SwissSign

SwissSign CA

SwissSign AG

RA Operator Manual

Revision

Rev	**Date**	**Who**	**Comment**
1.0	23.03.2022	SwissSign AG	Initial document
1.1	13.06.2022	SwissSign AG	Update screenshots
1.2	06.10.2022	SwissSign AG	Updated points to reflect the current state of the CA

Acronym	Meaning
ACME	Automatic Certificate Management Environment
Administrator	User that has the admin rights on the Admin UI part.
AIA	Authority Information Access
AKI	Authority Key Information
ARL	Authority Revocation List
BC	Basic Constraint
CA	Certification Authority
CAA	Certification Authority Authorization Rule
CAO	User that has admin rights on the Operator UI part.
CDP	CRL Distribution Point
Client	The concept of a client is a logical grouping of the distinct PKIs that can be created for a realm.
CMC	Certificate Management over CMS (Cryptographic Message Syntax)
CNG	Microsoft's CryptoAPI Next Generation
CMP	Certificate Management Protocol
CP	Certificate Policy
CPS	Certificate Practise Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request. A base64 encoded PKCS#10 (see PKCS#10) including begin and end beacons
CT	Certificate Transparency
DC	Domain Controller
DIT	Directory Information Tree (LDAP)
DSS	Document Signer Service
EKU	Extended key Usage
KU	Key Usage
IIS	Microsoft Internet Information Server
LDAP	Lightweight Directory Access Protocol
MAP	Microsoft Application Policies
MCT	Microsoft Certificate Template
MSCA	Microsoft Certification Authority
NC	Name Constraint
OCSP	Online Certificate Status Protocol
PKCS#10	A certificate request in binary format (see CSR)
PKCS#12	A data structure which usually contains a certificate chain and the corresponding leaf certificate's private key. The file is encrypted with a PIN.
QCv2	Qualified Statement v2
RA Operator	RA Operator Can issue, revoke, recover or renew certificates.
RP	Relying Party (OIDC)
SAN	Subject Alternative Name
SKI	Subject Key Identifier

Contents

1 SwissSign CA

SwissSign CA is building upon SwissPKI^{TM} by LibC which is a CA (Certification Authority) software which delivers robust hardware based centralized key management backed up by strong cryptography to protect business processes.
The solution addresses large scale cryptographic key management lifecycle, online hardware-to-hardware key distribution, tamper proof audit as well as usage logs for compliance with standards and covers the complete certificate and key management life cycle.

SwissSign CA is a feature rich, fully integrated Public Key Infrastructure service which helps expand your enterprise security. Our managed PKI Services provide all necessary out-of-the box capabilities and services to increase your digital security in a safe, simple and quick way.
SwissSign CA helps you keep your certificates up-to-date and maintain complete visibility over them.

1.1 Standards

SwissSign CA supports issuance and management of publicly trusted and qualified certificates. Its implementation is governed by the following standards and specifications:

- ✓ "Certificate Issuing and Management Components Protection Profile" defines requirements for components that issue, revoke, and manage public key certificates, such as X.509 public key certificates. The requirements are specified in the Common Criteria (CC).
- ✓ ETSI standards for issuing Qualified Certificates meeting requirements of Regulation
- ✓ ETSI standards for issuing Web Site certificates meeting requirements of the CA/Browser Forum documents
- ✓ ETSI Other Trust services including time-stamping and CAs issuing certificates other than qualified certificates
- ✓ CA/Browser Forum Baseline Requirement Guidelines, Extended Validation Guidelines and Network and Certificate System Security Requirements (CT Log, DNS Owner Checks and CAA Checks)
- ✓ Swiss law on electronic signatures and certificates ZertES
- ✓ X.509v3
- ✓ PKIX RFCs

2 Introduction

The RA UI is the end user interface for issuing certificates and managing their life cycle.

You access the RA UI in your role as Registration Authority Operator (RA Operator).

An RA Operator role authorizes you to carry out PKI tasks for one or more Clients; where a Client identifies an organization or entity which has an agreement with SwissSign. As an RA Operator you are responsible for accepting requests for digital certificates and authenticating the person, organization or system making the request for a specific certificate product.

The RA Operator role assigned to your user account is coupled to permissions. Your role being assigned to one or more Clients, SwissSign may assign you different permissions on a Client basis. For example, you may grant certificate issuance and revocation permissions for Client A and certificate issuance permission for Client B.

The RA Operator permissions are:

- ✓ Search for certificates and certificate orders and download certificates in various formats such as PEM, DER or PKCS#7
- ✓ Issue certificates
- ✓ Revoke certificates
- ✓ Publish/un-publish certificates (if the option is enabled for a certificate product)
- ✓ Update certificate meta data such as renewal Emails or certificate comments
- ✓ Search for ACME Tokens, their status and associated domain names
- ✓ Pre validate domain names for SSL certificate issuance
- ✓ Manage your API Keys. API Keys are used in conjunction with the REST API for automating your registration processes

As an RA Operator, you have access to certificates issued by all RA Operators assigned to the same Client~~s~~ as well as certificates issued by automated protocol handlers over protocols such as ACME , CMC or OpenAPI (RESTful RA API).

Issuing or revoking certificates via the RA UI is a manual process whereas protocols mentioned before are entirely automated. Depending on the product and protocol configuration assigned to the Client of the PKI, you will find certificates which have not been issued or revoked by yourself.

SwissSign CA supports several automated and non-automated enrolment protocols. Those protocols are:

Protocol	Description
RA UI	Manual certificate issuance and life cycle management (this document)
RA API	OpenAPI v3 specification for automating and integrating your MPKI with your services.
ACME	RFC8555 ACME HTTPS Service exposed to clients. Any client software compliant to this standard may be used. However, recommended and tested client software is - the Certbot ACME Client from Red Hat Enterprise Linux or - ACMESharp for Microsoft platforms
CMC	Certificate Management over CMS (Cryptographic Message Syntax) according to RFC 5272

3 RA UI

As a RA Operator, you are granted access to the following sections of the RA UI:

Section	Description
Dashboard	Overview page displaying - all certificates expiring in '*d*' days
Issuance	A searchable list of certificate products you can issue for selected Client(s)
Orders and Certificates	A searchable list of issued certificates and certificate orders
ACME	A searchable list of requested ACME Tokens, domain names and associated status. This section is available if you have certificate products associated with a Client which is enabled to issue certificates through the ACME protocol Note: ACME is only displayed if the protocol is used for certificate issuance.
Domain Validation	A searchable list of pre validated domain names.
Account	Your account information and settings In addition you find the service account for automated access over the RA API.

3.1 Login with SwissID

The RA Operator uses SwissID to log into the MPKI Service on SwissSign CA.

3.1.1 Onboarding on SwissID

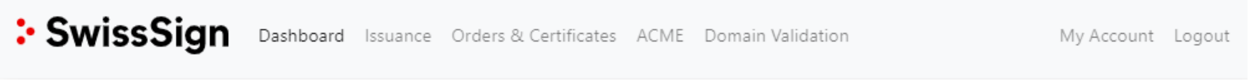
SwissID is a secure login of SwissSign. To onboard onto SwissID simply follow the instructions available under the following link:

https://www.swisssign.com/support/dokumentationen/ra-operator-onboarding

IMPORTANT: Please use as an RA Operator the same email-Adress as an Identifier which you used on the order Form for your MPKI Service as a or the Email-Adress under which you have been contacted by SwissSign as an already existing RA Operator of SwissSign's MPKI Service.

3.2 Main Menu

The RA UI gives you access to the different sections of the application through the main menu:



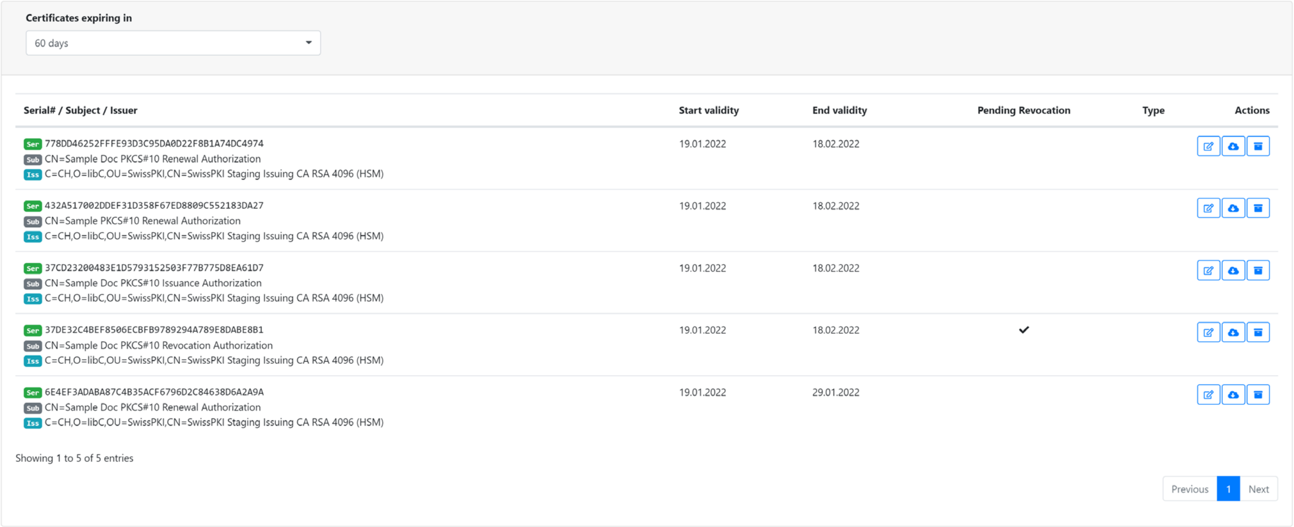
- For accessing the Dashboard see section *3.3 Dashboard*
- For accessing the Certificate Issuance see section *3.4 Issuance*
- For accessing the Orders and Certificates see section 3.5 *Orders and Certificates*
- For accessing the ACME Tokens see section 3.6 *ACME*
- For accessing the DNS see section 3.7 *DNS*
- For accessing the Account see section 3.8 *Account*

3.3 Dashboard

When logging into the RA UI, you will land on the dashboard page. There, you have access to a list of certificates expiring soon.

3.3.1 Expiring Certificates

The expiring certificates table displays a list of certificates which are about to expire. Use the dropdown menu located at the top of the panel to filter the list of expiring certificates.



Certificates expiring in

60 days

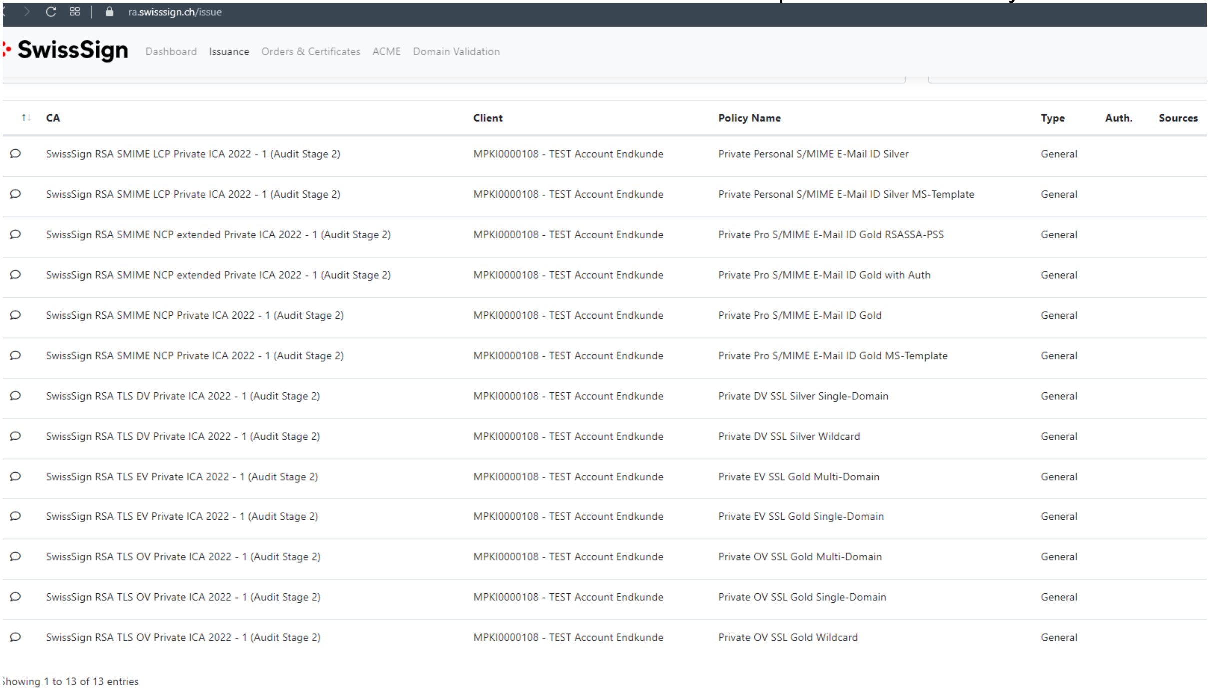
Serial# / Subject / Issuer	Start validity	End validity	Pending Revocation	Type	Actions
Ser 778DD46252FFFE93D3C95DA0D22F8B1A74DC4974 Sub CN=Sample Doc PKCS#10 Renewal Authorization Iss C=CH,O=libC,OU=SwissPKI,CN=SwissPKI Staging Issuing CA RSA 4096 (HSM)	19.01.2022	18.02.2022			
Ser 432A517002DDEF31D358F67ED8809C552183DA27 Sub CN=Sample PKCS#10 Renewal Authorization Iss C=CH,O=libC,OU=SwissPKI,CN=SwissPKI Staging Issuing CA RSA 4096 (HSM)	19.01.2022	18.02.2022			
Ser 37CD23200483E1D5793152503F77B775D8EA61D7 Sub CN=Sample Doc PKCS#10 Issuance Authorization Iss C=CH,O=libC,OU=SwissPKI,CN=SwissPKI Staging Issuing CA RSA 4096 (HSM)	19.01.2022	18.02.2022			
Ser 37DE32C4BEF8506ECBFB9789294A789E8DABE8B1 Sub CN=Sample Doc PKCS#10 Revocation Authorization Iss C=CH,O=libC,OU=SwissPKI,CN=SwissPKI Staging Issuing CA RSA 4096 (HSM)	19.01.2022	18.02.2022	✓		
Ser 6E4EF3ADABA87C4B35ACF6796D2C84638D6A2A9A Sub CN=Sample Doc PKCS#10 Renewal Authorization Iss C=CH,O=libC,OU=SwissPKI,CN=SwissPKI Staging Issuing CA RSA 4096 (HSM)	19.01.2022	29.01.2022			

Showing 1 to 5 of 5 entries

Column	Description
Serial#	The certificate's serial number
Subject	The certificate's subject DN
Issuer	The issuing CA's subject DN
Type	Indicates if the certificate is of type: - External certificate (imported from the current MPKI) -
Actions	1. Edit links to the certificate's detailed page 2. Download the certificate in PEM format 3. Send a publication request (only available if the certificate has the LDAP publication option enabled. This option is only available for S/MIME certificates)

3.4 Issuance

The issuance menu gives you access to the list of certificate products (policy instances) available for certificate issuance. The “search” and “clients” fields located on top of the table allow you to filter this list.



