SwissSign

SwissSign CA

SwissSign AG

Kurzanleitung zur Inbetriebnahme Ihrer neuen MPKI auf der neuen SwissSign CA

SwissSign

Revision

Rev	Date	Who	Comment
1.0	08.07.2022	SwissSign AG	Initiales Dokument

SwissSign

Inhalte

SwissSign

1. Anmelden im Konto

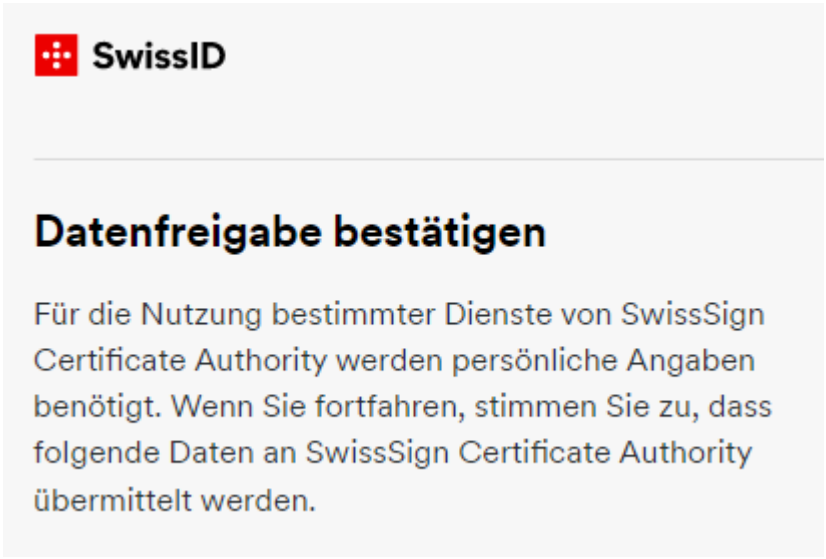
Zum Login wird eine geprüfte SwissID benötigt. Diese muss auf der E-Mail-Adresse erstellt werden, welche in der Bestellung für RA Operatoren angegeben wurde.

Falls Sie noch keine geprüfte SwissID besitzen, können Sie auf unserer Webseite das Onboarding durchführen. Bitte folgen Sie der Schritt-für-Schrittanleitung für das Onboarding. Nutzen Sie für die Erstellung Ihrer SwissID die gleiche E-Mail-Adresse, die sie auf der MPKI-Bestellung angegeben haben.

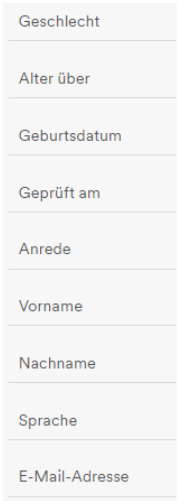
1. Öffnen Sie die Webseite https://ra.swisssign.ch/
2. Loggen Sie sich mit Ihrer SwissID ein.

Bitte beachten Sie, dass zum Einloggen auf die MPKI ein Zwei-Faktor-Authentisierung (SwissID App oder SMS-Code) nötig ist:

3. Zur Nutzung der MPKI als RA Operator müssen bestimmte Daten des SwissID Accounts an die MPKI freigegeben werden.

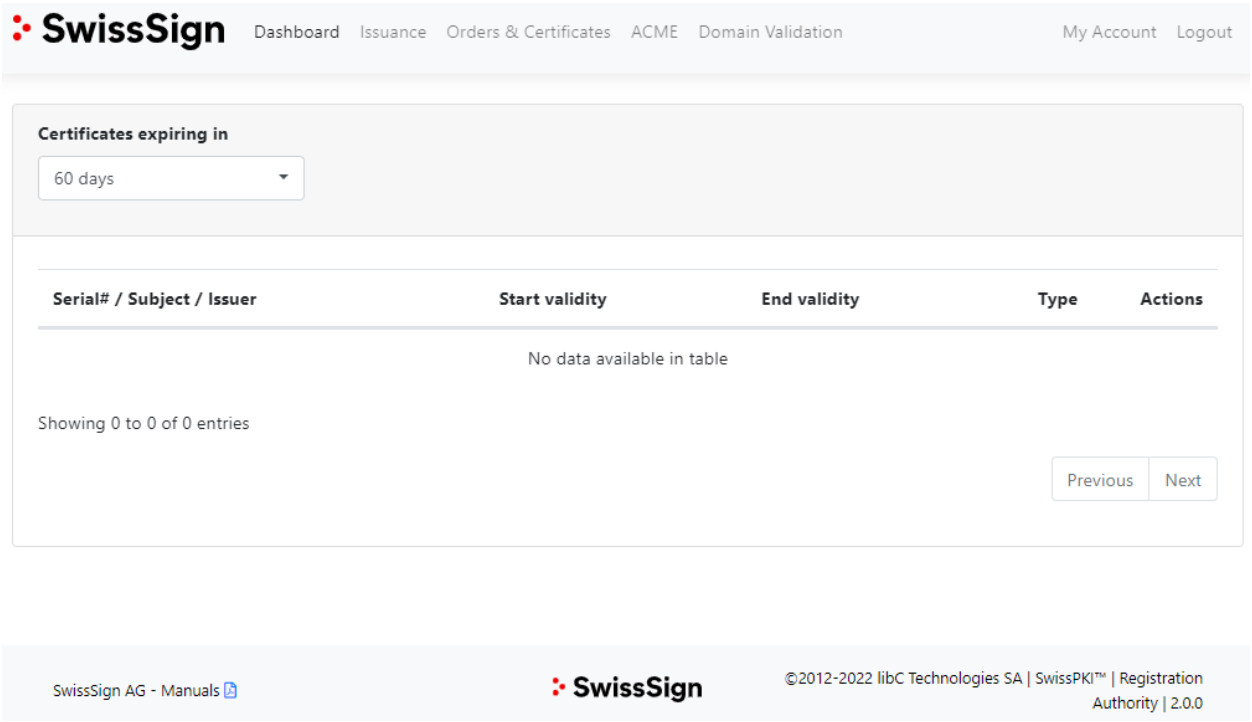


Die für den Zugang zur MPKI benötigten Daten werden im Consent angezeigt:



Mit dem Button «Freigeben» geben Sie die entsprechenden Daten frei und fahren mit dem Login fort:

Sie sind nun eingeloggt und sehen Ihr MPKI GUI:

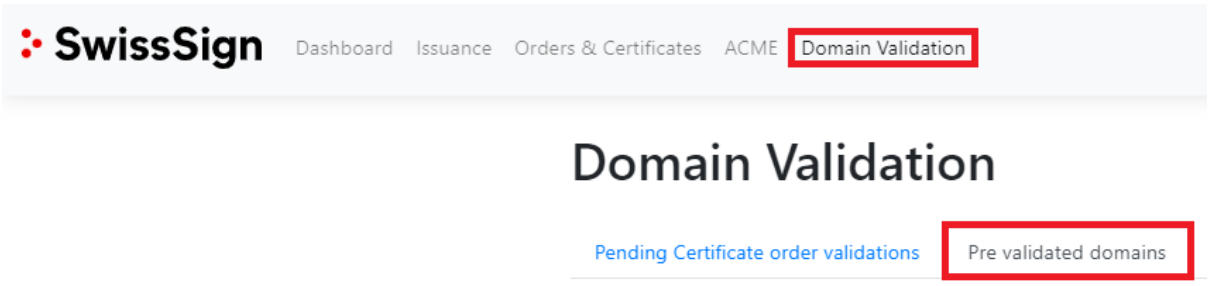


2. Domänen validieren auf der neuen SwissSign MPKI

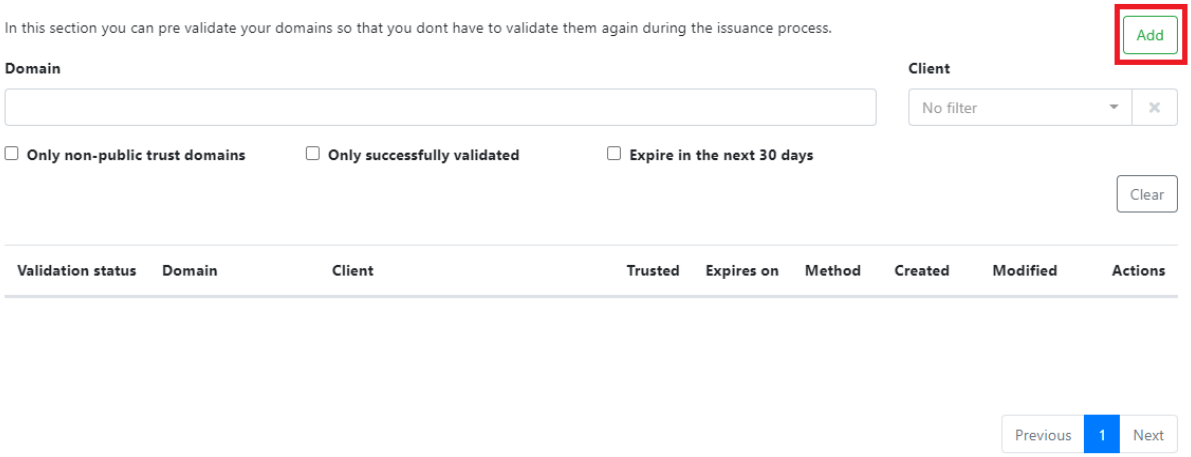
Bevor Zertifikate ausgestellt werden können, müssen die dazugehörigen Domänen validiert werden. Es muss also noch der Eigentumsnachweis ausgewiesen werden.

Als RA Operator haben Sie die Möglichkeit, im Rahmen des vom CA Browser Forums zugelassenen Verfahrens, neue Hauptdomänen für die Managed PKI zu beantragen und automatisch prüfen zu lassen. Hierzu müssen Sie sich auf der Zertifikatsplattform ra.swisssign.ch einloggen.

Auf dem GUI klicken Sie auf «Domain Validation» und anschliessend im Untermenü auf «Pre validated domains».

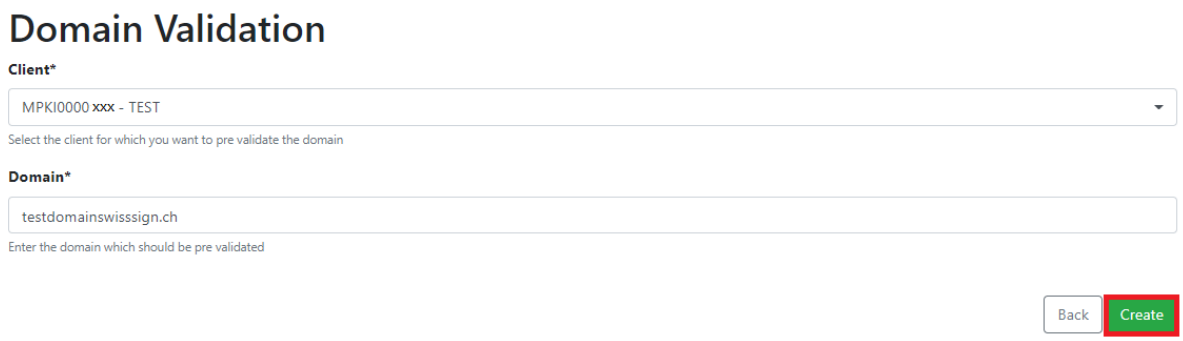


Auf dieser Seite können Sie mit «Add» den Prozess zum Hinzufügen einer neuen Domäne starten.

