung eines Zertifikats. Diese Option ist verfügbar, wenn für das Zertifikat die Veröffentlichung aktiviert ist.
	Das Zertifikat im PEM-Format herunterladen.
	Leitet Sie zu der Seite mit den Zertifikatsdaten weiter.


### 3.5.1 Bestelldetails des Zertifikats

Die Seite mit den Daten der Zertifikatsbestellung ist in zwei Abschnitte unterteilt:

1. Ausgestelltes Zertifikat
2. Zugehörige Bestellabwicklungstasks und ihr jeweiliger Status

#### 3.5.1.1 Ausgestelltes Zertifikat

Dieser Abschnitt enthält das der Bestellung zugeordnete Zertifikat. Die Bestellung muss über den Status ISSUED verfügen.

 [Dashboard](#) [Vorlage](#) [Bestellungen & Zertifikate](#) [ACME](#) [Domänenüberprüfung](#) [Mein Konto](#) [Abmeldung](#)

**ISSUED** Zertifikatsbestellung

### Zertifikate

---

**Zertifikatsinformationen**

[Zertifikat herunterladen \(PEM\)](#) [Zertifikat herunterladen \(DER\)](#) [Zertifikatskette herunterladen \(PKCS#7\)](#)

Auftragsnummer	ord-f1537de4-52e3-4253-bad4-0ba87164c842
Auftragstyp	Regular
Produktname	SwissSign OV SSL Gold Single-Domain
Ausgestellt von	MPKI0000107 AutoRAO (MPKI0000107.AutoRAO)
Protokoll	rao
SHA1-Fingerprint	3aa0868ef206b997b1538573e18d5c3185c8fbf7
SHA256-Fingerprint	b15e92d6f6c0456e8c7336dbba529a14b7a9db35f76e1fba46570fdd7b848b53
Zertifikatsseriennummer	08FDC6C2968145CE7446AA45E20C31DD1EC47A50
Subject	C=CH,ST=ZH,L=Glattbrugg,O=SwissSign AG,CN=ov-rsa-tls-2022-valid-cert-demo.signdemo.com
Aussteller	C=CH,O=SwissSign AG,CN=SwissSign RSA TLS OV ICA 2022 - 1 - STAG
Gültigkeit	08.07.2022 12:59 - 08.07.2023 12:59

**Zertifikatserweiterungen**

### 3.5.1.2 Tasks zur Bearbeitung von Zertifikatsbestellungen















Im Abschnitt Aufgaben (Bestellabwicklungstasks) werden die für diese Bestellung ausgeführten Aufgaben mit ihrem jeweiligen Status aufgelistet. Die Daten jeder Aufgabe können einzeln aufgerufen werden, indem Sie auf die Schaltfläche klicken, die sich in der Spalte "Aktion" der Tabelle befindet.

Aufgabenstatus	Beschreibung
<b>WAITING</b>	Aufgabe wurde angelegt aber nicht eingeplant, beispielsweise wenn eine übergeordnete Aufgabe darauf wartet, dass untergeordnete Aufgaben beendet werden
<b>PENDING</b>	Aufgabe wurde erstellt und befindet sich in der Warteschlange
<b>PROCESSING</b>	Aufgabe befindet sich in der Warteschlange und wird verarbeitet
<b>SUCCESS</b>	Aufgabe wurde erfolgreich verarbeitet
<b>FAILED</b>	Aufgabe ist fehlgeschlagen
<b>SCHEDULE_REQUEST</b>	Aufgabe wurde erstellt aber noch nicht an die Warteschlange gesendet
<b>SCHEDULE_RESPONSE</b>	Aufgabe wurde verarbeitet, hat aber noch keine Antwort von der Warteschlange erhalten
<b>RETRY</b>	Aufgabe wurde verarbeitet und für Wiederholung markiert







Liste der Aufgaben und ihres jeweiligen Status, die während der Bestellabwicklung ausgeführt wurden

### Jobs

Status	Typ	Geplant am	Antwort	Aktionen
SUCCESS	Submit certificate order	13.07.2022 15:54:21.087 (5.655s)		
SUCCESS	Certificate key validation	13.07.2022 15:54:29.824 (5.632s)		
SUCCESS	Authorization	13.07.2022 15:54:37.899 (5.902s)	No Authorization on issuance required	
SUCCESS	Generate TBS certificate	13.07.2022 15:54:46.715 (2.772s)		
SUCCESS	Policy validation	13.07.2022 15:54:52.500 (1.956s)		
SUCCESS	Certificate pre validation	13.07.2022 15:54:52.500 (2.889s)		
SUCCESS	Pre issue certificate	13.07.2022 15:55:04.855 (2.652s)		
SUCCESS	Issue certificate	13.07.2022 15:55:10.110 (4.830s)		
SUCCESS	Post issue certificate	13.07.2022 15:55:17.481 (1.923s)		
SUCCESS	Notify Issued Certificate	13.07.2022 15:55:21.816 (11.446s)		
SUCCESS	Finalize issue certificate	13.07.2022 15:55:21.816 (1.754s)		
SUCCESS	Publish certificate order	13.07.2022 15:55:41.540 (2.894s)	Certificate rule publishing is disabled for certificate with Subject 'CN= [REDACTED]' and Serial '568B6BA04CB4EDF7CA07790F5E29D376481DF445'	

Wenn die Bestellabwicklung E-Mail-Benachrichtigungen an Empfänger sendet, wird die Liste der gesendeten Benachrichtigungen unterhalb der Aufgaben angezeigt. Als RA-Operator können Sie die Benachrichtigung erneut versenden, wenn der SMTP-Server oder das SMTP-Relay die E-Mail nicht zugestellt hat.

### Emails

Status	Typ	Erstellt am	Aktionen
SENT	ISSUANCE_EMAIL_ENDUSER	13.07.2022 15:55	
SENT	ISSUANCE_EMAIL_RAO	13.07.2022 15:55	
SENT	ISSUANCE_EMAIL_RAO	13.07.2022 15:55	
SENT	ISSUANCE_EMAIL_RAO	13.07.2022 15:55	

## 3.5.2 Zertifikat revozieren

Sie können ein Zertifikat widerrufen, indem Sie auf die Widerruf-Schaltfläche in der Spalte "Aktionen" in der Tabelle "Bestellungen und Zertifikate" klicken. Nachdem Sie auf die Schaltfläche geklickt haben, werden Sie in einem Popup-Dialog aufgefordert, die Aktion zu bestätigen. Standardmässig ist als Revozierungsgrund "Unspecified" ausgewählt. Erklärungen zu den verschiedenen Revozierungsgründen finden Sie im [Subscriber Agreement](#) unter Annex A.

