PrimeKey

White paper

# Security for IIoT environments

**By PrimeKey Solutions AB**
Andreas Philipp, Business Development Director
Martin Oczko, VP Products

# Table of content

# 1 Abstract

Concepts like Industry 4.0 and Smart Factory are based on connecting "things" such as machines, sensors and vehicles. But the Industrial Internet of Things requires a comprehensive and simultaneously practicable security strategy where both OT (Operational Technology) systems and IT systems are covered. Otherwise, cyber criminals will have an easy time getting in. Mainstream tools such as a Public Key Infrastructure, code signing and new innovative solutions like the Secure Execution Environment have proven effective counter-measures.

# 2 Smart Factory and IIoT

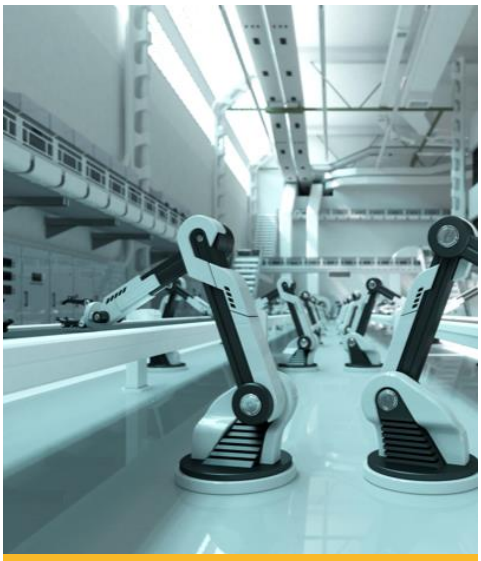
Traditional production processes are increasingly inching towards the direction of Smart Factory and Industry 4.0 [1]. One defining characteristic of these new working environments is the interconnectivity of machines, facilities and products with each other and their networking with established back-office systems, such as MES (Manufacturing Execution System), PLM (Product Lifecycle Management), warehousing software or ERP (Enterprise Resource Planning) solutions. Employees can get involved in this communication flow via mobile devices such as tablets, augmented reality and mixed reality peripherals.

The goal of a Smart Factory is to digitize the entire value chain, from product design down to manufacturing, sales and service. Through that, companies expect higher efficiency and speed as well as optimized logistics processes.

The Industrial Internet of Things (IIoT) plays a crucial role in the Smart Factory. It is the bridge between two worlds [2]:

- OT (Operational Technology) systems in production: These are, for example, sensors and embedded components in machines.
- IT systems: They are responsible for the management of product lifecycles, task management and connection to cloud services.

Compared to the Internet of Things (IoT), an IIoT infrastructure must meet additional requirements within the manufacturing environment. These include low delay times (latency), so that real-time processes can run smoothly, as well as high availability and reliability. Security also plays an important role. Internal or external attackers cannot be allowed to hack or manipulate any IIoT components. Otherwise, disruptions of manufacturing processes or data theft are inevitable.



Compared to the Internet of Things (IoT), an Industrial IoT infrastructure must meet additional requirements within the manufacturing environment. These include low delay times (latency), so that real-time processes can run smoothly, as well as high availability and reliability.

## 2.1 Market data on Smart Manufacturing and security

According to the Hamburg market research firm IoT Analytics, worldwide sales of solutions for Smart Manufacturing and Industry 4.0 will amount to 310 billion dollars in 2023[3]. The experts expect a wide range of applications to develop in the field of smart manufacturing. These would go beyond familiar approaches such as predictive maintenance and the development of digital products and services. Offers such as quality assurance or employee training as-a-service as well as the use of augmented reality solutions will then establish themselves.

This means that manufacturing companies will increasingly rely on the services of partners and at the same time be forced to expand their range of digital offerings themselves. However, this will only

work if the security of data and applications is guaranteed. This is all the more true as cloud-based IIoT platforms gain ground. They offer companies the opportunity to book the IIoT “as a service”. Leading manufacturing and automation companies have developed such IIoT cloud platforms, including Bosch, GE, IBM, Siemens (with MindSphere) and PTC.

Manufacturing in particular must be ensured that its data, applications and firmware are protected against manipulation and theft. Otherwise, there are severe risks, such as the loss of customers, the outflow of vital know-how to competitors or disruptions in the production process. It is therefore understandable that, according to a study by the consulting firm Bain & Company [4], around 45 percent of companies see security concerns as the greatest obstacle when it comes to implementing (I)IoT projects. For 30 percent, linking operating technology in manufacturing environments (OT) with IT represents the greatest challenge.

