

SwissSign CA
SwissSign AG

Kurzanleitung zur Inbetriebnahme Ihrer neuen
MPKI auf der neuen SwissSign CA

Revision

| Rev | Date | Who | Comment |
|------------|-------------|--------------|--------------------|
| 1.0 | 08.07.2022 | SwissSign AG | Initiales Dokument |

Inhalte

| | |
|--|---|
| 1. Anmelden im Konto | 4 |
| 2. Domänen validieren auf der neuen SwissSign MPKI | 6 |
| 3. Ausstellung von Zertifikaten auf der MPKI | 9 |

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.

 ×

Einloggen für SwissSign Certificate Authority

🗕



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



Mit SMS-Code bestätigen

Bitte geben Sie den Code ein, den wir an Ihre Mobilnummer
gesendet haben.

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



Datenfreigabe bestätigen

Für die Nutzung bestimmter Dienste von SwissSign
Certificate Authority werden persönliche Angaben
benötigt. Wenn Sie fortfahren, stimmen Sie zu, dass
folgende Daten an SwissSign Certificate Authority
übermittelt werden.

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

| |
|----------------|
| Geschlecht |
| Alter über |
| Geburtsdatum |
| Geprüft am |
| Anrede |
| Vorname |
| Nachname |
| Sprache |
| E-Mail-Adresse |

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

Wenn Sie diese Daten nicht freigeben, werden Sie bestimmte Dienste von SwissSign Certificate Authority nur eingeschränkt nutzen können.

Sie sind nun eingeloggt und sehen Ihr MPKI GUI:

 [Dashboard](#) [Issuance](#) [Orders & Certificates](#) [ACME](#) [Domain Validation](#)[My Account](#) [Logout](#)

Certificates expiring in

60 days ▼

| Serial# / Subject / Issuer | Start validity | End validity | Type | Actions |
|----------------------------|----------------|--------------|------|---------|
| No data available in table | | | | |

Showing 0 to 0 of 0 entries

SwissSign AG - Manuals [🔗](#)©2012-2022 IlibC Technologies SA | SwissPKI™ | Registration Authority | 2.0.0

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.swissign.ch einloggen.

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

SwissSign Dashboard Issuance Orders & Certificates ACME **Domain Validation**

Domain Validation

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

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

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

Domain

Client

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 |
|-------------------|--------|--------|---------|------------|--------|---------|----------|---------|
|-------------------|--------|--------|---------|------------|--------|---------|----------|---------|

1

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.

Domain Validation

Client*

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

Domain*

Enter the domain which should be pre validated

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

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 | testdomainswissign.ch | MPKI0000*** - TEST | - | | UNKNOWN | 28.06.2022 | 28.06.2022 |   |

Showing 1 to 2 of 2 entries

Previous **1** Next

Auf dem entsprechenden Check klicken Sie den Edit Button:

| | | | | | | | | |
|---------------|-----------------------|--------------------|---|--|---------|------------|------------|---|
| NOT_VALIDATED | testdomainswissign.ch | MPKI0000*** - TEST | - | | UNKNOWN | 28.06.2022 | 28.06.2022 |   |
|---------------|-----------------------|--------------------|---|--|---------|------------|------------|---|

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

Domain validation information

Status

not_validated

DNS validation token

Start domain validation

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

DNS validation token

swissign-check=vE6KrcfZ67tfh0QuugnmdIH7ZaCY

Expires on 28.07.2022 14:04

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

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

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

DNS validation token

swissign-check=vE6KrcfZ67tfh0QugnmDIH7ZaCY

Expires on 28.07.2022 14:04



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

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 | |

Showing 1 to 1 of 1 entries

Previous 1 Next

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 57m*

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.swissign.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

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

Subject Distinguished Name

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

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.

^ Subject Alternative Name

DNS required.

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

| | |
|--------|----------------------|
| DNS | |
| DNS 1* | <input type="text"/> |

DNS required.

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.

^ 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

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

| | |
|------|--------------------------|
| Back | Issue certificate |
|------|--------------------------|

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.