CA	Client	Policy Name	Type	Auth.	Sources
SwissSign RSA SMIME LCP Private ICA 2022 - 1 (Audit Stage 2)	MPKI0000108 - TEST Account Endkunde	Private Personal S/MIME E-Mail ID Silver	General		
SwissSign RSA SMIME LCP Private ICA 2022 - 1 (Audit Stage 2)	MPKI0000108 - TEST Account Endkunde	Private Personal S/MIME E-Mail ID Silver MS-Template	General		
SwissSign RSA SMIME NCP extended Private ICA 2022 - 1 (Audit Stage 2)	MPKI0000108 - TEST Account Endkunde	Private Pro S/MIME E-Mail ID Gold RSASSA-PSS	General		
SwissSign RSA SMIME NCP extended Private ICA 2022 - 1 (Audit Stage 2)	MPKI0000108 - TEST Account Endkunde	Private Pro S/MIME E-Mail ID Gold with Auth	General		
SwissSign RSA SMIME NCP Private ICA 2022 - 1 (Audit Stage 2)	MPKI0000108 - TEST Account Endkunde	Private Pro S/MIME E-Mail ID Gold	General		
SwissSign RSA SMIME NCP Private ICA 2022 - 1 (Audit Stage 2)	MPKI0000108 - TEST Account Endkunde	Private Pro S/MIME E-Mail ID Gold MS-Template	General		
SwissSign RSA TLS DV Private ICA 2022 - 1 (Audit Stage 2)	MPKI0000108 - TEST Account Endkunde	Private DV SSL Silver Single-Domain	General		
SwissSign RSA TLS DV Private ICA 2022 - 1 (Audit Stage 2)	MPKI0000108 - TEST Account Endkunde	Private DV SSL Silver Wildcard	General		
SwissSign RSA TLS EV Private ICA 2022 - 1 (Audit Stage 2)	MPKI0000108 - TEST Account Endkunde	Private EV SSL Gold Multi-Domain	General		
SwissSign RSA TLS EV Private ICA 2022 - 1 (Audit Stage 2)	MPKI0000108 - TEST Account Endkunde	Private EV SSL Gold Single-Domain	General		
SwissSign RSA TLS OV Private ICA 2022 - 1 (Audit Stage 2)	MPKI0000108 - TEST Account Endkunde	Private OV SSL Gold Multi-Domain	General		
SwissSign RSA TLS OV Private ICA 2022 - 1 (Audit Stage 2)	MPKI0000108 - TEST Account Endkunde	Private OV SSL Gold Single-Domain	General		
SwissSign RSA TLS OV Private ICA 2022 - 1 (Audit Stage 2)	MPKI0000108 - TEST Account Endkunde	Private OV SSL Gold Wildcard	General		

Showing 1 to 13 of 13 entries

Column	Description
CA	The certificate product Issuing CA
Client	The client associated to the certificate product (you may have the permission to manage certificates for multiple clients. Use the client dropdown menu to filter the available clients)
Policy Name	The certificate product name
Type	The certificate product type (always displayed as *General* for RA Operator issuance)
Auth	Displays a tick if an authorization rule is associated to the policy instance.
Sources	Displays a tick if issuance occurs over a given set of pre-filled data sources (DB and/or LDAP). Pre-defined data sources restrict certificate issuance to the available records found in the data source(s)
Actions	Issue certificate redirects to the certificate’s issuance page.

3.4.1 Certificate Policies

Issuing a certificate is done by completing the policy details on the certificate issuance page. The fields you fill will vary depending on a number of parameters:

- Policy fields which are visible and non-editable are greyed out. Those values are set by SwissSign and you cannot override the content.
- Some policy fields may not be displayed but will be part of the issued certificate
- Policy fields which are visible and editable may be filled or edited by you. Some of the fields may be mandatory or optional. Mandatory fields are marked with an ‘*’
- The type of key generation (PKCS#10, PKCS#12).

If the policy requires PKCS#10, you are required to provide a CSR matching the key generation parameters defined in the policy. Note that you can provide a CSR with a key pair size which is larger than the value defined in the policy. The key pair must match the defined algorithm. When copy/pasting a CSR, the values contained in the request are pre-filled in the form for all editable values.
If the policy requires PKCS#12 key generation, SwissSign will generate a key pair for you and notify the certificate recipients for certificate download including the key pair for PKCS#12

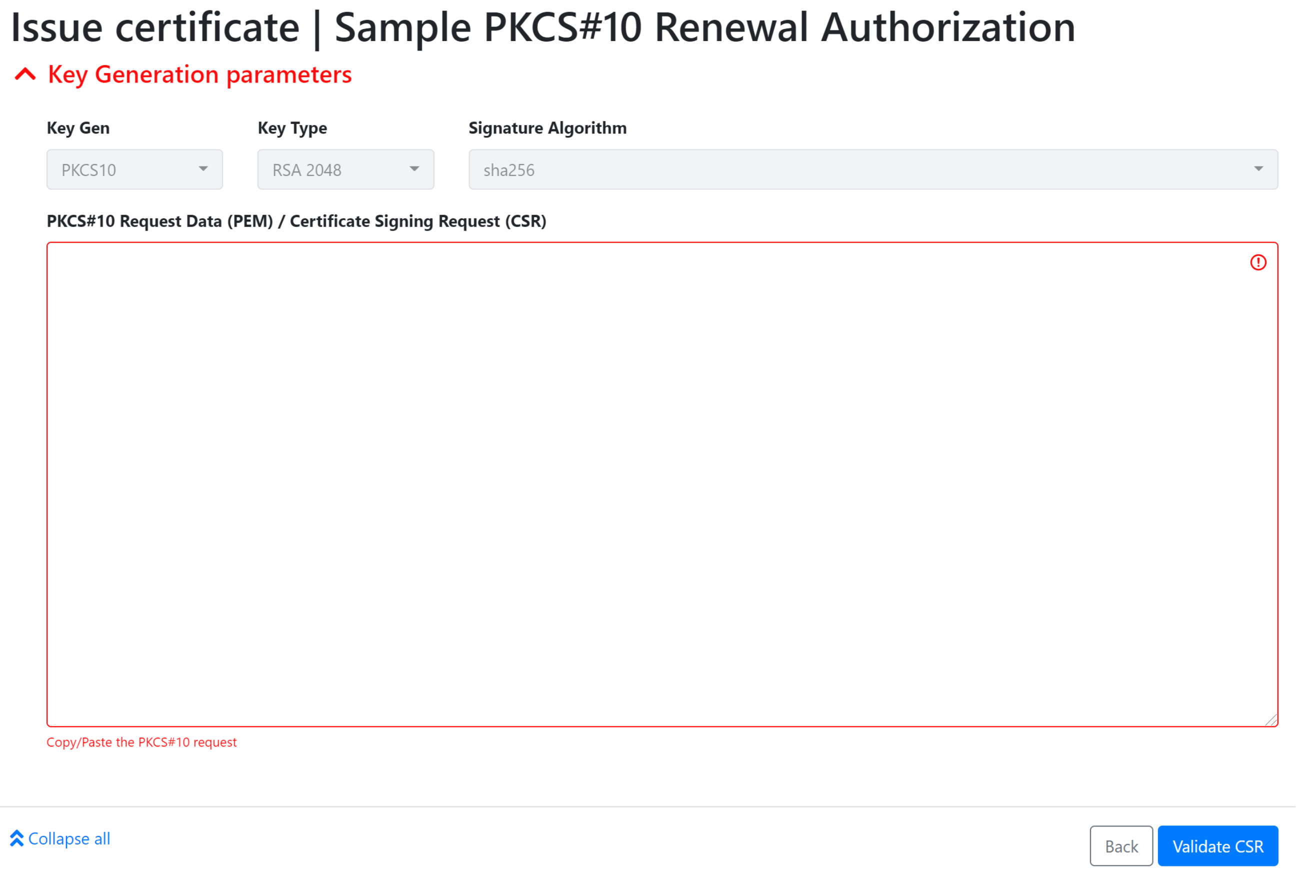
- The modules activated in the policy template
- The rules associated to the policy instance

3.4.2 Issuing PKCS#10

When issuing for a policy requiring PKCS#10, you must generate a PKCS#10 (CSR) using for example OpenSSL, Microsoft CNG or any generation tool which produces a base64 encoded PKCS#10 request. The format of a PKCS#10 is as follows:

```
-----BEGIN CERTIFICATE REQUEST-----
MIICqTCCAZECAQAwPzEdMBsGA1UECgwUbGliQyBUZWNobm9sb2dpZXMgU0ExETAP
[snipped] … [snipped]
H+aC3/oJkApfonUK5m7eFzDsrN/cMWFQUQ5xFNDCzGmqBdX4U/Ft+s323otQMTN6
nl6IHYxn7IGxyCIAVg==
-----END CERTIFICATE REQUEST-----
```

The certificate issuance page displays the text area, as illustrated below, where you paste the generated PKCS#10 request:



Issue certificate | Sample PKCS#10 Renewal Authorization

Key Generation parameters

Key Gen: PKCS10

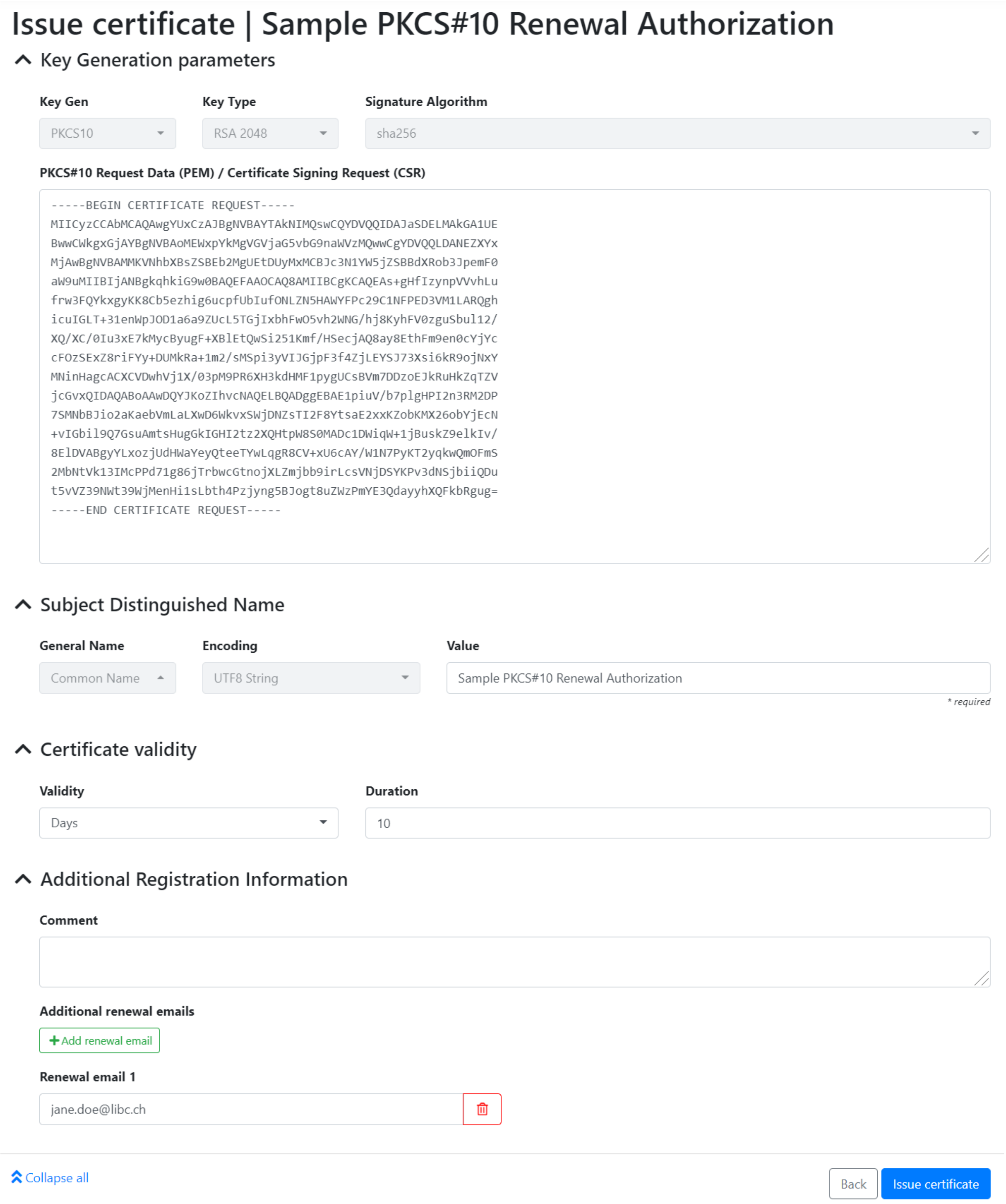
Key Type: RSA 2048

Signature Algorithm: sha256

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

Copy/Paste the PKCS#10 request

Once the request is pasted, the UI automatically validates the certificate request. If the validation of the request succeeds, the remaining part of the pre-filled policy is displayed. If the validation of the request fails, a validation error message is displayed.



