SwissSign

SwissSign CA

SwissSign AG

Handbuch für RA-Operatoren

SwissSign

Revision

Rev.	Datum	Wer	Kommentar
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

SwissSign

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

SwissSign

Inhalt

SwissSign

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

SwissSign

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:

Protokoll	Beschreibung
RA-Benutzeroberfläche	Manuelle Ausstellung von Zertifikaten und die Lebenszyklusmanagement (dieses Dokument)
RA API	OpenAPI v3-Spezifikation zur Automatisierung und Integration Ihrer MPKI in Ihre Dienste.
ACME	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: - Certbot ACME Client von Red Hat Enterprise Linux oder - ACMESharp für Microsoft-Plattformen
CMC	Zertifikatsverwaltung über CMS (Cryptographic Message Syntax) nach RFC 5272

SwissSign

3 RA-Benutzeroberfläche

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

Bereich	Beschreibung
Dashboard	Übersichtseite, die das Folgende anzeigt: - Alle Zertifikate, die in '*d*' Tagen ablaufen
Ausstellung	Eine durchsuchbare Liste aller Zertifikatsprodukte, die Sie für ausgewählte Client(s) ausstellen können
Bestellungen und Zertifikate	Eine durchsuchbare Liste aller ausgestellten Zertifikate und Zertifikatsbestellungen
ACME	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. HINWEIS: ACME wird nur dann angezeigt, wenn das Protokoll für die Ausstellung von Zertifikaten angewendet wird.
Domain-Validierung	Eine durchsuchbare Liste von vorab validierten Domainnamen.
Konto	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

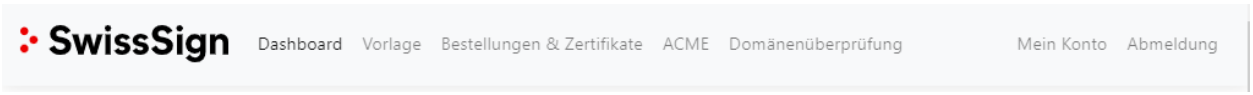
Bei SwissID handelt es sich um ein sicheres Login von SwissSign. Für das Onboarding auf SwissID folgen Sie den Anweisungen unter folgendem Link:

https://www.swisssign.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:



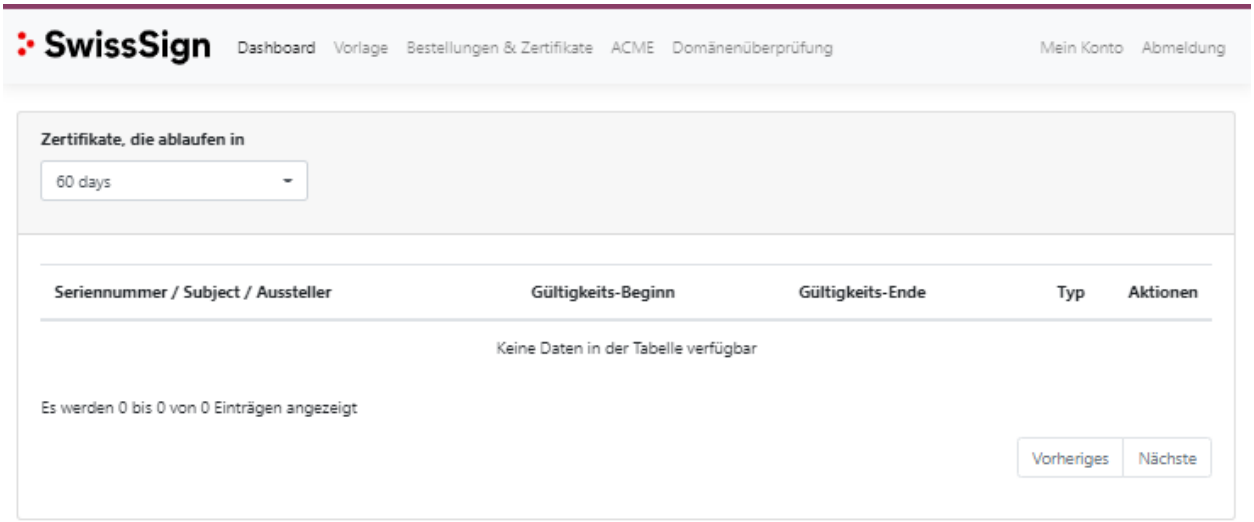
- Für den Zugriff auf das Dashboard siehe Kapitel *3.3 Dashboard*
- Für den Zugriff auf die Zertifikatsausstellung siehe Kapitel *3.4 Issuance*
- Für den Zugriff auf Bestellungen und Zertifikate siehe Kapitel 3.5 *Orders and Certificates*
- Für den Zugriff auf die ACME-Token siehe Kapitel 3.6 *ACME*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

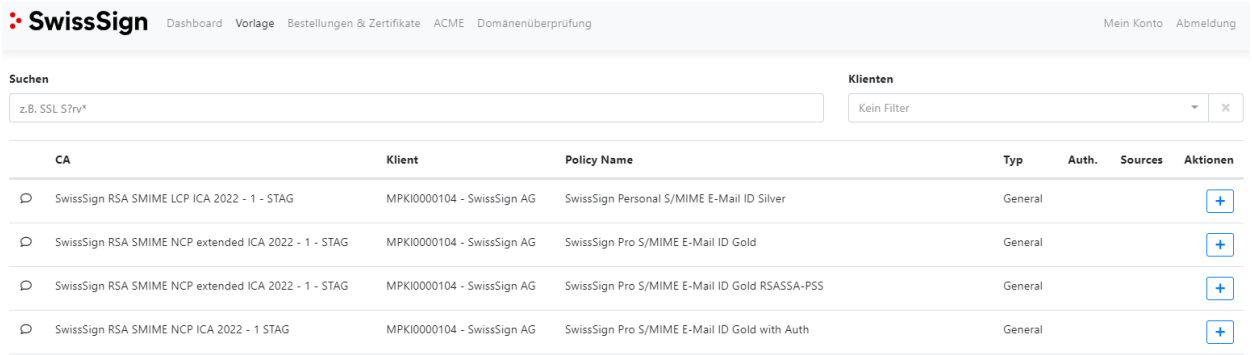
In der Tabelle für ablaufende Zertifikate finden Sie eine Liste von Zertifikaten, die demnächst ablaufen. Verwenden Sie das Dropdown-Menü oberhalb des Bereichs, um die Liste zu filtern.



Spalte	Beschreibung
Serien#	Die Seriennummer des Zertifikats
Antragsteller	Definierter Name (DN) des Antragstellers des Zertifikats
Aussteller	Antragsteller-DN der ausstellenden CA
Typ	Zeigt den Zertifikatstyp an: - Externes Zertifikat (aus der aktuellen MPKI importiert) -
Aktionen	1. Links zur Detailseite des Zertifikats bearbeiten 2. Das Zertifikat im PEM-Format herunterladen 3. Eine Veröffentlichungsanfrage senden (nur verfügbar, wenn für das Zertifikat die Option LDAP-Veröffentlichung aktiviert ist. Nur für S/MIME-Zertifikate verfügbar.)

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.



Spalte	Beschreibung
CA	Die CA, die das Zertifikatsprodukt ausstellt
Client	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)
Richtlinienname	Der Name des Zertifikatsprodukt
Typ	Der Produkttyp des Zertifikats (bei der Ausgabe durch RA-Operator immer als *Allgemein* angezeigt)
Auth	Zeigt ein Häkchen an, wenn der Richtlinieninstanz eine Autorisierungsregel zugeordnet wurde.
Quellen	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
Aktionen	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 Zertifikatsempfänger 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-----

