SwissSign

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

☐ order as a new Customer

☐ Upgrade order as an existing Costumer. The current MPKI Service ID is:

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 EUR per year, excluding VAT

ⓘ Please note that for an MPKI OV order, a **minimum amount of EUR 300.00 per year** shall be invoiced.

		Number	Individual price	EUR
DV	**DV SSL Silver Single-Domain** domain validated		109	0.00
	DV SSL Silver Wildcard* domain validated | for all subdomains		299	0.00
	Personal S/MIME E-Mail ID Silver Email domain validated | Liability limited to a maximum of EUR 10,000.00		17	0.00
OV	**OV SSL Gold Single-Domain** organisation validated		219	0.00
	OV SSL Gold Wildcard* organisation validated | for all subdomains		519	0.00
	OV SSL Gold Multi-Domain organisation validated | max. 60 SAN (Subject Alternative Name) entries | with/without www		999	0.00
	Pro S/MIME E-Mail ID Gold Email and organisation validated | Surname | First name | Email | Organisation | Place | Liability limited to a maximum of EUR 100,000.00		35	0.00
	Pro S/MIME E-Mail ID Gold with Auth. Email and organisation validated | Surname | First name | Email | Organisation | Place | Also suitable for authentication | Liability limited to a maximum of EUR 100,000.00		35	0.00
	Pro S/MIME E-Mail ID Gold RSASSA-PSS Email and organisation validated | Surname | First name | Email | Organisation | Place | Also suitable for authentication | Liability up to a maximum of EUR 100,000.00		439	0.00

Certificate prices			0.00
Volume discount		0%	0.00
Minimum amount surcharge	OV minimum amount EUR 300.00	0.00	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. General provisions

SwissSign is an accredited provider of certification services in Switzerland pursuant to the Swiss Federal Act on Certification Services in the Area of Electronic Signature and other Digital Certificate Applications (Swiss Federal Act on Electronic Signatures, ZertES) as well as a trusted Certification Authority ("CA") for the relevant software and operating system manufacturers.

Certification Authorities have the task, inter alia, of identifying applicants for certificates.

In accordance with applicable national statutory provisions and international regulations, such as the Swiss Federal Act on Electronic Signatures, ZertES; eIDAS – EU Regulation, ETSI – Standards or CA/Browser Forum Guidelines, recognised Certification Authorities may delegate their responsibility for verifying the identity of an applicant to third parties.

SwissSign intends, in the context of the issuance of certificates, to allow verification of the identity of the applicants by Registration Authorities, within the meaning of the aforementioned jurisprudence and regulations, to be carried out by carefully selected and monitored organisations and expects in relation to this Order that the obligations indicated will be approved of.

In placing this MPKI order, the Customer assumes the role of a limited or full registration authority for the purposes of requests for certificates and authorisations.

2. 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)

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)

Organization Validated TLS certificates are also subject to:

- SwissSign OV CP – Certificate Policy for Organization Validated certificates (OVCP) (SwissSign-CP-OV.pdf)

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

- Authorised signatories of the Customer: page 11, section 9
- MPKI RA Operators: page 5, section 3
- General email address, notifications and publication of certificates: page 6

In addition, a valid copy of an identification document (ID card, front and reverse side, or passport), which must be dated and signed by the relevant holder, must be attached to the order for each added signature. Submission by scanned copy is sufficient for the dated and signed copies of the identity documents.

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)

Organizational Validation NCP S/MIME certificates are also subject to:

- Certificate Policy according to Normalized Certificate Policy (NCP) (SwissSign-CP-NCP.pdf)

Organizational Validation NCP S/MIME certificates with special EKU are also subject to:

- Certificate Policy according to Normalized Certificate Policy (NCP) with extended EKU (SwissSign-CP-NCP-extended.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.

3. Appointment of RA Operators for the registration authority activity and notifications

The Customer may arrange for the tasks which are required in the context of certificate application, approval and administration to be performed by the following undersigned persons to whom it hereby grants power of representation for the registration authority activity (said power being limited to performance of the said tasks). They are **not** authorised to act as a representative in any additional way, and they are specifically not authorised to amend this agreement. For the registration authority activity, said persons shall be given access for the purpose of approving certificate applications. The persons indicated are each entitled to sign alone and to release certificates in accordance with the registration process (Section 4).