The screenshot shows the SwissSign dashboard with a table of certificates. A modal dialog is open, asking for confirmation to revoke a certificate with the serial number 205C8D49A17C6EA97D71C34F3903945025050D77. The dialog also allows selecting a reason for revocation, with 'Unspecified' currently selected. The table below contains the following data:

Order ID	Serial	Status	Organization	Product	Issued	Expires	Actions
ord-86c86b25-4645-4111-9fc9-5daa91ea567d	56310687E2C27F2B828124D9CFA6751208640536	ISSUED	MPKI0000117 - SwissSign AG	SwissSign EV SSL Single-Domain	15.07.2022	15.07.2023	[i] [🔄] [🗑️] [🔗]
ord-882ec9e7-ae5-4266-8eb6-cb6fafc47a5d	7AD5840A80A86C25E083C7D8385ACF0CB388957	ISSUED	MPKI0000117 - SwissSign AG	SwissSign DIV SSL Single-Domain (y validity for page)	15.07.2022	16.07.2022	[i] [🔄] [🗑️]
ord-5c1468d9-f0d9-4092-bw30-0c5e3ad32bc7	5B9607E0566457E398FF9F6F068E9ED077F83F88	ISSUED	MPKI0000117 - SwissSign AG	SwissSign DIV SSL Silver Single-Domain	14.07.2022	14.07.2023	[i] [🔄] [🗑️] [🔗]
ord-1ff7dc31-eb7e-4324-b37f-9bbb19f2ad53	205C8D49A17C6EA97D71C34F3903945025050D77	ISSUED	MPKI0000117 - SwissSign AG	SwissSign RSA SMIME NCP extended ICA 2022 - 1	12.07.2022	12.07.2023	[i] [🔄] [🗑️] [🔗]
ord-793dc477-4412-4038-8ca3-31ab2df9c229	1F1F8E08C272F93137EA93837840E14C08B1288B	ISSUED	MPKI0000117 - SwissSign AG	SwissSign RSA SMIME NCP ICA 2022 - 1	12.07.2022	12.07.2023	[i] [🔄] [🗑️] [🔗]
ord-8a6da496-f82c-4677-ac7b-33166d762baa	7BE3A5B99834187288C53E728BACEEC7DDE87162	ISSUED	MPKI0000117 - SwissSign AG	SwissSign RSA SMIME LCP ICA 2022 - 1	12.07.2022	12.07.2023	[i] [🔄] [🗑️] [🔗]

Bestätigen Sie den Widerruf des Zertifikats, indem Sie auf die Schaltfläche "Ja" klicken. Hinweis: Die Widerrufsaktion sendet eine Anfrage an die Zertifizierungsstelle und wenn für das ausgewählte Zertifikat eine Regel definiert ist, kann es sein, dass eine Autorisierung ausgelöst wird. Nach dem Widerruf ist die Widerruf-Schaltfläche nicht mehr verfügbar.

### 3.5.3 Zertifikat veröffentlichen

Um ein Zertifikat zu veröffentlichen, klicken Sie auf die Veröffentlichen-Schaltfläche in der Spalte "Aktionen" in der Tabelle "Bestellungen und Zertifikate". Nachdem Sie auf die Schaltfläche geklickt haben, werden Sie in einem Popup-Dialog aufgefordert, die Veröffentlichung des Zertifikats zu bestätigen.

Bitte beachten Sie, dass diese Veröffentlichungs-Aktion nur dann verfügbar ist, wenn die Veröffentlichung in LDAP für das ausgewählte Zertifikat aktiviert ist und die Berechtigung dazu erteilt wurde.

The screenshot shows the SwissPKI web interface. A modal dialog box is open, asking for confirmation to publish a certificate with serial number 7E577165307F51A16CF7AF6F53A7CF0FD4FA046D7. The dialog has 'No' and 'Yes' buttons. In the background, a table lists certificates with columns for ID, Status, Client, CA, Subject CN, Policy, Start validity, End validity, and Actions. The table contains several rows with different statuses like 'ISSUED', 'REVOKED', and 'PENDING AUTH'.

ID	Status	Client	CA	Subject CN	Policy	Start validity	End validity	Actions
ord-b3759e7b-038f-4811-aafe-483419fd1630 6e4ef3ad48a87c4835acf6796d2c8469806a2a0a	ISSUED	Sample Client A	SwissPKI Staging Issuing CA RSA 4096 (HSM)	Sample Doc PKCS#10 Renewal Authorization	Sample PKCS#10 Renewal Authorization	19.01.2022	29.01.2022	[i] [G] [M] [U] [E]
ord-13e31978-0808-4683-92dc-7c9f7d95121f 7780d46252fffe93d3c95da002f881a74dc4074	ISSUED	Sample Client A	SwissPKI Staging Issuing CA RSA 4096 (HSM)	Sample Doc PKCS#10 Renewal Authorization	Sample PKCS#10 Renewal Authorization	19.01.2022	18.02.2022	[i] [G] [M] [U] [E]
ord-46f239bb-24bf-4512-4455-c6778c7ad716 7e577165307f51a16cf7af6f53a7cf0fd4fa046d	REVOKED	Sample Client A	SwissPKI Staging Issuing CA RSA 4096 (HSM)	Sample Doc PKCS#10 Issuance Authorization	Sample PKCS#10 Renewal Authorization	19.01.2022	18.02.2022	[i] [G] [M] [U] [E]
ord-e6b86a4c-5f60-4e1d-a384-8ea56022b4d5 432a517002d0ef31d358f67ed8809c552183da27	ISSUED	Sample Client A	SwissPKI Staging Issuing CA RSA 4096 (HSM)	Sample PKCS#10 Renewal Authorization	Sample PKCS#10 Renewal Authorization	19.01.2022	18.02.2022	[i] [G] [M] [U] [E]
ord-76ab8ac8-b3be-480c-b578-ac7e2e4f4f69 37cd32200483e1d5793152583f77b77508ea61d7	REVOKED	Sample Client B	SwissPKI Staging Issuing CA RSA 4096 (HSM)	Sample Doc PKCS#10 Issuance Authorization	Sample PKCS#10 Renewal Authorization	19.01.2022	18.02.2022	[i] [G] [M] [U] [E]
ord-f078986d-f138-467e-98da-8a44f254c766 4e04c179add085045cfe94843e9a02c41edc66a5	REVOKED	Sample Client B	SwissPKI Staging Issuing CA RSA 4096 (HSM)	Sample Doc PKCS#10 Renewal Authorization	Sample PKCS#10 Renewal Authorization	19.01.2022	18.02.2022	[i] [G] [M] [U] [E]
ord-3387f068-630e-4aa6-bb16-2192feaedf9a -	PENDING AUTH	Sample Client A	SwissPKI Staging Issuing CA RSA 4096 (HSM)	-	Sample PKCS#12	-	-	[i]
ord-34f98586-77a2-4c7f-9b7e-fa9b7ab9db64 370e32c48ef8586ec8f89789294a789e804b8eb1	REVOKED	Sample Client A	SwissPKI Staging Issuing CA RSA 4096 (HSM)	Sample Doc PKCS#10 Revocation Authorization	Sample PKCS#10 Revocation Authorization	19.01.2022	18.02.2022	[i] [G] [M] [U] [E]