## 2.2 About centralized and decentralized architectures

In IIoT, decentralized infrastructures are currently establishing themselves, for example on the basis of edge computing or mesh networking. In Industry 4.0 environments and IIoT infrastructures, decentralized data processing is necessary solely because of the low latency. Since machines and processing centers have to react to changes within the span of seconds or milliseconds, if sensor data is first transmitted to a central computer center for evaluation, it simply costs too much time. However, ‘decentralized’ also takes on another meaning: Production processes for example, could be distributed among several stakeholders, like the maintenance of machines. That can be booked as a service by companies directly from the manufacturer. The latter then uses an IIoT infrastructure to access data from the customer's system, such as the status of their equipment or the degree of wear and tear of their components. This data can then be used for predictive maintenance of these machines.

*Gartner defines OT as hardware and software that detects or triggers changes by monitoring or controlling physical devices, processes and events in the company.*

## 2.3 Bridging IT and OT infrastructures

One development that affects the areas of the Internet of Things and Industrial Internet of Things (IIoT) is the move away from central IT and OT architectures. The consulting firm Gartner defines OT as hardware and software that detects or triggers changes by monitoring or controlling physical devices, processes and events in the company. Just like in everyday life, IIoT and OT focus increasingly on applications.

### 2.3.1 Example: Selling drill holes instead of drills [5]

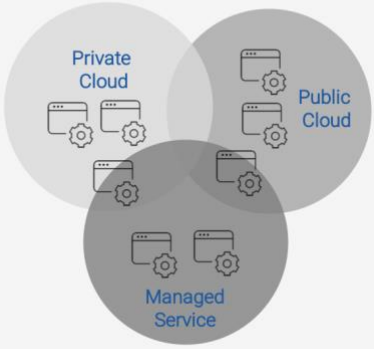
One example of how the Internet of Things is changing business models can be found at a well-known manufacturer of drills and hammer drills for construction site. Instead of offering its customers machines for upwards of a thousand euros, the manufacturer now instead sells drill holes: Customers can lease hammer drills and only pay for all the holes they actually drill with it. The supplier can check this number through an IoT application. The application also provides customers and the manufacturer with further information,

like the maintenance status of the drill and on which construction site it is being used.

Comparable models based on the as-a-service approach can now be found in many industries: A manufacturer of combine harvesters and farm equipment offers farmers “harvesting capacity by the hour”; a producer of machine tools offers its customers a guaranteed production capacity, which includes proactive system maintenance (predictive maintenance). That minimizes downtime and enables detailed billing based on machine uptime or the number of workpieces produced.

## 2.4 On-premises vs cloud/managed service deployment

How such applications reach the user is rapidly changing right now. Instead of an in-house data center, as cloud/managed services approaches are becoming more prominent; use of public clouds, private cloud environments or hybrid clouds and managed services is rising.




Use of public clouds, private cloud environments or hybrid clouds and managed services is rising.

Each approach has advantages and disadvantages when it comes to security. If a company makes applications available via its own servers, it can guarantee the highest level of security. The IT and OT departments then determine who and which IoT components have access to the applications. It is also easier to set up and implement security policies. If application development is handled internally, a company has maximum control over all stages of development and deployment processes.

In turn, the disadvantages are high costs for development and management of applications. Add to that the costs for the necessary IT infrastructure and specialized personnel. It is also difficult to open up this closed system for partners, customers and new service models.

### 2.4.1 Cloud/managed services deployment models

A cloud/managed service approach offers more flexibility. Depending on customer requirements and the own departments and partners, applications are rolled out via cloud or an enterprise data center.

One advantage is the high flexibility and scalability. If additional resources are needed, they can easily be ordered from a cloud service provider. This also applies to specialized services within the IIoT. As of now, industrial companies can order services and applications from providers of IIoT platforms. Depending on the provider, it is also possible to set up such a platform in one's own data center.

Another point is even more important: global cloud/managed infrastructure services enable industrial companies to provide digital services, such as predictive maintenance. Without IIoT and cloud platforms, models in which manufacturing systems located in other countries are connected to design centers or IT components in the company headquarters – offshore manufacturing – would not be possible.

However, this flexibility has its price. It makes application management a lot more complex. In general, users have to accept that a cloud/managed deployment of applications means a loss of control. This in turn increases the risk, for example, that unauthorized entities access an IIoT infrastructure. It is also more difficult to establish a uniform security level for all IIoT components that are involved in the design and manufacturing processes.

