Digital certificates

SwissSign, a data security specialist by Swiss Post

Managed Public Key Infrastructure (MPKI)
Automated certificate management to secure your IT infrastructure

New data connections between applications, apps and other devices are being created every day. These open up opportunities, but each new network also increases the potential risk. Cybercriminals exploit potential security vulnerabilities. The Managed Public Key Infrastructure from data security specialist SwissSign protects your applications with Swiss certificates for SSL and Secure eMail based on the strictest security standards. What's more, SwissSign-MPKI is a modern state-of-the-art solution for simple, 24/7 certificate management. All operations and data management are handled in Switzerland.

What is MPKI?

You can use a subscription model for the managed PKI from data security specialist SwissSign to obtain 24/7 access to unlimited Public Key Certificates for

- SSL and
- Secure eMail

At the same time, you benefit from attractive volume discounts for higher purchase volumes.

The benefits for you

- Guarantee privacy and data protection for your customers and partners.
- Encrypt and authenticate your e-mail traffic.
- Increase your customers' trust in your web application and demonstrate the authenticity of your web presence.
- Protect yourself from phishing and man-in-the-middle attacks.
- Benefit from better visibility in Google's rankings.
- SwissSign – swiss made software – Swiss quality

How MPKI works

You can manage certificates for your employees, customers and partners independently 24/7. You can instantly issue any type of certificate at any time via an automated interface or the web administration tool. And thanks to the ACME and openAPI interface standards, you can also perform complete auto-enrolment with partner products. The main functions at a glance:

- A clear web portal for managing MPKI
- Automated certificate lifecycle management (Rest API, ACME or CMC)
- Reports by certificate types, groups or expiration dates
- Electronic processing of contract documents

Trust levels

Select the trust level for your SSL certificates. As a certified Certificate Authority (CA), data security specialist SwissSign complies with well-established standards:

- **Domain Validation (DV):** For websites with simple security requirements (e.g. blogs, mail servers or similar)
- **Organization Validation (OV):** For companies that want to offer their customers a high level of protection (e.g. web stores or similar)
- **Extended Validation (EV):** For companies that want to demonstrate the highest trust level (e.g. banks, large web stores or similar)

E-mail certificates

You will also find a selection of e-mail certificates for authenticating, signing and encrypting e-mails:

- **E-Mail ID Silver (Personal):** Certificates for e-mail addresses. *(E-mail only; also called "Mailbox Validated")*
- **E-Mail ID Gold (Pro):** In addition to the e-mail address, the certificates also include the organization and the name (or pseudonym) of a person. *(For employees; also called "Sponsor Validated")*

The benefits of MPKI

- Data security specialist SwissSign is a Swiss Trust Service Provider (TSP) recognized by the Confederation.
- The data is held entirely in Switzerland – in accordance with the highest, annually audited security standards.
- Only Swiss law is applicable.
- Data security specialist SwissSign meets national and international standards and legal requirements.

Interfaces

In addition to manual issuance via a clear WebGUI, MPKI also supports modern protocols for the automated certificate lifecycle:

- ACME (Automatic Certificate Management Environment) is provided for issuing SSL certificates
- The REST API based on OpenAPI V3 allows automated management of e-mail and SSL certificates (including wildcard)
- Likewise, the CMC (Certificate Management over CMS) interface allows automation of the lifecycle for all certificates as per Internet RFC5272

For automation, data security specialist SwissSign provides a large partner network for certificate lifecycle management systems and e-mail gateway solutions.

Private Managed Public Key Infrastructure (MPKI)

Outsourcing of MPKI to the certified SwissSign environment

Operation of an internal Public Key Infrastructure (PKI) often results in high financial and personnel costs. The solution for this is cloud outsourcing of the internal, private PKI to the certified environment provided by data security specialist SwissSign (in combination with a partner application). This enables you to focus all your attention on your core business. Examples of a private MPKI are certificates for the Microsoft environment, Mobile Device Management (MDM) or the Internet of things (IoT). You can also benefit from the extensive SwissSign partner network when automating certificate management.

What is Private MPKI?

Within the Managed PKI, data security specialist SwissSign operates your Public Key Infrastructure (PKI) at your request as per your specifications and under your root certificate (Root CA).

The Private Managed PKI is aimed in particular at customers who need a cloud solution and want to benefit from the secure, certified SwissSign environment.

You define the scope and parameters according to your needs. In all cases, the service includes a customer-specific certificate hierarchy, i.e.

- an individual root certification authority (root CA),
- one or more issuing certification authorities (sub-CA) and
- the application-specific user or device certificates.

The benefits for you

- Maximum flexibility
- Low costs and reduced workload
- High level of security
- Certified, secure providers

The benefits of Private MPKI

- Data security specialist SwissSign is a Swiss Trust Service Provider (TSP) recognized by the Confederation.
- The data is held entirely in Switzerland – in accordance with the highest, annually audited security standards.
- Only Swiss law is applicable.
- Data security specialist SwissSign meets national and international standards and legal requirements.

How private MPKI works

Private Managed PKI is based on the same certified system that is used for issuing “public” SSL and e-mail certificates.

Thanks to standardized REST or CMC interfaces, powerful partner applications are available for auto-enrolment of certificates, for use in the mail gateway or in your encryption solution. Your certificates are automatically managed and installed on end devices.

Post CH Communication Ltd
Digital Health
Wankdorfallee 4
3030 Bern

E-mail digitalhealth@swisspost.ch
swisspost.ch/digital-health

Certificates as a Service (CaaS)
Automated certificate management to secure your IT infrastructure

The terms of digital certificates for the Internet are growing shorter, and the need to encrypt data streams is continuously increasing. Undetected expired certificates can jeopardize operational safety and result in legal consequences. These and other developments are significantly increasing the volumes of certificates to be managed, and processing them is becoming more complex and costly from a technical perspective. Without tool support, therefore, this issue is barely manageable anymore. The Certificates-as-a-Service (CaaS) solution from data security specialist SwissSign enables simple, secure and automated certificate management.

What is CaaS?

With the CaaS solution from data security specialist SwissSign, you can manage certificates of all types and use cases centrally and at any time. In addition, the entire administrative process can be mapped in one place. This ranges from monitoring, applying for and renewing certificates, to distributing them to the surrounding target systems. CaaS is scalable to meet any requirements and is therefore particularly suitable for small and medium-sized enterprises that want to focus fully on their core business without compromising on IT security. Simple onboarding means you're ready to go in just a few steps.

The benefits for you

- Coverage of the full certificate lifecycle
- Central and uniform management of all certificates
- High degree of automation, no more expired certificates
- No additional software required
- Cloud-based solution with attractive pricing

How CaaS works

CaaS is a cloud-based solution and combines the certificate management tool essendi xc with the Managed PKI from data security specialist SwissSign. Connectors make the link to the last mile and bring the certificates directly to your servers and target devices. Once set up, most processes run automatically. The solution includes the following certificate products:

SSL certificates

Select the trust level for your SSL certificates. As a certified Certificate Authority (CA), data security specialist SwissSign complies with well-established standards:

- Silver domain-validated (DV)
- Gold organization-validated (OV)
- Gold extended validation (EV)

E-mail certificates

You will also find a selection of e-mail certificates for authenticating, signing and encrypting e-mails:

- E-Mail ID Silver (Personal)
- E-Mail ID Gold (Pro)

Post CH Communication Ltd
Digital Health
Wankdorfallee 4
3030 Bern

E-mail digitalhealth@swisspost.ch
swisspost.ch/digital-health