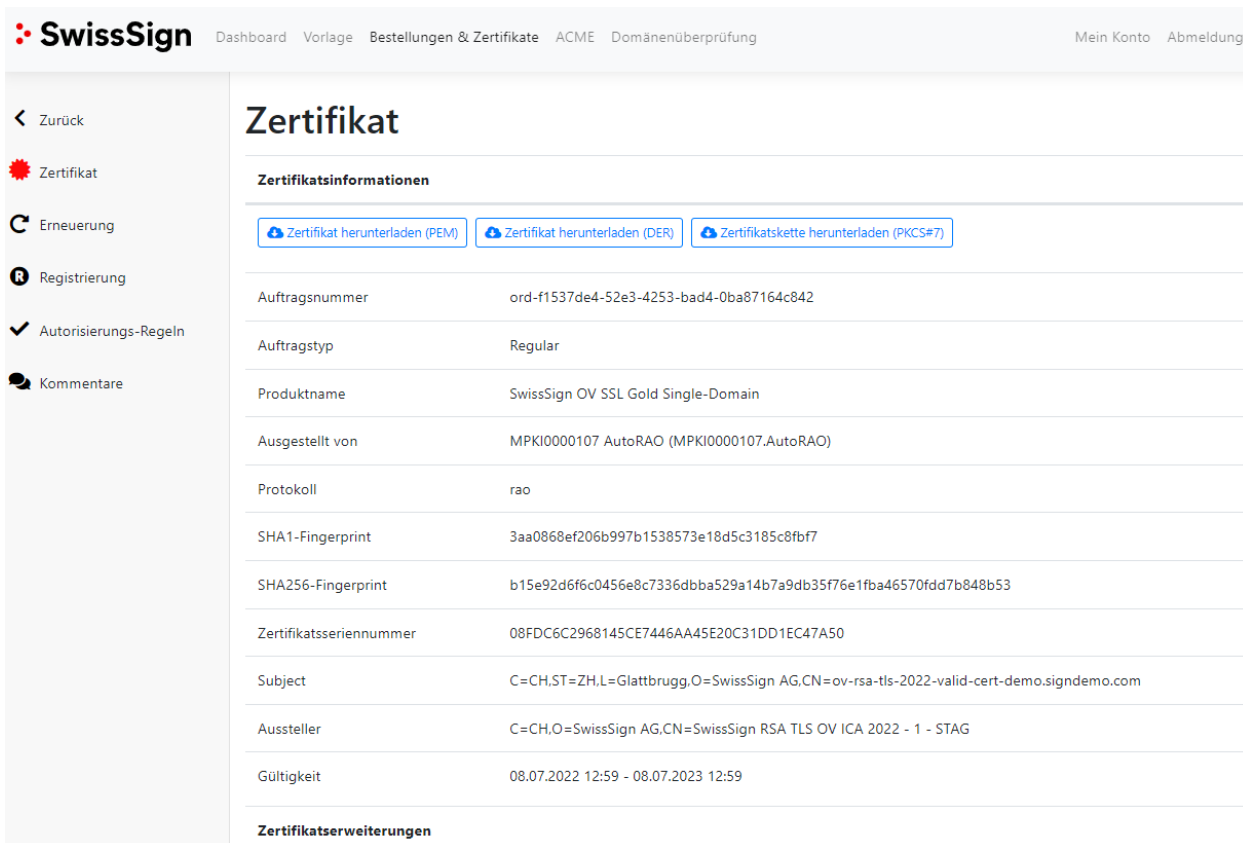
### 3.5.4 Informationen zum Zertifikat

Wenn Sie auf die Bearbeiten-Schaltfläche in der Spalte "Aktionen" in der Tabelle "Bestellungen und Zertifikate" klicken, werden Sie auf die Detailseite des Zertifikats weitergeleitet. Über das linke Menü erhalten Sie Zugriff auf die Zertifikat-Informationen zu den folgenden Punkten:

- Details zum Zertifikat mit Download-Optionen
- Informationen zur Zertifikatserneuerung
- Registrierungsdokumente des Zertifikats
- Empfänger von Erinnerungen bezüglich des Zertifikatsschlüssels
- Regeln für die Zertifikatsautorisierung
- Zertifikatskommentare

#### 3.5.4.1 Einzelheiten zum Zertifikat

In der Zertifikats-Detailansicht können Sie die Zertifikate in den verschiedenen Formaten (PEM, DER und PKCS#7) herunterladen. Ausserdem werden allgemeine Informationen zur Zertifikatsbestellung und zu den Fingerabdrücken des Zertifikats angezeigt.



The screenshot shows the SwissSign user interface for a certificate detail page. The page title is "Zertifikat". On the left is a navigation menu with options: Zurück, Zertifikat (selected), Erneuerung, Registrierung, Autorisierungs-Regeln, and Kommentare. The main content area is titled "Zertifikatsinformationen" and contains three download buttons: "Zertifikat herunterladen (PEM)", "Zertifikat herunterladen (DER)", and "Zertifikatskette herunterladen (PKCS#7)". Below these buttons is a table of certificate details.

Auftragsnummer	ord-f1537de4-52e3-4253-bad4-0ba87164c842
Auftragstyp	Regular
Produktname	SwissSign OV SSL Gold Single-Domain
Ausgestellt von	MPKI0000107 AutoRAO (MPKI0000107.AutoRAO)
Protokoll	rao
SHA1-Fingerprint	3aa0868ef206b997b1538573e18d5c3185c8fbf7
SHA256-Fingerprint	b15e92d6f6c045e8c7336dbba529a14b7a9db35f76e1fba46570fdd7b848b53
Zertifikatsseriennummer	08FDC6C2968145CE7446AA45E20C31DD1EC47A50
Subject	C=CH,ST=ZH,L=Glattbrugg,O=SwissSign AG,CN=ov-rsa-tls-2022-valid-cert-demo.signdemo.com
Aussteller	C=CH,O=SwissSign AG,CN=SwissSign RSA TLS OV ICA 2022 - 1 - STAG
Gültigkeit	08.07.2022 12:59 - 08.07.2023 12:59

Below the table, there is a section titled "Zertifikatserweiterungen" which is currently empty.


