

SwissSign CA
SwissSign AG

A brief guide to setting up your new MPKI on the
new SwissSign CA

Revision			
Rev	Date	Who	Comment
1.0	08.07.2022	SwissSign AG	Initial document

Contents

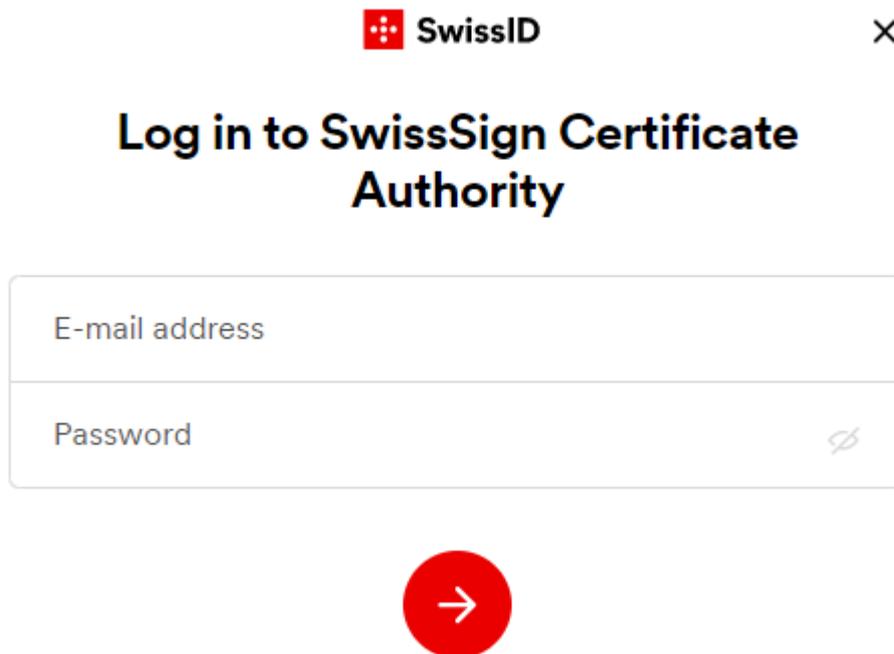
1. Logging into your account.....	4
2. Validate Domains.....	6

1. Logging into your account

To log in, a SwissID is required. The SwissID needs to exist for the email address that was indicated for the RA Operator in the order form.

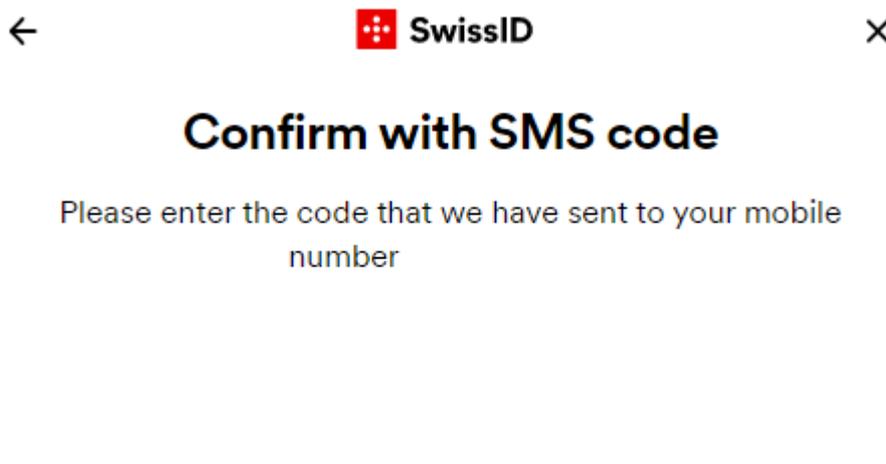
If you do not own a verified SwissID yet, you can follow the [onboarding manual](#) on our website.

1. Open the website <https://ra.swisssign.ch/>
2. Log in with your SwissID login information.



The screenshot shows the login interface for the SwissID Certificate Authority. At the top, there is a header with the SwissID logo and a close button (X). The main heading is "Log in to SwissSign Certificate Authority". Below this, there are two input fields: "E-mail address" and "Password". The password field has a toggle icon for visibility. A large red circular button with a white right-pointing arrow is centered below the input fields.