MIICqTCCAZECAQAwPzEdMBsGA1UECgwUbGliQyBUZWNobm9sb2dpZXMgU0ExETAP

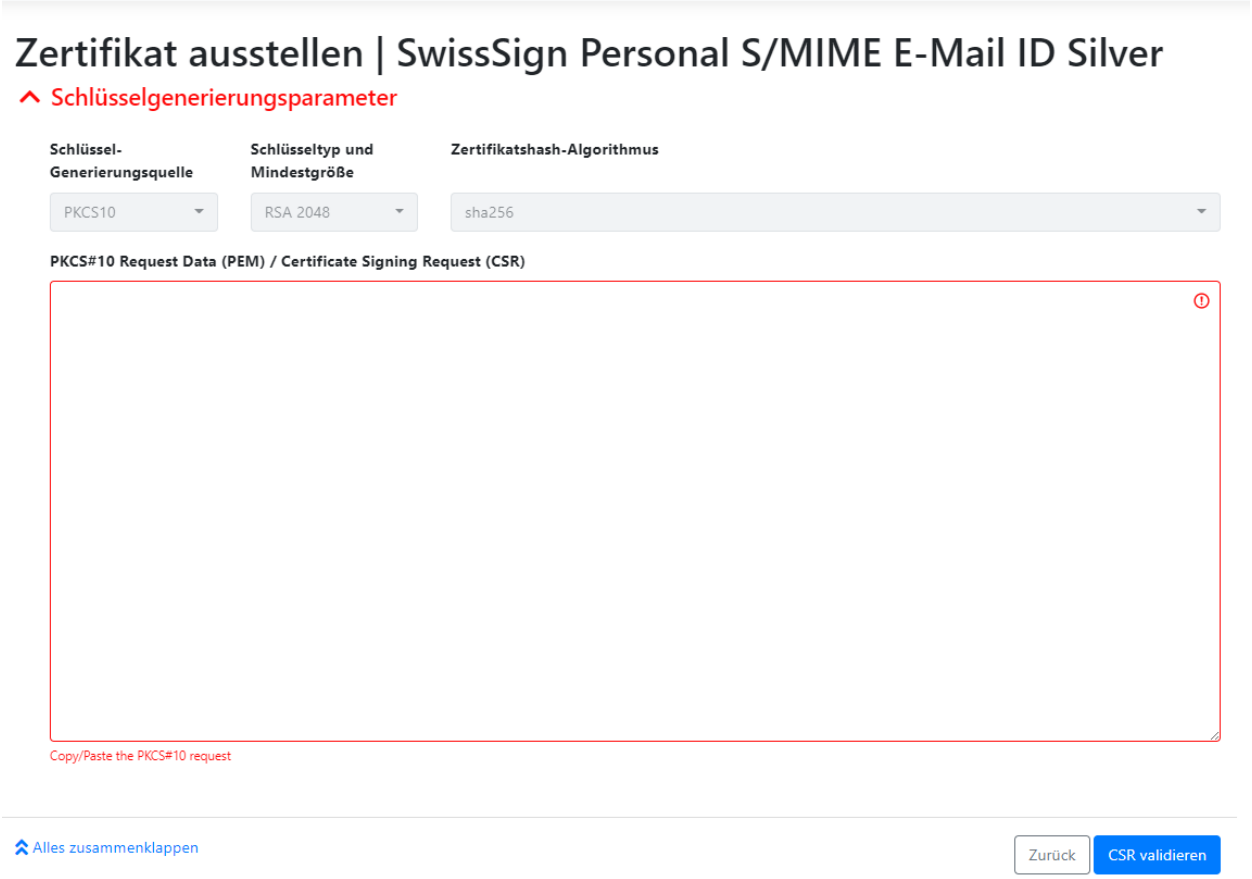
[ausgeblendet]

H+aC3/oJkApfonUK5m7eFzDsrN/cMWFQUQ5xFNDCzGmqBdX4U/Ft+s323otQMTN6

nl6IHYxn7IGxyCIAVg

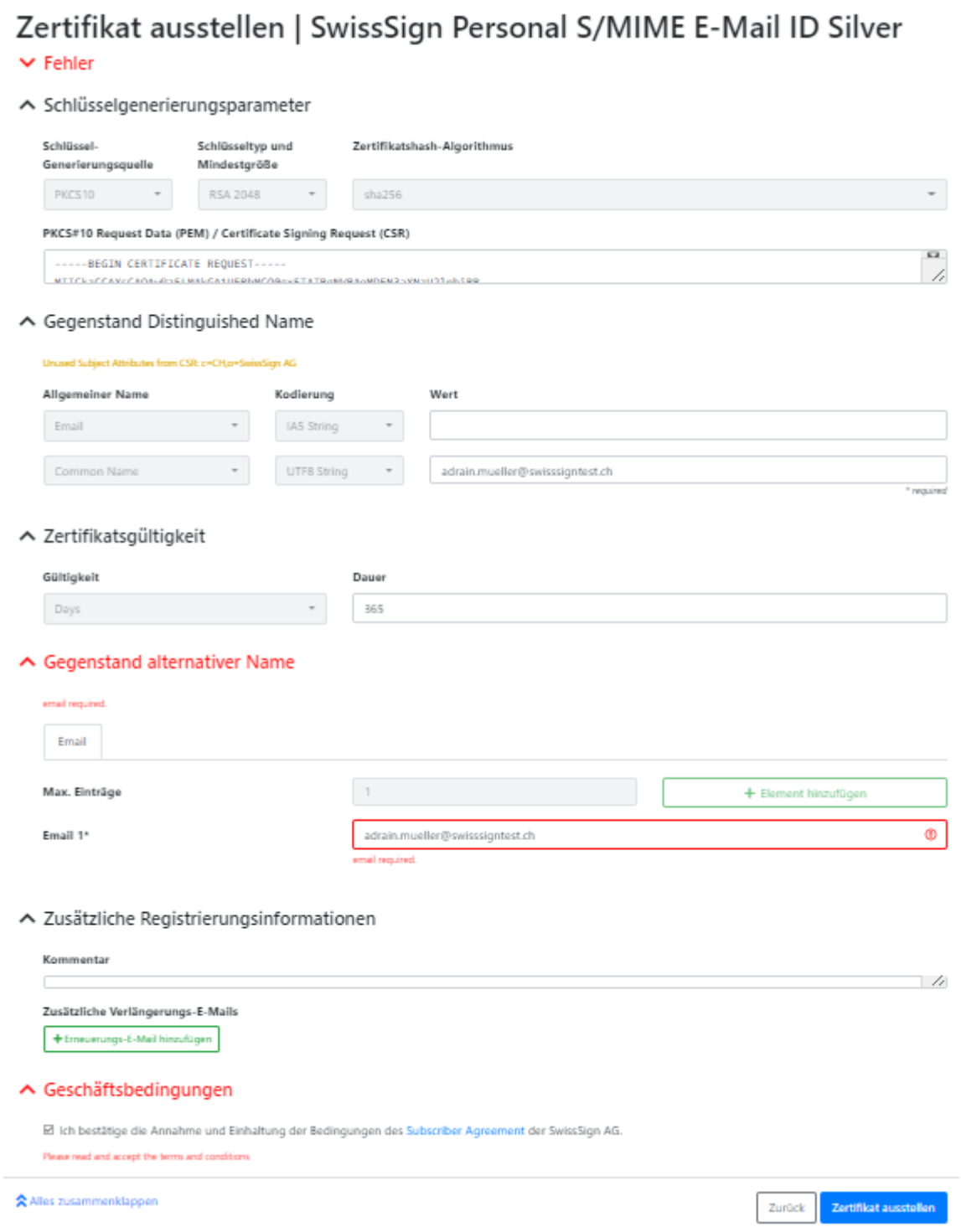
-----END CERTIFICATE REQUEST-----

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



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.

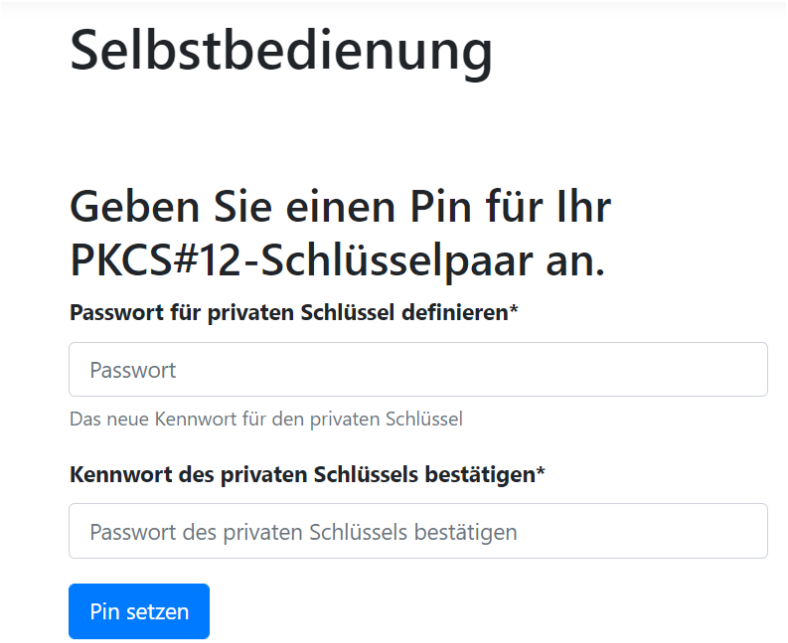
SwissSign


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-----
Gegenstand Distinguished Name
Unused Subject Attributes from CSR: c=CH,o=SwissSign AG
Allgemeiner Name
Kodierung
Wert
Email
IA5 String
Common Name
UTF8 String
adrain.mueller@swisssigntest.ch
* required
Zertifikatsgültigkeit
Gültigkeit
Dauer
Days
365
Gegenstand alternativer Name
email required.
Email
Max. Einträge
1
+ Element hinzufügen
Email 1*
adrain.mueller@swisssigntest.ch
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.