### 3.5.4.2 Zertifikatserneuerung

Wenn für das ausgewählte Zertifikat eine Regel für die automatische Zertifikatserneuerung definiert ist, finden Sie hier Informationen zu:

1. Informationen zur Erneuerung des Zertifikats  
Informationen über die Bestellkennung, den Erneuerungsstatus und optional das Erneuerungsdatum
2. Informationen zur Erneuerungsregel  
Enthält Details zur Erneuerungsregel, die dem Zertifikat zugeordnet sind:
  - Name der Erneuerungsregel
  - Automatische/manuelle Erneuerung
  - Anzahl der erlaubten Erneuerungen
  - Wie viele Tage vor Ablauf der Zertifikatsgültigkeit die Erneuerung durchgeführt wird
  - Ob nach der erfolgreichen Erneuerung des Zertifikats ein Widerruf erfolgt
3. Liste von vorhergehenden Zertifikaten (erneuert)  
Hier können Sie zwischen vorhergehenden/nächsten Zertifikatsbestellungen navigieren, indem Sie auf die Schaltflächen Vorherige/Nächste klicken oder zu den vorhergehenden Zertifikaten blättern, indem Sie auf die Seriennummer des Zertifikats klicken
4. Liste mit zusätzlichen Erneuerungs-E-Mails  
Diese Liste enthält zusätzliche Erneuerungs-E-Mail-Adressen, an die Erneuerungsbenachrichtigungen gesendet werden. Diese sind nützlich für Zertifikate ohne SAN RFC822, bei denen trotzdem Benachrichtigungen an andere Empfänger gesendet werden müssen.

#### Erneuerung |

Erneuerungsinformationen	
Auftragsnummer	ord-a7f95484-f388-457b-8600-44c12c6447e9
Erneuerungsstatus	WAIT_ON_RENEWAL
Verlängert am	
Informationen zur Erneuerungsregel	
Erneuerungsregel	renewal.auto.rao_recipient
Automatische Erneuerung	true
Anzahl der möglichen Erneuerungen	unbegrenzt
Erneuerung	Erneuerung '364' Tage vor Ablauf des Zertifikats
Schlüssel bei Erneuerung erneuern	true

Zusätzliche Verlängerungs-E-Mails	Aktionen
	

### 3.5.4.3 Veröffentlichung des Zertifikats

Wenn das Zertifikat mit einem oder mehreren Publishern verknüpft ist, finden Sie auf dieser Seite Informationen zu den verschiedenen Zertifikat-Veröffentlichungen. Jedes Veröffentlichungsereignis in Bezug auf das Zertifikat wird hier aufgelistet. Ausserdem haben Sie die Möglichkeit, die Veröffentlichung aufzuheben.

Nachdem Sie bei dem Zertifikat, das Sie überprüfen möchten, auf die "Bearbeiten"-Schaltfläche geklickt haben, können Sie den Veröffentlichungsstatus einsehen und bei Bedarf die Veröffentlichung des Zertifikats aufzuheben.



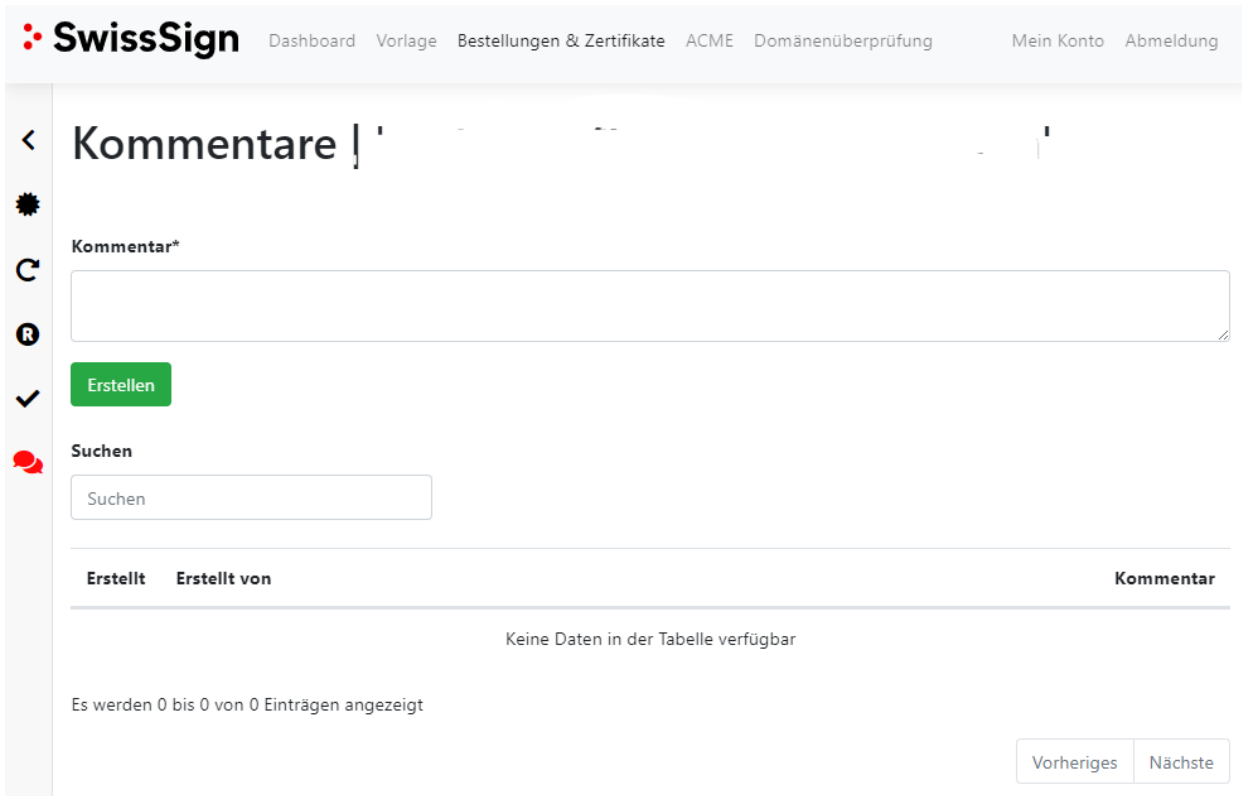
Created	Status	Type	Name	Actions
01.02.2022 06:50	UNPUBLISHED	LDAP	ldap.swisspki.com	
01.02.2022 06:50	PUBLISHED	LDAP	ldap.swisspki.com	

Showing 1 to 2 of 2 entries

Previous **1** Next

### 3.5.4.4 Kommentare

Die Registerkarte "Kommentare" der Zertifikatsdetails zeigt eine Liste mit allen Kommentaren zu diesem Zertifikat an. Hier können Sie einen neuen Kommentar hinzufügen, indem Sie den Textbereich oben auf der Seite ausfüllen und auf die Schaltfläche "Erstellen" klicken.



