

90 days certificate term.

Get ready with essendi xc.



Due to increasing digitalisation, companies are depending more and more on complex IT infrastructures. Therefore, the security of sensitive data and communication is becoming increasingly important. A central role in IT security is played by SSL/TLS/x.509 certificates, which are essential for **encryption during data transmission on the internet**. They form the backbone of secure data transmission on the internet. They enable the encryption of sensitive information. They ensure the protection of confidential data from unauthorised access.

Long-term certificates may be convenient, but they carry many risks. Therefore, **shortening the certificate term to 90 days is** an important step towards limiting damage caused by compromised keys or incorrectly issued certificates.

But requesting and exchanging a large number of certificates in the systems every 90 days is hardly manageable manually. The processes must therefore be automated. This is done using defined request processes that minimise the risk of incorrectly issued requests and increase the security of the systems.

In order to keep track of all certificates in dynamic IT environments, specialised tools are required that automate processes and thus save time and resources.

One of these tools is **essendi xc**. It not only enables **efficient management of digital certificates**, but also comprehensive automation of certificate processes, including **renewal, revalidation and installation in the target systems**. In this way, it contributes to security to a high degree.



The eight most important functionalities at a glance

1 Automatic renewal of certificates

Thanks to essendi xc, the expiry dates of certificates no longer have to be tracked manually. The tool takes over the monitoring and automatic renewal of certificates before they expire. This ensures that your websites and applications are always equipped with valid and secure certificates. xc thus minimises the risk of downtimes and disruptions in the IT infrastructure.

2 Central management and monitoring

With essendi xc you have a **central platform** from which you can overview all certificates in your company. The user-friendly interface makes it easy to enter and organise certificates and to centrally monitor the entire certificate inventory. Admins can use user groups to control who may request certificates with which characteristics. This minimises errors when requesting certificates.

3 Automatic configuration of certificates according to compliance requirements

The tool enables the configuration and procurement of certificates according to individual compliance requirements. **Key and certificate policies are documented** and adhered to. No matter which IT components are involved, essendi xc always applies for the correct certificate specifications. At the same time, it complies with the highest security standards, because **essendi and the development processes of the xc product family are certified according to DIN ISO 27001**.

4 Safety and security

For comprehensive protection, essendi xc uses the **latest encryption technologies** and ensures secure storage of private keys to prevent unauthorised access.

5 Scalability and integration

No matter whether you are a medium-sized company or a large corporation - essendi xc adapts to your individual requirements. The tool can be seamlessly **integrated into existing IT infrastructures** and supports various certificate providers and technologies. Additional products from the essendi xc family (e.g. essendi cd) extend the range of functions if required.

6 Reporting

With the comprehensive reporting functions of essendi xc, you always have an overview of your certificate inventory. All key handling processes are documented for audits. Thus, you fulfil your requirements of compliance guidelines and IT security standards such as **ISO 27001, German IT-Grundschutz (basic protection of the BSI) or NIST**.

7 CA independence

essendi xc supports the rapid change of CA or the switch to quantum-resistant encryption (post-quantum readiness) through **volume handling**, if required. It thus makes a valuable contribution to the **crypto-agility** of companies.

8 Secure storage of keys

The tool supports the secure storage of private keys. These remain on your **own systems** and are managed according to CI specifications. For an additional security level, the **connection of HSMs** (hardware security modules) from different manufacturers is also possible.

With essendi xc you can rest assured,
that your certificates are reliably managed and automatically renewed
and your IT infrastructure is protected in the best possible way.



A concrete date for the lifetime reduction of certificates has not yet been published. It is expected to come into force at the end of 2024. Use the time until that date to prepare yourself for the massive increase in administrative effort.

You are welcome to check out essendi xc in a live demo.