Please note, that the login requires a second factor (App or SMS code):



The screenshot shows the confirmation page for the SwissID. At the top, there is a header with a back arrow, the SwissID logo, and a close button (X). The main heading is "Confirm with SMS code". Below this, there is a text prompt: "Please enter the code that we have sent to your mobile number". A dashed horizontal line is positioned below the text prompt.

3. To use the MPKI as RA Operator you have to provide a consent that the following attributes of your SwissID account can be shared with the MPKI.



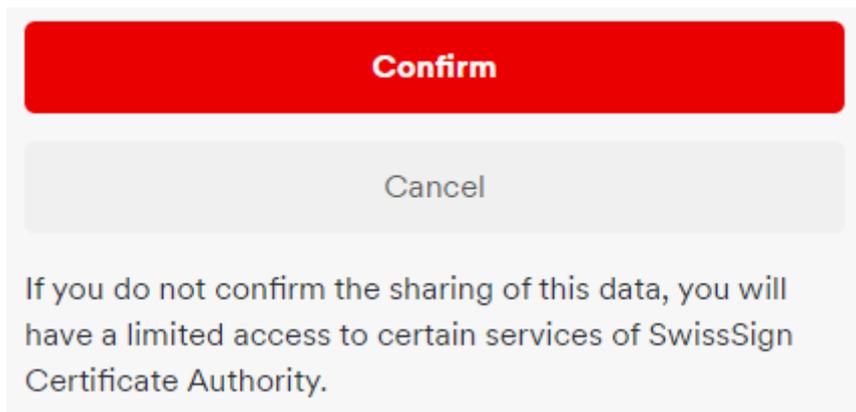
Confirm sharing of data

Personal information is required for the use of certain services of SwissSign Certificate Authority. If you continue, you agree that the following data will be transferred to SwissSign Certificate Authority.

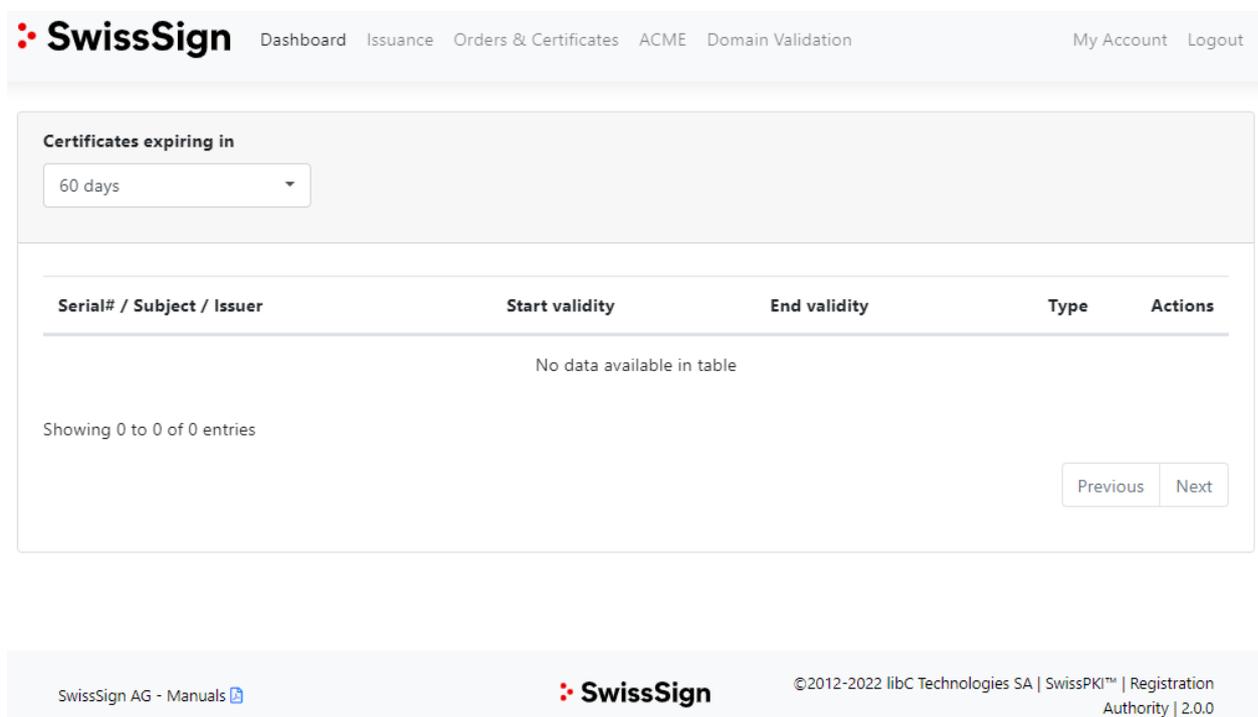
The required information is displayed:

Gender
Age over
Date of birth
Verified on
Salutation
First name
Last name
Language
E-mail address

Clicking the button «Confirm» will allow the information above to be released to the MPKI and complete the login.



Now you are logged in and can see your MPKI GUI:



2. Validate Domains

As a final step, the associated domains must be validated before you can issue certificates. The aim of this process is to prove that you are the owner of those domains.

As RA Operator, you have the option to request new main domains for the Managed PKI and have them checked automatically as part of the procedure approved by the CA Browser Forum. To do so, you must log into the certificate platform ra.swisssign.ch.

Once logged into the MPKI GUI, click on «Domain Validation» and in the following submenu on «Pre validated domains».

Domain Validation

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

On this page you can start the process of adding a new domain with the button «Add».

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

[Add](#)

Domain

Client

No filter

[Clear](#) 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
-------------------	--------	--------	---------	------------	--------	---------	----------	---------

Previous **1** Next

If you are the RA Operator of only a single MPKI, the correct MPKI will automatically be selected.

In the case of being the RA Operator of multiple MPKIs, please choose the MPKI you wish to add a domain to.

In the domain field you may fill in the domain you wish to add to the MPKI. Afterwards, click on «Create» to create the domain check.

Domain Validation

Client*

MPKI0000 xxx - TEST

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

Domain*

testdomainswissign.ch

Enter the domain which should be pre validated

[Back](#)[Create](#)

The created check is now listed as «not_validated» in the domain check section:

Domain Validation

Pending Certificate order validations

Pre validated domains

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

Add

Domain

Client

No filter

Only non-public trust domains

Only successfully validated

Expire in the next 30 days

Clear

Validation status	Domain	Client	Trusted	Expires on	Method	Created	Modified	Actions
VALID				13.05.2023	CAB_DNS	13.05.2022	13.05.2022	 
NOT_VALIDATED	testdomainswisssign.ch	MPKI0000xxx - TEST	-	-	UNKNOWN	28.06.2022	28.06.2022	 

Showing 1 to 2 of 2 entries

Previous 1 Next

On the new check, click the edit button:

NOT_VALIDATED	testdomainswisssign.ch	MPKI0000xxx - TEST	-	-	UNKNOWN	28.06.2022	28.06.2022	 
---------------	------------------------	--------------------	---	---	---------	------------	------------	---

Clicking «Start domain validation» will start the validation process and create the required validation token:

Domain validation information

Status **not_validated**

DNS validation token **Start domain validation**

Once the validation token has been created it will be shown in the “DNS validation token” row:

DNS validation token **swissign-check=vE6KrcfZ67tfh0QugnmDIH7ZaCY**
Expires on 28.07.2022 14:04

With the validation code you are now able to follow the instructions in the «Validation instructions» row:

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

Once the validation token has been saved according to the instructions, you may start the check with «Verify token»:

DNS validation token

swissign-check=vE6KrcfZ67tfh0QugnmdIH7ZaCY

Expires on 28.07.2022 14:04



If the check is successful, you can now see the domain listed as “VALID”:

Domain Validation

[Pending Certificate order validations](#)

Pre validated domains

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

Add

Domain

Client

No filter

Only non-public trust domains

Only successfully validated

Expire in the next 30 days

Clear

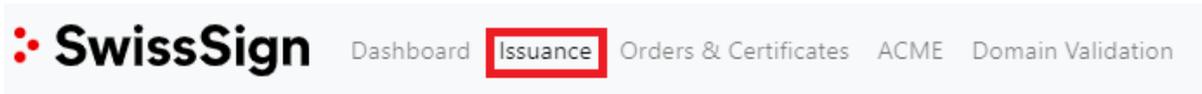
Validation status	Domain	Client	Trusted	Expires on	Method	Created	Modified	Actions
VALID	Domäne	MPKI0000xxx - Test		1.1.2023	CAB_DNS	1.1.2022	1.1.2022	<input type="button" value="trash"/> <input type="button" value="edit"/>

