SwissSign

SwissSign CA

SwissSign AG

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

SwissSign

Revision

Rev	Date	Who	Comment
1.0	08.07.2022	SwissSign AG	Initial document

SwissSign

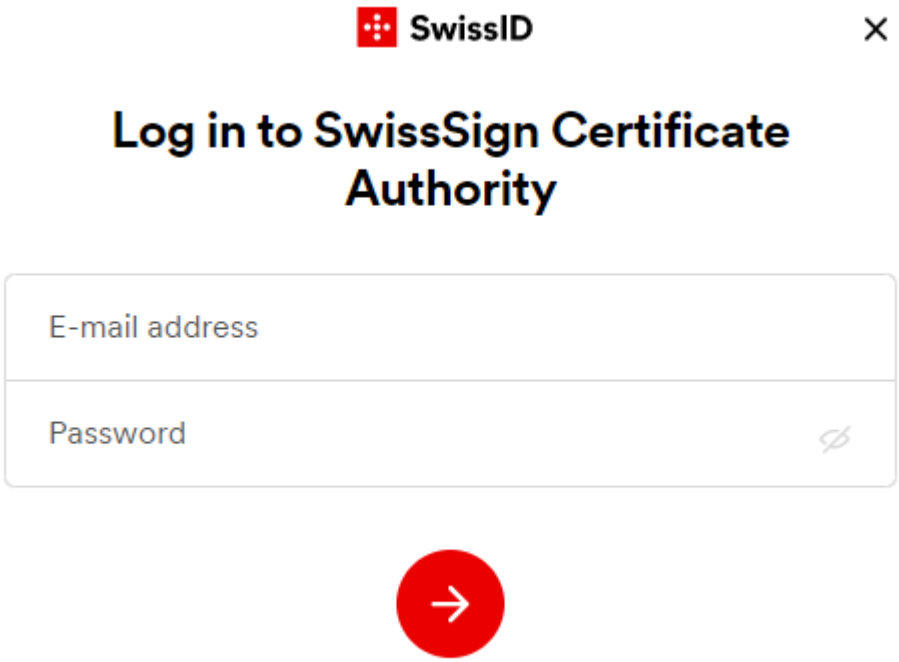
Contents

SwissSign

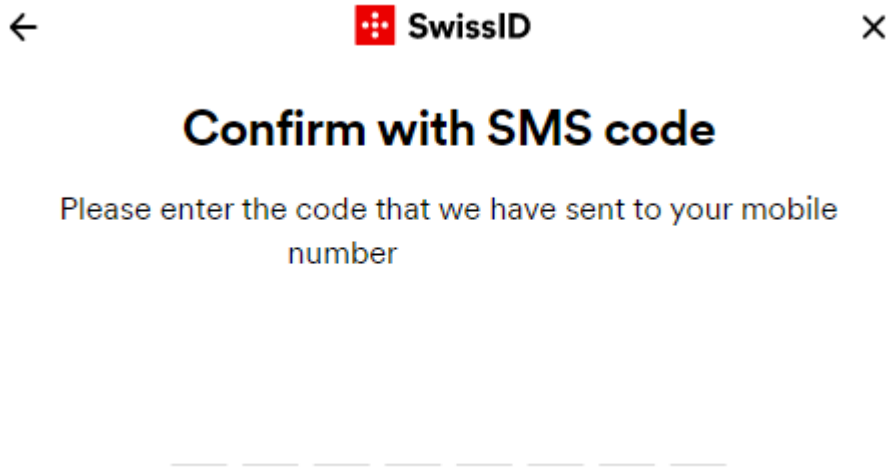
1. Logging into your account

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.

