Certificates simple - secure - automated

Automatic certificate management as a standardised managed cloud service

Less hassle with certificates, no more unnoticed expiring certificates

Since September 2020, SSL certificates may only be issued with a term of 12 months. A further reduction of the terms in the near future is on the horizon. Considering that recognised studies assume a workload of up to 6 hours for the change of a certificate, the necessary recurring exchange of the certificates increases this workload considerably and ties up the capacities of the system admins with routine tasks.

At the same time, new areas of application for certificates are emerging, e.g. end-to-end encryption of emails, cloud/containers, identities for digital signatures or devices. As a result, the number of certificates for digital identification, protection and encryption of data flows is continuously increasing. This increases the number of certificates to be managed and the certificate handling becomes technically more complex and costly.

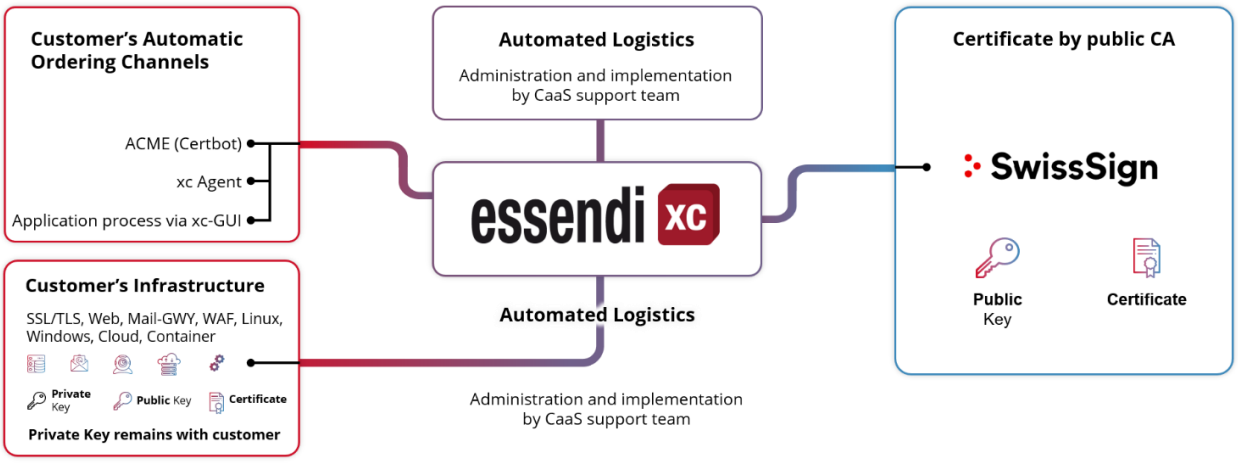
Undetected expired certificates endanger operational security, can have legal consequences and cause lasting damage to the company's image. But the entire administration process - from monitoring to applying for and renewing certificates to distributing them to the surrounding target systems - takes time and ties up valuable resources for IT admins. If different certificate authorities (CAs) are used, handling becomes even more difficult and the process costs increase.

Certificate management can hardly be mastered without tool support any more.

The solution: Certificates as a Service (CaaS)

Our CaaS solution combines the certificate management essendi xc with the Managed PKI from SwissSign. You can automatically request, manage, install and activate certificates in the target environments. Connectors create the connection to the last mile and bring the certificates directly to your servers and target environments where they are needed. Once set up, the processes run automatically.

Thanks to the simple onboarding, you are ready to go in just a few steps and can independently request, change and revoke certificates around the clock.



Certificate management with CaaS

The essendi xc management tool (CaaS edition) is used as a web application. Its dashboard provides an overview of all issued, active certificates and the various management functions. By means of a wizard, certificates can be requested with a few clicks on the basis of pre-configurated profiles. Connectors installed in your customer's system ensure automation of the certificate processes.

