

# IoT Security: Digital Certificates to Protect Connected Devices

## How to make your IoT/OT landscapes more secure with the xc product family

### Rapid Growth

According to statista.com, the number of IoT devices will almost double from 2023 to **2030**, rising to around **29.5 billion devices**. This gigantic number and the rapid growth show that securing IoT devices is a key cyber security challenge.

In fact, the various devices are usually interconnected to form entire IoT systems. The more extensive the system, the more numerous the attack vectors and the more serious the consequences of a successful cyber attack. Once an attacker has managed to penetrate a network of IoT systems, he can **paralyse processes** or even **destroy components** and thus cause great damage.

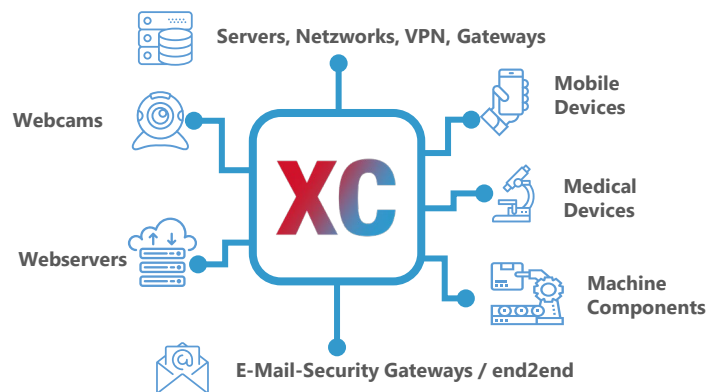
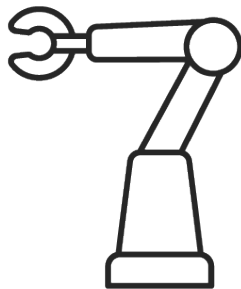
The targets of attack are diverse. While smart home devices were the main targets in the past, it is now mainly business systems that are of interest to cyber criminals.

### Danger for all Technical Equipment

In recent years, news about successful cyberattacks have increasingly been in the press. Besides e.g. automotive suppliers, even hospitals were among the victims.

**Vulnerable environments** may include

- Industrial facilities
- Shopfloor systems
- Manufacturing and production control
- Packaging machines
- Building technology and lift controls
- Alarm systems
- Robots
- Cash machines (ATMs)
- And many more



**Risks** arise especially when

- The communication between the components is not secured, i.e. the devices communicate unencrypted with each other
- Insecure keys and certificates are used for encryption
- Keys and certificates without expiry date are used
- Devices and equipment are not clearly identifiable.

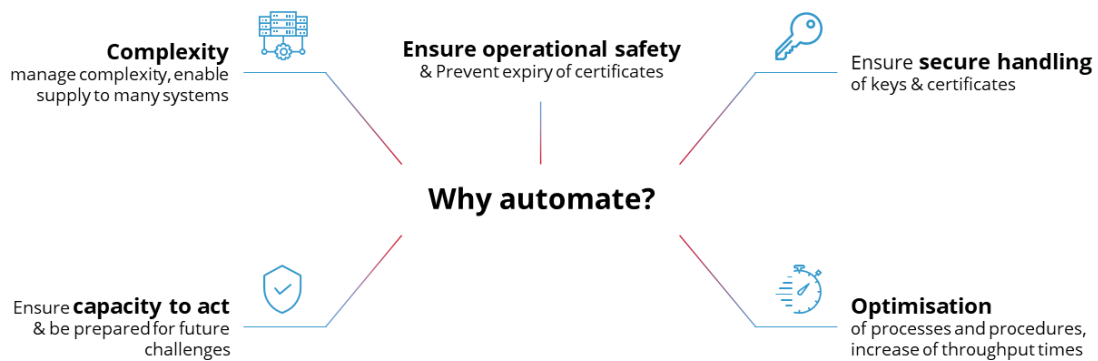
If cyber criminals have managed to hack into an insufficiently protected IoT device, they can take over the entire system from there. In this case, the threats are

- Data theft
- Data manipulation
- Failure of building technology (employees can no longer enter buildings, lifts no longer operate)
- Malfunction or shutdown of production and control systems

Restoring a secure and functioning network is time-consuming and expensive, so **delays in delivery** or even **loss of production** are to be expected.

Would you like to learn more or get to know the xc product family in a live demo? We will be happy to advise you.

To ensure the security of IoT/OT systems, there is a need for Action in various areas.



## Effective Protective Measures

It is important to recognise your own weaknesses. Only then can you take effective protective measures. A **comprehensive overview of the devices' status**, as well as their **monitoring and management**, is therefore necessary. That way, potential threats can be recognised in time and countermeasures can be taken.

This is especially crucial as in the course of **Industrial IoT (IIoT)** or **Industry 4.0**, the areas of operational technology and IT have an increasing number of contact points and are merging. Vulnerabilities are not only a threat to industrial companies, but also to KRITIS companies such as electricity and energy suppliers, water management, the food industry and even banks.

## Secure IoT-Landscapes

In addition to regularly installing security patches and updates, the following measures make **communication between IoT devices** more secure:

- Encrypted data traffic between all components (TLS/SSL)
- Management of the components' private keys by means of certificates
- Secure keys and certificates with regular expiry and renewal dates
- Inventory management for the devices
- A digital identity for every device
- Authorisation management for the devices
- Multifactor authentication
- Monitoring and surveillance to detect attacks at an early stage

## The essendi xc Product Family as a Bridge between IoT/OT and IT

Security measures require a great deal of effort from IT system administrators, which is impossible to manage manually given the large number and complexity of devices.

The essendi xc product family offers proven solutions to make IoT landscapes more secure and at the same time relieve IT administrators of routine tasks in the certificate area.

For example, **essendi cd** finds certificates of all types from a wide variety of sources throughout your data centre and can integrate them into the central repository of essendi xc.

**essendi xc** then takes over the management of the certificates throughout their entire life cycle. With essendi xc, all processes are fully automated:

- Request, issue and install certificates in the target system
- Alerting on upcoming certificate expirations
- Renew certificates if necessary
- All components and devices are uniquely identified

The key material is under central control. If required (and if the devices support it), keys can be generated directly on the IoT devices. Cryptographic operations - such as signing the CSR, etc. - are also possible.

The high degree of automation relieves the IT administrators or rather makes IoT security possible at all.

Would you like to learn more or get to know the xc product family in a live demo? We will be happy to advise you.