Dashboard Vorlage Bestellungen & Zertifikate ACME Domänenüberprüfung Mein Konto Abmeldung

## Kommentare | 'Sample End User'

Kommentar\*

**Erstellen**

Suchen

Erstellt	Erstellt von	Kommentar
Keine Daten in der Tabelle verfügbar		

Es werden 0 bis 0 von 0 Einträgen angezeigt

Vorheriges Nächste

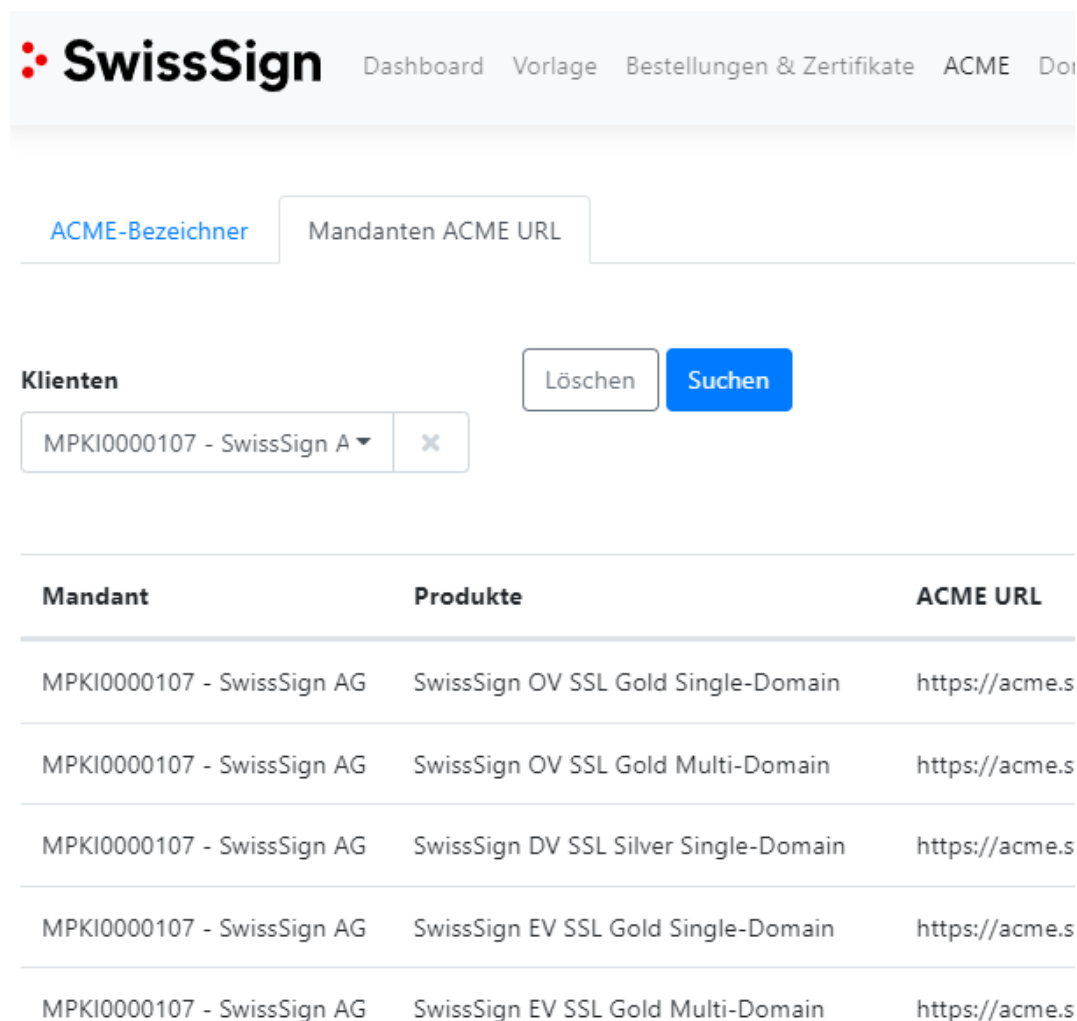
### 3.6 ACME

Als RA-Operator können Sie Zertifikate über das ACME-Protokoll ausstellen (wird typischerweise für die automatische \*Nix-Serveranmeldung verwendet) und Sie haben Zugriff auf den ACME-Bereich.

In diesem Abschnitt finden Sie Informationen über die registrierten Domainnamen, das für die Registrierung verwendete Protokoll (dns-01 oder http-01), die Gültigkeit der ACME-Challenge-Tokens und den Client, der die Registrierung angefordert hat.

Bitte beachten Sie: Die Ausstellung von SSL/TLS-*Platzhalter*-Zertifikaten (ausgestellt für FQDNs mit einem vorangestellten Asterisk, z. B. \*.example.com) ist NICHT möglich, wenn das ACME-Protokoll aktiviert ist. Regulatorische Bestimmungen verbieten das ACME-Protokoll für Platzhalter-Zertifikate.

- Wenn Sie ACME nutzen, können Sie jede Client-Software verwenden, die mit diesem Standard kompatibel ist. Wir empfehlen jedoch die getestete Open-Source-Client-Anwendung Certbot Client (ACME Client von Red Hat Enterprise Linux) und
- Für Microsoft Internet Information Server (IIS) können Sie auch den ACMESharp-Client verwenden.



The screenshot shows the SwissSign ACME management interface. At the top, there is a navigation bar with the SwissSign logo and menu items: Dashboard, Vorlage, Bestellungen & Zertifikate, ACME, and Domains. Below the navigation bar, there are two input fields: "ACME-Bezeichner" and "Mandanten ACME URL". Underneath these fields, there is a section titled "Klienten" with a search bar containing "MPKI0000107 - SwissSign A" and buttons for "Löschen" and "Suchen". Below the search section is a table with three columns: Mandant, Produkte, and ACME URL. The table contains five rows of data.

Mandant	Produkte	ACME URL
MPKI0000107 - SwissSign AG	SwissSign OV SSL Gold Single-Domain	https://acme.s
MPKI0000107 - SwissSign AG	SwissSign OV SSL Gold Multi-Domain	https://acme.s
MPKI0000107 - SwissSign AG	SwissSign DV SSL Silver Single-Domain	https://acme.s
MPKI0000107 - SwissSign AG	SwissSign EV SSL Gold Single-Domain	https://acme.s
MPKI0000107 - SwissSign AG	SwissSign EV SSL Gold Multi-Domain	https://acme.s

Hinweis: Zertifikate, die über das ACME-Protokoll ausgestellt wurden, können Sie in "Bestellungen und Zertifikate" durchsuchen.