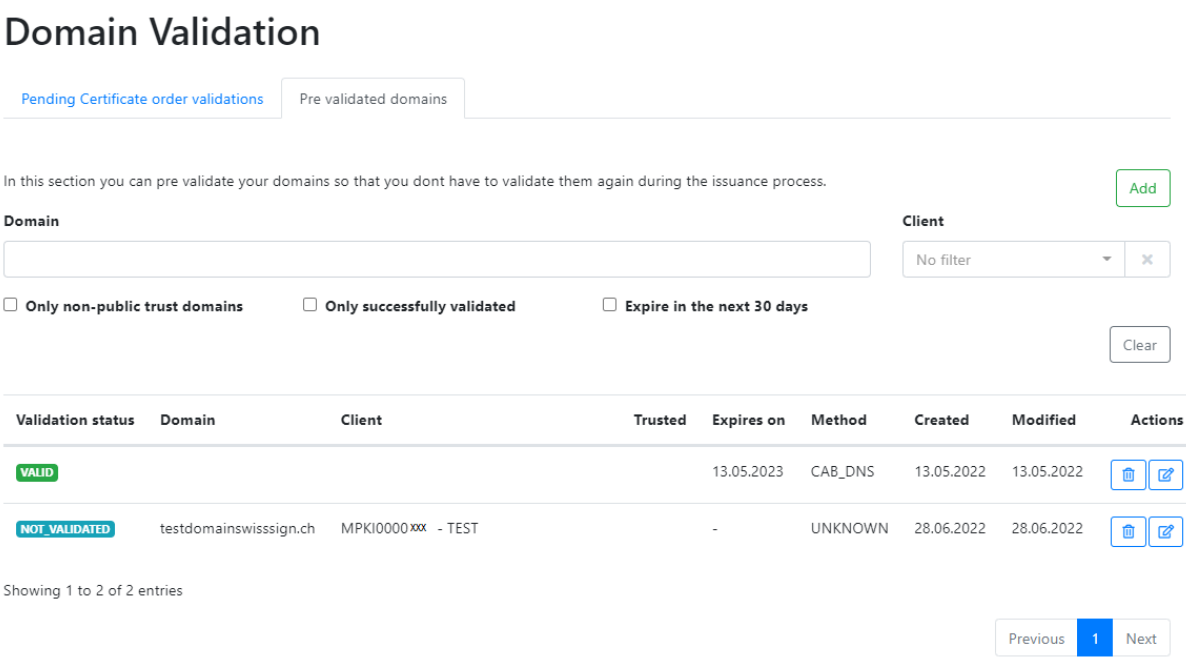


Wenn Sie RA Operator von nur von einer MPKI sind, ist automatisch die korrekte MPKI ausgewählt. Ansonsten wählen Sie bitte die MPKI aus, auf welcher Sie eine neue Domäne hinzufügen möchten.

Unter Domäne geben Sie die hinzuzufügende Domäne ein. Anschliessend klicken Sie auf «Create» um den Domänen Check zu erstellen.

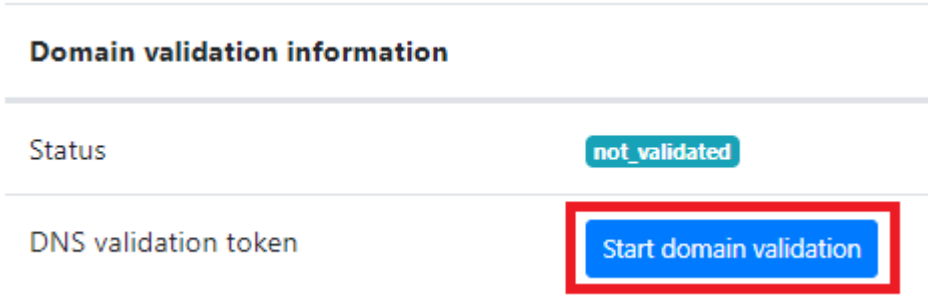


Der erstellte Check wird nun als «not_validated» unter den Domänen Checks angezeigt:

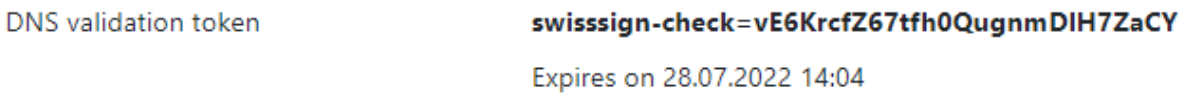


Auf dem entsprechenden Check klicken Sie den Edit Button:

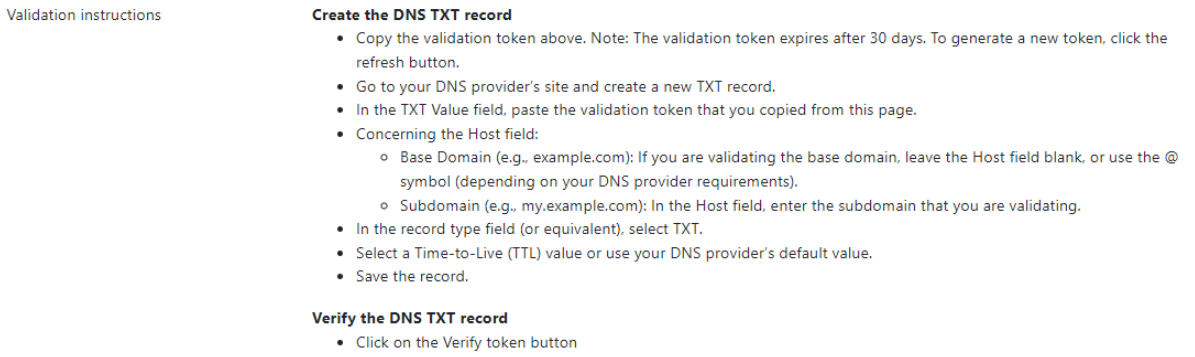
Hier können Sie mit «Start domain validation» die Validierung starten und den Validierungscode erstellen.



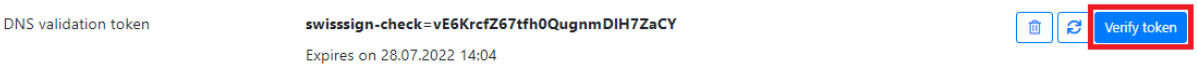
Der Validierungscode wurde erstellt und wird nun unter «DNS validation token» angezeigt.



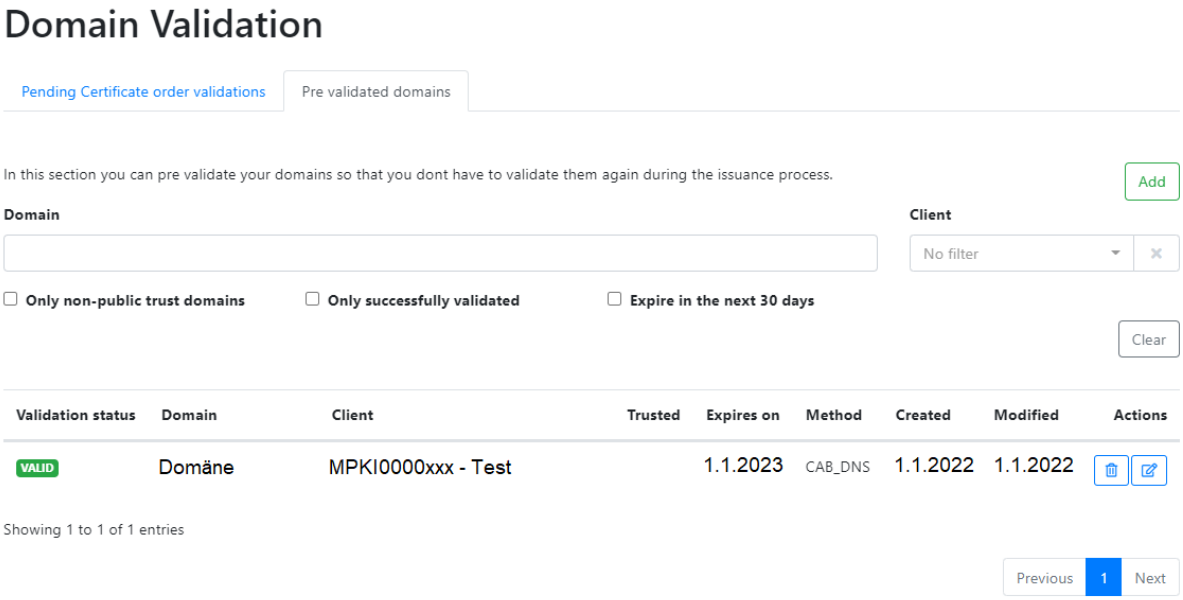
Mit dem Validierungscode können Sie die Instruktionen unter «Validation instructions» durchführen.