# 3 IIOT and security considerations

## 3.1 Attacks on data and machines

A study by the VDMA in 2018 on the subject of product piracy [6] indicates the importance of comprehensive protection of IIoT infrastructures. According to the study, 71 percent of German industrial engineering companies have been victims of product or brand piracy. The association estimates the damage at more than seven billion euros per year. In particular, counterfeit products sold on the Internet have become a problem.

More than 80 percent of the counterfeit products originate in China. This is for example problematic for German companies because the majority of German industrial companies have branches and production sites in China already. This means that it must be ensured that employees of service providers do not have access to data that they could misuse to make copies of original products.

*No longer is it just the reputation of the company that is at stake, but the entire value chain of the company.*

A second risk factor is direct attacks on control and monitoring systems of industrial plants and power stations (ICS, Industrial Control Systems). In 2018, the experts of the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) published more than 190 advisories that could be used to eliminate weak points in ICS systems [7]. Attacks on such systems are much easier to mount than they were in the past, since IoT and IIoT components are increasingly accessible from the outside. Appropriate security measures on the other hand are often not yet available or are inadequate. One can be certain that these attacks will increase drastically in the coming years.

The more companies focus their business models on as-a-service offerings and the trust they require, the more critical the impact of

successful cyber attacks becomes. No longer is it just the reputation of the company that is at stake, but the entire value chain of the company.

## 3.2 Public Key Infrastructure for secure IIoT usage

An essential aspect within the IIoT is the identification and authentication of different subcomponents. Starting with the so-called edge devices, gateway solutions and connected IoT platforms up to the back-office systems. The aim here is to establish a continuous chain of trust, as the only way to guarantee a reliable and trustworthy avenue for exchanging data. But in order for these advantages to materialize, an IIoT solution must first be

reliable. Which means users must be sure the IIoT systems will behave as intended and are safe from attacks and manipulation attempts – without restricting the reliability and availability of the application. That's achievable through two basic and established security technologies:

- a Public Key Infrastructure (PKI) in conjunction with
- Code Signing, a digital signature on the program's code, put in place by the manufacturer.

PKIs – as of today – are widely established and used in many areas of IT, server certificates for application servers, data servers, certificates for Smart Energy etc. They establish a bond of trust between the respective IT systems, in the case of Smart Energy, for example, between electricity meters and energy supply systems. The basis for this is the aforementioned certificates, which are generated individually for each device, and thus contain the device's identification data as well as providing it with an individual electronic signature. This prevents an attacker from imitating the identity of the device within the network. Without the use of these certificates, a cyber-criminal could, for example, plant a device in an IIoT infrastructure and have it infiltrate and hijack the IIoT network.

## 3.3 Protecting communication

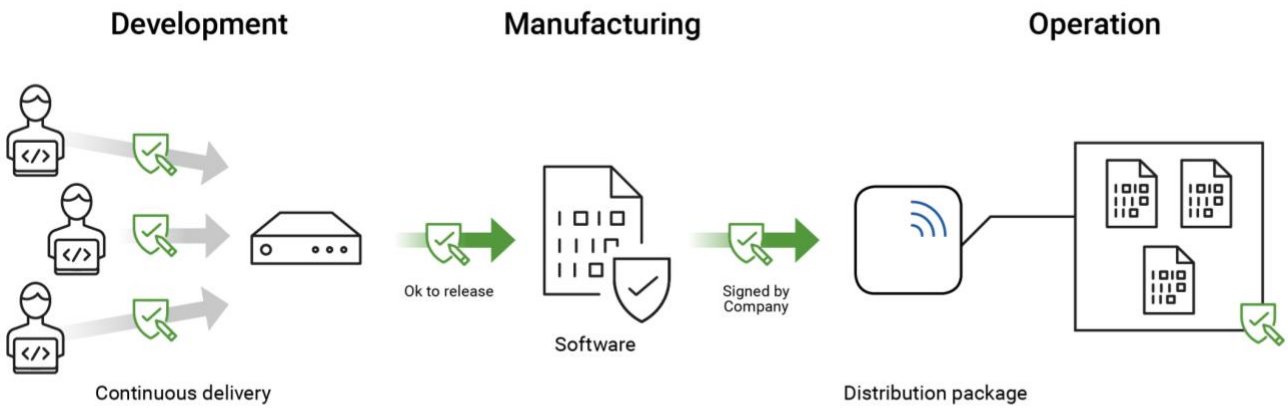
One of the characteristics of IIoT environments is that systems in different locations often need to communicate with each other. But this doesn’t always happen via secure network connections. Here, too, a PKI can be the solution by verifying the identity and integrity of the respective communication participants. In conjunction with transport protocols such as TLS (Transport Layer Security), this solution ensures a secure data exchange between IIoT components, gateways and IIoT platforms.