## 3.7 Domänenüberprüfung (Domain-Validierung)

### 3.7.1 DNS Vor-Validierung

Bei den Richtlinienvorlagen, die über eine "DNS-Eigentümerregel" verfügen, müssen die Domainnamen bei der Ausstellung des Zertifikats validiert werden. Um Arbeitsschritte einzusparen, kann der Kunde eine Domain vorab validieren (i. d. R. validiert der Kunde seine Basis- bzw. Haupt-Domain), sodass er in der Lage ist, Zertifikate für diese Domain und die zugehörigen Subdomains auszustellen, ohne jede Zertifikatsanfrage einzeln validieren zu müssen.

Durch Klicken auf die Schaltfläche "Hinzufügen" kann ein RA-Operator eine neue, vorvalidierte Domain eingeben



Feld	Beschreibung
Client	Client, für den die vorab validierte Domain hinzugefügt werden soll. HINWEIS: Da ein RA-Operator Zugriff auf mehr als nur einen Client haben kann, muss der Client hier aufgeführt werden
Domäne	Name der Domain, die vorab validiert werden soll

## Domänenüberprüfung

### Mandant\*

MPKI0000104 - SwissSign AG

Wählen Sie den Mandant aus, für den Sie die Domäne vorvalidieren möchten

### Domäne\*

[REDACTED]

Geben Sie die Domäne ein, die überprüft werden soll

Die Domain wurde erfolgreich auf **03.06.2022 16:00** mit der Validierungsmethode **CAB\_DNS** validiert

### Informationen zur Domänenüberprüfung

Status

valid

DNS-Validierungs-Token

Domäne erneut validieren

Validierungsergebnis

CAB\_DNS validation PASSED: Domain 'digital-id.ch' contains a TXT record with the value 'swiss-pki=WPsv7NmF5yxNybKLiy81cyd3cRw'

Zeitpunkt der Validierung

03.06.2022 16:00 ( CAB\_DNS )

Zurück

Für die DNS-Eigentümerprüfung mit öffentlichem Vertrauen kopieren Sie das DNS-Challenge-Token in den DNS-Server. Auf der Seite wird eine Anleitung dazu angezeigt. Als Operator können Sie den DNS-Eintrag gegebenenfalls manuell validieren, indem Sie auf "Domaineigentümerschaft validieren" klicken. Klicken Sie auf "Neues Validierungstoken generieren", um eine neue Challenge zu generieren. Folgen Sie den Anweisungen auf dem Bildschirm für die von Ihnen erstellte Domain. Das Token ist 30 Tage lang gültig. Danach muss ein neues Token generiert werden.

### 3.7.2 Ausstehende Validierung von Zertifikatsbestellungen

In diesem Bereich erhält der RA-Operator einen Überblick über die ausstehenden Domaininvalidierungen für seine Zertifikatsbestellungen. Klicken Sie auf die Schaltfläche "Bearbeiten", um die Details der Validierung anzuzeigen.

SwissSign Dashboard Vorlage Bestellungen & Zertifikate ACME Domänenüberprüfung Mein Konto Abmeldung

## Domänenüberprüfung

Pending Certificate order validations [Pre validated domains](#)

In diesem Abschnitt können Sie Ihre Domains vorvalidieren, so dass Sie sie während des Ausstellungsprozesses nicht erneut validieren müssen.

Certificate Order UUID  Domain

Zertifikatsbestellstatus  Mandant

Nur ausstehende Validierungen

Löschen

Validierungsstatus	Auftragsstatus	Zertifikatsauftrags-UUID	Domain	Aktionen
SUCCESS	ISSUED	ord-10f79a07-5051-40d0-8237-621fac4e8dfe	test.signdemo.com	<a href="#">✎</a>
SUCCESS	ISSUED	ord-118cd2e3-e61b-437b-9684-b0c6ca69a371	swissign.com	<a href="#">✎</a>
SUCCESS	ISSUED	ord-133c0df5-1d0d-4f4e-8090-2898db3e68c0	swissign.com	<a href="#">✎</a>
SUCCESS	ISSUED	ord-1437c284-c21e-473e-bfe3-c612f3949331	test.signdemo.com	<a href="#">✎</a>
PENDING	PRE_VALIDATION	ord-14660b1f-8321-4237-ae00-80bc42648ce0	swissign.com	<a href="#">✎</a>

Im Bearbeitungsfenster werden die Validierungsmethoden und Tokens angezeigt, die für die Validierung der Domain verwendet werden können. Nachdem Sie die korrekten Geheimnisse im DNS oder auf dem Webserver eingestellt haben, können Sie die Domain mit der Aktion auf der rechten Seite der Tabelle manuell validieren.

Alternativ wird die DNS-Eigentümerprüfung einmal pro Stunde automatisch über einen Hintergrundjob durchgeführt. Die Validierung der Domain muss innerhalb von 30 Tagen erfolgen.

SwissSign Dashboard Vorlage Bestellungen & Zertifikate ACME Domänenüberprüfung Mein Konto Abmeldung

## PRE\_VALIDATION Zertifikatsbestellung

### Domaininvalidierungen


Status	Domäne	Validierungsinformationen	Ergebnis	Letzte Überprüfung	Aktionen
PENDING	swissign.com	DNS: Add TXT entry with swissign-check=MhZTb_d26a3-fxJ-udRbnBTzrvY	CAB_DNS validation FAILED: Domain 'swissign.com' contains a TXT record with value 'swissign-check=nrr9RHkG6Tpp9MJeZVNvr31kDOlpylLFAK674MT8kx' but it does not match the expected value swissign-check=MhZTb_d26a3-fxJ-udRbnBTzrvY		<a href="#">✎</a>




## 3.8 Konto

### 3.8.1 Kontodaten

Auf dieser Seite können Sie Ihre Kontodaten überprüfen. Folgende Felder werden angezeigt:

Felder	Beschreibung
<b>Benutzername</b>	Ihr Benutzername
<b>E-Mail</b>	Die mit Ihrem Konto verbundene E-Mail-Adresse
<b>SwissID Subjekt</b>	Die mit Ihrem Konto verknüpfte SwissID
<b>Vorname</b>	Ihr Vorname
<b>Nachname</b>	Ihr Nachname
<b>Titel</b>	Ihr Titel
<b>Sprache</b>	Ihre bevorzugte Sprache
<b>Benachrichtigungen stumm schalten</b>	<p>Gilt für RA-Operator-Rollen. Als RA-Operator möchten Sie unter Umständen Benachrichtigungen von anderen RA-Operatoren innerhalb des Teams stumm schalten. Benachrichtigungen können Sie auf Ihrer Kontoseite aktivieren/deaktivieren.</p> <p><b>Hinweis:</b> Sie müssen über die erforderlichen Berechtigungen verfügen, um Ihre Kontoinformationen zu ändern.</p>