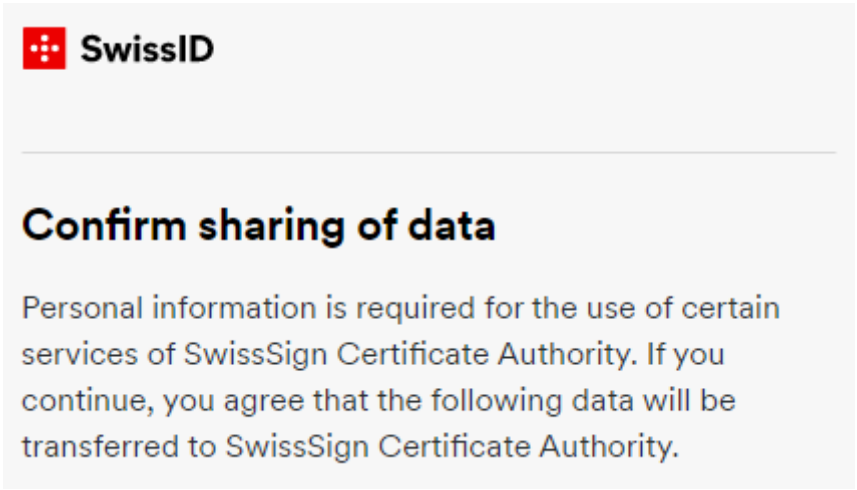
1. Open the website https://ra.swisssign.ch/
2. Log in with your SwissID login information.



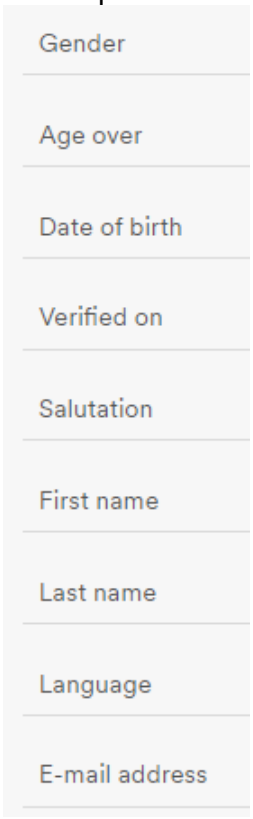
Please note, that the login requires a second factor (App or SMS code):



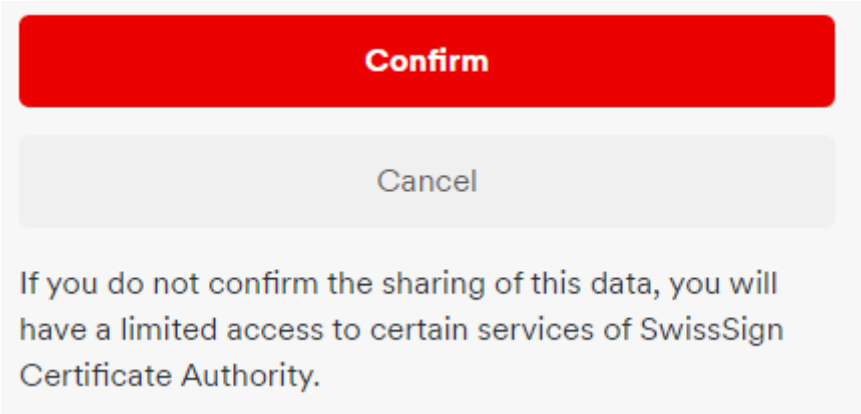
3. To use the MPKI as RA Operator you have to provide a consent that the following attributes of your SwissID account can be shared with the MPKI.