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.*

4. Declaration of Consent to the registration process for publicly trusted certificates

For all publicly trusted certificates, the Customer shall verify the identity and, if required, the organisation membership and other specific attributes of a certificate applicant. The basic certificate issuance process under this Agreement is based on the following conditions:

A) Employees and part-time employees (in the case of email certificates)

The Customer warrants under an MPKI that it will clearly verify the identity or arrange for clear verification of the identity of the full-time and part-time employees of its organisation by performing the following checks:

- Employment contract and
- A copy of a passport or a copy of the front and reverse sides of a valid identity card (CH, EU, EFTA) in Latin script.

B) Subcontractors and consultants (in the case of email certificates)

The Customer warrants under an MPKI that it will clearly verify the identity or arrange for clear verification of the identity of the subcontractors and consultants by performing the following checks:

- Contractual agreement between the Customer and the subcontractor/consultant, which explicitly identifies the subcontractor or consultant (this may include, for example, a confidentiality agreement) and
- A copy of a passport or a copy of the front and reverse sides of a valid identity card (CH, EU, EFTA) in Latin script.

C) Machines, equipment and (web) servers (for SSL certificates), possibly:

- Domain Validation

D) Other:

The Customer warrants that it will verify or arrange for verification of the identity of all other persons, and will proceed with them, as follows:

- Signing of an agreement which prescribes the careful use of the certificates and in which the person fully accepts the obligations and required cooperation in the context of use of the certificate, and
- A copy of a passport or a copy of the front and reverse sides of a valid identity card (CH, EU, EFTA) in Latin script.

Disclosure obligation to SwissSign

In all cases, the Customer warrants that it has the ability to comply with the following:

- to check or arrange for the checking of the registration and of all documents pertaining thereto in accordance with the aforementioned rules;
- in particular, it must be ensured that, in respect of all persons for whom certificates are issued (email certificates with an organisation entry), the organisation's membership has been checked;
- the Customer must be able to provide evidence corroborating these checks at any time upon request by SwissSign.

5. Contracted data processing

Within the framework of this agreement, SwissSign provides data processing services to the Customer. In this respect, SwissSign shall receive access to personal data, which it shall process exclusively on behalf of the Customer in accordance with its instructions. Within the context of the delegation of registration authority activity, the Customer assumes tasks relating to certificate issuance involving identification, registration and archival. Pursuant to the regulatory provisions (e.g. ZertES, eIDAS, CA/Browser Forum Baseline Requirements), SwissSign remains liable towards the certificate holder and the third party relying on it.

5.1 Scope of application

Performance of the agreement includes the processing of personal data. The subject matter, duration, scope and purpose of the data processing performed by SwissSign is governed exclusively by this agreement.

The Parties undertake to process the data (including in particular surname, first name, identity document type, address, email address, residence/registered office) in accordance with the relevant applicable statutory regime, specifically including the Swiss Federal Act on Data Protection (FADP) and the European General Data Protection Regulation (EU GDPR).

5.2 Personal data

Personal data means any information defined under Article 5 (a) FADP or Article 4 (1) and Article 9 GDPR.

5.3 Nature and purpose of processing

SwissSign shall refrain from using the personal data for its own purposes or for any purposes other than those referred to in this agreement. Personal data shall be processed by SwissSign for purposes of the identification, registration, issuance and management of certificates as follows:

- Issuance of certificates
- Publication of certificate status information (Revocation Status Service)
- Identification
- Registration
- Verifications and approvals
- Archiving
- Revocation
- Correspondence and contact with data subjects

5.4 Data categories

The following categories of data shall be processed by SwissSign:

- Personal master data (name, title, professional title/academic title, date of birth, address)
- Contact details (address, email address, telephone number)
- Contract data (contract details, services, product or contract interest, Customer number)
- Customer history
- Contract accounting data and payment information (invoice details, bank details, credit card information)
- Log data (log files)
- Identity data
- Authentication data
- System data (log, configuration and audit data)
- Data relating to disclosures (e.g. from public registers)

5.5 Categories of data subjects

The above types of personal data are to be processed in respect of the following categories of data subjects:

- Certificate holders
- Contact persons/partners

5.6 Processing location

The data processing performed by SwissSign shall take place exclusively in Switzerland.

The outsourcing of data processing to a third country outside of the EU/EFTA shall require the prior, written consent of the Customer.

5.7 Contract processing and use of third parties

SwissSign shall process personal data exclusively on behalf of Customer and in accordance with its instructions (within the meaning of Article 9 FADP and Article 28 GDPR). The activities and service descriptions are set out in this agreement, including the aforementioned accompanying documents. Any changes to contract service obligations and instructions must be stated in writing.

In accordance with Article 12 FADP and Article 30 GDPR, SwissSign shall maintain a data processing record for the purposes of this contracted data processing.

