SwissSign

Order for a SwissSign Managed Public Key Infrastructure **MPKI-DV**

Customer

According to the (commercial) register entry in the state register of the relevant country

Company name

Street

Street number

Postcode

Place

Canton/Federal state

Country

Registration number/VAT ID no. *or other information about the organisation, e.g. URL*

Email address

Invoicing address

☐ Use Customer's invoicing address

Company name

Email address for invoicing by SwissSign

First name of contact person

Surname of contact person

Street

Street number

Postcode

Place

Country

Invoicing language

EN

Product order: The prices are stated in CHF per year, excluding VAT

		Number	Individual price	CHF
DV	**DV SSL Silver Single-Domain** domain validated		129	0.00
	DV SSL Silver Wildcard* domain validated | for all subdomains		329	0.00
	Personal S/MIME E-Mail ID Silver Email domain validated | Liability limited to a maximum of CHF 10,000.00		19	0.00
	Certificate prices			0.00
	Volume discount		0%	0.00
	Total annual price (net)			**0.00**

The advance invoice for the following years either corresponds to the active certificates on the billing date of the last contract year or if this is lower than the initial advance invoice, then the initial advance invoice of the first order is billed.

* Wildcard certificates cannot be ordered over the ACME interface

1. Other applicable documents

The following documents, in the following descending order of priority, form an integral part of this order:

- this duly completed and signed order
- Applicable SwissSign AG GTC: https://www.swisssign.com/agb-swisssign.html

Conduct guidelines (the most up-to-date version of these documents can be found at https://repository.swisssign.com)

- PDS; PKI Disclosure Statement Certificate Services
- Subscriber Agreement (EUA); Subscriber Agreement
- RPA; Relying Party Agreement
- RA Policy; Guidelines on the delegation of registration authority activity

At the time of issuance of the certificate, the latest versions of the following documents shall also apply (These SwissSign documents are published at https://repository.swisssign.com. New versions of these documents will be published on the date of entry into force and will be communicated via the following system status page: https://www.swisssign.com/support/systemstatus.html);

For all certificates:

- Trust Services Practice Statement (TSPS) (SwissSign-TSPS.pdf)

ⓘ Please note that for an order to be valid, this document must be completed as follows:

- MPKI RA Operators: page 4, section 2
- General email address, notifications and publi- cation of certif- icates: page 5

All TLS certificates are also subject to:

- Certificate Practice Statement for TLS Certificates (CPS TLS) (SwissSign-CPS-TLS.pdf)
- Certificate, CRL and OCSP Profiles for TLS Certificates (CPR TLS) (SwissSign-CPR-TLS.pdf)

Domain Validated TLS certificates are also subject to:

- SwissSign DV CP – Certificate Policy for Domain Validated certificates (DVCP) (SwissSign-CP-DV.pdf)

All S/MIME certificates are also subject to:

- Certificate Practice Statement for S/MIME certificates (CPS S/MIME) (SwissSign-CPS-SMIME.pdf)
- Certificate, CRL and OCSP Profiles for S/MIME certificates (CPR S/MIME) (SwissSign-CPR-SMIME.pdf)

Domain Validation LCP S/MIME certificates are also subject to:

- Certificate Policy according to Lightweight Certificate Policy (LCP) (SwissSign-CP-LCP.pdf)

These documents are subject to oversight by the auditors of SwissSign and cannot be amended in terms of their content. They must be and are adjusted on an ongoing basis in line with regulations and standards applicable to Certification Authorities. Alerts notifying changes to the content of the system status page may be signed up for on that page. They shall be deemed to be approved unless the Customer objects in writing thereto within one month of their adoption. An objection shall constitute ordinary termination of the associated contracts and may result in the revocation of certificates with an issue date after the change. A new version of the Guidelines on the Delegation of Registration Authority Activity must always be approved and accepted in writing by means of a renewal of this declaration of acceptance.

General Terms and Conditions of the Customer shall not apply.

2. Appointment of RA Operators and notifications

The individuals holding access rights may carry out the tasks necessary in connection with the applications for and administration of certificates. The designated persons are authorised to order and manage domain-validated certificates.

At least two RA Operators must be appointed as authorised representatives for the registration authority activity.