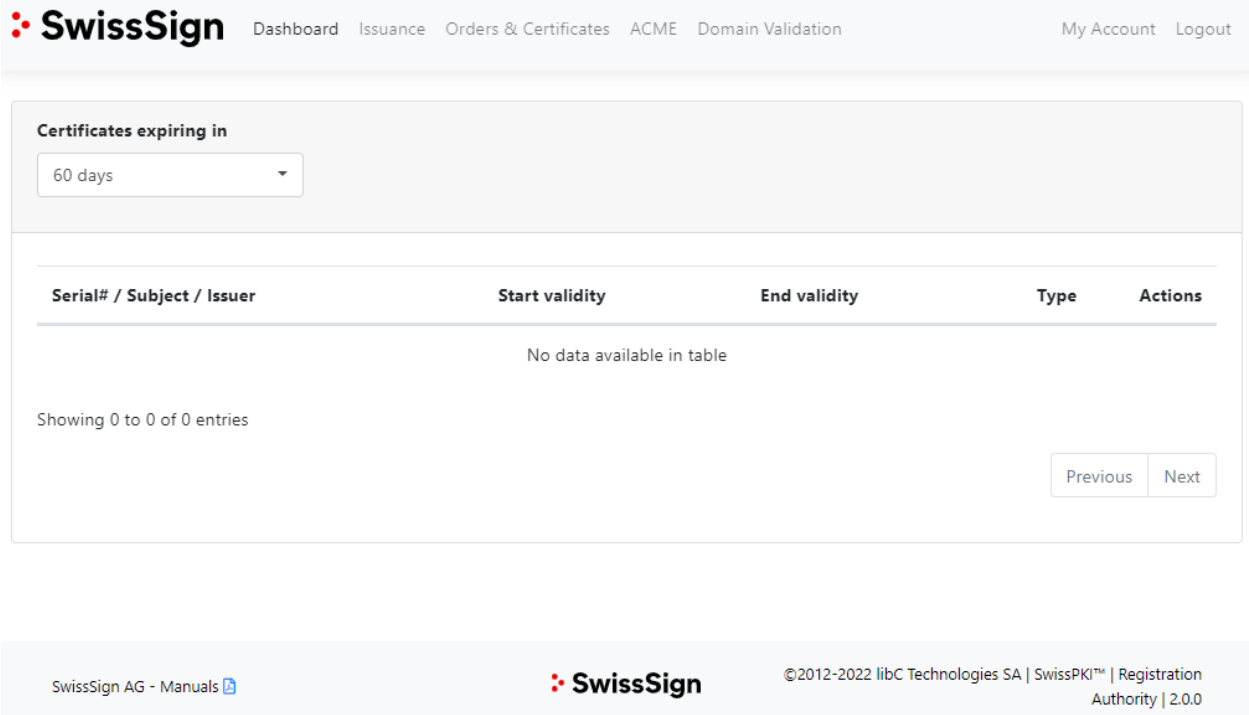
The required information is displayed:



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:

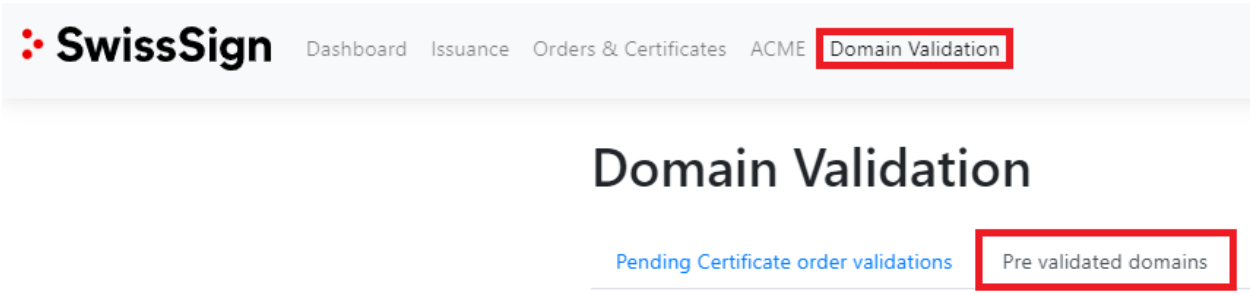


2. Validate Domains

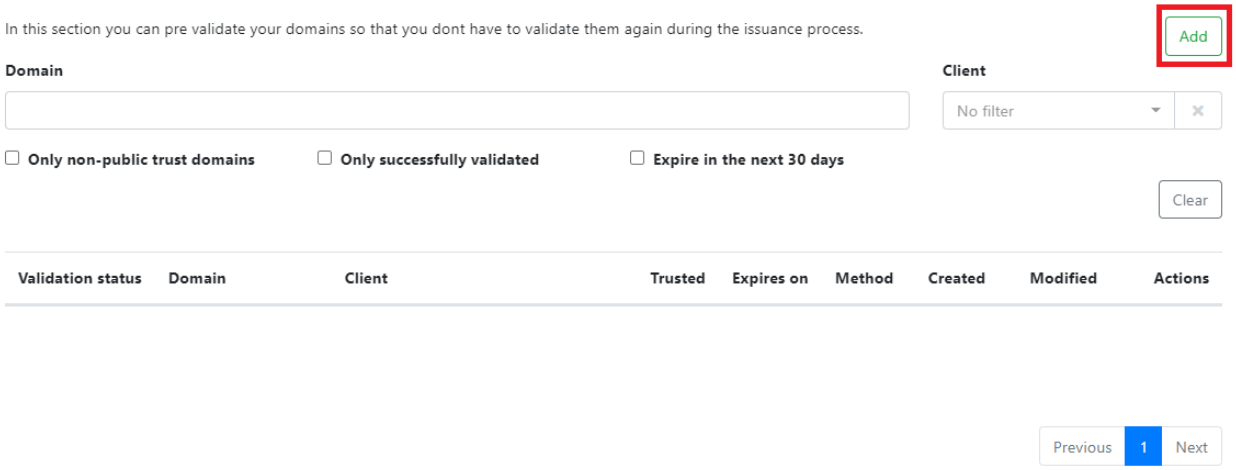
As a final step, the associated domains must be validated before you can issue certificates. The aim of this process is to prove that you are the owner of those domains.

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.

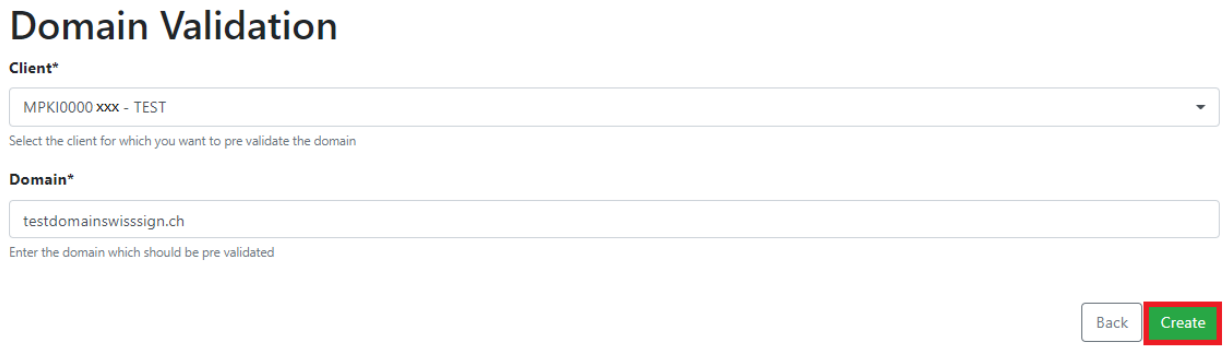
Once logged into the MPKI GUI, click on «Domain Validation» and in the following submenu on «Pre validated domains».