SwissSign warrants that the staff responsible for processing data and other auxiliary agents shall be prohibited from processing data except in accordance with instructions. Steps shall be taken to ensure that the above-referenced persons are subject to an appropriate duty of confidentiality and non-disclosure, which shall continue to apply even after termination of the employment or contractual relationship, etc.

Any third parties involved in the provision of services shall be subject to the same obligations as the Parties in relation to the processing of personal data. The Parties warrant that they will impose their respective obligations on any third parties. They shall remain responsible for compliance with these obligations.

5.8 Technical and organisational measures

SwissSign undertakes to put in place all reasonable and necessary technical and organisational measures to protect personal data, specifically in order to prevent unauthorised third party access to the data or the loss, damage, erasure or destruction thereof. The protective measures taken must comply at least with the requirements set forth in Article 7 FADP and Article 32 GDPR.

The technical and organisational measures must ensure the long-term confidentiality, integrity, availability and load capacity of the processing systems and services. In addition to digitised information and data security, access to the premises on which data are processed must be protected.

In this respect, SwissSign shall take the following measures in particular:

- Physical access control: Premises/IT systems
- Transfer control
- Disclosure control
- Storage control
- User control
- User access control
- Separation control

5.9 Customer's control and audit rights

SwissSign undertakes, upon the Customer's oral or written request, to provide the Customer, within a reasonable period of time, with all information and evidence necessary to carry out a control check to verify that SwissSign is processing Customer personal data in a contractually compliant manner.

The Customer shall have the right to commission, at its own expense, a suitably qualified external auditor, who must be subject to a duty of confidentiality, to carry out, to the extent necessary, a review of compliance with the applicable data protection requirements. In this respect, the principle of proportionality must be observed and the legitimate interests of SwissSign (in particular those of confidentiality) must be taken into account. Control checks carried out at SwissSign's premises must be performed without any avoidable disruptions to its business operations and shall be subject to a reasonable period of advance notice.

5.10 Customer's duties of cooperation

The Customer's duties of cooperation arising from the registration authority activity, particularly in connection with the identification of applicants, are set out in this agreement and the accompanying documents.

The Customer warrants that all necessary legal bases for data processing (consent, etc.) are applicable.

5.11 Duties to provide information and support

Both Parties shall inform each other in good time of non-contractually compliant incidents relating to data governance, data protection and information security.

The Parties undertake to provide each other with mutual assistance in complying with the applicable data protection requirements under this agreement as well as in the event of any official orders.

The Parties shall inform each other promptly in the event that they discover any personal data breach in relation to the provision of the contractual services. The Parties shall also report any such breach to the competent supervisory authority within 72 hours.

5.12 Rights of data subjects

The Parties undertake to honour and guarantee the rights of data subjects.

Specifically, a data subject shall have the right of access, the right of erasure, the right of rectification, the right to have a block placed on the data, and the right of data portability (Article 25 et seq. FADP and Article 12 et seq. GDPR).

If data cannot be erased due to legal or business obligations, access to the data shall be blocked. If the accuracy or inaccuracy of any data cannot be proven, they shall be flagged with a comment to the effect that their accuracy has been disputed.

The Parties undertake that, upon request by the data subject, they shall provide the data that the data subject furnished for processing in a commonly-used, machine-readable format.

If a data subject contacts SwissSign, SwissSign shall refer the data subject to the Customer and await its instructions. The Parties shall support each other to the extent agreed in handling requests by data subjects. SwissSign shall not bear any liability if there is no response by the Customer to the request made by the data subject, or if the Customer provides an incorrect response, or fails to provide a response within the time limit.

5.13 Data Protection Officer

SwissSign shall appoint a Data Protection Officer in writing insofar as this is required under the applicable data protection regulations. SwissSign's Data Protection Officer is:

General Counsel
SwissSign AG
Sägereistrasse 25
CH-8152 Glattbrugg
privacy@swisssign.com

The Customer shall be informed of any change in the identity of the Data Protection Officer and/or their contact details immediately and in writing.

5.14 Confidentiality

Both Parties shall be obliged to treat in confidence all information obtained in connection with the contractual relationship that concerns the business secrets and data security measures of the other Party, including after termination of the agreement. If there is any doubt as to whether any information is subject to a requirement of confidentiality, it shall be treated as confidential until a written release is provided by the other Party.

5.15 Duty of retention, erasure and return

Upon termination of this agreement, SwissSign shall deliver to the Customer, or destroy or securely erase in accordance with data protection law and in consultation with the Customer, all documents in its possession along with any results of processing or usage, or any personal or otherwise confidential data created or copied for the purposes of providing the services under the contract between the Parties, unless SwissSign is subject to a statutory or regulatory obligation to store the data. The erasure must be appropriately documented. Any statutory retention obligations or other obligations to store the data remain unaffected.