Please keep in mind, that you require a SwissID to log into the MPKI. The filled out email address will be the account that will be able to access the MPKI.

RA Operator 1

First name, Surname

Position

Company name

Canton/Federal state of the company

Country of the company

Email address

Telephone

RA Operator 2

First name, Surname

Position

Company name

Canton/Federal state of the company

Country of the company

Email address

Telephone

RA Operator 3

First name, Surname

Position

Company name

Canton/Federal state of the company

Country of the company

Email address

Telephone

RA Operator 4

First name, Surname

Position

Company name

Canton/Federal state of the company

Country of the company

Email address

Telephone

RA Operator Delegation

I will delegate the operation of the MPKI to the following company which is already validated by SwissSign AG.

Exact name of the company with an existing MPKI installation:

General email address for notifications to the Customer and for potential interface access

As part of the registration authority activity, the RA Operators shall receive emails, for example, concerning the status of the certificates. These emails are to be sent to the following general email address of the Customer, e.g. it-info@example.com

Email address for notifications and for potential interface access:

ⓘ If regulatory requirements require additional or other notifications, SwissSign shall comply with these requirements, irrespective of the selection made.

Notifications concerning end of validity of a certificate

- ☐ No notification at all, since, for example, the system used for autoenrolment or mail gateway will handle the notifications or renewals
- ☐ Notification only to the RA Operators, but no notification to the certificate owner, 10 and 30 days before end of validity of the certificate
- ☐ Certificate owners and RA Operators will be notified, 10 and 30 days before end of validity of the certificate.

ⓘ *The RA Operators will always be informed via the email address stored in the Customer's account.*

Autoenrolment for Personal S/MIME E-Mail ID Silver

- ☐ The Customer wishes to activate the Autoenrolment for Personal S/MIME E-Mail ID Silver certificates. (This can only be ensured if the notifications are turned on).
  Autoenrolment will send emails 30 days prior to the expiration of certificates with the option of renewing the corresponding certificate.

Publication of S/MIME certificates by SwissSign

- ☐ The Customer wishes to publish its certificates in the general directory of directory.swisssign.ch (LDAP) so that they can be seen by everyone and everyone can communicate with the Customer using encryption.
- ☐ The Customer does not wish to publish its certificates.

ⓘ *Please note, that TLS certificates are always published for regulatory reasons.*

Domains to be set up for publicly trusted emails and SSL certificates

Using your RA Operator account, enter the domain in the SwissSign MPKI portal via the "MPKI Domains" menu and verify successful access by making a change to the DNS entry. You can find instructions for the MPKI Setup here.

You hereby warrant that you have either entered SwissSign as the issuing Certification Authority in the DNS entries (CAA) for the specified domains, or that there are no restrictions on the issuing Certification Authorities. Details of the necessary entries can be found at https://sslmate.com/caa. You must ensure that, during the term of your agreement, you do not add any restrictions to the DNS entry in respect of SwissSign, as the issuing certification authority for this domain.

3. Conclusion, term and termination of the agreement

Sending in the order form establishes a binding order for a fee-based service.

By sending in the order, you confirm your purchase of the MPKI with the initial agreement term specified below; you furthermore confirm that you have read, understood and accepted SwissSign's GTC, including the annexes that are relevant to this agreement.

The contractual term and invoicing period shall begin on the date of the order.

The initial term of the agreement shall be for one year; upon expiry of the initial term, the agreement shall be automatically extended each year by a further year.

After the expiry of the initial term of the agreement, the contract may be terminated at the end of the respective agreement term, subject to a 3-month notice period.

SwissSign

Checklist and instructions for sending the documents

Please check the order using the following checklist before returning it:

- Can you provide proof of access to the domains? Does the DNS permit issuance by SwissSign (CAA entry)?

Send the scanned documents to **registration@swisssign.com**

or:

Send the documents in the paper original by post to SwissSign.

SwissSign AG
Sales & Partner Management
Sägereistrasse 25
8152 Glattbrugg
Switzerland

Receipt of the order shall be confirmed by SwissSign by email.

Sign up for the RSS notification feed through system status reports (recommended)

https://www.swisssign.com/en/support/systemstatus.html