Secure communication in tandem with these authentications is especially critical, since mobile radio or wireless LAN frequencies are still commonly used in IIoT scenarios, like remote oil drilling facilities or wind farms. They transmit important status information and error messages via wireless communication networks but are much easier to tap into than wired industrial Ethernet infrastructures in a factory.

## 3.4 Securing software with code signing

In order to protect the software of IIoT systems from unauthorized access, different approaches are possible, for example with a dongle or an integrated security chip in the electronic circuits of the device. Another common tool is code signing. Here, the developer or provider puts signatures in the application software. That way, they ensure the integrity and authenticity of the application and protect both the software itself and their own copyright. For this purpose, the provider or manufacturer of the application requires a digital certificate with the corresponding cryptographic key. By using this private key as part of a digital signature, the program code of the application is then sealed. If the public key is then integrated within the code of IIoT components, the integrity and authenticity of the signed application software executed on the system can be verified at any time. If a software update is pending, the IIoT system can recognize from the signature of the update package whether

this new iteration actually comes from the provider or from a hacker impersonating them.




From the organizations' point of view, it is important that they can choose from multiple code signing solutions. PrimeKey offers software versions that can be implemented on premises, i.e. in the company's own data center. Alternatively, PrimeKey also offers the same software as a cloud version and a hardware supplement with integrated HSM. The organization can then decide which variant to use, or combine, depending on their individual protection requirements and application scenarios. For branch offices and contract manufacturers, for example, the hardware device would be the right choice. The on-premises solution, on the other hand, would be the right fit for the data center at the company headquarters.
A code signing solution should support all common signing methods. This includes MS Authenticode (for Windows code signing), JAR (for Java and Android code), CMS/PKCS#7 and Plain Signature.

Trust in IoT and IIoT environments rests on multiple pillars and PKI is one of the enables:

**Authentication of users**, devices and infrastructure components (e.g. gateways, routers, etc.), systems (data) and control devices (commands): This ensures that only authorized and trusted communication partners exchange information. Firstly, all participants must identify themselves. The system then checks whether the communication partner is actually the one in question or an instance that only pretends to be.

**Integrity**: Data and commands cannot not be easily manipulated or substituted.

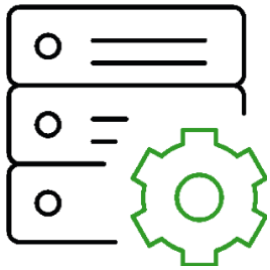
**Confidentiality**: Sensitive information must be protected from unauthorized access. This applies to data that is transmitted as well as persistent data. “Sensitive” in this context includes data for operating machines or data that is part of the production process.

**System security:** IoT or IIoT systems must be designed to prevent attackers from inserting malware or taking over individual components. Hijacked IoT systems (IoT bots), which hackers abuse for distributed denial of service attacks (DDoS), account for around 16 percent of all infected systems within the networks of cloud service providers. The Nokia Threat Intelligence Report 2019 [8] found that risk-free remote updates are only realistic if these attacks can be fully excluded.

**Certifications and compliance:** A PKI and its complementary solutions such as a secure execution hardware solution should fulfill the standards of relevant certificates such as the FIPS 140-2. Prospective customers should always check whether a provider takes the required compliance regulations into account. These include the Charter of Trust, an association of companies such as Allianz, Daimler, IBM, NXP, Siemens and Telekom, as well as the "Framework for Improving Critical Infrastructure Cybersecurity" of the American NIST (National Institute of Standards and Technology). Their framework aims to secure critical infrastructures such as power plants, critical industrial plants and utility providers.

# 4 The role of secure execution hardware

One problem in IIoT environments and connected manufacturing is their bigger attack surface. In addition to connecting the production site to the Internet, this is also due to the growing complexity of supply chains. Many companies work with an Original Design Manufacturer (ODM) or Electronic Manufacturing Services (EMS) provider from the country where their production is located. This means they have to be sure that such a service provider cannot manipulate or copy production and design data as well as process controls and machine programs of the customer.



In an IIoT environment, sensitive programs and information can be protected through secure execution hardware appliances when they are sent to or deployed in potentially unsafe locations.

An example: It would be disastrous if firmware updates or new application releases for products by the contracted manufacturer would contain malicious code or backdoors. Such discussions have arisen, for example, in connection with server boards and IIoT components built in the Far East [9]. And in certain regions, intellectual property protection isn't enforced as rigorously than in the EU or North America. There, intellectual property theft, for example in the form of production data, may be considered a trivial offence.