Dashboard Vorlage Bestellungen & Zertifikate ACME Domänenüberprüfung
Mein Konto Abmeldung

-  Konto
-  Berechtigungen
-  Service API-Schlüssel

## Konto | [Redacted]

**Benutzername\***

**E-Mail\***

**SwissID Subjekt**

**Sprache**

**Titel**

**Nachname\***

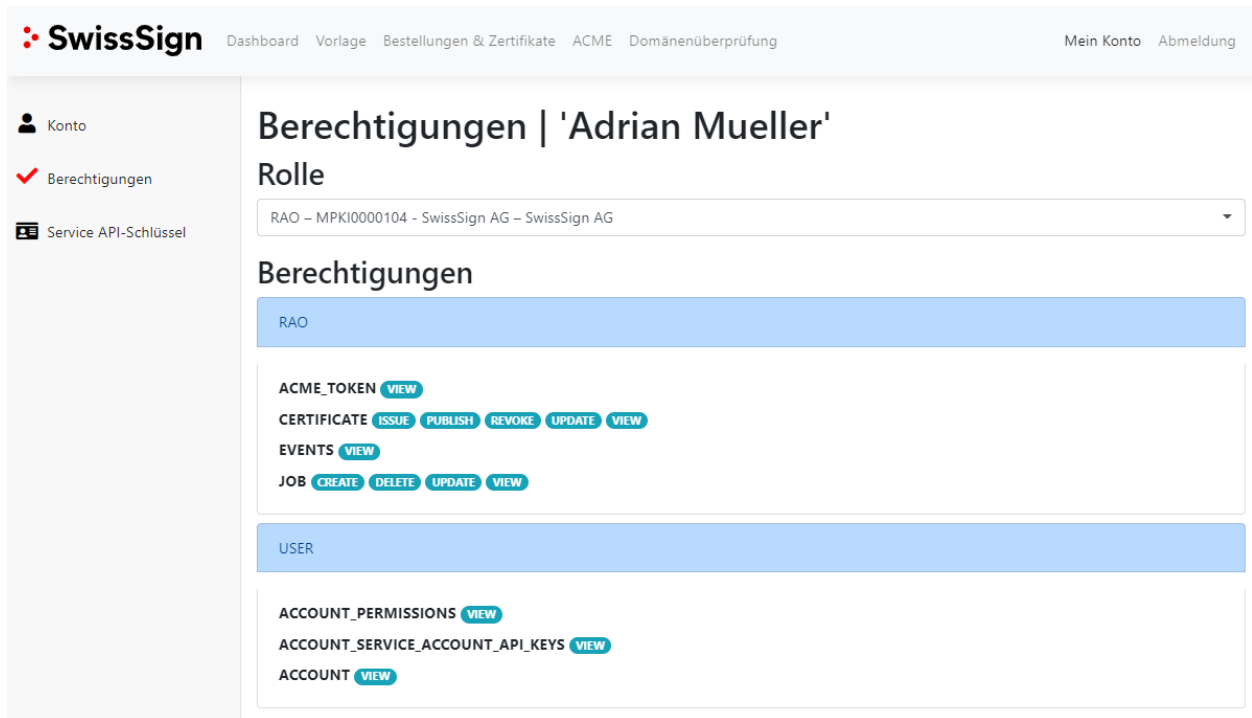
**Vorname\***

**Nachname\***

- Stummschaltung von Erneuerungsmeldungen anderer RAOs
- Stummschalten von Ausgabemeldungen von anderen RAOs
- Stummschaltung von Widerrufsbenechtigungen anderer RAOs
- Stummschaltung von DNS-Änderungsbenechtigungen von anderen RAOs
- Autorisierungsbenechtigungen von anderen RAOs stummschalten
- Stummschaltung von Wiederherstellungsbenechtigungen von anderen RAOs
- Stummschaltung von E-Mail-Validierungsbenechtigungen für Endbenutzer von anderen RAOs

### 3.8.2 Berechtigungen

Die Kontoberechtigungen zeigen die Berechtigungen an, jeweils für die Ihrem Benutzerkonto zugewiesenen Rollen zugewiesen wurden. Wählen Sie aus dem Dropdown-Menü „Rolle“ die Rollen aus, um die Ihnen zugewiesenen Berechtigungen anzuzeigen. Sie können Ihre eigenen Berechtigungen/Rollen nicht bearbeiten.



The screenshot shows the SwissSign user interface. At the top, there is a navigation bar with the SwissSign logo, a dashboard menu (Dashboard, Vorlage, Bestellungen & Zertifikate, ACME, Domänenüberprüfung), and user account options (Mein Konto, Abmeldung). On the left, a sidebar contains navigation items: 'Konto', 'Berechtigungen' (highlighted with a red checkmark), and 'Service API-Schlüssel'. The main content area is titled 'Berechtigungen | 'Adrian Mueller'' and 'Rolle'. A dropdown menu shows the selected role: 'RAO - MPKI0000104 - SwissSign AG - SwissSign AG'. Below this, the 'Berechtigungen' section is divided into two role categories: 'RAO' and 'USER'. The 'RAO' role has permissions for ACME\_TOKEN (VIEW), CERTIFICATE (ISSUE, PUBLISH, REVOKE, UPDATE, VIEW), EVENTS (VIEW), and JOB (CREATE, DELETE, UPDATE, VIEW). The 'USER' role has permissions for ACCOUNT\_PERMISSIONS (VIEW), ACCOUNT\_SERVICE\_ACCOUNT\_API\_KEYS (VIEW), and ACCOUNT (VIEW).

## 3.8.3 Service-API-Schlüssel

Der Service-API-Schlüssel wird unter dem entsprechenden Menü angezeigt. Der Service-API-Schlüssel wird für die Authentifizierung eines automatischen Clients verwendet, der über die RA API auf das System zugreift. Der Service-API-Schlüssel für eine Managed PKI wird automatisch generiert.