Showing 1 to 1 of 1 entries

Previous **1** Next

3. Certificate issuance with your MPKI on the new SwissSign CA

To issue a certificate on the MPKI GUI, navigate to the "Issuance" tab:



Here you will find the listing of your available products. You can also search for a specific product. If you are registered as an RA operator in several MPKIs, you can select the desired MPKI under "Clients":



We start the process of creating a certificate with the "Actions" button behind the desired product:

CA	Client	Policy Name	Type	Auth.	Sources	Actions
	RSA SMIME LCP ICA 2022 - 1	MPKI0000	Personal S/MIME E-Mail ID Silver	General		
	RSA SMIME NCF extended ICA 2022 - 1	MPKI0000	Pro S/MIME E-Mail ID Gold RSASSA-PSS	General		
	RSA SMIME NCF extended ICA 2022 - 1	MPKI0000	Pro S/MIME E-Mail ID Gold with Auth	General		
	RSA SMIME NCF ICA 2022 - 1	MPKI0000	Pro S/MIME E-Mail ID Gold	General		
	RSA TLS DV ICA 2022 - 1	MPKI0000	DV SSL Silver Single-Domain	General		
	RSA TLS DV ICA 2022 - 1	MPKI0000	DV SSL Silver Wildcard	General		
	RSA TLS EV ICA 2022 - 1	MPKI0000	EV SSL Gold Multi-Domain	General		
	RSA TLS EV ICA 2022 - 1	MPKI0000	EV SSL Gold Single-Domain	General		
	RSA TLS OV ICA 2022 - 1	MPKI0000	OV SSL Gold Multi-Domain	General		
	RSA TLS OV ICA 2022 - 1	MPKI0000	OV SSL Gold Single-Domain	General		
	RSA TLS OV ICA 2022 - 1	MPKI0000	OV SSL Gold Wildcard	General		

Showing 1 to 11 of 11 entries

Previous 1 Next

In the next step you enter your CSR.

Out of regulatory reasons, SwissSign is not allowed to support you in this. How to create a CSR can be found in the "Example of CSR creation with OpenSSL" on the following page:

<https://www.swisssign.com/support/systemstatus/details~newsID=02715d1b-9102-4148-8992-846a75d7fdf2~.html>

Issue certificate | SwissSign EV SSL Gold Single-Domain

^ Key Generation parameters

Key generation source	Key type and minimum size	Certificate Hash Algorithm
PKCS10	RSA 2048	sha256

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

Copy/Paste the PKCS#10 request

[Collapse all](#)

[Back](#) [Validate CSR](#)

If the CSR contains attributes that are not supported in the selected product, you will receive the following message:

^ Subject Distinguished Name

Unused Subject Attributes from CSR: o=Test org,ou=Test unit,state=Zurich,l=Test loc

You can insert your DNS entries in the DNS field.

In single domain and e-mail certificates, you can use the same entry as for the "Common Name" (domain and e-mail address respectively).

In multi-domain certificates, you can enter all your SANs if they were not already present in the CSR.

^ Subject Alternative Name

DNS required.

'0' out '1' Subject Alt Name (rfc822) used.

DNS 1*

DNS required.

Finally, in order to continue, you must accept the Subscriber Agreement. If you click on Subscriber Agreement (blue text), you will open the corresponding document.

After you have taken note of the participant agreement, click on the box and on "I accept these conditions" to continue.

^ Terms & Conditions

I confirm acceptance and adherence to the terms and conditions of the [Subscriber Agreement](#) of SwissSign AG.

Please read and accept the terms and conditions

Now you can issue the certificate with the button "Issue certificate".

If the domain has already been pre-validated, the certificate is issued directly.

If the domain has not yet been validated, the validation process starts and a DNS token is generated. The certificate is only issued after this validation.