Wenn alles gemäss Instruktionen hinterlegt ist, können Sie mit dem «Verify token» Button die Validierung überprüfen.

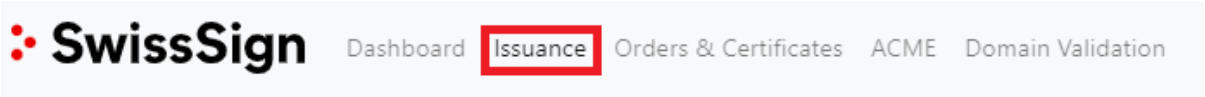


Bei einem erfolgreichen Check wird nun die Domäne als validiert angezeigt:



3. Ausstellung von Zertifikaten auf der MPKI

Auf dem MPKI GUI navigieren Sie zum Tab «Issuance»:



Hier finden Sie die Auflistung Ihrer verfügbaren Produkte auf Ihrer MPKI. In der Spalte «Policy Name» sehen Sie alle Zertifikatsprodukte, wie Sie auch im Bestellformular ersichtlich sind. Ebenfalls ist es möglich nach einem spezifischen Produkt suchen. Falls Sie in mehreren MPKIs als RA Operator eingetragen sind, können sie unter «Clients» die gewünschte MPKI auswählen:

Search

e.g. SSL S?rv*

Clients

No filter

Den Prozess zum Erstellen eines Zertifikates starten wir mit dem «Actions» Button hinter dem gewünschten Produkt:

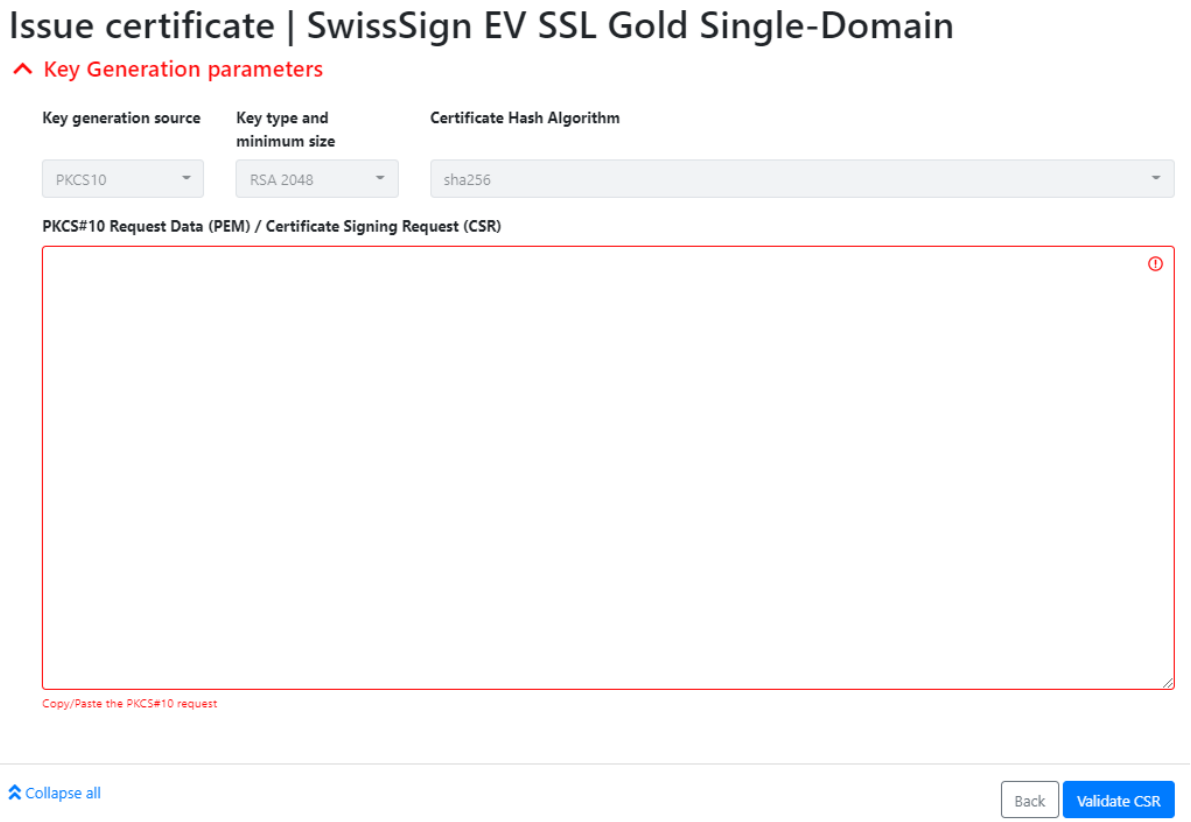
	CA	Client	Policy Name	Type	Auth.	Sources	Actions
	RSA SMIME LCP ICA 2022 - 1	MPKI0000	Personal S/MIME E-Mail ID Silver	General			
	RSA SMIME NCP extended ICA 2022 - 1	MPKI0000	Pro S/MIME E-Mail ID Gold RSASSA-PSS	General			
	RSA SMIME NCP extended ICA 2022 - 1	MPKI0000	Pro S/MIME E-Mail ID Gold with 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