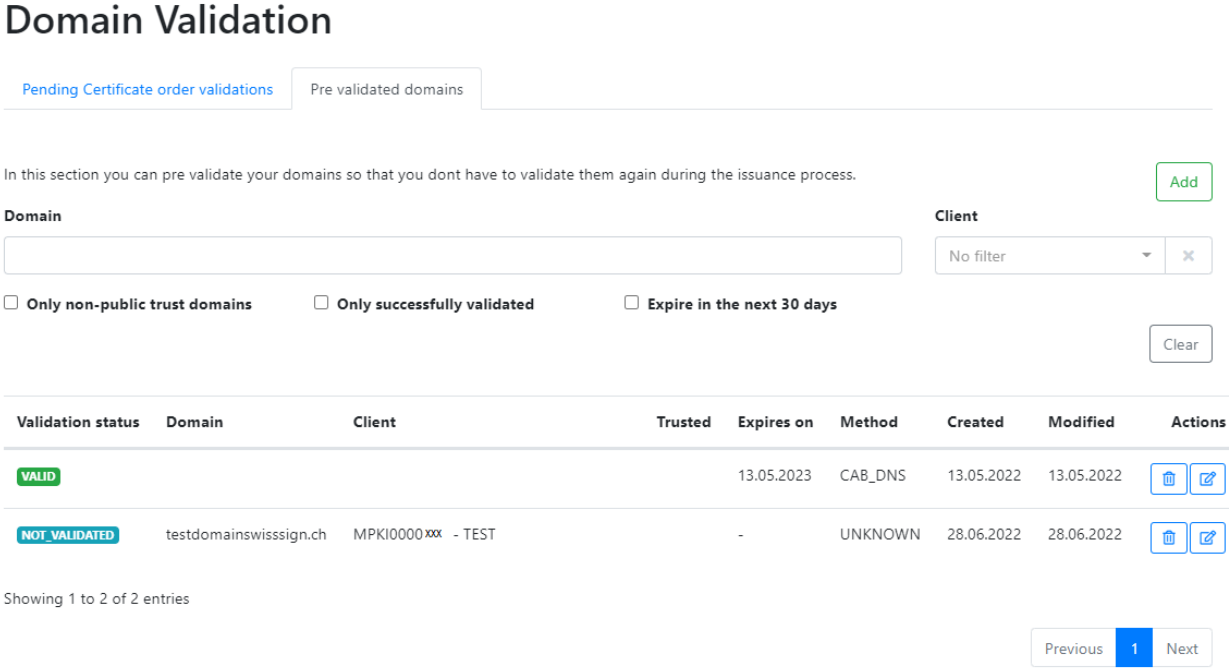
On this page you can start the process of adding a new domain with the button «Add».



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.

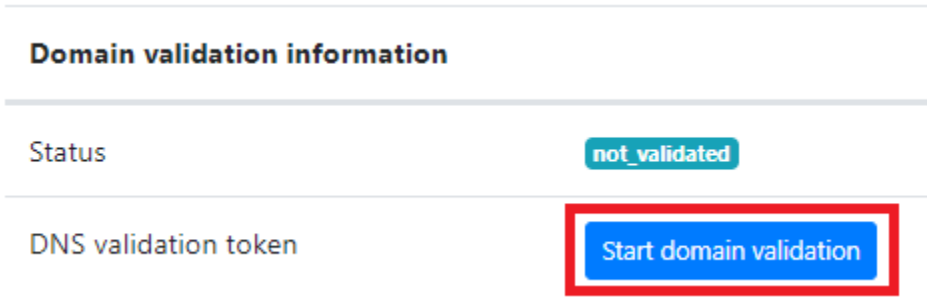


The created check is now listed as «not_validated» in the domain check section:

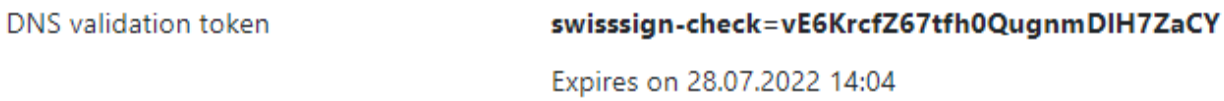


On the new check, click the edit button:

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

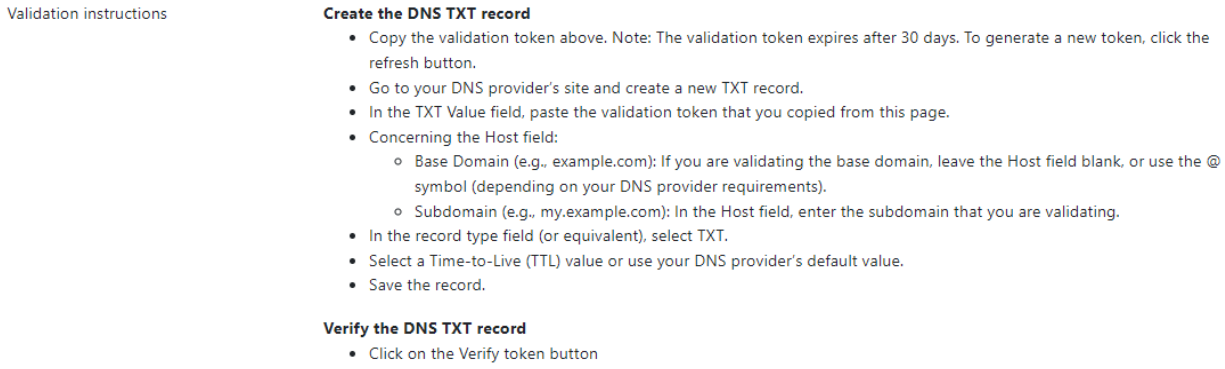


Once the validation token has been created it will be shown in the “DNS validation token” row:

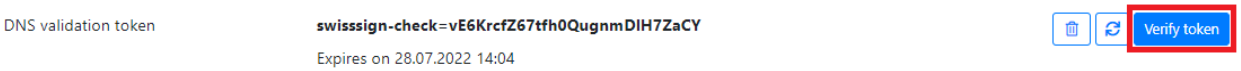


With the validation code you are now able to follow the instructions in the «Validation instructions» row:

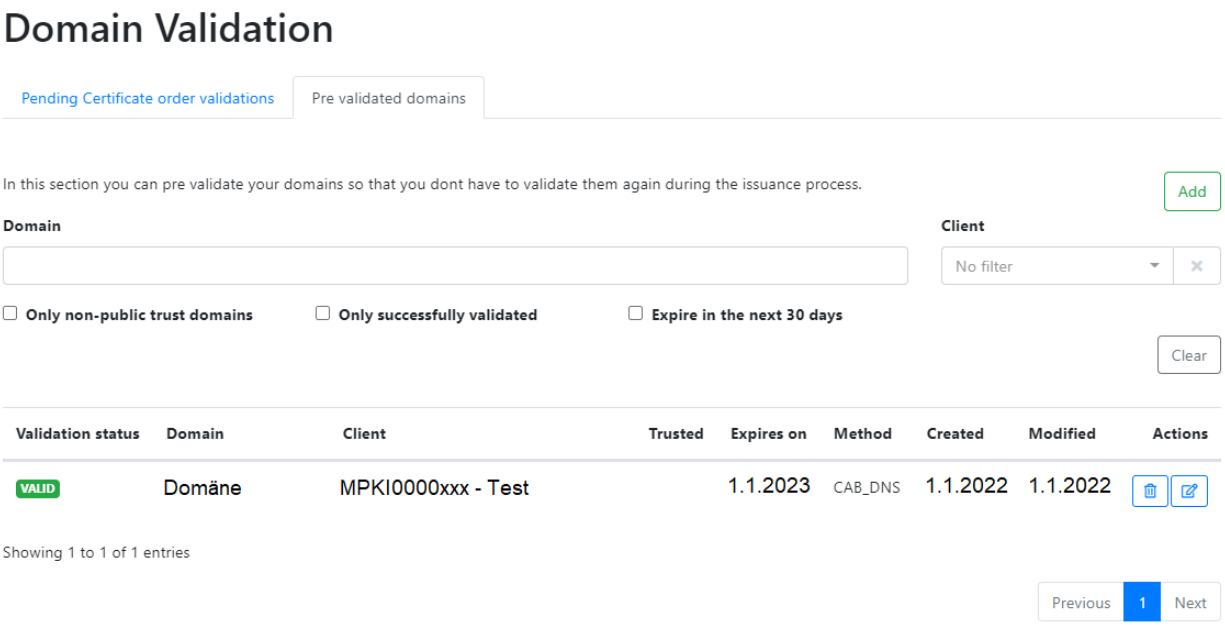
SwissSign



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

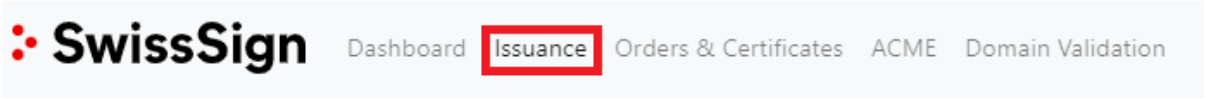


If the check is successful, you can now see the domain listed as “VALID”:

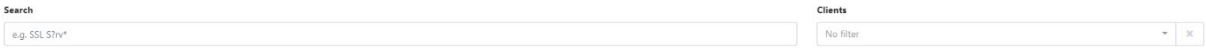


3. Certificate issuance with your MPKI on the new SwissSign CA

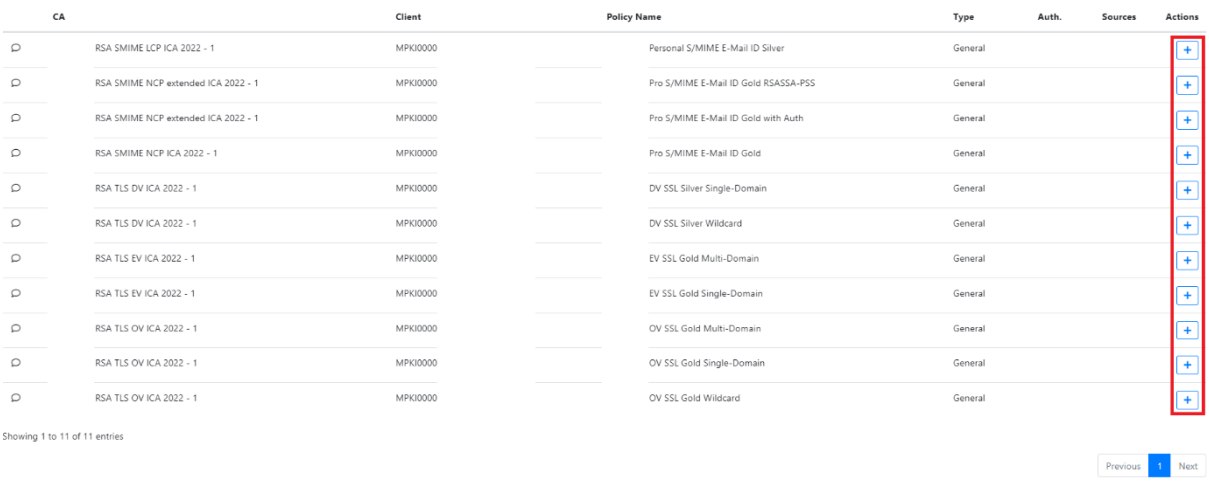
To issue a certificate on the MPKI GUI, navigate to the "Issuance" tab:



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 NCP extended ICA 2022 - 1	MPKI0000	Pro S/MIME E-Mail ID Gold RSASSA-PSS	General			+
RSA SMIME NCP extended ICA 2022 - 1	MPKI0000	Pro S/MIME E-Mail ID Gold with Auth	General			+
RSA SMIME NCP 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			+