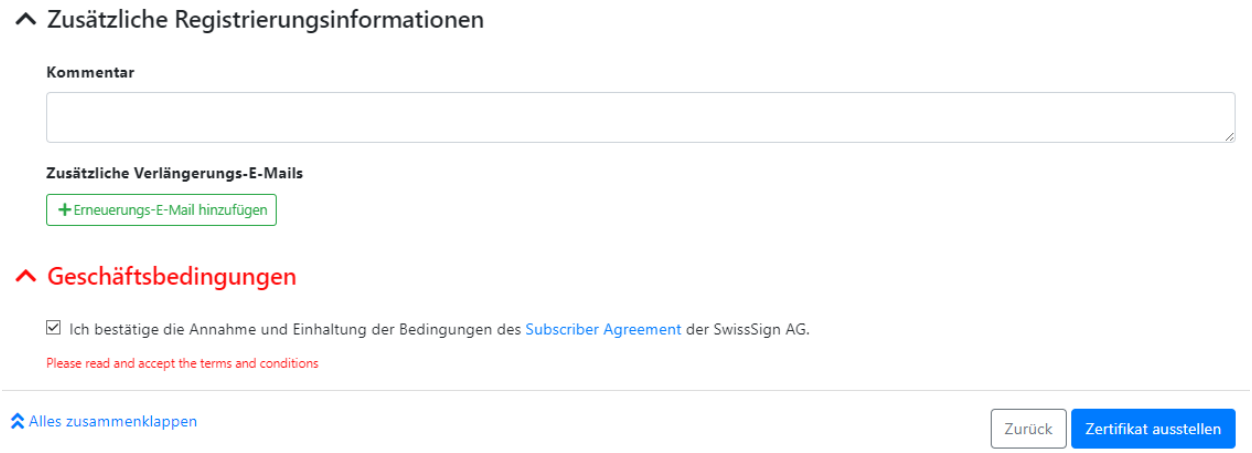
3.4.4 Zusätzliche Informationen für die Registrierung

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.

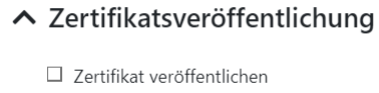
3.4.5 Zusätzliche E-Mails über Erneuerungen

Diese Option wird angezeigt, wenn der Richtlinieninstanz eine Erneuerungssregel 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.



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.



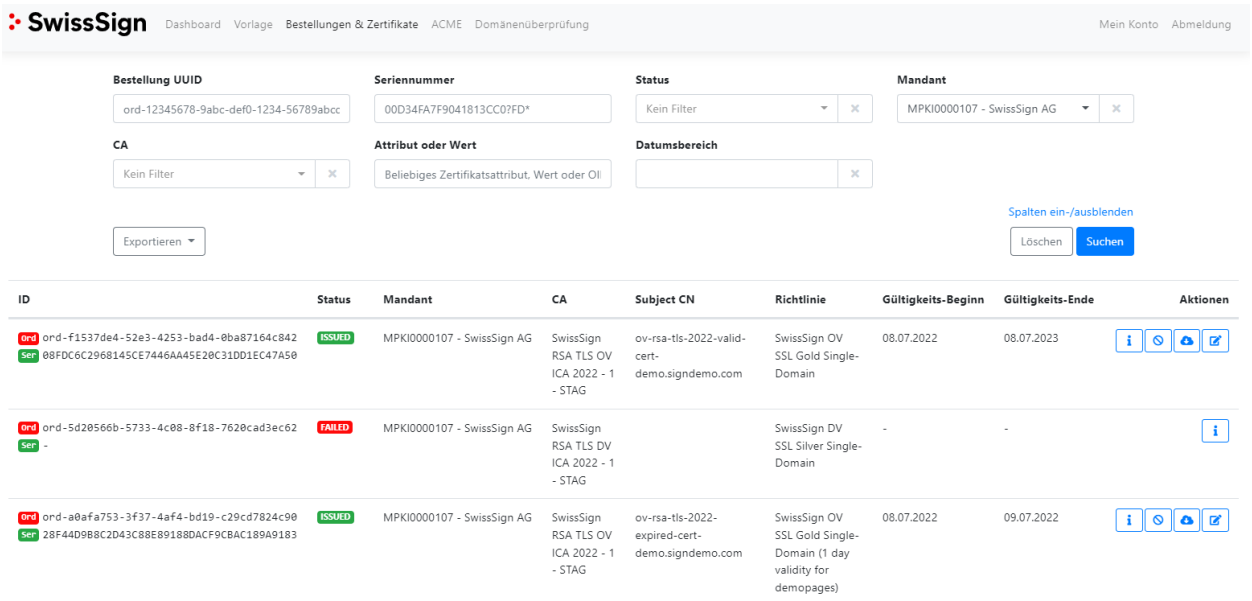
3.5 Bestellungen und Zertifikate

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
NEU	Eine neue Zertifikatsbestellung wird erstellt und die Zertifikatsrichtlinie wird validiert (sowohl statisch als auch zur Laufzeit). Der Ausstellungsprozess beginnt.	nein
PENDING_CSR_RENEWAL	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
SCHLÜSSEL_VALIDIERUNG	Das Schlüsselpaar wird validiert und optional generiert, wenn es sich bei der Zertifikatsrichtlinie um den Typ PKCS#12 handelt	nein
TBS_GENERIEREN	Die Strukturgenerierung des TBS („to-be-signed“) basierend auf der Richtlinie des Zertifikats. Mit Ausnahme der CT-Erweiterung ist diese Struktur unveränderlich.	nein
VORAB_VALIDIERUNG	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
VOR_AUSSTELLUNG	Führt bei Bedarf den Pre-Cert-CT-Log-Eintrag aus	nein
AUSSTELLUNG	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
NACH_VALIDIERUNG_	Bei Bedarf wird ein Post-Linting durchgeführt und das CT-Protokoll veröffentlicht, sofern aktiviert.	ja
FINALIZE_ISSUANCE	Die Bestellabwicklung wird bereinigt und bei Bedarf werden Benachrichtigungen versendet. Eine Anfrage zur	ja

	Veröffentlichung des Zertifikats wird versendet, falls diese Option aktiviert ist.	
AUSGESTELLT	Die Bestellabwicklung ist abgeschlossen und die Zertifikatsbestellung wird auf den Status AUSGESTELLT gesetzt.	ja
WIDERRUFEN	Die Zertifikatsbestellung wird widerrufen	ja
FEHLGESCHLAGEN	Bestellabwicklung fehlgeschlagen. Wenn ein Zertifikat ausgestellt wird und die Verarbeitung nach der ISSUE-Phase fehlschlägt, wird das Zertifikat widerrufen	–
UNBEKANNT	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.



Spalte	Beschreibung
ID	Enthält die Bestell-UUID und die Seriennummer des Zertifikats.
Status	Enthält den Status des Zertifikats.
Client	Enthält den Client, der zum Ausstellen dieses Zertifikats verwendet wurde.
CA	Enthält die Zertifizierungsstelle, die zum Ausstellen dieses Zertifikats verwendet wurde.
Antragsteller-CN	Enthält den allgemeinen Antragstellernamen des Zertifikats.
Policy	Enthält die Richtlinieninstanz (Zertifikatsprodukt), die zum Ausstellen dieses Zertifikats verwendet wurde.
Start Validity	Enthält das Startdatum der Zertifikatslaufzeit.
End Validity	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.