CaaS offers the following functions:

- Automated application processes via essendi xc self-service portal, system-guided certificate request, issue and download via wizard
- Full integration of the SwissSign MPKI
- Certificates of all types, domain-validated, organisation-validated, extended validation for SSL/TLS and S/MIME (secure e-mail) e-mail only or personal with organisation entry.
- Automated certificate management (generate CSR on target device, request certificate, issue, distribute, install, renew, revoke) for Windows and Linux systems
- Request and manage certificates via essendi xc agents (centrally controlled pull method)
- Request and manage certificates via essendi xc ACME connector as well as SCEP adapter (decentralised controlled pull method)
- Dashboard with management graphics, inventory list, inventory management
- Information, evaluations and reporting on the certificate portfolio
- Monitoring, alerting, logging, certificate expiry and life cycle
- Generation of keys, request and installation of certificates on target devices (Linux / Windows)
- Supply of further target appliances via activation scripts, if the necessary interfaces (e.g. REST) are available
- Execution of scripts for activation on the target system
- Providing Microsoft keystores on personal devices with S/MIME certificates for email signature and encryption end-to-end
- Supply MS keystore for Outlook 365 with S/MIME certificates for email signature and end-to-end encryption
- Supply MS keystore on servers with TLS/SSL certificates
- Supply Apache Tomcat web server (Linux) on servers with TLS/SSL certificates
- Providing IIS web servers with certificates
- (REST) interface for the automated application for certificates

Not included in the standard scope, can be implemented at extra cost

- Central generation and management of private keys using essendi xc and storage in a hardware security module (HSM)
- Connection of an internal private PKI (internal or aaS)
- Distribute wildcard certificates on more than one target device
- Issuing S/MIME certificates on iOS and Android mobile devices
- Issuing certificates for firewalls, virtualisation, VPN authentication, C/S authentication, load balancers, e.g. Citrix Netscaler
- Connection to SAP systems
- Key recovery for certificates NOT held in Windows keystores
- Automation of the annually required domain validation (DNS secret-based)

SwissSign certificates and services

The solution includes the purchase of all certificate products and services from SwissSign. Confirmation of the digital identity of persons, organisations, web servers, etc. with the common methods (domain validated / DV, organisation validated OV and extended validated / EV).

Internationally accredited CA based in Switzerland.

SSL certificates

Encryption of confidential data during transmission and authentication of the web server.

You protect your servers and websites and build trust among your customers.

Domain Validation

Organisation Validation

Extended Validation

E-mail certificates

E-mail communication with your customers and business partners can be given a trusted signature and encryption with all common e-mail programmes and mail gateways.

Domain Validation

Organisation Validation

SwissSign Managed PKI products are available for publicly trusted and private certificates.

MPKI Services are a good choice for customers who want to purchase more than a single certificate. The advantage over purchasing individual certificates is that validation is not required for each certificate and the certificates are available 24/7.

You also benefit from higher volume discounts when purchasing larger volumes.

MPKI

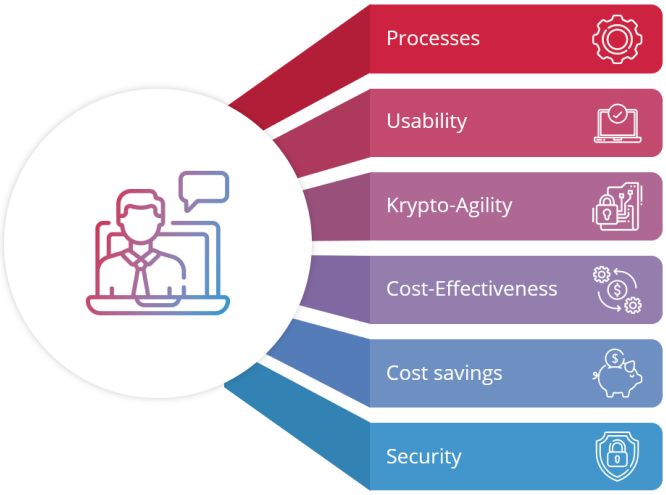
Private MPKI

Simple onboarding, operation and support

We accompany you during the pre-validation of the company for organisation-validated certificates and support you in setting up the local components (essendi xc Agent, essendi xc-ACME Adapter, xc-SCEP Adapter, etc.). After that, you can already issue certificates automatically around the clock. If there are any problems, the competent staff of our multilingual telephone hotline will help you.

We advise you on the selection of certificates provided by SwissSign. In addition, you will receive up-to-date information about changes in the certificate environment.