Issue certificate | Sample PKCS#10 Renewal Authorization

Key Generation parameters

Key Gen	Key Type	Signature Algorithm
PKCS10	RSA 2048	sha256

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

```
-----BEGIN CERTIFICATE REQUEST-----
MIICyzCCAbMCAQAwgYUxCzAJBgNVBAYTAkNIMQswCQYDVQQIDAJaSDELMAkGA1UE
BwwCWkgxGjAYBgNVBAoMEWxpYkMgVGVjaG5vbG9naWVzMQwwCgYDVQQLDANEZXYx
MjAwBgNVBAMMKVNhbXBsZSBEb2MgUEtDUyMxMCBJc3N1YW5jZSBBdXRob3JpemF0
aW9uMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAs+gHfIzynpVVvhLu
frw3FQYkxgyKK8Cb5ezhig6ucpfUbIufONLZN5HAWYFPc29C1NFPED3VM1LARQgh
icuIGLT+31enWpJOD1a6a9ZUcL5TGjIxbhFwO5vh2WNG/hj8KyhFV0zguSbul12/
XQ/XC/0Iu3xE7kMycByugF+XBlEtQwSi251Kmf/HSecjAQ8ay8EthFm9en0cYjYc
cFOzSExZ8riFYy+DUMkRa+1m2/sMSpi3yVIJGjpF3f4ZjLEYSJ73Xsi6kR9ojNxY
MNinHagcACXCVDwhVj1X/03pM9PR6XH3kdHMF1pygUCsBVm7DDzoEJkRuHkZqTZV
jcGvxQIDAQABoAAwDQYJKoZIhvcNAQELBQADggEBAE1piuV/b7plgHPI2n3RM2DP
7SMNbBJio2aKaebVmLaLXwD6WkvxSWjDNZsTI2F8YtsaE2xxKZobKMX26obYjEcN
+vIGbil9Q7GsuAmtsHugGkIGHI2tz2XQHtpW8S0MADc1DWiqW+1jBuskZ9elkIv/
8ElDVABgyYLxozjUdHWaYeyQteeTYwLqgR8CV+xU6cAY/W1N7PyKT2yqkwQmOFmS
2MbNtVk13IMcPPd71g86jTrbwcGtnojXLZmjbb9irLcsVNjDSYKPv3dNSjbiiQDu
t5vVZ39NWt39WjMenHi1sLbth4Pzjyng5BJogt8uZWzPmYE3QdayyhXQFkbRgug=
-----END CERTIFICATE REQUEST-----
```

Subject Distinguished Name

General Name	Encoding	Value
Common Name	UTF8 String	Sample PKCS#10 Renewal Authorization

** required*

Certificate validity

Validity	Duration
Days	10

Additional Registration Information

Comment

Additional renewal emails

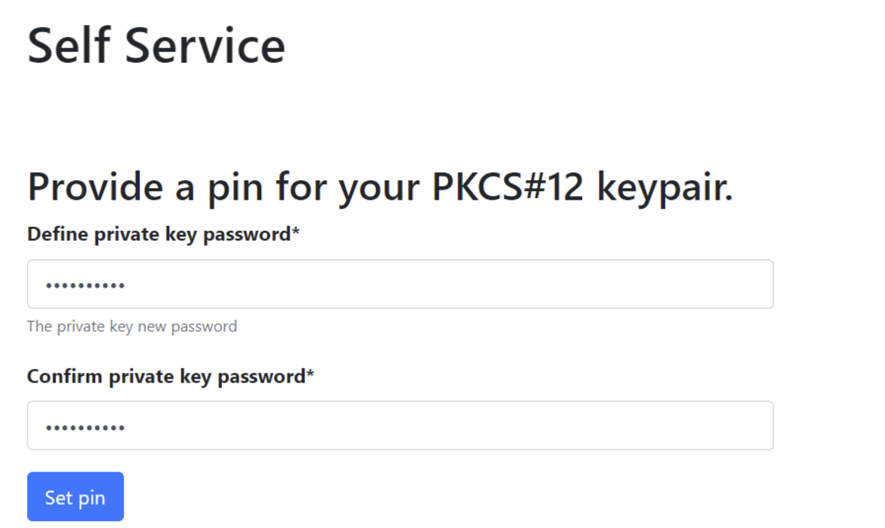
Renewal email 1: jane.doe@libc.ch

The holder of the email address for the certificate receives a confirmation mail to his address. Upon confirmation he receives a specific download link where he can enter his PIN/password:

3.4.3 **Issuing PKCS#12**

To issue certificate with server-side key generation (PKCS#12), you simply fill in all mandatory editable policy fields values on issuance page.

Note: When the key generation is PKCS#12 with PIN, the end user must provide the PKCS#12 protection PIN before key generation. This implies that the PKCS#12 private key cannot be escrowed and therefore not available for download to other recipients for recovery. An email with a link to set the PKCS#12 PIN is sent to the recipient (email in the SAN RFC822 extension of the certificate) for providing the information before issuing the certificate and associated key pair. Additionally, the PKCS#12 data is deleted after 3 months from the PKI database.



Self Service

Provide a pin for your PKCS#12 keypair.

Define private key password*

••••••••••

The private key new password

Confirm private key password*

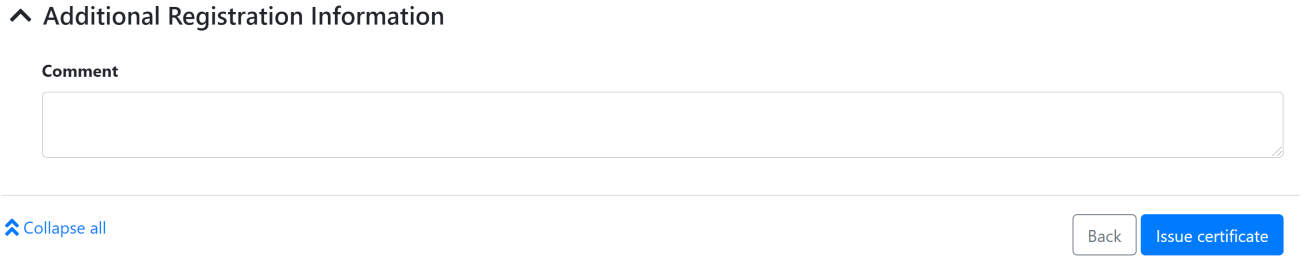
••••••••••

3.4.4 Additional Registration Information

The additional registration information collects meta data about the certificate order. You can provide contextual information in the ‘comment’ text area. This information is added to the certificate order and can be consulted at a later time by other RA Operators. Comments for a certificate order can also be added at a later time.

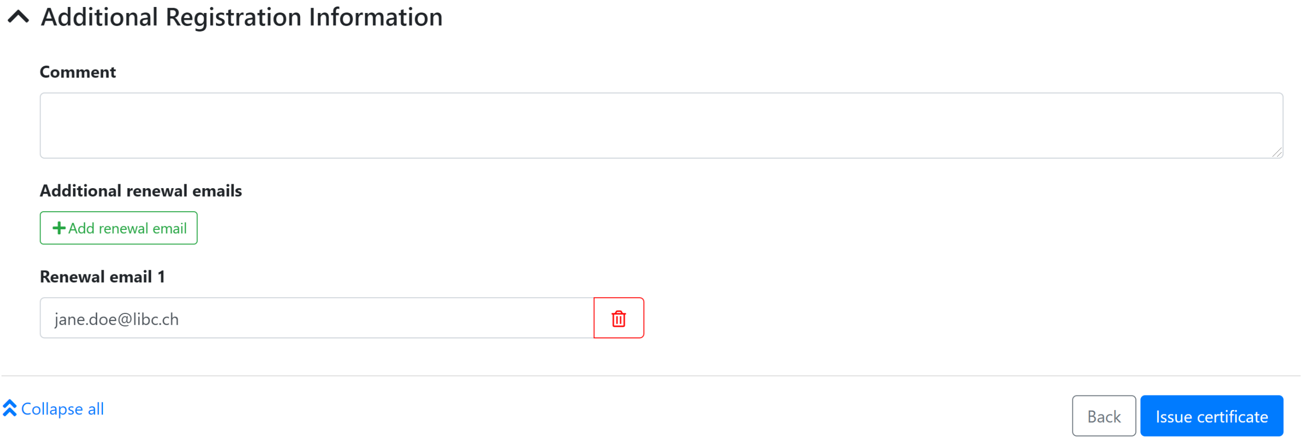
Comment text area

This is always active and allows you to attach comments to your certificate. These comments are then displayed when users go to the certificate’s details page.



3.4.5 Additional renewal emails

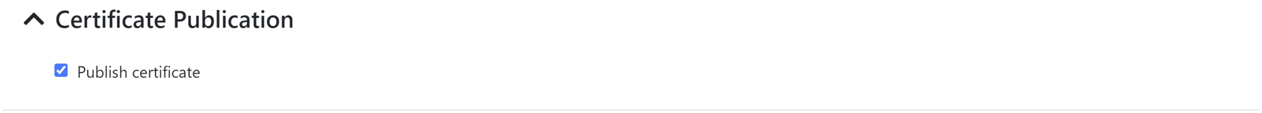
This is displayed when a renewal rule is assigned to the policy instance. Email addresses in this list receive renewal notifications. It is possible that your issued certificate does not contain any email address in the Subject Alternative Name (RFC822). Use the ‘Additional renewal email’ fields to include recipients you want to inform about certificate renewal. RA Operators receive renewal notifications, if requested.


Additional Registration Information
Comment
Additional renewal emails
Add renewal email
Collapse all
Back
Issue certificate

Renewal email 1: jane.doe@libc.ch

3.4.6 Certificate Publication

Only for S/MIME certificates: When LDAP publication of the certificate is enabled on the certificate policy, you have the option to enable or disable the publication of the issued certificate in the LDAP. The information for accessing the LDAP is provided by SwissSign.
When enabled, the issued certificate is published to the LDAP and removed from the LDAP when revoked.



Certificate Publication

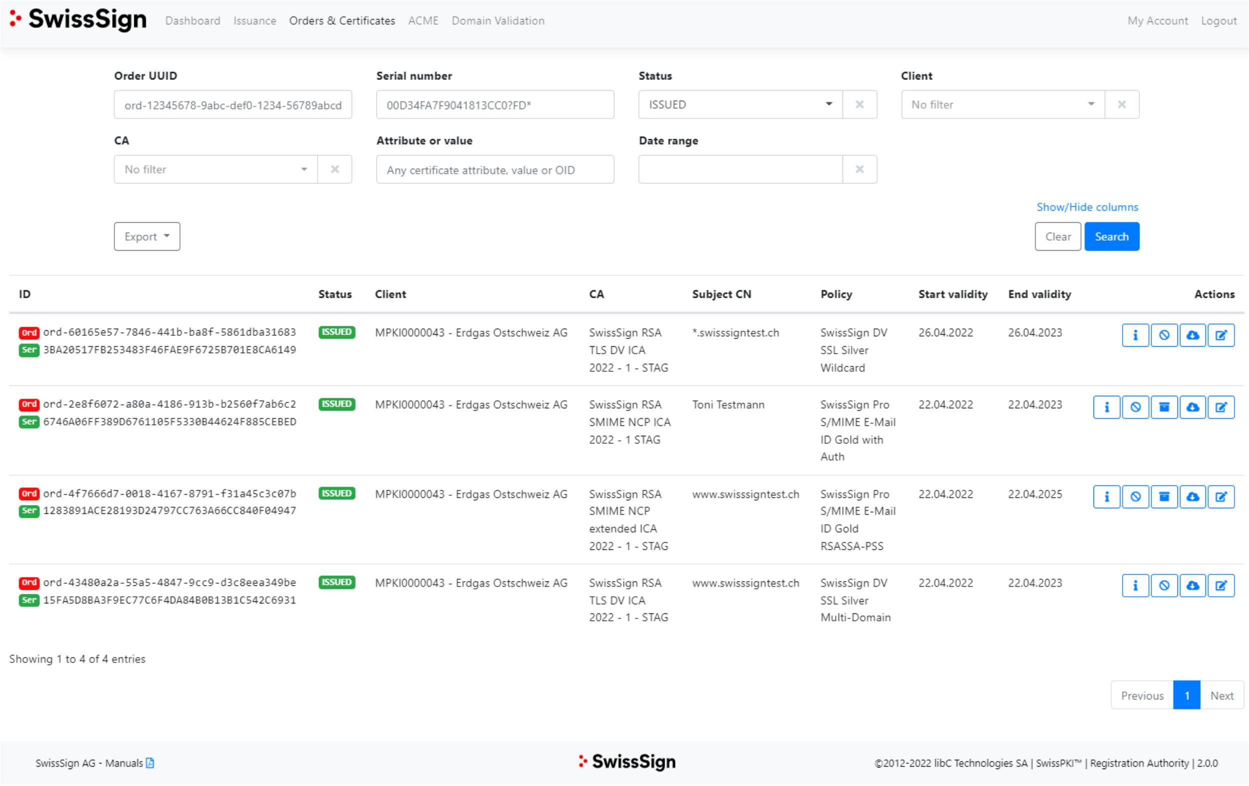
☑ Publish certificate

3.5 Orders and Certificates

Every certificate issuance request creates a certificate order. The certificate order is identified by a unique Id in the form a UUID prefixed with ‘ord-‘.
Example: ord-4068d5fe-feab-4c15-a1f2-a0cdd9268320
The certificate issuance process sets the certificate order into different status depending on the processing stage.

Certificate Order Status	Description	Has certificate
NEW	A new certificate order is created and the certificate policy is validated (statically and runtime). The issuance process starts.	no
PENDING_CSR_RENEWAL	The certificate order is an automatic certificate renewal for which a rule is defined. The recipient of the renewed certificate must provide a CSR such that the processing can continue. The processing job is paused and put into WAIT state.	no
KEY_VALIDATION	Key pair is validated, optionally generated if the certificate policy is of type PKCS#12	no
GENERATE_TBS	TBS structure generation based on the certificate’s policy. This structure is immutable except for the CT extension.	no
PRE_VALIDATION	Starts multiple child jobs to validate once more the static content and the runtime values, effectuates a CAA check if required, proceeds with DNS Owner check and/or end user email validation if required and TBS pre-linting	no
PRE_ISSUE	Executes the pre cert CT log entry if required	no
ISSUE	Issue the certificate. Remove the poison pill from the CT log structure if required and signs the TBS structure to produce the final certificate	yes
POST_VALIDATION	Execute post linting if required and CT log publication when enabled	yes
FINALIZE_ISSUANCE	Clean up the order processing and send out notifications if required. Send a certificate publication request if option is enabled.	yes
ISSUED	Order processing is done, set the certificate order to ISSUED state.	yes
REVOKED	Certificate order is revoked	yes
FAILED	Order processing failed. If a certificate is issued and the processing fails after the ISSUE stage, then it is revoked	-
UNKNOWN	Undefined state, the order is lost and is cleaned up by the scheduler optionally revoking the certificate if present and valid.	-

The orders and certificates page list all certificates and orders associated to your clients. The search section at the top of the page allows you to filter the list.