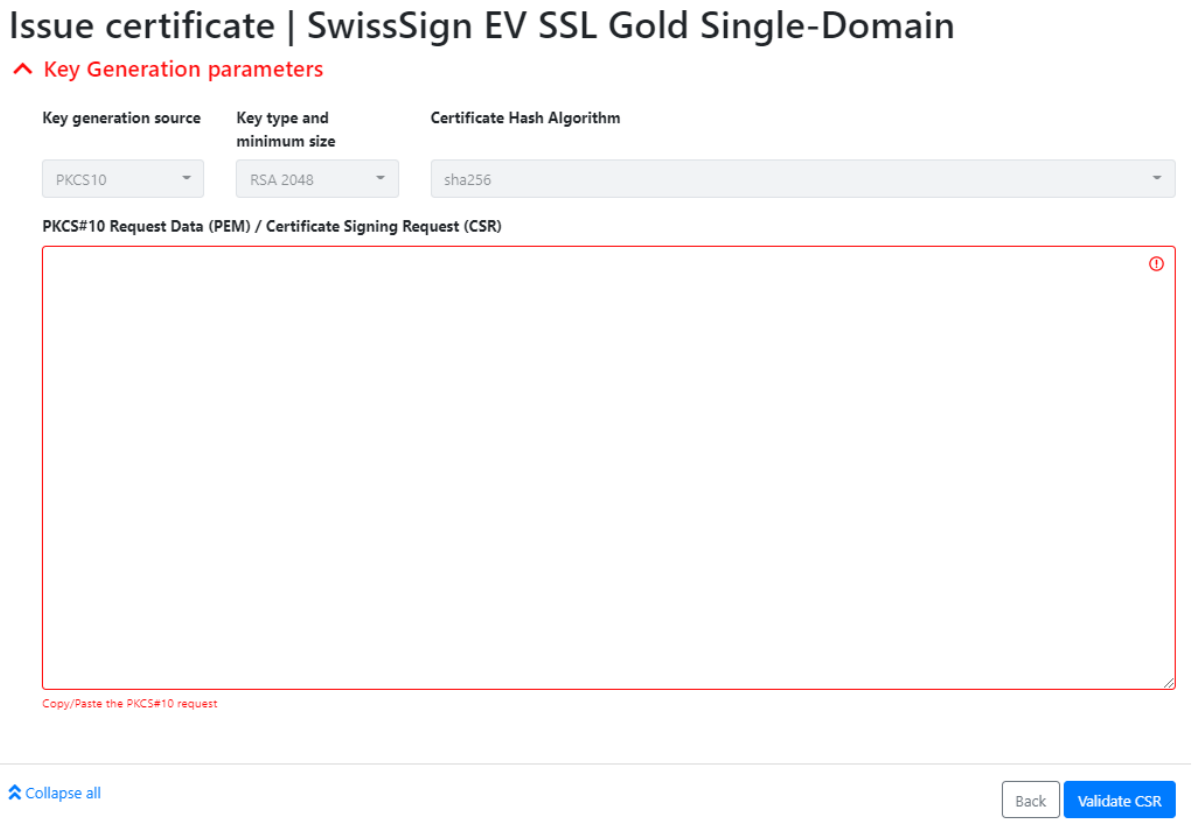
Showing 1 to 11 of 11 entries

Previous 1 Next

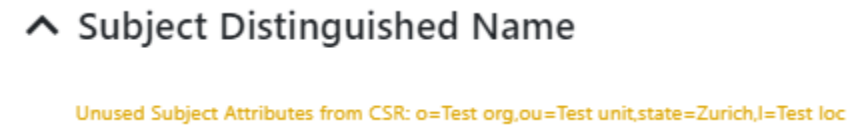
In the next step you enter your CSR.

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

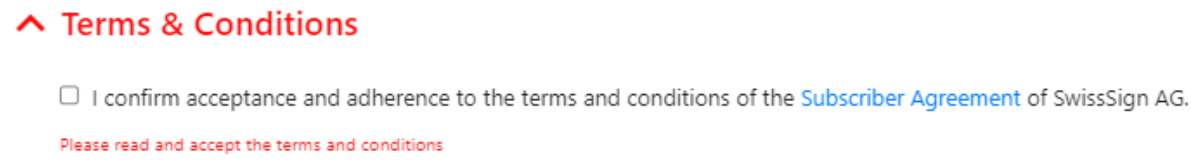


If the CSR contains attributes that are not supported in the selected product, you will receive the following message:

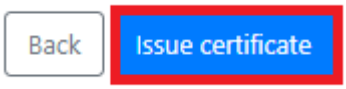


You can insert your DNS entries in the DNS field.
In single domain and e-mail certificates, you can use the same entry as for the "Common Name" (domain and e-mail address respectively).
In multi-domain certificates, you can enter all your SANs if they were not already present in the CSR.

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.



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.