In order to comply with regulatory requirements (including ZertES, VZertES, CA/Browser Forum Baseline Requirements), any documents and evidence that are relevant for the approval of applications for certificates must be retained for eleven (11) years after expiration of the validity of the certificate. Within the context of its registration authority activity, the Customer undertakes to retain these documents and items of evidence for the prescribed period.

After the purpose has been fulfilled, and otherwise upon termination, expiry or notice to terminate this Agreement, the Customer shall retain all data for the prescribed statutory archival period in a manner compliant with applicable law, and if necessary provide them to SwissSign free of charge.

6. Approval in the context of MPKI

The power of representation of the RA Operators for the registration authority activity according to Section 3 includes in addition without any further specific review the authorisation of the registration and publication of all certificates for the specified organisation, which shall be identical to the entry in the Commercial Register or to the proof or organisation. The name of the organisation may then also be published in the publicly trusted certificate, if this is provided for in the certificate. The above is subject to the proviso that certain other entries in the publicly trusted certificate which do not concern the organisation (e.g. domains, names of individuals) may have to be authorised by the Customer.

Usage of all certificates issued under an MPKI after the commercial agreement with SwissSign or a SwissSign-Partner has ended shall not be permitted. All certificates that are still technically valid must be revoked by the Customer or, upon payment of a fee, by SwissSign.

If a SwissSign partner's contract is terminated, SwissSign shall be authorised to inform the MPKI Customers of the termination and, if so requested, to take the appropriate steps to ensure that the service can continue to be provided.

7. Approval and Declaration of Consent

The Customer hereby states its consent to the Guidelines on the Delegation of Registration Authority Activity and the Subscriber Terms and Conditions Certificate Services. It further acknowledges that SwissSign will issue certificates on the basis of the requests for certificates approved by it.

The Customer shall inform SwissSign in writing of any changes in the RA Operators by means of an amendment form.

8. Conclusion, term and termination of the agreement

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

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.

9. Signatures

The Customer's authorised signatories must sign in accordance with the Commercial Register or in the official proof of organisation.

By signing this document, the Customer confirms its purchase of the MPKI with the above-mentioned initial agreement term; it furthermore confirms that it has read, understood and accepted SwissSign's GTC, including the annexes that are relevant to this agreement.

The signatories confirm, that the RA Operators are authorized to the following duties:

- Changes to the current MPKI Setup
- Downgrade of the MPKI
- Adding/Removing of RA Operators

Authorised signatory 1

Place, date

Email address

Telephone number

Surname, first name, position, in block capitals

Signature

Authorised signatory 2

Place, date

Email address

Telephone number

Surname, first name, position, in block capitals

Signature

In addition to the signatures in this document, a copy of a valid identity document (ID, front and reverse side, passport), which must be dated and signed by the relevant person, must be attached for each signatory.
Submission by scanned copy is sufficient for the dated and signed copies of the identity documents.

Please note that without the copies of the identification documents, the MPKI cannot be set up, and that a re-validation must be carried out at certain intervals pursuant to regulatory requirements.

SwissSign

Checklist and instructions for sending the documents

- Are those signing the agreement authorised to sign and can this be corroborated by the Commercial Register extract? (Section 9)
- Have personally dated and signed copies of the identification documents (ID card, front and reverse sides, or passport) been attached for those signing the agreement? (Section 9)
  Submission by scanned copy is sufficient for the dated and signed copies of the identity documents.

- 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.

Information and comments

Ensure that the order is sent to SwissSign.

The review process can only be carried out if all the necessary documents are attached. Particular attention should be paid to the following points:

- a copy of the ID card or passport which has been dated and signed by the signatory must be attached for all signatories to this order
- only those persons listed as authorised signatories in the Commercial Register or official proof of organisation can sign this form under Section 9 “Signatures”

Unless the order is signed by those persons listed in the Commercial Register or proof of organisation, we shall contact your HR officers or the representatives of your organisation, as stated in the Commercial Register or proof of organisation, in order to verify authority to sign this agreement. Please factor in several additional days or weeks of processing time, depending upon the availability of the people who are to be contacted.

The domain check will be carried out using an automated SwissSign check procedure.

The procedures approved by the CAB Browser Forum are described, in each case, on the SwissSign support page accessible at: https://www.swisssign.com/support/mp-ki-setup.html.

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

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