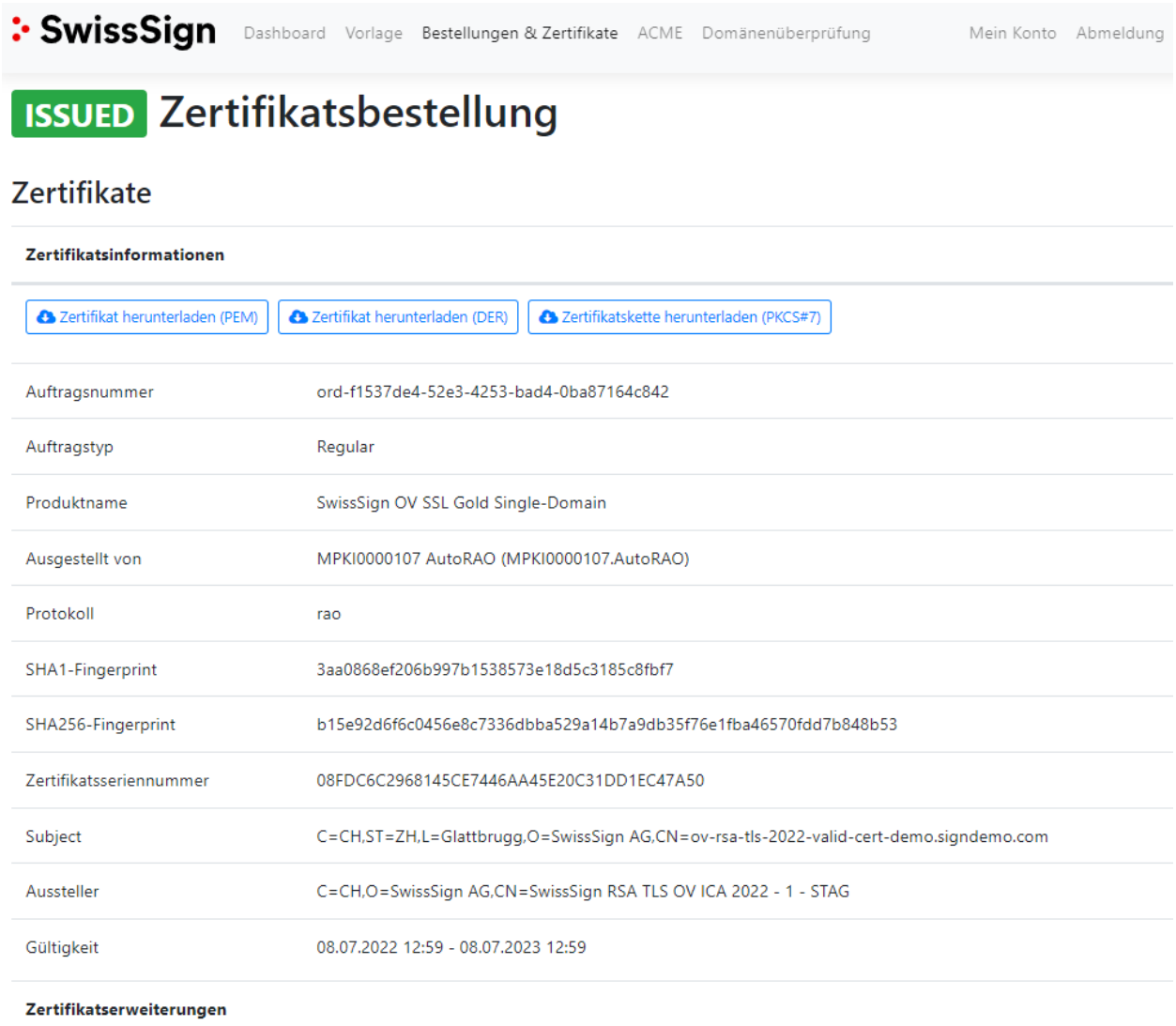
3.5.1 Bestelldetails des Zertifikats

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.

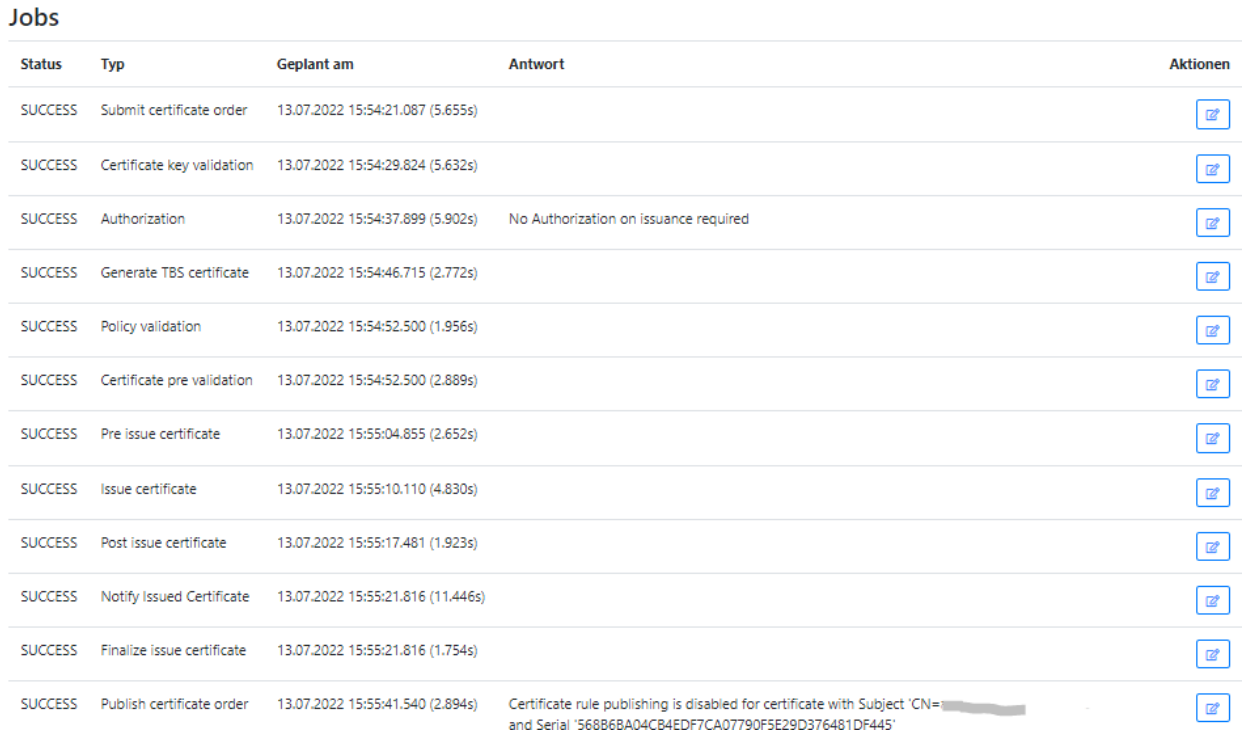


3.5.1.2Tasks zur Bearbeitung von Zertifikatsbestellungen

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

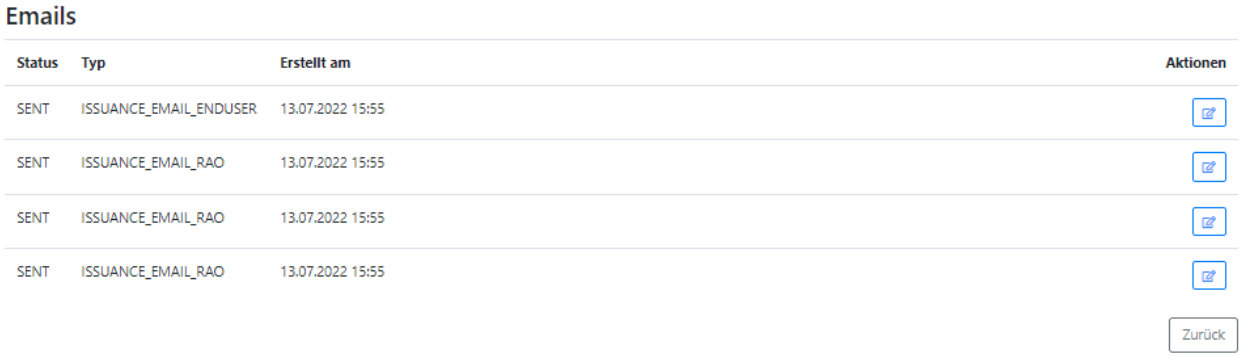
Liste der Aufgaben und ihres jeweiligen Status, die während der Bestellabwicklung ausgeführt wurden



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.