Im nächsten Schritt tragen Sie Ihren CSR ein.

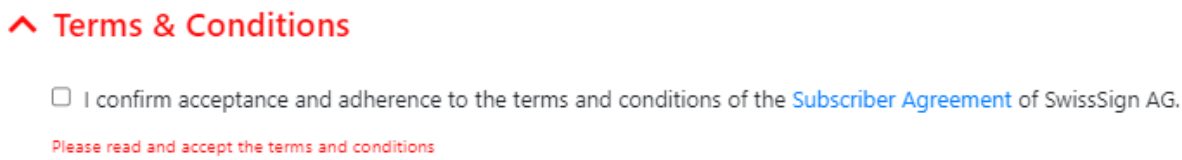
Aus regulatorischen Gründen darf Sie SwissSign hierbei nicht unterstützen. Wie Sie ein CSR erstellen entnehmen Sie dem «Beispiel zur CSR Erstellung mit OpenSSL» welches auf folgender Seite hinterlegt ist:
https://www.swisssign.com/support/systemstatus/details~newsID=02715d1b-9102-4148-8992-846a75d7fdf2~.html



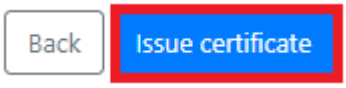
Sind im CSR Attribute enthalten, welche im ausgewählten Produkt nicht unterstützt werden, erhalten Sie die folgende Meldung:

Im DNS-Feld können Sie Ihre DNS-Einträge einfügen.
In Single-Domain und E-Mail Zertifikaten können Sie denselben Eintrag wie beim «Common Name» verwenden (Domäne respektive E-Mail-Adresse).
In Multi-Domain Zertifikaten können Sie alle Ihre SANs eintragen, falls diese nicht bereits im CSR vorhanden waren.

Zum Schluss müssen Sie, um weiterzufahren, die Teilnehmerbedingungen akzeptieren. Wenn Sie auf Subscriber Agreement (blauer Text) klicken, öffnen Sie das entsprechende Dokument.
Klicken Sie, nachdem Sie die Teilnehmervereinbarung zur Kenntnis genommen haben, auf das Kästchen und auf «Ich akzeptiere diese Bedingungen», um weiterzufahren.



Nun können Sie mit dem Button «Issue certificate» das Zertifikat ausstellen.



Wenn die Domäne bereits vorvalidiert wurde, wird das Zertifikat direkt ausgestellt.
Wenn die Domäne noch nicht validiert wurde, startet der Validierungsprozess und ein DNS-Token wird generiert. Das Zertifikat wird erst nach dieser Validierung ausgestellt.