Order UUID: ord-12345678-9abc-def0-1234-56789abcd

Serial number: 00D34FA7F9041813CC0?FD*

Status: ISSUED

Client: No filter

CA: No filter

Attribute or value: Any certificate attribute, value or OID

Date range:

ID	Status	Client	CA	Subject CN	Policy	Start validity	End validity	Actions
Ord ord-60165e57-7846-441b-ba8f-5861dba31683 Ser 3BA20517FB253483F46FAE9F6725B701E8CA6149	ISSUED	MPKI0000043 - Erdgas Ostschweiz AG	SwissSign RSA TLS DV ICA 2022 - 1 - STAG	*.swisssigntest.ch	SwissSign DV SSL Silver Wildcard	26.04.2022	26.04.2023	ℹ ⊘ ☁ ✎
Ord ord-2e8f6072-a80a-4186-913b-b2560f7ab6c2 Ser 6746A06FF389D6761105F5330B44624F885CEBED	ISSUED	MPKI0000043 - Erdgas Ostschweiz AG	SwissSign RSA SMIME NCP ICA 2022 - 1 STAG	Toni Testmann	SwissSign Pro S/MIME E-Mail ID Gold with Auth	22.04.2022	22.04.2023	ℹ ⊘ ▬ ☁ ✎
Ord ord-4f7666d7-0018-4167-8791-f31a45c3c07b Ser 1283891ACE28193D24797CC763A66CC840F04947	ISSUED	MPKI0000043 - Erdgas Ostschweiz AG	SwissSign RSA SMIME NCP extended ICA 2022 - 1 - STAG	www.swisssigntest.ch	SwissSign Pro S/MIME E-Mail ID Gold RSASSA-PSS	22.04.2022	22.04.2025	ℹ ⊘ ▬ ☁ ✎
Ord ord-43480a2a-55a5-4847-9cc9-d3c8eea349be Ser 15FA5D8BA3F9EC77C6F4DA84B0B13B1C542C6931	ISSUED	MPKI0000043 - Erdgas Ostschweiz AG	SwissSign RSA TLS DV ICA 2022 - 1 - STAG	www.swisssigntest.ch	SwissSign DV SSL Silver Multi-Domain	22.04.2022	22.04.2023	ℹ ⊘ ☁ ✎

Showing 1 to 4 of 4 entries

©2012-2022 libC Technologies SA | SwissPKI™ | Registration Authority | 2.0.0

Column	Description
ID	Contains certificate's order UUID and serial number.
Status	Contains the certificate's status.
Client	Contains the client used to issue this certificate.
CA	Contains the certification authority used to issue this certificate.
Subject CN	Contains the certificate's subject common name.
Policy	Contains the policy instance (certificate product) used to issue this certificate.
Start Validity	Contains the certificate's start validity date.
End Validity	Contains the certificate's end validity date.
ℹ	Redirects you to the certificate order's page. Displays the list of tasks executed for the certificate order.
⊘	This button allows you to send a certificate revocation request.
▬	This button allows you to send a certificate publication request. The option is present when publication is enabled for the certificate.
☁	Download the certificate in PEM format.
✎	Redirects to the certificate details page.

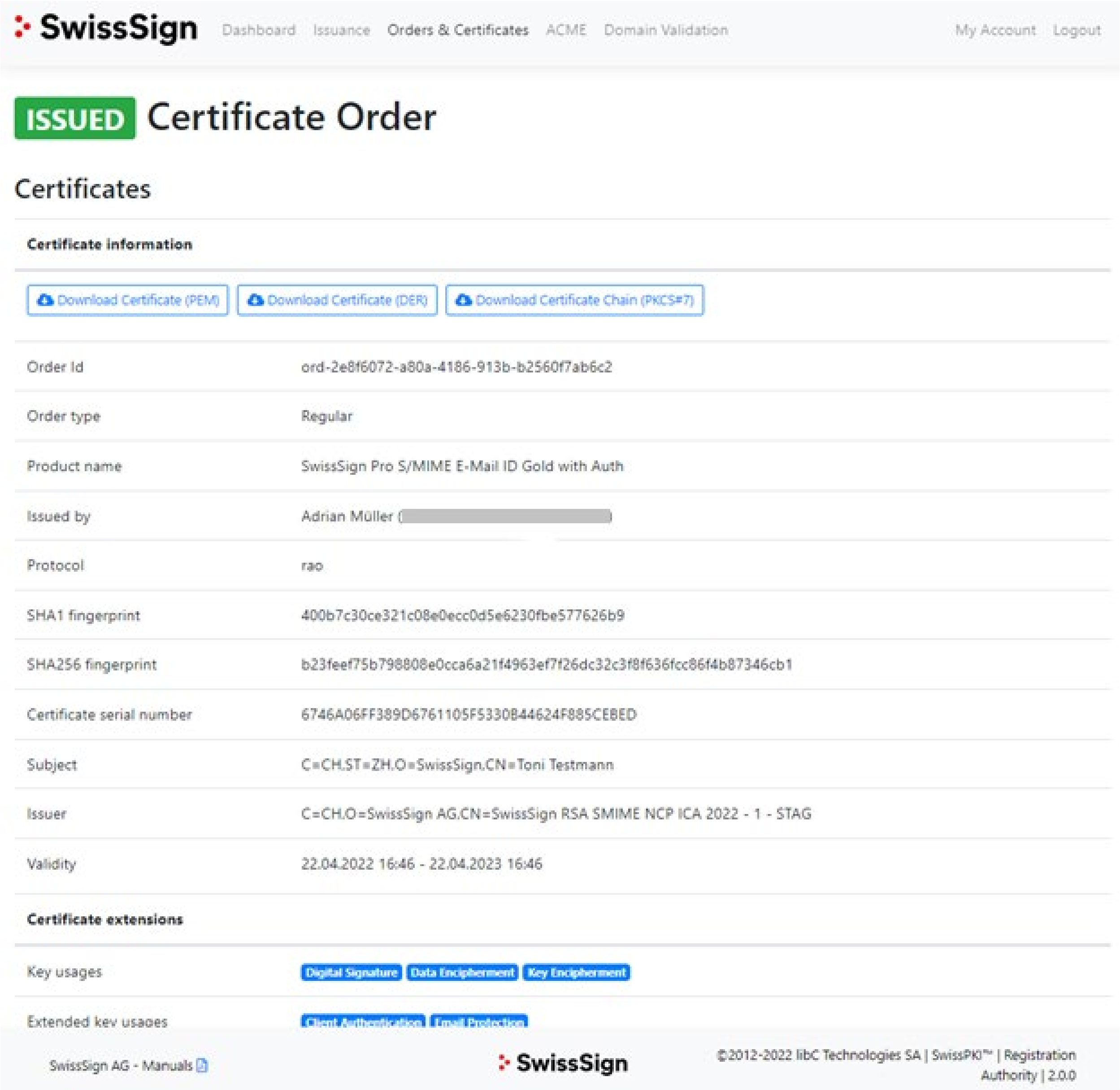
3.5.1 Certificate Order Details

The certificate order details page is divided in two sections:

1. Issued certificate
2. Associated order processing tasks and their respective status

3.5.1.1Issued Certificate

This section contains the certificate associated to the order. The order must be status ISSUED.



SwissSign
Dashboard
Issuance
Orders & Certificates
ACME
Domain Validation
My Account
Logout

ISSUED Certificate Order

Certificates

Certificate information

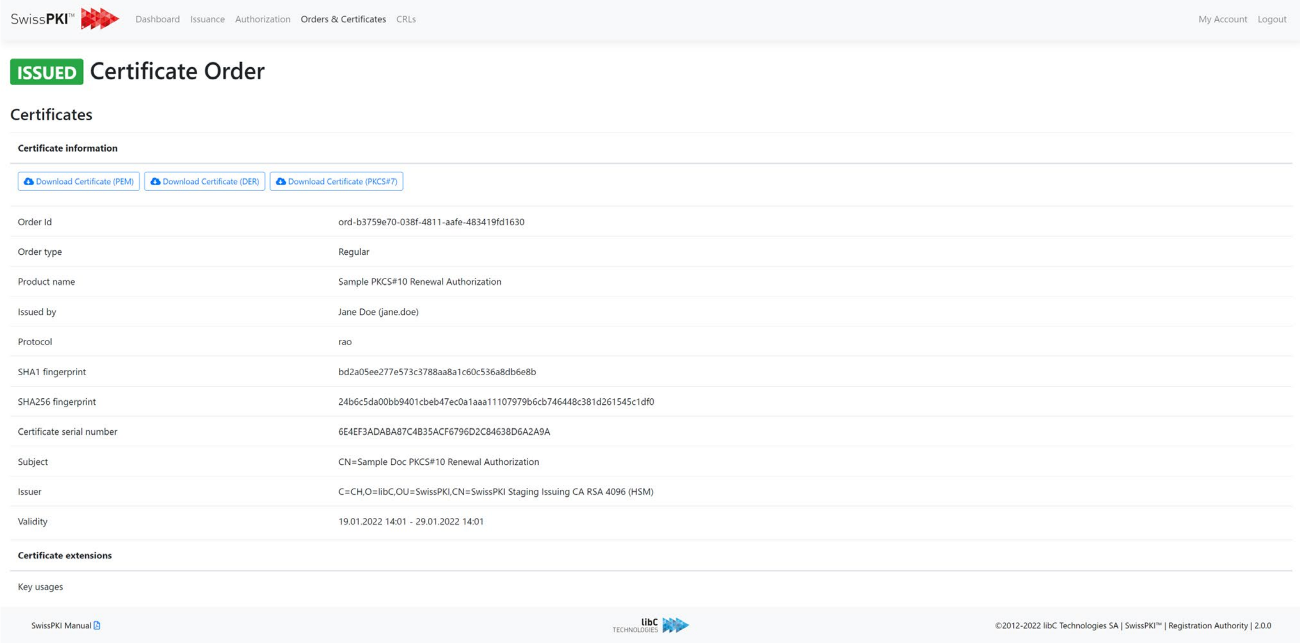
Download Certificate (PEM)
Download Certificate (DER)
Download Certificate Chain (PKCS#7)

Order Id	ord-2e8f6072-a80a-4186-913b-b2560f7ab6c2
Order type	Regular
Product name	SwissSign Pro S/MIME E-Mail ID Gold with Auth
Issued by	Adrian Müller ([redacted])
Protocol	rao
SHA1 fingerprint	400b7c30ce321c08e0ecc0d5e6230fbe577626b9
SHA256 fingerprint	b23feef75b798808e0cca6a21f4963ef7f26dc32c3f8f636fcc86f4b87346cb1
Certificate serial number	6746A06FF389D6761105F5330B44624F885CEBED
Subject	C=CH,ST=ZH,O=SwissSign,CN=Toni Testmann
Issuer	C=CH,O=SwissSign AG,CN=SwissSign RSA SMIME NCP ICA 2022 - 1 - STAG
Validity	22.04.2022 16:46 - 22.04.2023 16:46

Certificate extensions

Key usages	Digital Signature Data Encipherment Key Encipherment
Extended key usages	Client Authentication Email Protection

SwissSign AG - Manuals
SwissSign
©2012-2022 libC Technologies SA | SwissPKI™ | Registration Authority | 2.0.0



SwissPKI™
Dashboard
Issuance
Authorization
Orders & Certificates
CRLs
My Account
Logout

ISSUED Certificate Order

Certificates

Certificate information

Download Certificate (PEM)
Download Certificate (DER)
Download Certificate (PKCS#7)

Order Id	ord-b3759e70-038f-4811-aafe-483419fd1630
Order type	Regular
Product name	Sample PKCS#10 Renewal Authorization
Issued by	Jane Doe (jane.doe)
Protocol	rao
SHA1 fingerprint	bd2a05ee277e573c3788aa8a1c60c536a8db6e8b
SHA256 fingerprint	24b6c5da00bb9401cbeb47ec0a1aaa11107979b6cb746448c381d261545c1df0
Certificate serial number	6E4EF3ADABA87C4B35ACF6796D2C84638D6A2A9A
Subject	CN=Sample Doc PKCS#10 Renewal Authorization
Issuer	C=CH,O=libC,OU=SwissPKI,CN=SwissPKI Staging Issuing CA RSA 4096 (HSM)
Validity	19.01.2022 14:01 - 29.01.2022 14:01

Certificate extensions

Key usages

SwissPKI Manual
libC TECHNOLOGIES
©2012-2022 libC Technologies SA | SwissPKI™ | Registration Authority | 2.0.0

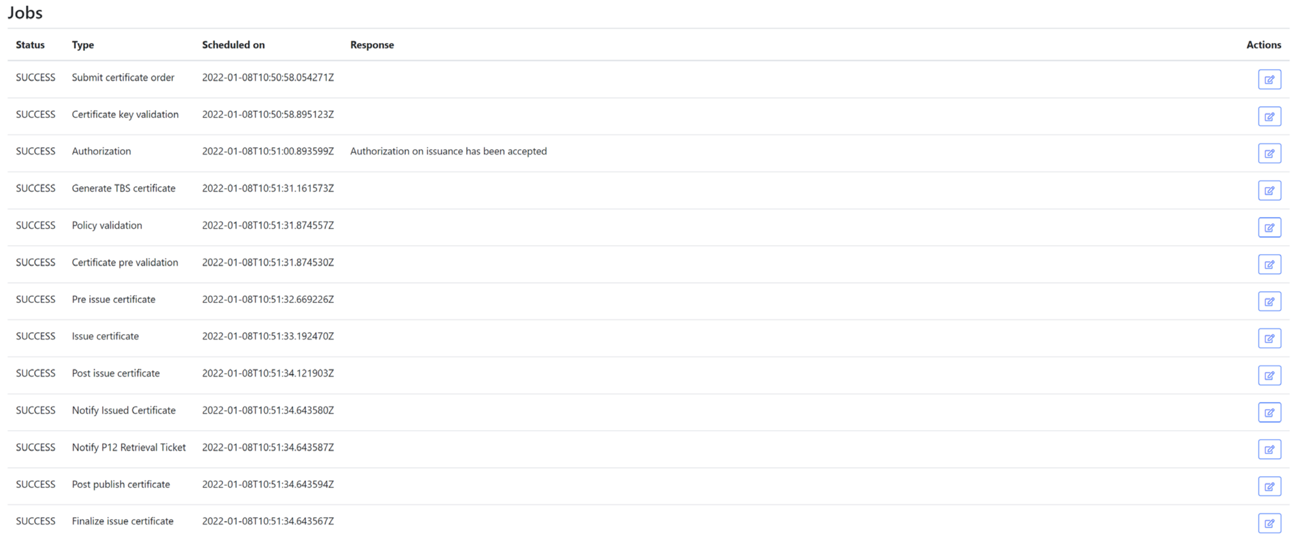
3.5.1.2Certificate Order Processing Tasks

ℹ

The jobs (order processing tasks) section lists the jobs executed for this order with their respective state. The data of each job can be accessed individually by clicking on the button located in the action column of the table.

Job Status	Description
WAITING	job created but not scheduled, e.g. parent job waiting for children jobs to finish
PENDING	job created and sent to the queue
PROCESSING	job being processed by the queue
SUCCESS	job successfully processed
FAILED	job failed
SCHEDULE_REQUEST	job created and not yet sent to the queue
SCHEDULE_RESPONSE	job processed and response not yet sent to the queue
RETRY	job processed and marked for retry

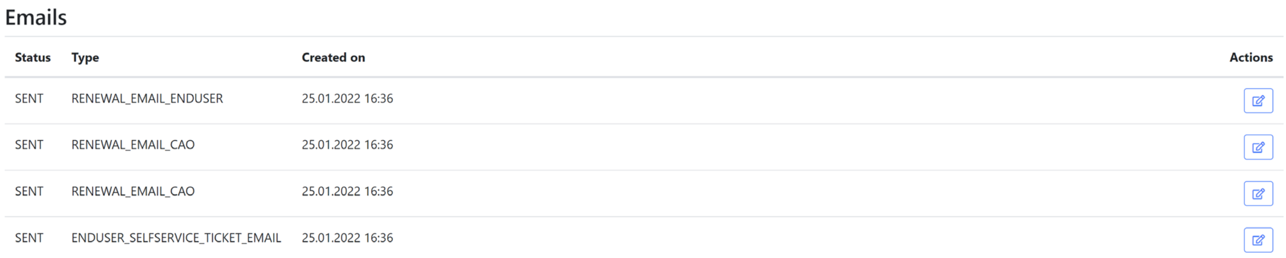
The list of jobs and respective status executed during the order processing



Jobs

Status	Type	Scheduled on	Response	Actions
SUCCESS	Submit certificate order	2022-01-08T10:50:58.054271Z		✎
SUCCESS	Certificate key validation	2022-01-08T10:50:58.895123Z		✎
SUCCESS	Authorization	2022-01-08T10:51:00.893599Z	Authorization on issuance has been accepted	✎
SUCCESS	Generate TBS certificate	2022-01-08T10:51:31.161573Z		✎
SUCCESS	Policy validation	2022-01-08T10:51:31.874557Z		✎
SUCCESS	Certificate pre validation	2022-01-08T10:51:31.874530Z		✎
SUCCESS	Pre issue certificate	2022-01-08T10:51:32.669226Z		✎
SUCCESS	Issue certificate	2022-01-08T10:51:33.192470Z		✎
SUCCESS	Post issue certificate	2022-01-08T10:51:34.121903Z		✎
SUCCESS	Notify Issued Certificate	2022-01-08T10:51:34.643580Z		✎
SUCCESS	Notify P12 Retrieval Ticket	2022-01-08T10:51:34.643587Z		✎
SUCCESS	Post publish certificate	2022-01-08T10:51:34.643594Z		✎
SUCCESS	Finalize issue certificate	2022-01-08T10:51:34.643567Z		✎

If the order processing sends email notification to recipients, the list of sent notification is displayed below the jobs. As an RA Operator, you have the option to resend the notification if the SMTP server or SMTP relay did not deliver the email to the recipient.