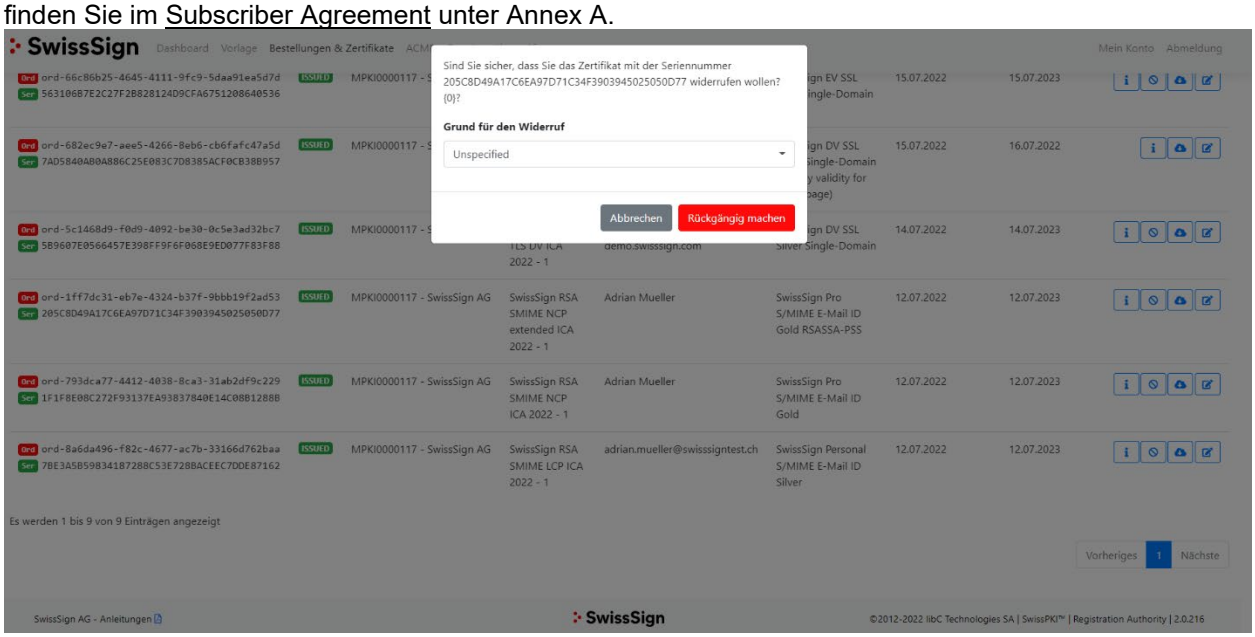
Emails

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	

Zurück

3.5.2 Zertifikat revozieren

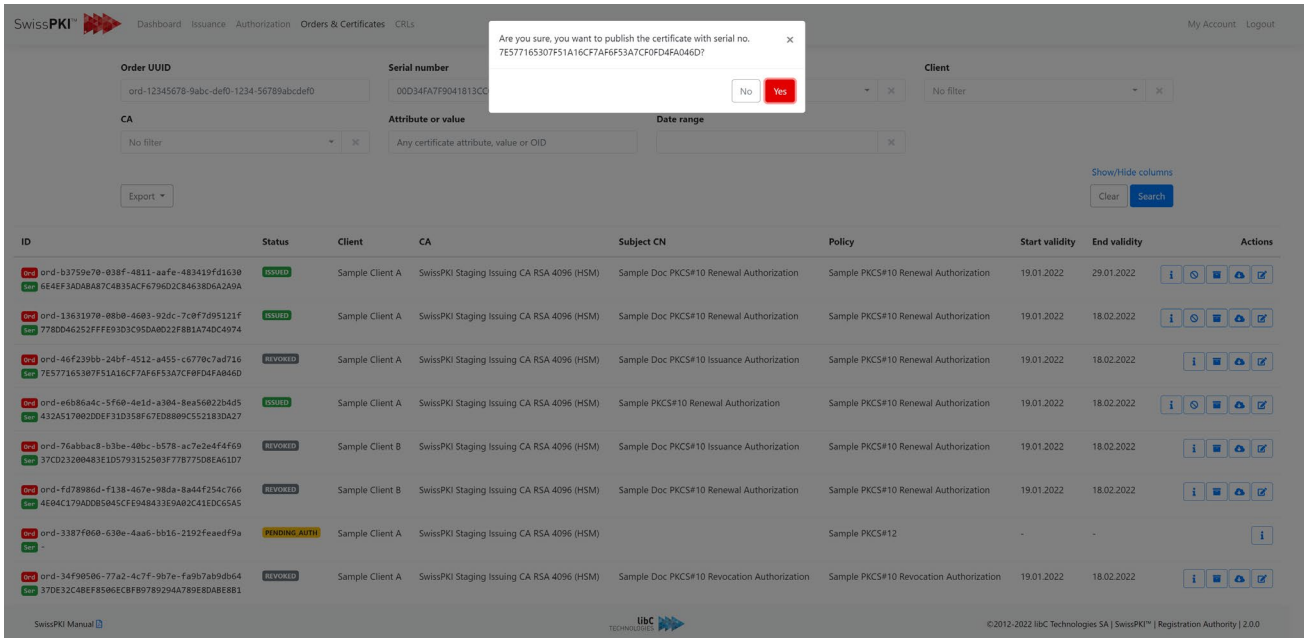
Sie können ein Zertifikat widerrufen, indem Sie auf die Widerruf-Schaltfläche in der Spalte "Aktionen" in der Tabelle "Bestellungen und Zertifikate" klicken. Nachdem Sie auf die Schaltfläche geklickt haben, werden Sie in einem Popup-Dialog aufgefordert, die Aktion zu bestätigen. Standardmässig ist als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



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.



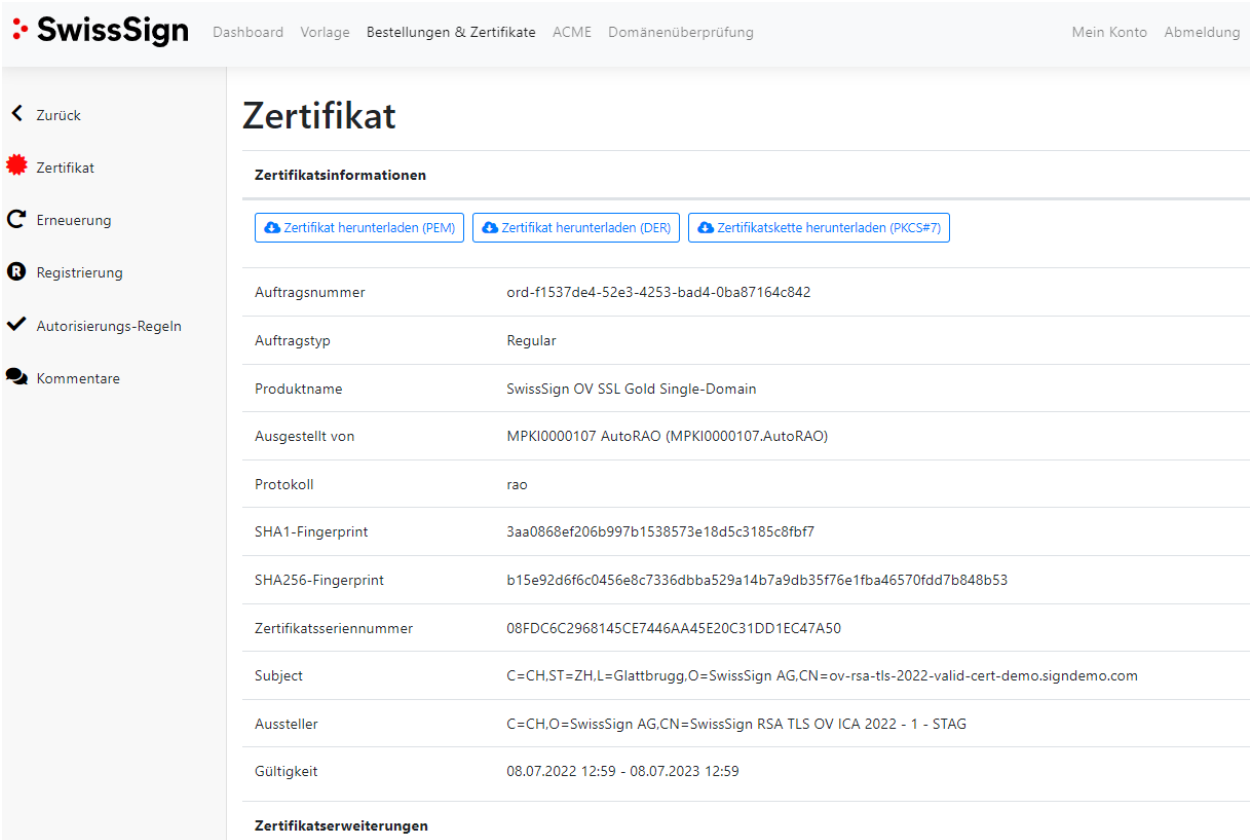
3.5.4 Informationen zum Zertifikat

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.



SwissSign

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.

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.