The screenshot shows a web interface for managing Service API Keys. On the left is a navigation menu with three items: 'Konto' (Account), 'Berechtigungen' (Permissions), and 'Service API-Schlüssel' (Service API Keys), which is currently selected. The main content area is titled 'Service API-Schlüssel' and contains a subtitle 'Liste der Servicekonten pro Client mit API-Schlüsseln'. Below this is a table with three columns: 'Client', 'Dienstkonto', and 'API-Schlüssel'. The table contains one entry for 'MPKI0000104 - SwissSign AG' with a service account of 'MPKI0000104.AutoRAO' and a redacted API key.

Client	Dienstkonto	API-Schlüssel
MPKI0000104 - SwissSign AG	MPKI0000104.AutoRAO	[REDACTED]

Der Service-API-Schlüssel kann auf Anfrage erneuert werden.

## 4 RA API

SwissSign CA bietet eine OpenAPI-Spezifikation für die Automatisierung und Integration Ihrer MPKI mit Ihren Diensten.

Mit der RA API können Sie Zertifikate registrieren, widerrufen und suchen sowie Registrierungsanfragen autorisieren. Die URL zu diesem Dienst wird von SwissSign bereitgestellt.

### 4.1 Rollen und Berechtigungen

Für einen gegebenen Nutzer und eine gegebene Rolle, der/die die Client-API verwenden, gelten die gleichen Rollen und Berechtigungen wie in der Benutzeroberfläche angegeben. Das heisst, wenn ein gegebener Nutzer und eine gegebene Rolle berechtigt sind, einen LESE-Vorgang über die Web-Benutzeroberfläche auszuführen, dann ist derselbe Vorgang auch über die generierte Client-API zugänglich. Wenn einem bestimmten Nutzer oder einer Rolle die LÖSCH-Berechtigung für einen bestimmten Vorgang entzogen wird, dann wird die LÖSCH-Berechtigung entsprechend auch für den Vorgang in der Client-API entzogen.

Um einen API-Schlüssel zu erhalten, muss das verknüpfte Konto für die angegebene Benutzerrolle mindestens über die Berechtigungen "ACCOUNT\_API\_KEY Anzeigen und Erstellen" verfügen. Mit den Berechtigungen "Aktualisieren und Löschen" kann der Benutzer ausserdem seine API-Schlüssel erneuern und/oder löschen.

Wenn für eine bestimmte Benutzerrolle keine ACCOUNT\_API\_KEY-Berechtigung aktiviert ist, kann eine höhere Rolle dennoch einen API-Schlüssel für diesen Benutzer ausstellen, sofern die Berechtigung erteilt wird.

Wenn ein Nutzer vom Typ DIENSTKONTO ist, kann der Nutzer zwar die API nutzen, sich aber nicht über die Web-Benutzeroberfläche anmelden.

### 4.2 Service-API-Schlüssel

Um die API nutzen zu können, muss ein Nutzer einen API-Schlüssel erhalten.

Ein Nutzer mit mehreren MPKI-Zugängen hat auch mehrere API-Schlüssel.

Bei dem API-Schlüssel handelt es sich um ein automatisch generiertes 64-Byte gemeinsames Geheimnis, das Ziffern, Buchstaben, Gross- und Kleinschreibung enthält und auf der Client-Seite (API) verwendet wird, um ein signiertes (HMAC-256) JW-Token zu erzeugen.

#### 4.2.1 API-Schlüssel-Rollover

Die generierten API-Schlüssel stehen dem Client sofort zur Verfügung und haben weder ein Ablaufdatum noch eine Ablaufzeit.

Wenn ein API-Schlüssel gelöscht wird, ist der Zugriff auf die Web Services sofort nicht mehr möglich. Deshalb kann der Löschvorgang nur von SwissSign durchgeführt werden.

Wenn ein API-Schlüssel aktualisiert wird, wird ein neuer API-Schlüssel generiert. Der vorherige API-Schlüssel ist weitere sieben Tage lang gültig. Der Nutzer hat maximal sieben Tage Zeit, um den API-Schlüssel auf seiner Implementierung (Client-Konfiguration) zu ersetzen.

### 4.3 Authentifizierung

Generieren Sie ein JW-Token (JWT) und signieren Sie es mit dem API-Schlüssel mit HMAC256 als 'text/plain'. Ein JW-Token ist standardmässig acht Stunden lang gültig.

### 4.3.1 Erstellung von JWTs

Ein JWT muss Folgendes enthalten:

Anspruch	Wert
Iss	SwissSign CA
Aud	REST API
Sub	<Benutzername> des SwissSign CA-Kontos
Iat	Normalisierte/s UTC-Datum/Uhrzeit
Nbf	Normalisierte/s UTC-Datum/Uhrzeit
Exp	Normalisierte/s UTC-Datum/Uhrzeit

### 4.3.2 HTTP-Anforderung

Wenn Sie HTTP-Anforderungen für den Zugriff auf die SwissSign CA-Webdienste verwenden, dann fügen Sie in jede Anforderung den folgenden HTTP-Header ein, wobei "codiertes JWT" dabei das signierte verschlüsselte Token darstellt:

Autorisierung: Bearer <codiertes JWT>

Nutzen Sie die mit dem openapi-generator generierte Java-Client-API, um das codierte JWT wie folgt festzulegen:

```
HttpBearerAuth bearerAuth = (HttpBearerAuth)defaultClient.getAuthentication("bearerAuth");  
bearerAuth.setBearerToken("codiertes JWT");
```

Jede Serviceanforderung MUSS zwingend ein JWT-Token enthalten. PKI-Webdienste geben kein verwendbares Sitzungs-Cookie zurück.

Für die Erstellung Ihres JW-Tokens steht Ihnen eine SSL-geschützte Hilfsmethode zur Verfügung:  
GET /pki/api/v2/jwt/:userName/:key

Dabei steht :userName für Ihr Benutzerkonto und :key für den API-Schlüssel Ihres Kontos, den Sie auf der Web-Benutzeroberfläche unter "Mein Konto" finden.

## 5 CMC

Um Zertifikatsvorgänge über die CMC-Schnittstelle (Zertifikatsverwaltung über CMS) gemäss IETF RFC 5272 durchzuführen, benötigen Sie ein spezielles Zertifikat für Ihren CMC-Client. Das Zertifikat wird Ihnen während des Onboarding-Prozesses zur Verfügung gestellt und wird in regelmässigen Abständen erneuert.

Die URLs und Parameter für die Verwendung der CMC-Schnittstelle sind in der Technischen Spezifikation der CMC-Schnittstelle beschrieben. Laden Sie diese hier herunter:

[https://www.swissign.com/dam/jcr:8ff02777-a6b6-4872-8a6c-535d3cb2d565/CMCInterface\\_EN.pdf](https://www.swissign.com/dam/jcr:8ff02777-a6b6-4872-8a6c-535d3cb2d565/CMCInterface_EN.pdf)