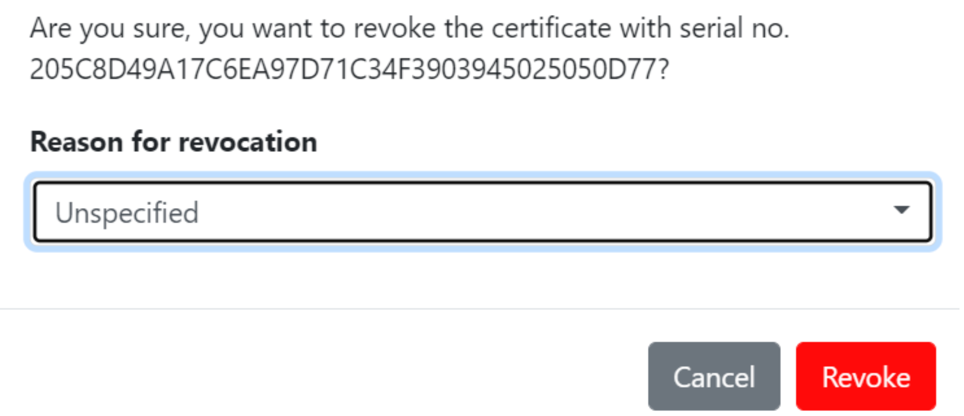


Emails

Status	Type	Created on	Actions
SENT	RENEWAL_EMAIL_ENDUSER	25.01.2022 16:36	✎
SENT	RENEWAL_EMAIL_CAO	25.01.2022 16:36	✎
SENT	RENEWAL_EMAIL_CAO	25.01.2022 16:36	✎
SENT	ENDUSER_SELFSERVICE_TICKET_EMAIL	25.01.2022 16:36	✎

3.5.2 Revoke Certificate

You revoke a certificate clicking on the revoke button located in the actions column of the orders and certificates table. After you click the button, a popup dialog will ask you to confirm the action.
By default, the reason of revocation will be set to “Unspecified”. More information to all different revocation reasons can be found in our Subscriber Agreement in Annex A.



Are you sure, you want to revoke the certificate with serial no. 205C8D49A17C6EA97D71C34F3903945025050D77?

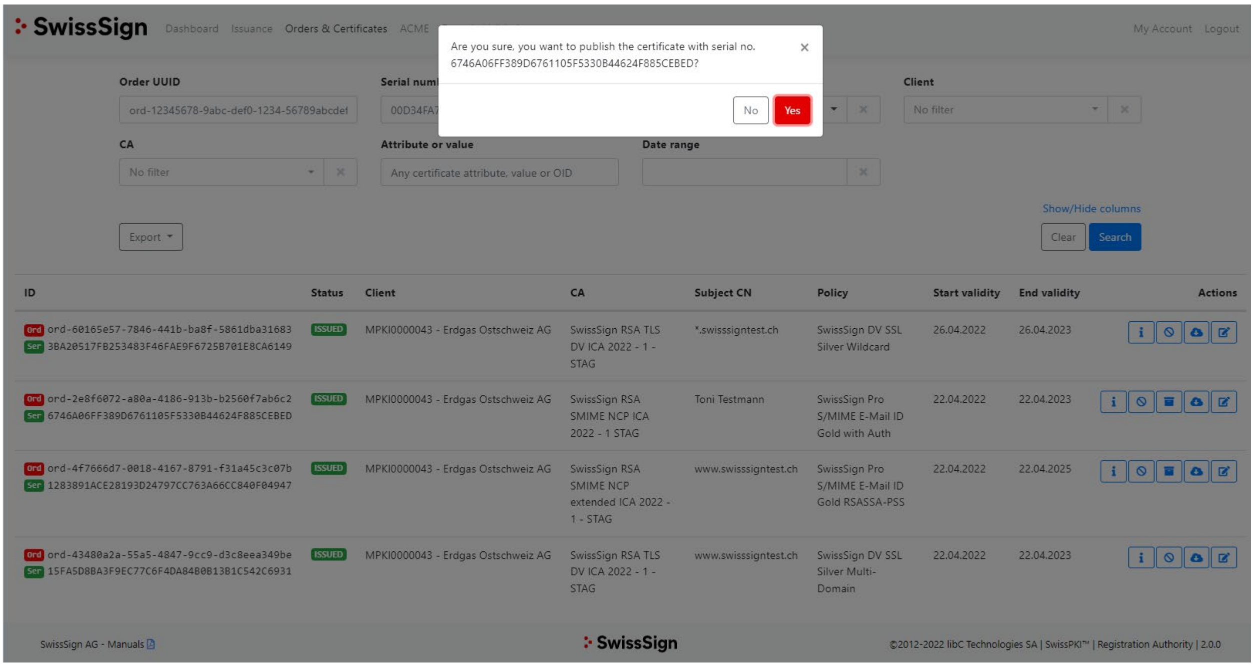
Reason for revocation: Unspecified

Confirm the certificate revocation by clicking on the yes button. Note that the revocation action sends a request to the CA and may trigger an authorization if a rule is defined for the selected certificate. Once revoked, the revocation action button is unavailable.

3.5.3 Publish Certificate

Publishing a certificate is done by clicking on the publish button located in the action column of the orders and certificates table. Once you clicked the button, a popup dialog will ask you to confirm the certificate publication.

Note that the publication action is available when the publication to LDAP is enabled for the selected certificate and permission is granted.



Are you sure, you want to publish the certificate with serial no. 6746A06FF389D6761105F5330B44624F885CEBED?

ID	Status	Client	CA	Subject CN	Policy	Start validity	End validity	Actions
Ord ord-60165e57-7846-441b-ba8f-5861dba31683 Ser 3BA20517FB253483F46FAE9F6725B701E8CA6149	ISSUED	MPKI0000043 - Erdgas Ostschweiz AG	SwissSign RSA TLS DV ICA 2022 - 1 - STAG	*.swisssigntest.ch	SwissSign DV SSL Silver Wildcard	26.04.2022	26.04.2023	i ⦸ ☁ ✎
Ord ord-2e8f6072-a80a-4186-913b-b2560f7ab6c2 Ser 6746A06FF389D6761105F5330B44624F885CEBED	ISSUED	MPKI0000043 - Erdgas Ostschweiz AG	SwissSign RSA SMIME NCP ICA 2022 - 1 STAG	Toni Testmann	SwissSign Pro S/MIME E-Mail ID Gold with Auth	22.04.2022	22.04.2023	i ⦸ ▬ ☁ ✎
Ord ord-4f7666d7-0018-4167-8791-f31a45c3c07b Ser 1283891ACE28193D24797CC763A66CC840F04947	ISSUED	MPKI0000043 - Erdgas Ostschweiz AG	SwissSign RSA SMIME NCP extended ICA 2022 - 1 - STAG	www.swisssigntest.ch	SwissSign Pro S/MIME E-Mail ID Gold RSASSA-PSS	22.04.2022	22.04.2025	i ⦸ ▬ ☁ ✎
Ord ord-43480a2a-55a5-4847-9cc9-d3c8eea349be Ser 15FA5D8BA3F9EC77C6F4DA84B0B13B1C542C6931	ISSUED	MPKI0000043 - Erdgas Ostschweiz AG	SwissSign RSA TLS DV ICA 2022 - 1 - STAG	www.swisssigntest.ch	SwissSign DV SSL Silver Multi-Domain	22.04.2022	22.04.2023	i ⦸ ☁ ✎

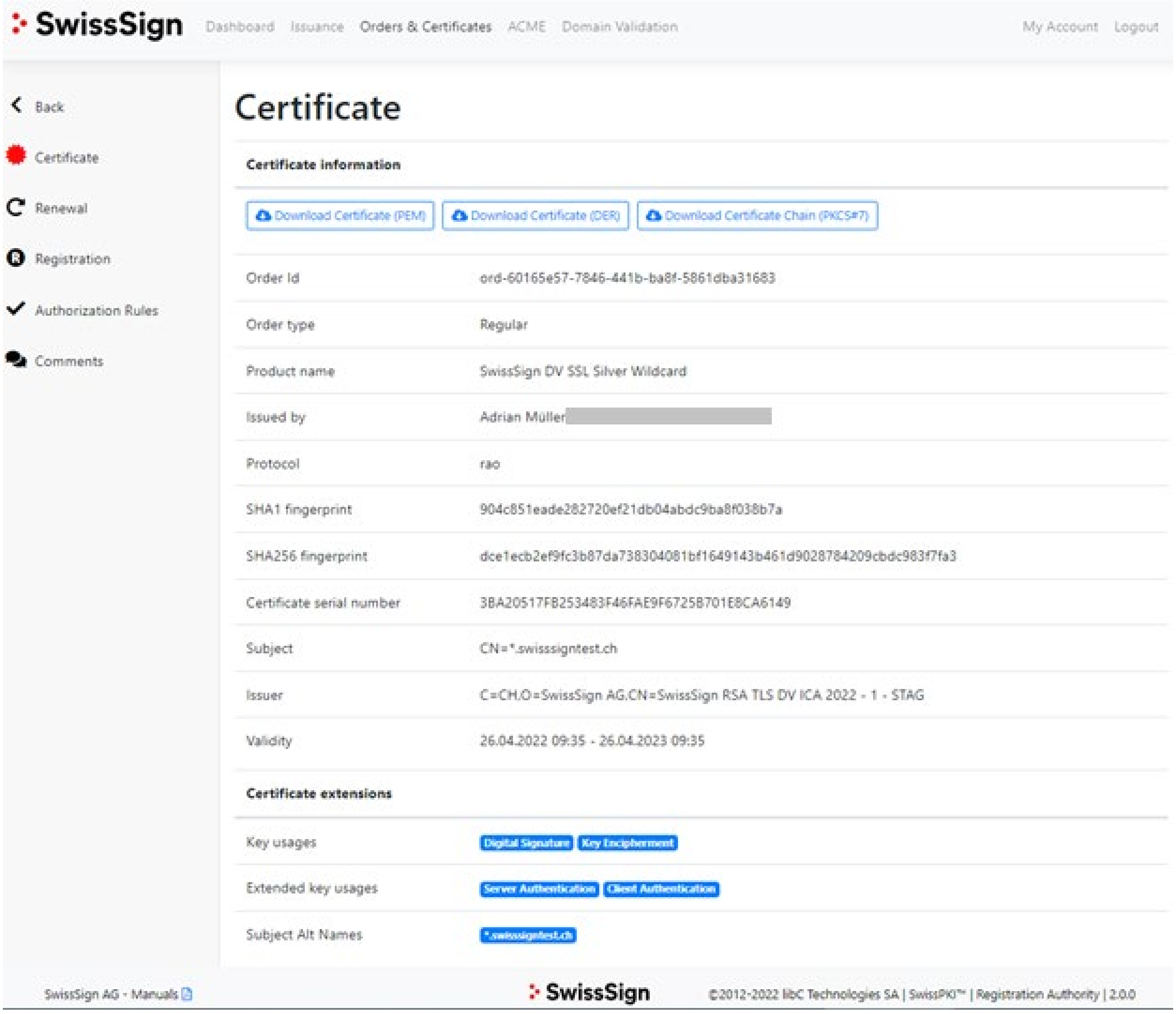
3.5.4 Certificate Information

By clicking on the edit button located in the action column of the orders and certificates table, you are redirected to the certificate details page. From the left menu, you access certificate information related to:

- Certificate details with download options
- Certificate renewal information
- Certificate registration documents
- Certificate key reminder recipients
- Certificate authorization rules
- Certificate comments

3.5.4.1Certificate Details

The certificate details view allows you to download the certificates in its various format (PEM, DER and PKCS#7). General certificate information related to the certificate order and certificate fingerprints are also displayed.