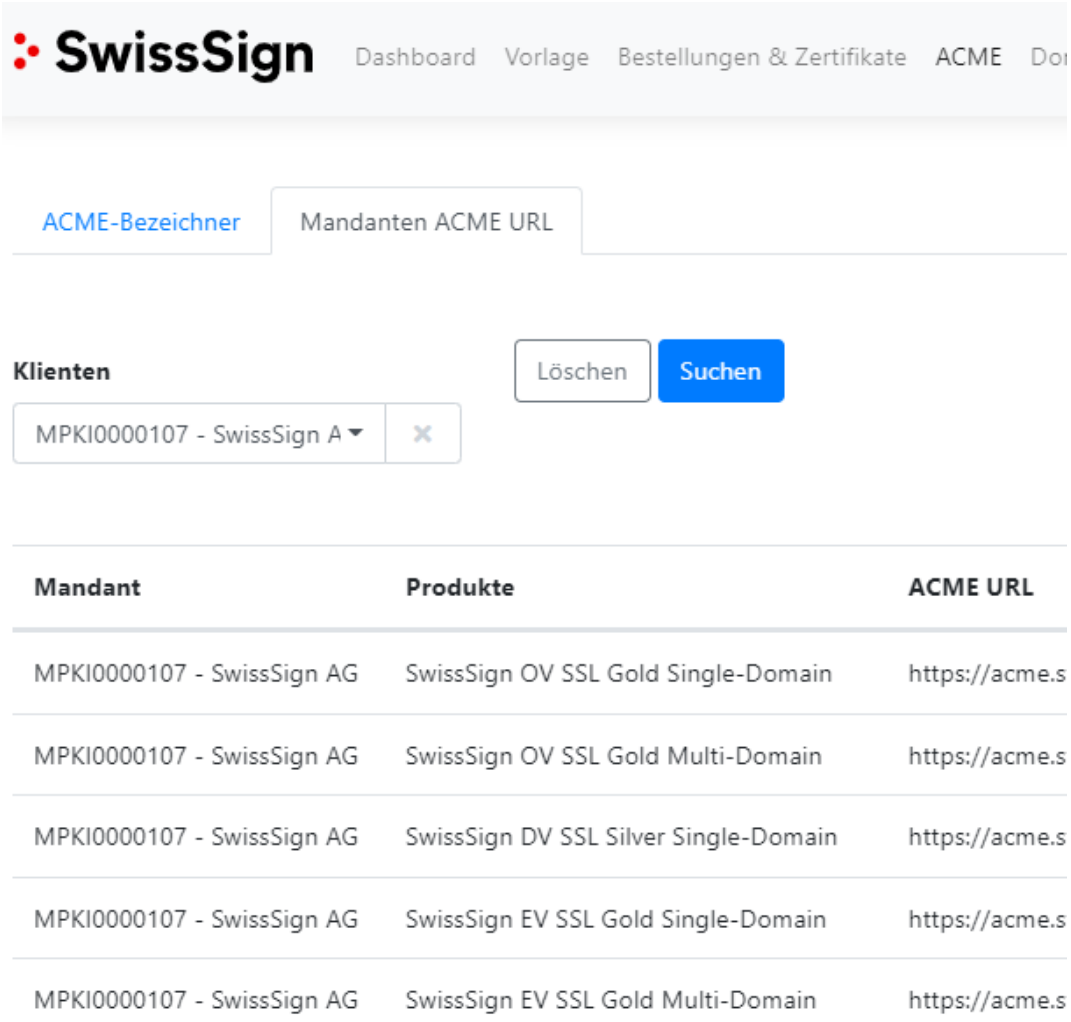
3.5.4.4Kommentare

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.

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.

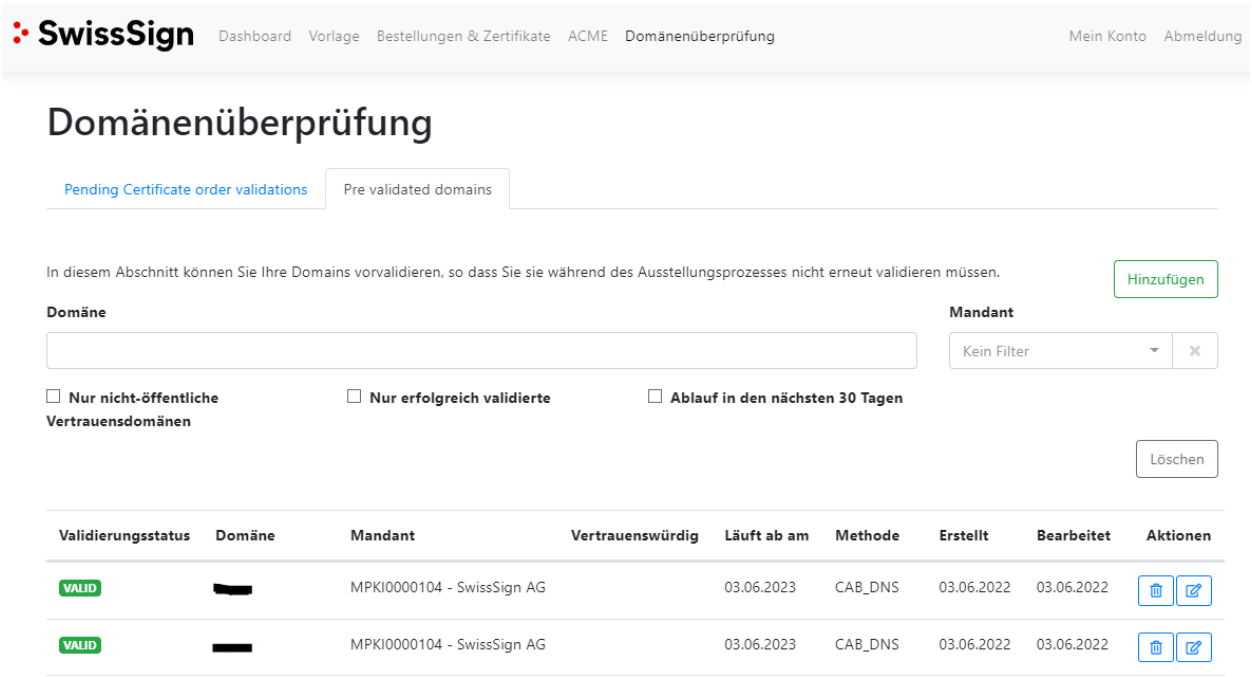


Hinweis: Zertifikate, die über das ACME-Protokoll ausgestellt wurden, können Sie in "Bestellungen und Zertifikate" durchsuchen.

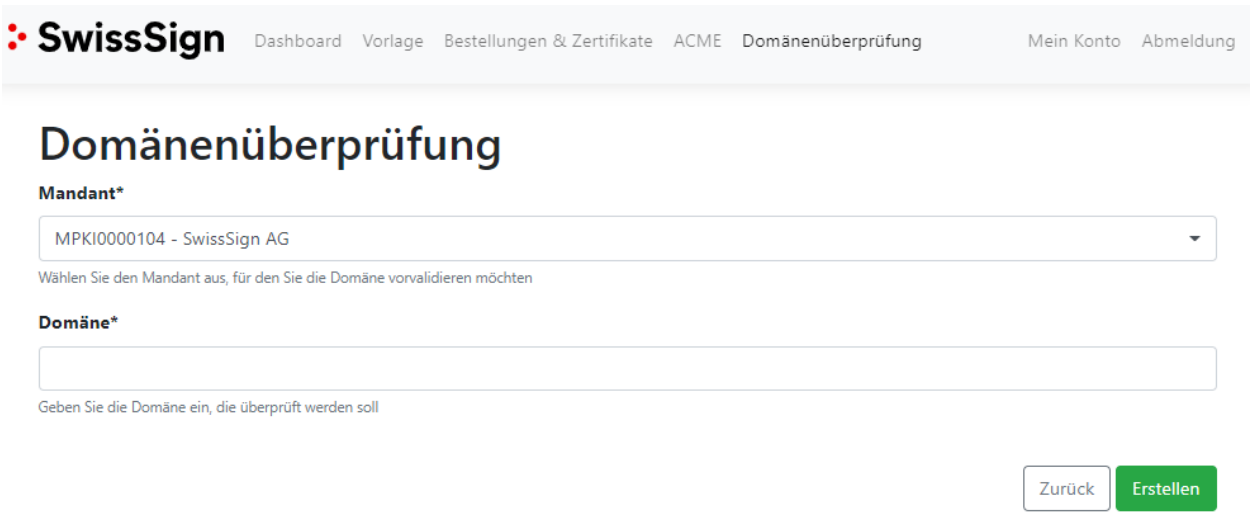
3.7 Domänenüberprüfung (Domain-Validierung)