Certificate management with CaaS - the benefits at a glance



Once set up, the processes run automatically. Simple onboarding, ready-to-go in just a few steps. Certificates can be issued and distributed automatically and around the clock.

Easy handling and use of the application
Standardised and automated, little detailed knowledge of certificates required

Ability to act quickly, e.g. if certificate data changes or keys are compromised, "policy agility".

Fair subscription model "pay as you go" for the overall service (certificates, managed services, certificate management platform). Customised supply, no purchase of individual certificates, no hidden additional costs.

Out of the box use due to our cloud solution
Staff capacities for certificate handling and PKI/infrastructure are released for other tasks or do not have to be built up at all.

Increased security in IT operations through automation and automatic renewal of certificates. Alert and monitoring prevent unnoticed expiry of certificates. The private keys remain under your control.

CaaS Customer benefits

- Complete certificate life cycle

CaaS automatically covers the entire lifecycle of certificates and installs them fully automatically on the target systems. Certificates can be installed in many target environments (TLS/SSL, email, Linux, Windows, Cloud).

- One provider for all certificate products

With CaaS, certificates of all types and use cases are managed centrally and uniformly. You receive certificate management and certificate products from a single source. Contracts can be concluded for a term of several years, and the associated certificates renew automatically.

- Support from a single source

Functions and systems are provided as managed services. You receive the application, certificates and telephone support from a single source.

- Two strong, independent brands with long-term experience

Two independent specialists with years of experience are behind CaaS. They receive certificates from a long-standing Swiss trust service provider and certificate management from a German software engineering expert.

- Convenient and transparent billing

The all-inclusive price depends on the required certificate types. If required, you can issue certificates at any time during the contract period. The corresponding subsequent billing for additional consumption takes place transparently and conveniently at the end of the billing period. This gives you full flexibility and transparency. You simply pay by invoice, credit card payment is not mandatory.

- Local and trustworthy

The certificates in CaaS and the platform brought together enjoy a level of trust because they are "made" in Switzerland and the EU. The relevant European and Swiss laws (DSGVO, eIDAS, DSG, ZertES) apply equally to CaaS.

- Simple and secure

With our cloud solution, it is very easy for you to use: apart from the connectors in your systems, no additional software is necessary. This eliminates the need for additional maintenance work.

Thanks to fully automated certificate management, you never run the risk of certificates expiring again. The availability of certificates remains guaranteed at all times. Capacities for administration can be used for other tasks.

- Personal and available

Our multilingual hotline is available to you for support enquiries. You can reach our staff personally, directly and without time difference.

- Economical and reasonably priced

CaaS is a cloud-based solution with simple, transparent and attractive pricing. CaaS is therefore particularly interesting for small and medium-sized enterprises. The transparent subscription model is all-inclusive, with no hidden additional costs. The costs for commissioning are already amortised in the first year of use.

Strong, independent brands and their competencies

Trust in the years of experience of two independent specialists.

Certificates powered by

SwissSign

SwissSign has two cornerstones: Identity services under the brand SwissID and certificate services under the brand SwissSign. SwissID is Switzerland's digital identity, which enables simple and secure access to the online world. Thanks to electronic certificates, data can be exchanged in encrypted form and thus protected from unauthorised access. As a Swiss Trust Service Provider (TSP), SwissSign protects all data according to the highest security standards and keeps it in Switzerland.

Certificate management powered by

essendi

Our company looks back on over two decades of experience in the IT industry. Founded in 2000, essendi it initially focused on IT solutions in the financial sector. Since then, we have expanded our products and services to the industrial and commercial sectors and are now securely operating in various industries.

Our product **essendi xc certificate manager** is used by well-known customers.

We are happy to advise you

Do you have any further questions or would you like to request a non-binding offer? We look forward to hearing from you.

EU contact
essendi it GmbH
Dolanallee 19, DE-74523 Schwäbisch Hall
xc@essendi.de, , xc.essendi.it
Tel.: +49 791 943 07 011

International contact
essendi it AG
Bahnhofplatz 1, CH-6460 Altdorf
xc@essendi.ch, xc.essendi.it
Tel.: +41 41 874 27 30