Certificate

Certificate information

Order Id	ord-60165e57-7846-441b-ba8f-5861dba31683
Order type	Regular
Product name	SwissSign DV SSL Silver Wildcard
Issued by	Adrian Müller [redacted]
Protocol	rao
SHA1 fingerprint	904c851eade282720ef21db04abdc9ba8f038b7a
SHA256 fingerprint	dce1ecb2ef9fc3b87da738304081bf1649143b461d9028784209cbdc983f7fa3
Certificate serial number	3BA20517FB253483F46FAE9F6725B701E8CA6149
Subject	CN=*.swisssigntest.ch
Issuer	C=CH,O=SwissSign AG,CN=SwissSign RSA TLS DV ICA 2022 - 1 - STAG
Validity	26.04.2022 09:35 - 26.04.2023 09:35

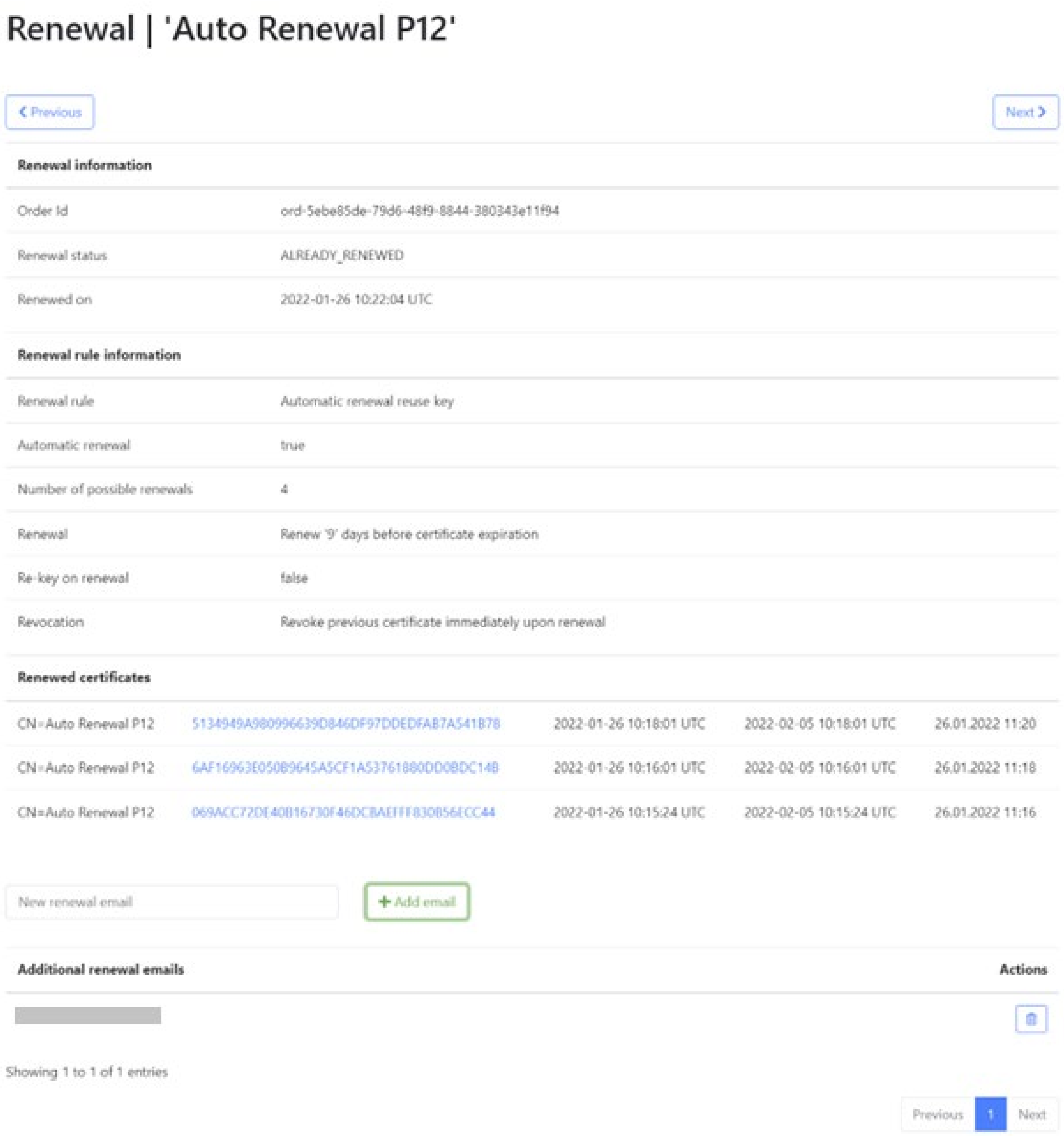
Certificate extensions

Key usages	Digital Signature Key Encipherment
Extended key usages	Server Authentication Client Authentication
Subject Alt Names	*.swisssigntest.ch

3.5.4.2Certificate Renewal

If an automatic certificate renewal rule is defined for the selected certificate you will find information with respect to:

1. Renewal information
   Information about the certificate’s order identifier, renewal status and optional renewal date
2. Renewal Rule Information
   Information about the details of the renewal rule associated to the certificate:
   - renewal rule name
   - automatic/manual renewal
   - number of allowed renewals
   - number of days the renewal is executed before expiration of the certificate
   - if a revocation occurs after the certificate is successfully renewed
3. List of preceding certificates (renewed)
   You can navigate between previous/next certificate orders using the previous/next buttons or jump to the previous certificates by clicking on the certificate’s serial number
4. List of additional renewal emails
   The additional list of renewal emails addresses to which renewal notifications are sent. These are useful for certificates without SAN RFC822 that still require notifications to be sent to other recipients.



Renewal | 'Auto Renewal P12'

Renewal information	
Order Id	ord-5ebe85de-79d6-48f9-8844-380343e11f94
Renewal status	ALREADY_RENEWED
Renewed on	2022-01-26 10:22:04 UTC

Renewal rule information	
Renewal rule	Automatic renewal reuse key
Automatic renewal	true
Number of possible renewals	4
Renewal	Renew '9' days before certificate expiration
Re-key on renewal	false
Revocation	Revoke previous certificate immediately upon renewal

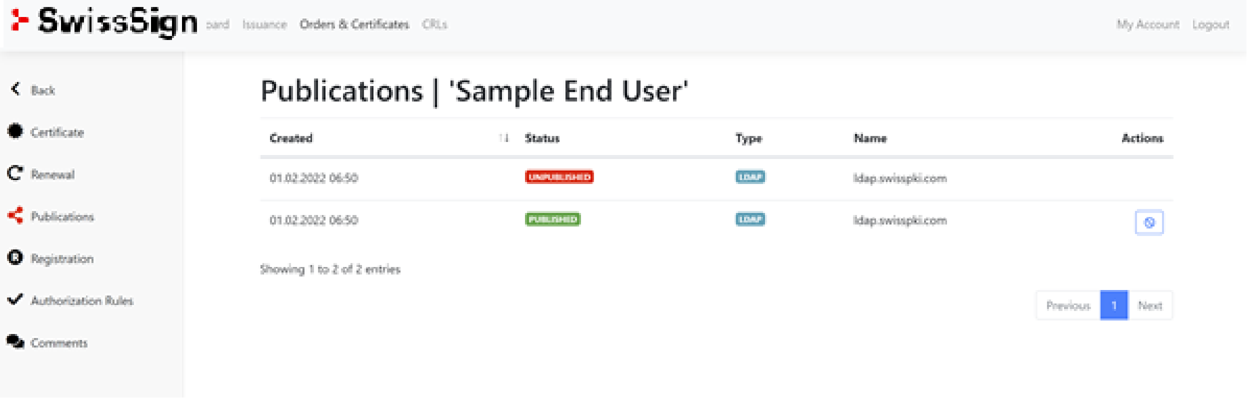
Renewed certificates				
CN=Auto Renewal P12	5134949A980996639D846DF97DDEDFAB7A541B78	2022-01-26 10:18:01 UTC	2022-02-05 10:18:01 UTC	26.01.2022 11:20
CN=Auto Renewal P12	6AF16963E050B9645A5CF1A53761880DD0BDC14B	2022-01-26 10:16:01 UTC	2022-02-05 10:16:01 UTC	26.01.2022 11:18
CN=Auto Renewal P12	069ACC72DE40B16730F46DCBAEFFF830B56ECC44	2022-01-26 10:15:24 UTC	2022-02-05 10:15:24 UTC	26.01.2022 11:16

Additional renewal emails	Actions
[redacted]	🗑

Showing 1 to 1 of 1 entries

3.5.4.3Certificate Publication

If the certificate is associated with one or several publishers, information about certificate publications can be found on this page. Every publication event concerning the certificate will be listed here and the option to un-publish will be available as well.
After clicking the edit button for a certificate, you wish to inspect you have the possibility to see the publication status and unpublish the certificate if required.



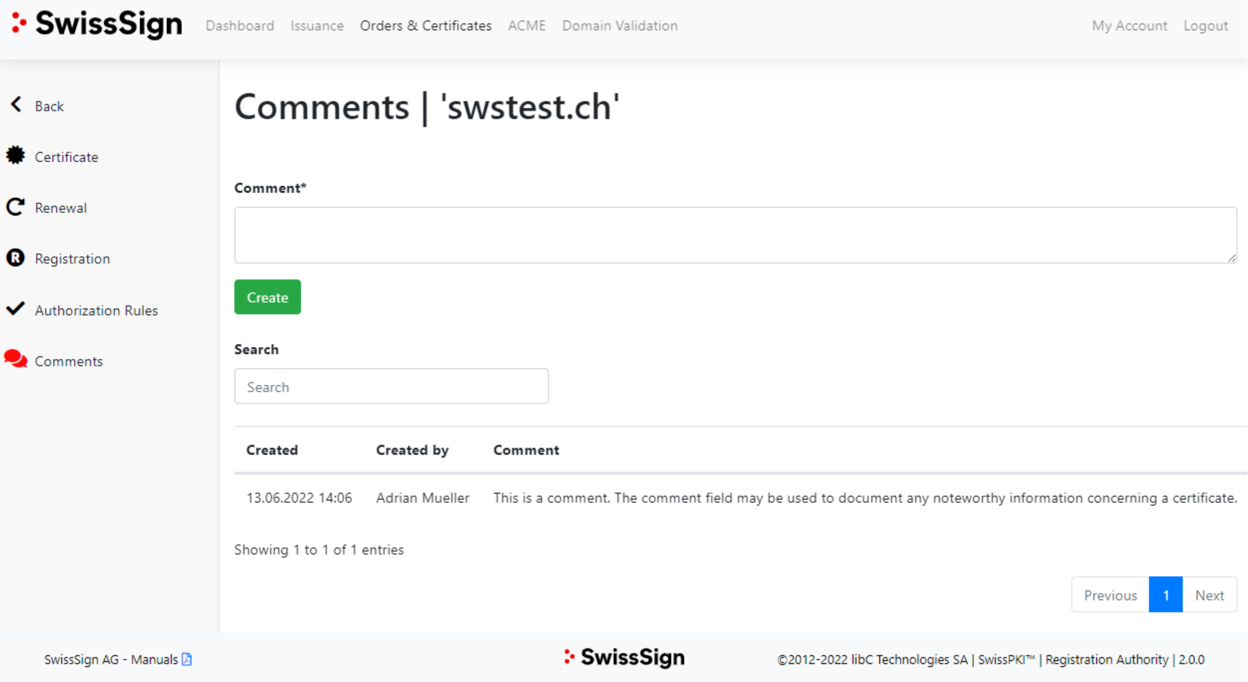
Publications | 'Sample End User'

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

3.5.4.4Comments

The certificate details' comments tab displays the list of all comments made on this certificate. You can add a new comment by using the text area located at the top of the page and clicking on the create button.



Comments | 'swstest.ch'

Comment*

Created	Created by	Comment
13.06.2022 14:06	Adrian Mueller	This is a comment. The comment field may be used to document any noteworthy information concerning a certificate.

Showing 1 to 1 of 1 entries

©2012-2022 libC Technologies SA | SwissPKI™ | Registration Authority | 2.0.0

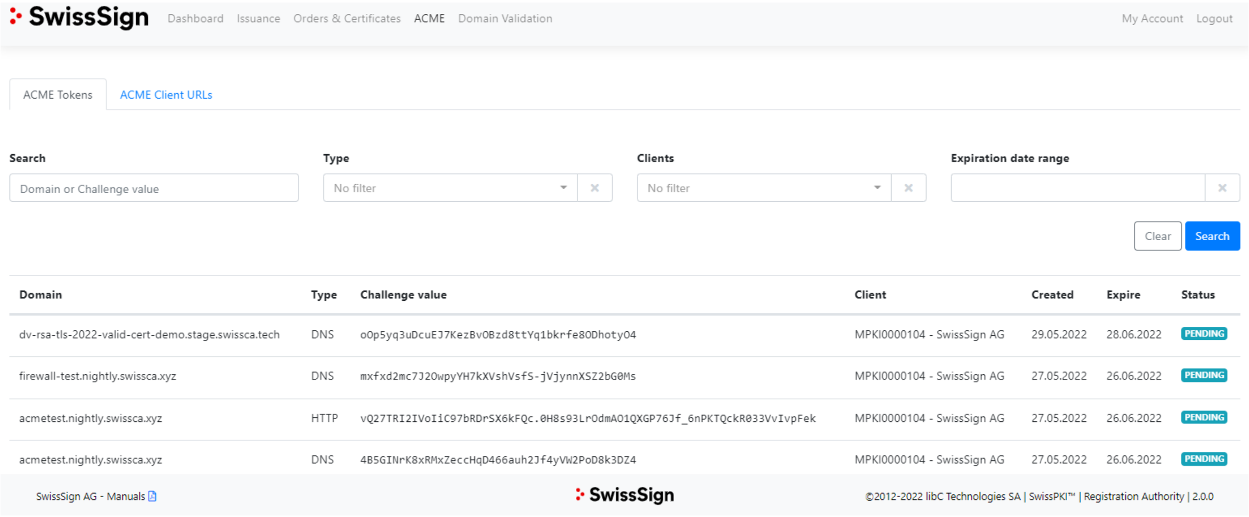
3.6 ACME

As an RA Operator you have the option to issue certificates through the ACME protocol (typically used for automatic *nix server enrolment) and you are allowed to access the ACME section.

The section provides you with information about the enrolled domain names, the protocol used for enrollment (dns-01 or http-01), the validity of the ACME challenge tokens and the Client requesting the enrollment.

Please note: The issuance of SSL/TLS *wildcard* certificates (issued to FQDNs with a leading asterisk, e.g. **.example.com*) is NOT possible with the ACME protocol enabled. Regulatory requirements forbid the ACME protocol for wildcard certificates.

- When relying on ACME any client software compliant to this standard may be used. However, recommended and tested open source client application is the Certbot client (ACME Client from Red Hat Enterprise Linux) and
- For Microsoft Internet Information Server (IIS) you may also use the ACMESharp client.