3.7.1 DNS Vor-Validierung

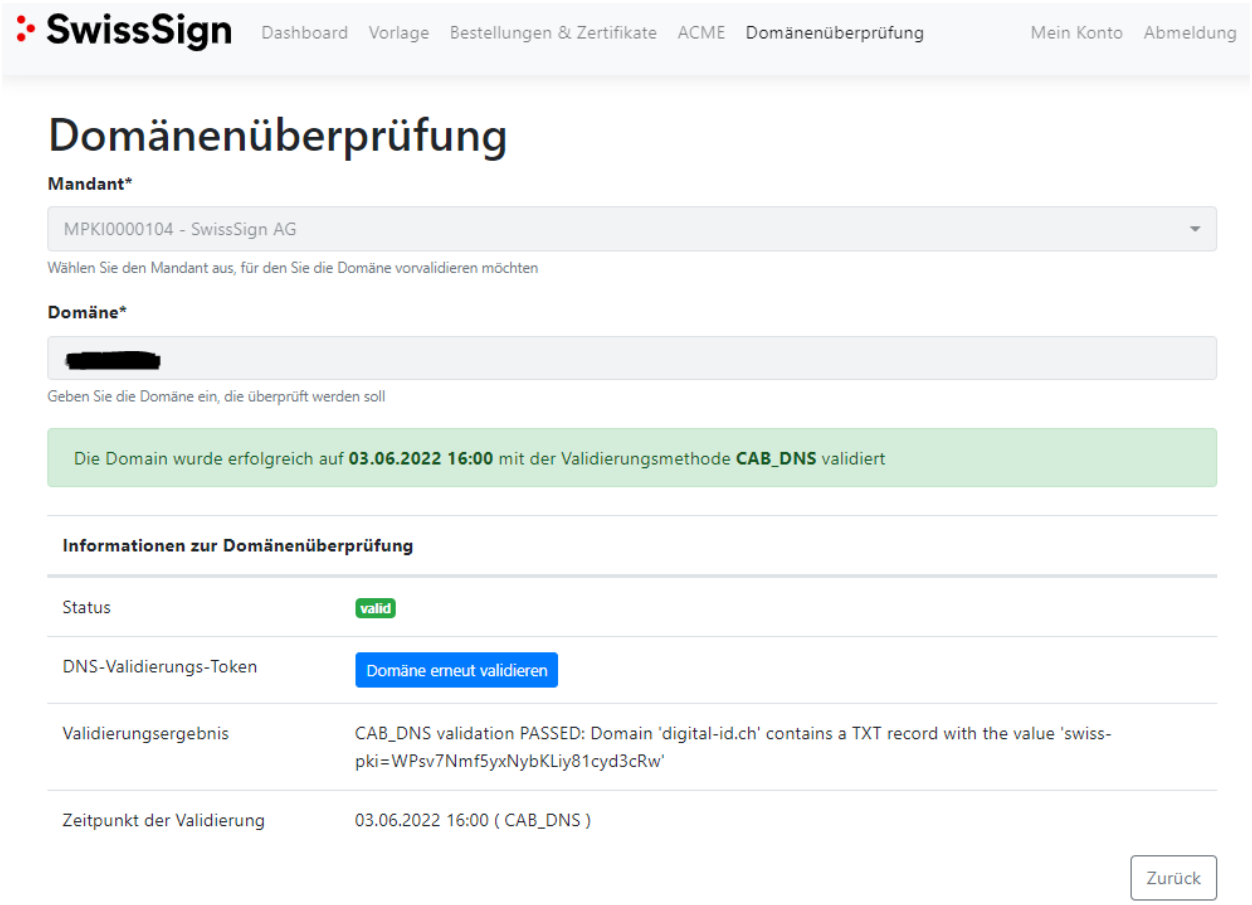
Bei den Richtlinienvorlagen, die über eine "DNS-Eigentümerregel" verfügen, müssen die Domainnamen bei der Ausstellung des Zertifikats validiert werden. Um
Arbeitschritte einzusparen, kann der Kunde eine Domain vorab validieren (i. d. R. validiert der Kunde seine Basis- bzw. Haupt-Domain), sodass er in 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



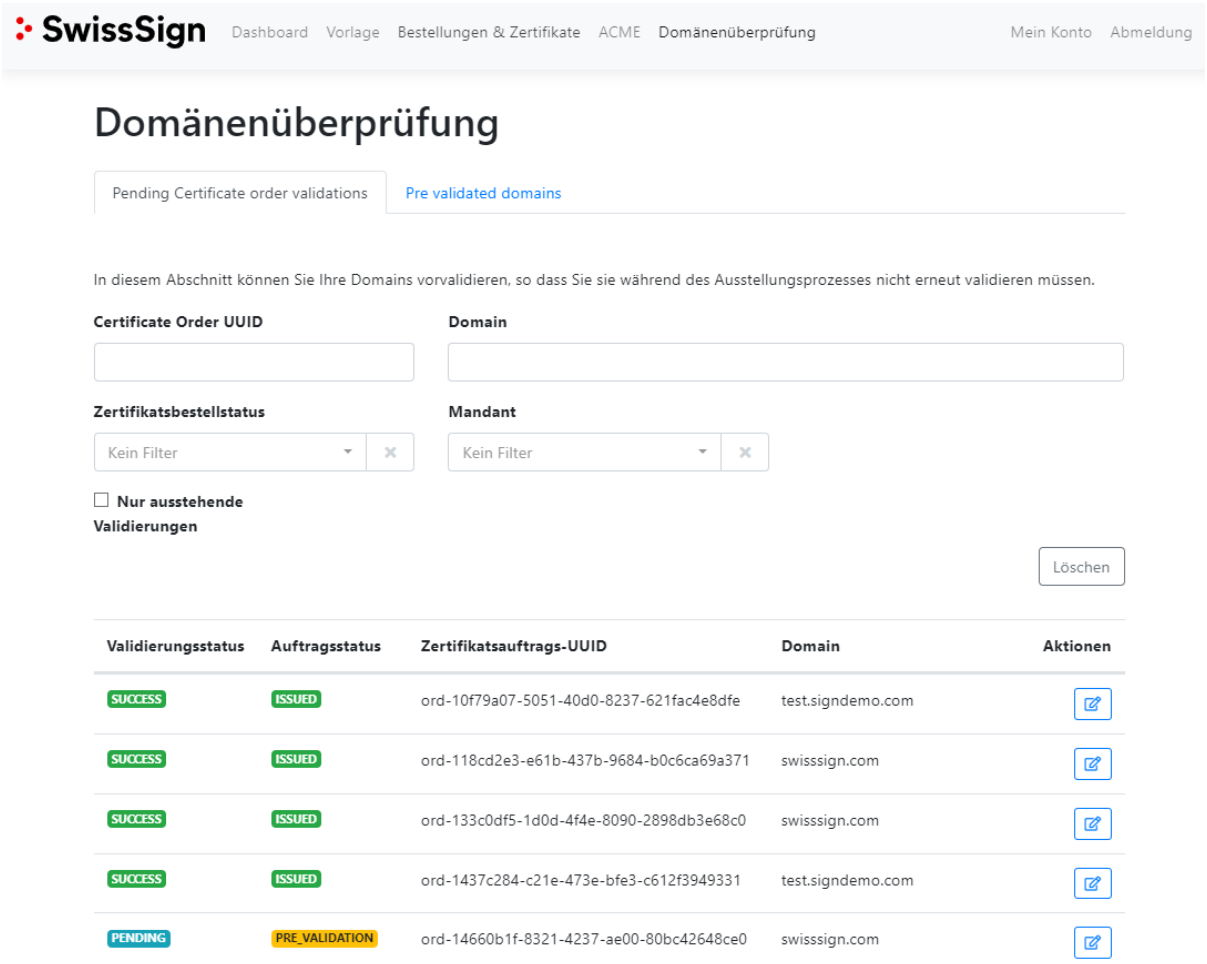
Feld	Beschreibung
Client	Client, für den die vorab validierte Domain hinzugefügt werden soll. HINWEIS: Da ein RA-Operator Zugriff auf mehr als nur einen Client haben kann, muss der Client hier aufgeführt werden
Domäne	Name der Domain, die vorab validiert werden soll



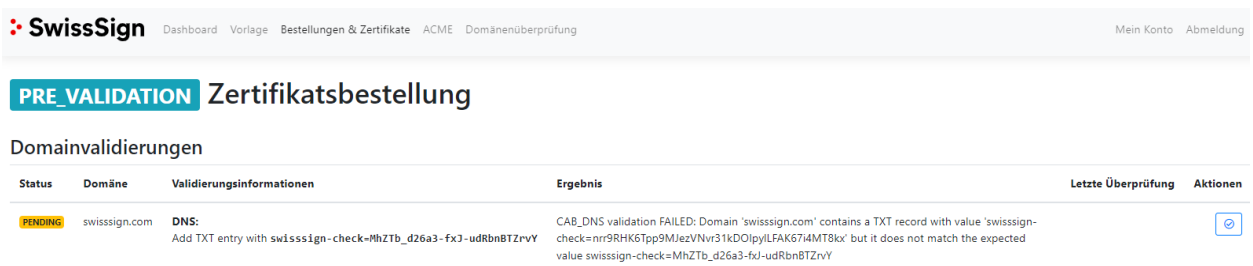
Für die DNS-Eigentümerprüfung mit öffentlichem Vertrauen kopieren Sie das DNS-Challenge-Token in den DNS-Server. Auf der Seite wird eine Anleitung dazu angezeigt. Als Operator können Sie den DNS-Eintrag gegebenenfalls manuell validieren, indem Sie auf "Domaineigentümerschaft validieren" klicken. Klicken 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 Domainvalidierungen für seine Zertifikatsbestellungen. Klicken Sie auf die Schaltfläche "Bearbeiten", um die Details der Validierung anzuzeigen.