Search: Domain or Challenge value

Type: No filter

Clients: No filter

Expiration date range:

Domain	Type	Challenge value	Client	Created	Expire	Status
dv-rsa-tls-2022-valid-cert-demo.stage.swissca.tech	DNS	o0p5yq3uDcuEJ7KezBvOBzd8ttYq1bkrfe8ODhotyO4	MPKI0000104 - SwissSign AG	29.05.2022	28.06.2022	PENDING
firewall-test.nightly.swissca.xyz	DNS	mxfxd2mc7J2OwpyYH7kXVshVsfS-jVjynnXSZ2bG0Ms	MPKI0000104 - SwissSign AG	27.05.2022	26.06.2022	PENDING
acmetest.nightly.swissca.xyz	HTTP	vQ27TRI2IVoIiC97bRDrSX6kFQc.0H8s93LrOdmAO1QXGP76Jf_6nPKTQckR033VvIvpFek	MPKI0000104 - SwissSign AG	27.05.2022	26.06.2022	PENDING
acmetest.nightly.swissca.xyz	DNS	4B5GINrK8xRMxZeccHqD466auh2Jf4yVW2PoD8k3DZ4	MPKI0000104 - SwissSign AG	27.05.2022	26.06.2022	PENDING

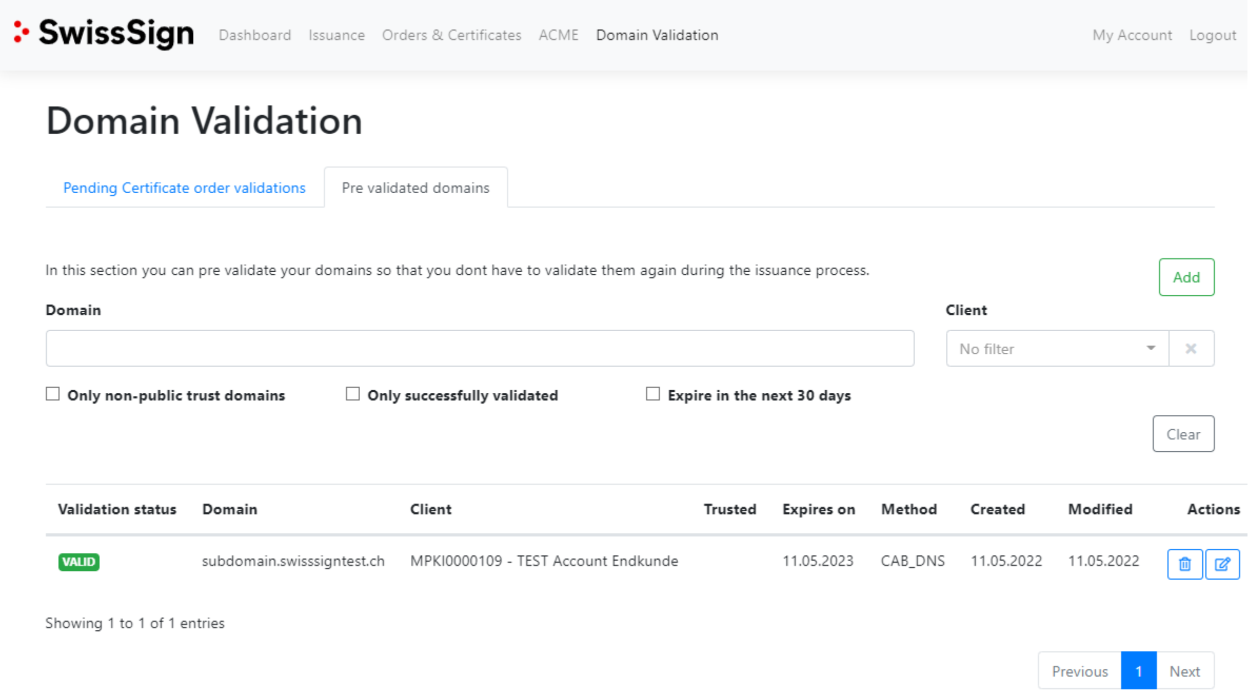
SwissSign AG - Manuals
SwissSign
©2012-2022 libC Technologies SA | SwissPKI™ | Registration Authority | 2.0.0

Note that certificates issued through ACME protocol are searchable in the ‘Orders and Certificates’.

3.7 Domain validation

3.7.1 DNS pre validation

For policy templates that have a “DNS owner rule”, domain names must be validated during issuance of the certificate. To make it easier for the client, he has the option to pre-validate a domain (usually the client validates his base(?) domain) so that he is able to issue certificates for that domain + subdomains without the need to validate every certificate request individually



Domain Validation

In this section you can pre validate your domains so that you dont have to validate them again during the issuance process.

Domain

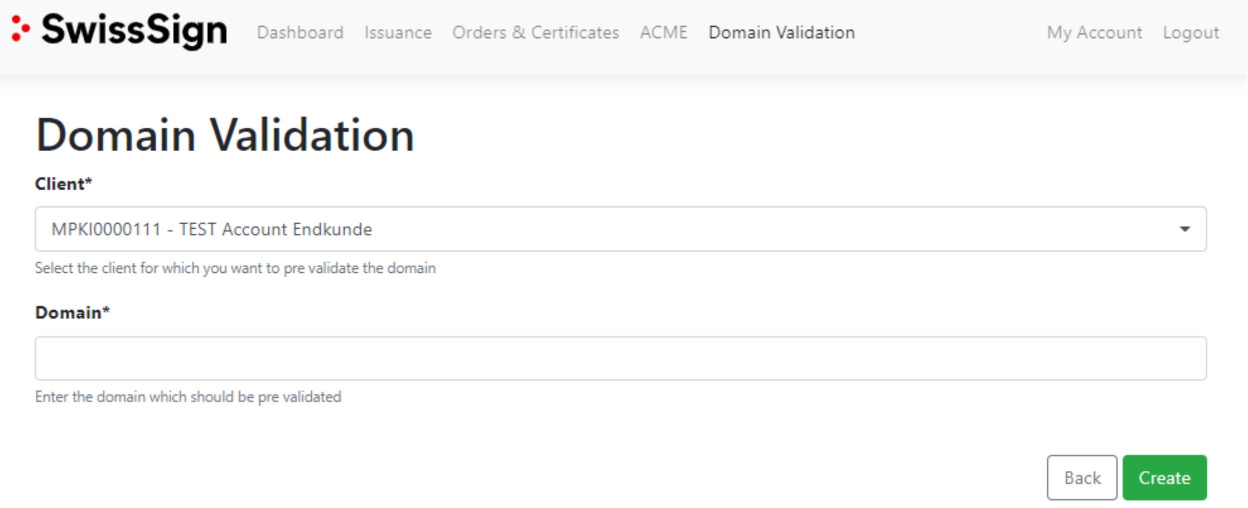
Client: No filter

□ Only non-public trust domains □ Only successfully validated □ Expire in the next 30 days

Validation status	Domain	Client	Trusted	Expires on	Method	Created	Modified	Actions
VALID	subdomain.swisssigntest.ch	MPKI0000109 - TEST Account Endkunde		11.05.2023	CAB_DNS	11.05.2022	11.05.2022	

Showing 1 to 1 of 1 entries

By clicking on the “Add” button the RA Operator can enter a new pre-validated domain



Domain Validation

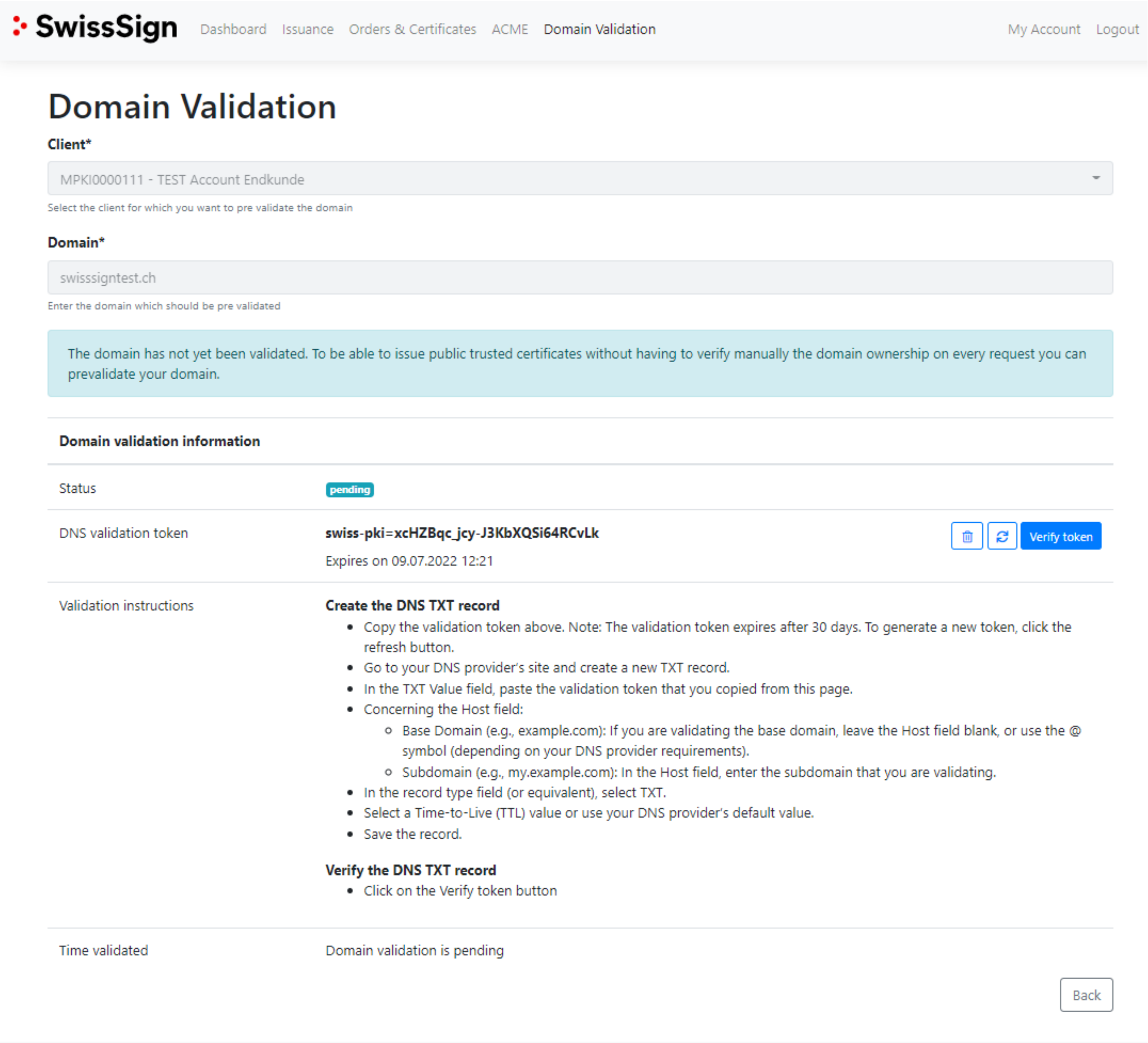
Client*: MPKI0000111 - TEST Account Endkunde

Select the client for which you want to pre validate the domain

Domain*

Enter the domain which should be pre validated

Field	Description
Client	Client for which the pre-validated domain should be added. Note: Since as an RA Operator can have access to more than one Client, the client needs to be specified here
Domain	Name of the domain which should be pre-validated



Domain Validation

Client*

MPKI0000111 - TEST Account Endkunde

Select the client for which you want to pre validate the domain

Domain*

swisssigntest.ch

Enter the domain which should be pre validated

The domain has not yet been validated. To be able to issue public trusted certificates without having to verify manually the domain ownership on every request you can prevalidate your domain.

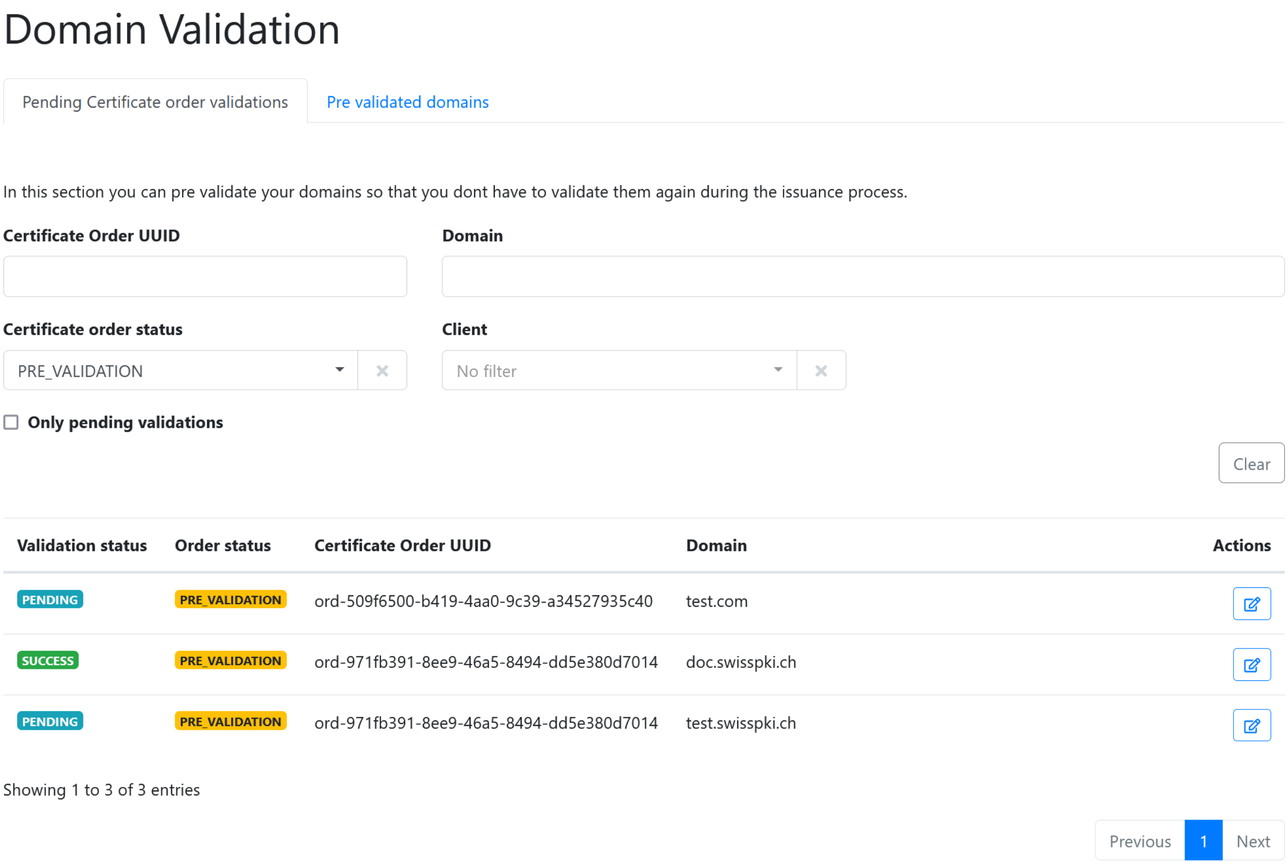
Domain validation information	
Status	pending
DNS validation token	**swiss-pki=xcHZBqc_jcy-J3KbXQSi64RCvLk** Expires on 09.07.2022 12:21
Validation instructions	**Create the DNS TXT record** • Copy the validation token above. Note: The validation token expires after 30 days. To generate a new token, click the refresh button. • Go to your DNS provider's site and create a new TXT record. • In the TXT Value field, paste the validation token that you copied from this page. • Concerning the Host field: ○ Base Domain (e.g., example.com): If you are validating the base domain, leave the Host field blank, or use the @ symbol (depending on your DNS provider requirements). ○ Subdomain (e.g., my.example.com): In the Host field, enter the subdomain that you are validating. • In the record type field (or equivalent), select TXT. • Select a Time-to-Live (TTL) value or use your DNS provider's default value. • Save the record. **Verify the DNS TXT record** • Click on the Verify token button
Time validated	Domain validation is pending

For public trust DNS Owner check, copy the DNS challenge token to the DNS server as defined in the instructions displayed on the page. As an operator, you can optionally manually validate the DNS entry by clicking on 'Validate domain ownership'.

Click on 'Generate new validation token' to generate a new challenge. Follow the instructions displayed on the screen for the domain you created. The token is valid 30 days. After this period a new token must be generated.

3.7.2 Pending certificate order validation

In this section the RA Operator can see an overview of pending domain validations for his certificate orders. To see the validation details, click on the Edit button.



Domain Validation

In this section you can pre validate your domains so that you dont have to validate them again during the issuance process.