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.

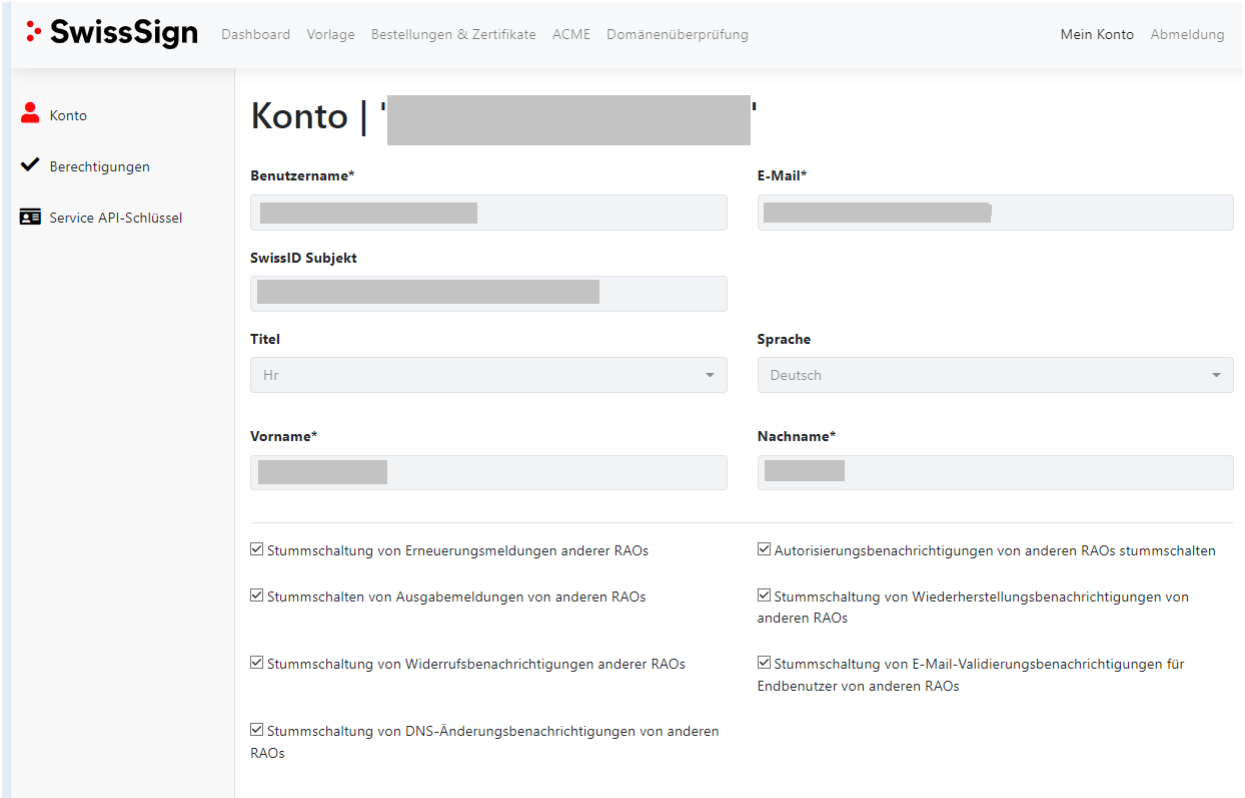


3.8 Konto

3.8.1 Kontodaten

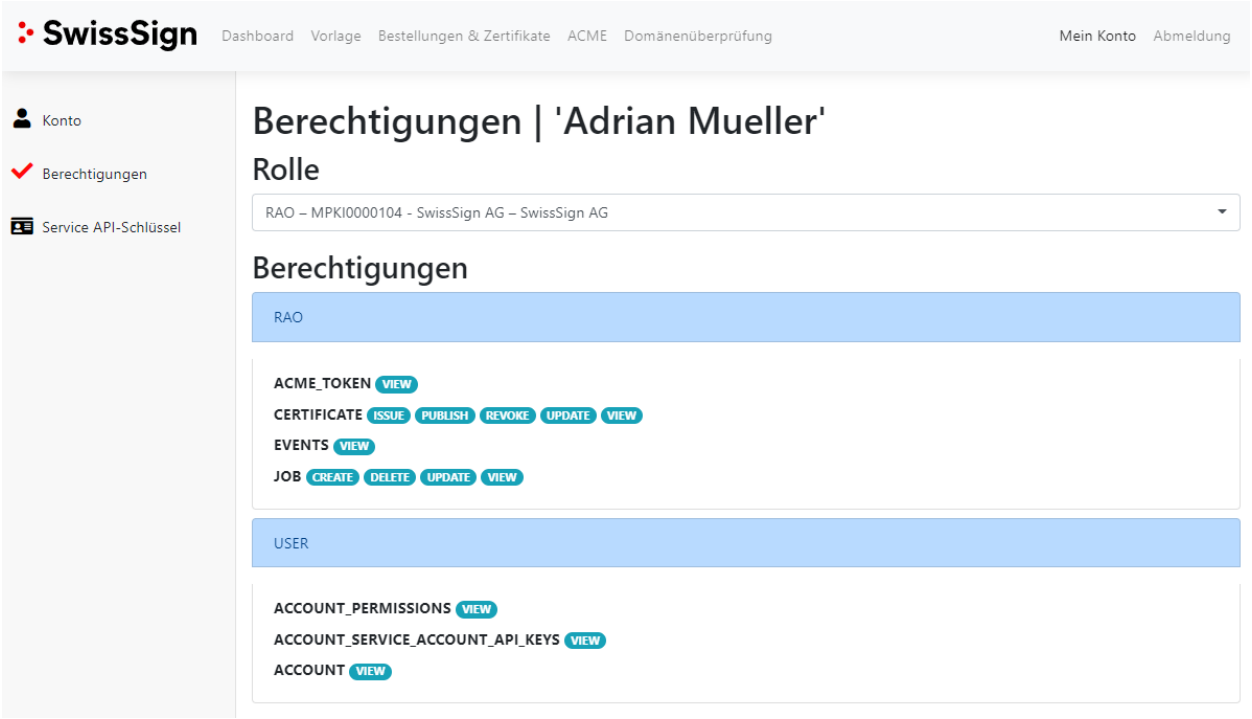
Auf dieser Seite können Sie Ihre Kontodaten überprüfen. Folgende Felder werden angezeigt:

Felder	Beschreibung
Benutzername	Ihr Benutzername
E-Mail	Die mit Ihrem Konto verbundene E-Mail-Adresse
SwissID Subjekt	Die mit Ihrem Konto verknüpfte SwissID
Vorname	Ihr Vorname
Nachname	Ihr Nachname
Titel	Ihr Titel
Sprache	Ihre bevorzugte Sprache
Benachrichtigungen stumm schalten	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. **Hinweis**: Sie müssen über die erforderlichen Berechtigungen verfügen, um Ihre Kontoinformationen zu ändern.



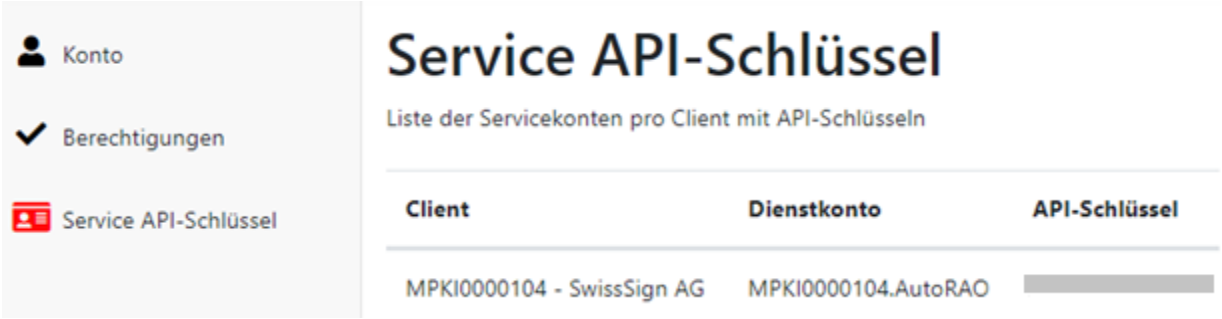
3.8.2 Berechtigungen

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.



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.



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

SwissSign

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 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.swisssign.com/dam/jcr:8ff02777-a6b6-4872-8a6c-535d3cb2d565/CMCInterface_EN.pdf