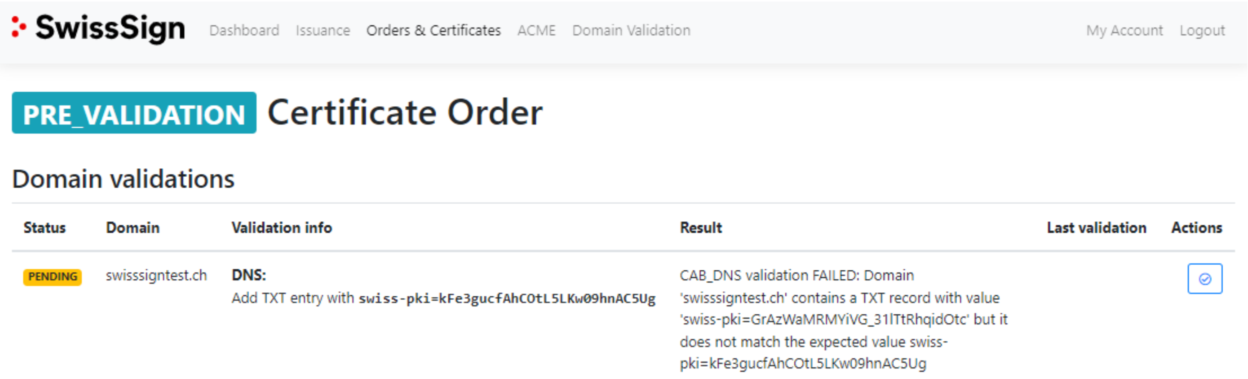
Certificate Order UUID	
Domain	
Certificate order status	PRE_VALIDATION
Client	No filter

□ Only pending validations

Validation status	Order status	Certificate Order UUID	Domain	Actions
PENDING	PRE_VALIDATION	ord-509f6500-b419-4aa0-9c39-a34527935c40	test.com	
SUCCESS	PRE_VALIDATION	ord-971fb391-8ee9-46a5-8494-dd5e380d7014	doc.swisspki.ch	
PENDING	PRE_VALIDATION	ord-971fb391-8ee9-46a5-8494-dd5e380d7014	test.swisspki.ch	

Showing 1 to 3 of 3 entries

The edit screen displays the validation methods and tokens which can be used to validate the domain. After setting the proper secrets in the DNS or on the webserver, the domain can be validated manually using the action on the right side of the table.
Alternatively, the domain owner check is performed once per hour automatically using a background job.
The domain validation must be done within 30 days.



PRE_VALIDATION Certificate Order

Domain validations

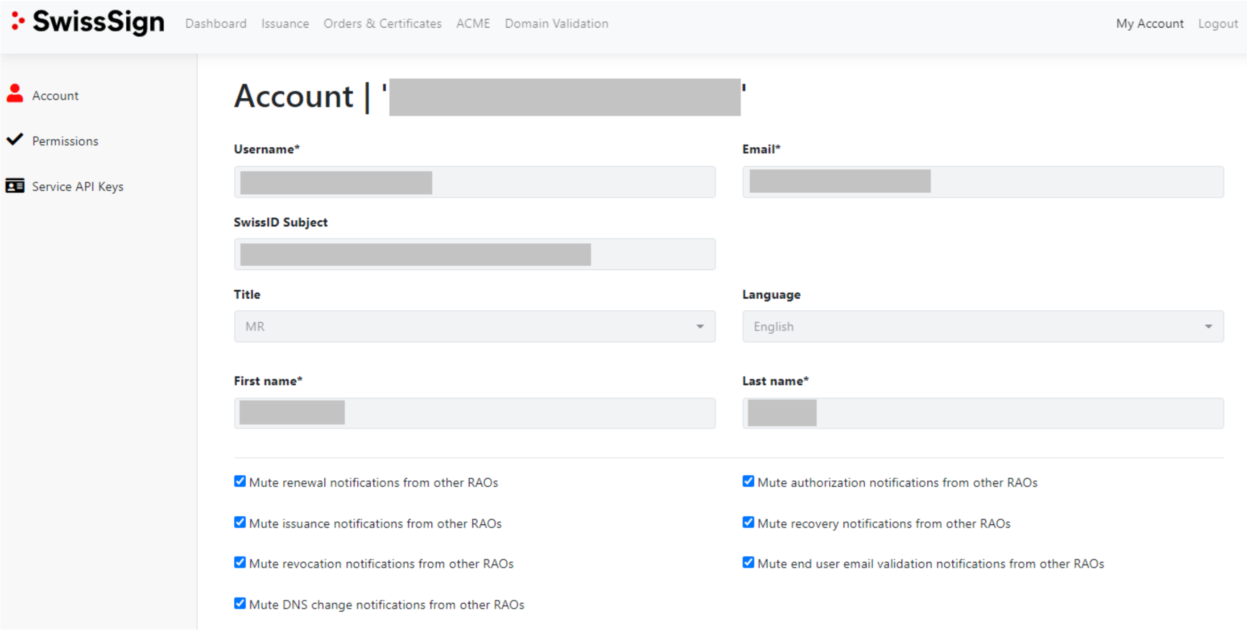
Status	Domain	Validation info	Result	Last validation	Actions
PENDING	swisssigntest.ch	**DNS:** Add TXT entry with `swiss-pki=kFe3gucfAhCOtL5LKw09hnAC5Ug`	CAB_DNS validation FAILED: Domain 'swisssigntest.ch' contains a TXT record with value 'swiss-pki=GrAzWaMRMYiVG_31lTtRhqidOtc' but it does not match the expected value swiss-pki=kFe3gucfAhCOtL5LKw09hnAC5Ug		

3.8 Account

3.8.1 Account details

This page allows you to review your account details. The following fields are available:

Fields	Description
User name	Your username
Email	The email associated with your account
SwissID Subject	The SwissID linked with your account
First name	Your first name
Last name	Your last name
Title	Your title
Language	Your preferred language
Mute notification	Applies to RA Operator roles. As an RA Operator, you may want to mute notifications from other RA Operators within the team. You can enable/disable notification from your account page. **Note**: you must have permissions to modify your account information



Account | '[redacted]'

Username*
[redacted]

Email*
[redacted]

SwissID Subject
[redacted]

Title
MR

Language
English

First name*
[redacted]

Last name*
[redacted]

☑ Mute renewal notifications from other RAOs

☑ Mute authorization notifications from other RAOs

☑ Mute issuance notifications from other RAOs

☑ Mute recovery notifications from other RAOs

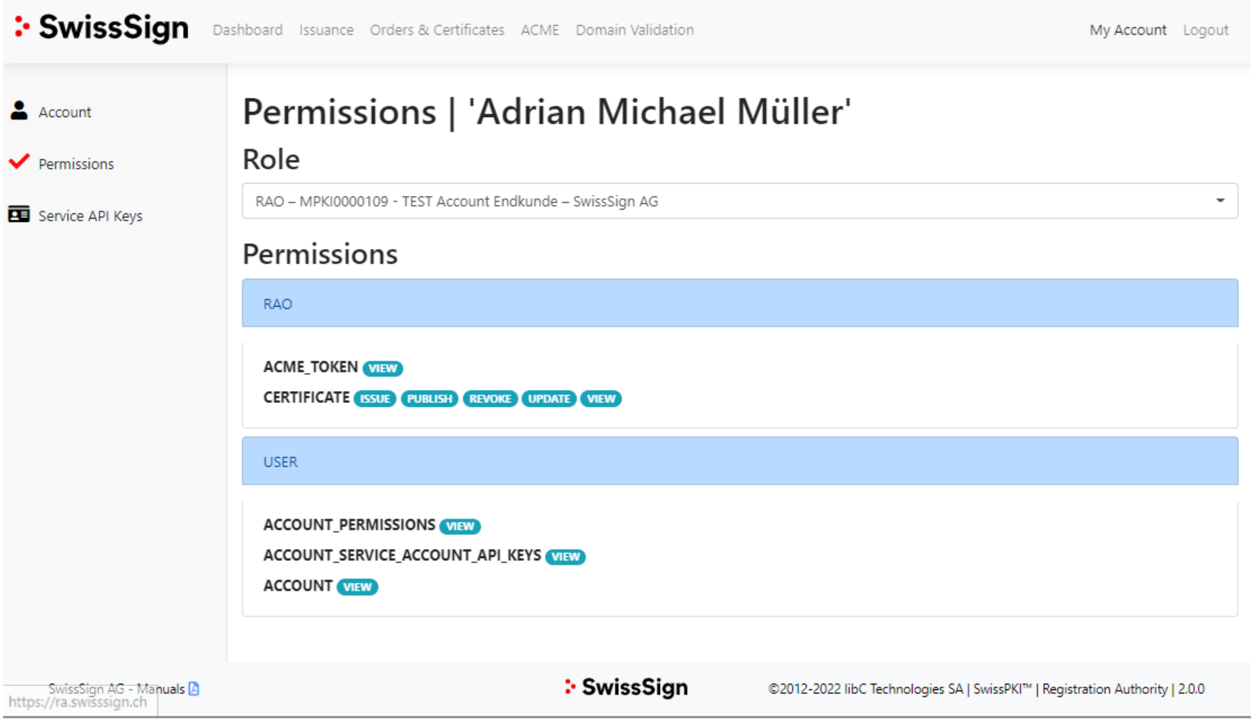
☑ Mute revocation notifications from other RAOs

☑ Mute end user email validation notifications from other RAOs

☑ Mute DNS change notifications from other RAOs

3.8.2 Account Permissions

The account permissions display the permissions per assigned roles to your user account. Select the roles from the 'Role' drop down to display the assigned permissions. You cannot edit your own permissions/roles.



Permissions | 'Adrian Michael Müller'

Role

RAO – MPKI0000109 - TEST Account Endkunde – SwissSign AG

Permissions

RAO

ACME_TOKEN VIEW

CERTIFICATE ISSUE PUBLISH REVOKE UPDATE VIEW

USER

ACCOUNT_PERMISSIONS VIEW

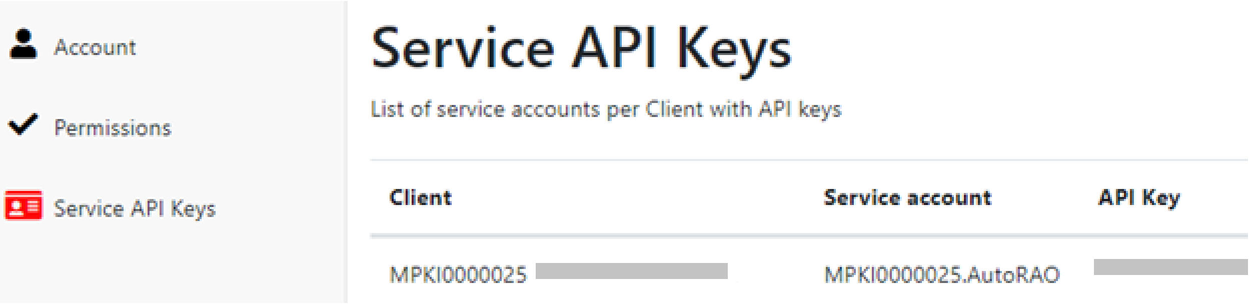
ACCOUNT_SERVICE_ACCOUNT_API_KEYS VIEW

ACCOUNT VIEW

SwissSign AG - Manuals
https://ra.swisssign.ch
SwissSign
©2012-2022 libC Technologies SA | SwissPKI™ | Registration Authority | 2.0.0

3.8.3 Service API Keys

The service API key is shown under the according menu. The Service API key is used for the authentication of an automatic client which accesses the system over the RA API. The Service API Key is automatically generated for a Managed PKI.



Service API Keys

List of service accounts per Client with API keys

Client	Service account	API Key
MPKI0000025 [redacted]	MPKI0000025.AutoRAO	[redacted]

Upon request the API Service Key may be renewed.

4 RA API

SwissSign CA offers an OpenAPI specification for automating and integrating your MPKI with your services.
The RA API enables you to register, revoke and search certificates as well as authorize registration requests. The URL to the service is provided by SwissSign.

4.1 Roles and Permissions

For a given user and role using the client API, the same Roles and Permissions apply as the ones specified in the user interface. That is, if a given user and role is authorized to fulfil a READ operation via the Web UI, then the same operation is accessible through the generated client API. If a DELETE permission is withdrawn from a specific user and role for a specific operation, then the DELETE permission is correspondingly withdrawn from the client API operation.
In order to obtain an API Key, the user role must at least have the permissions *ACCOUNT_API_KEY* View and Create associated to its user account for the specified role. Additionally, the Update and Delete permissions enable the user to renew and/or delete its API Keys.
If the user role has no *ACCOUNT_API_KEY* permission enabled, it is still possible to issue an API Key to this particular user by a higher role if permission is granted.
Additionally, if a user is of type *SERVICE ACCOUNT*, then the user can use the API but not log in to the Web UI.

4.2 Service API Key

In order to use the API, a user must obtain an API Key.
A user with multiple MPKI accesses has multiple API Keys.
The API Key is an auto generated 64 bytes shared secret using digit, alpha, upper and lowercase and is used on the client side (API) to generate a signed (HMAC-256) JW Token.

4.2.1 API Key Rollover

Generated API Keys are immediately available to the client and have no expiration date and time set.
Deleting an API Key prevents immediately access to the Web Services. Therefore, the deletion can only be performed by SwissSign.
When an API Key is updated, a new API Key is generated and the previous API Key is valid for another 7 days. The user has maximum 7 days to replace the API Key on its deployment (client configuration)

4.3 Authentication

Generate a JW Token (JWT) and signing it with the API Key using HMAC256 as ‘text/plain’. By default, a JW Token is valid for 8 hours.

4.3.1 JWT Generation

The JWT must include:

Claim	Value
iss	SwissSign CA
aud	REST API
sub	<*UserName*> of the SwissSign CA account
iat	Normalized UTC date/time
nbf	Normalized UTC date/time
exp	Normalized UTC date/time

4.3.2 HTTP Request

Using HTTP requests to access the SwissSign CA web services, include in each request the following HTTP header, where encoded JWT is the signed encoded token:

```
 Authorization: Bearer <encoded JWT>
```

Using generated Java client API with the openapi-generator, set the encoded JWT as follows:

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

Each service request MUST include the JWT token. The PKI web services do not return a usable session cookie.
An SSL protected helper method is available to you for generating your JW Token:

```
GET /pki/api/v2/jwt/:userName/:key
```

Where :userName is your user account and :key your user account API Key which is available from the Web UI under ‘My Account’ menu.

5 CMC

In order to perform certificate operations over the CMC (Certificate Management over CMS) interface according to IETF RFC 5272 you need a dedicated certificate for your CMC-client. The certificate is provided to you during the onboarding process and renewed on a periodic basis.
The URLs and parameters for using the CMC-interface are described in the Technical Specification CMC Interface which can be downloaded here: https://www.swisssign.com/dam/jcr:8ff02777-a6b6-4872-8a6c-535d3cb2d565/CMCInterface_EN.pdf

Please note: The CMC interface is deprecated and only used by existing customers.