The code also offers attack angles for crypto operations – even if it runs in enclaves, the protected memory areas of processors. Researchers have successfully introduced malware into Intel's Software Guard Extensions (SGX), which are primarily used in cloud data centers. This attack is particularly dangerous because the malicious code is shielded by the enclave itself and can therefore no longer be removed, even by system administrators.

Solutions that execute applications and data in a secure environment – a so-called secure execution hardware – can correct that. It should be a priority that users, i.e. experts from industrial companies, can implement and operate such a solution without much effort –expert knowledge of cryptographic procedures and the management of keys and certificates should not be required.

## 4.1 Functionalities of secure execution hardware solutions

But what do secure execution hardware solutions do and how does it work? It is a standard x86-based server system. This hardware forms the basis for running a KVM (Kernel-based Virtual Machine), which is the foundation for application execution and the operating system environment. This makes it possible to back up existing applications and to run complex, multiple virtual machine environments.

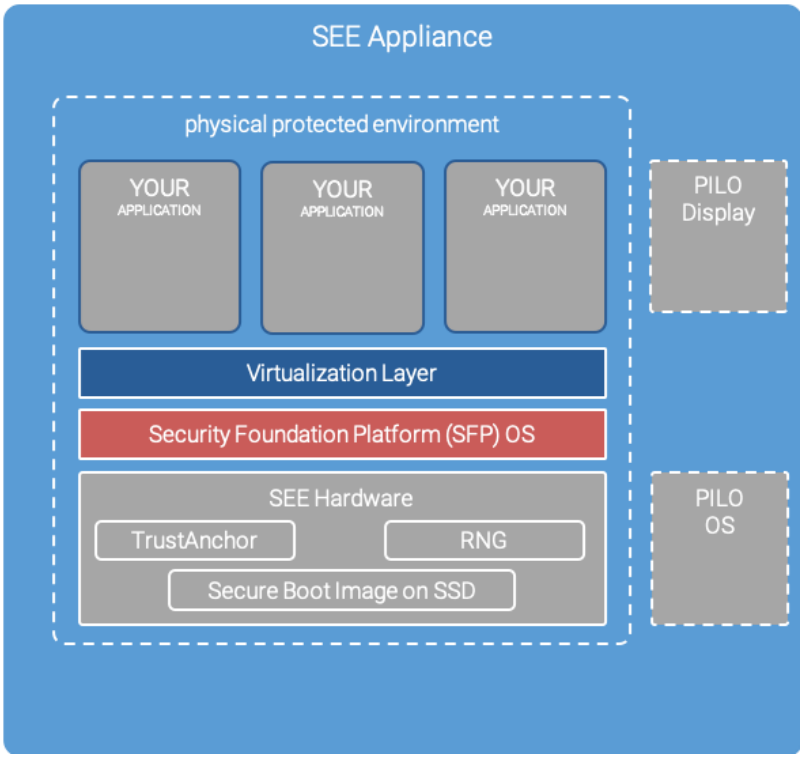
The security of the execution environment is ensured by using a so-called trust anchor in combination with the physical protection of the computer unit. The trust anchor ensures that:

- The integrity of the KVM and the user device is checked and ensured from the very start.
- A clear assignment of rights and roles for installation, configuration and runtime of the system is established.
- The server environment is only started after a successful integrity check.

In addition, the secure execution hardware consistently restricts the system's communication interfaces, so that only required interfaces are available during operation and all unnecessary interfaces (for example USB ports, which can be found and supported on servers but 99 percent of which are not used during operation) are switched off. This can be changed by the user, if needed.

Due to the physical structure of the system, a safety level up to a verified FIPS 140-2 Level 3 is applicable.

*The picture shows the architecture of PrimeKey's secure execution hardware.*




In an IIoT environment, sensitive programs and information can be protected through secure execution hardware appliances when they are sent to or deployed in potentially unsafe locations. Extracting or copying this data from the secure execution hardware server system is not possible for unauthorized personnel, whether they are humans or IIoT components. Even theft of the entire system is useless, since the attack does not reach the motherboard or the hard disks due to the physical protection measures of secure execution hardware. Only those who have authorized access can use the application and the data stored within it. This means no risk of loss or theft of data and knowledge as well as no problems with products whose firmware or applications have been tampered with in advance.

## 4.2 Selection criteria

There are several secure execution hardware solutions on the market. However, interested parties should ensure that the system meets the following criteria:

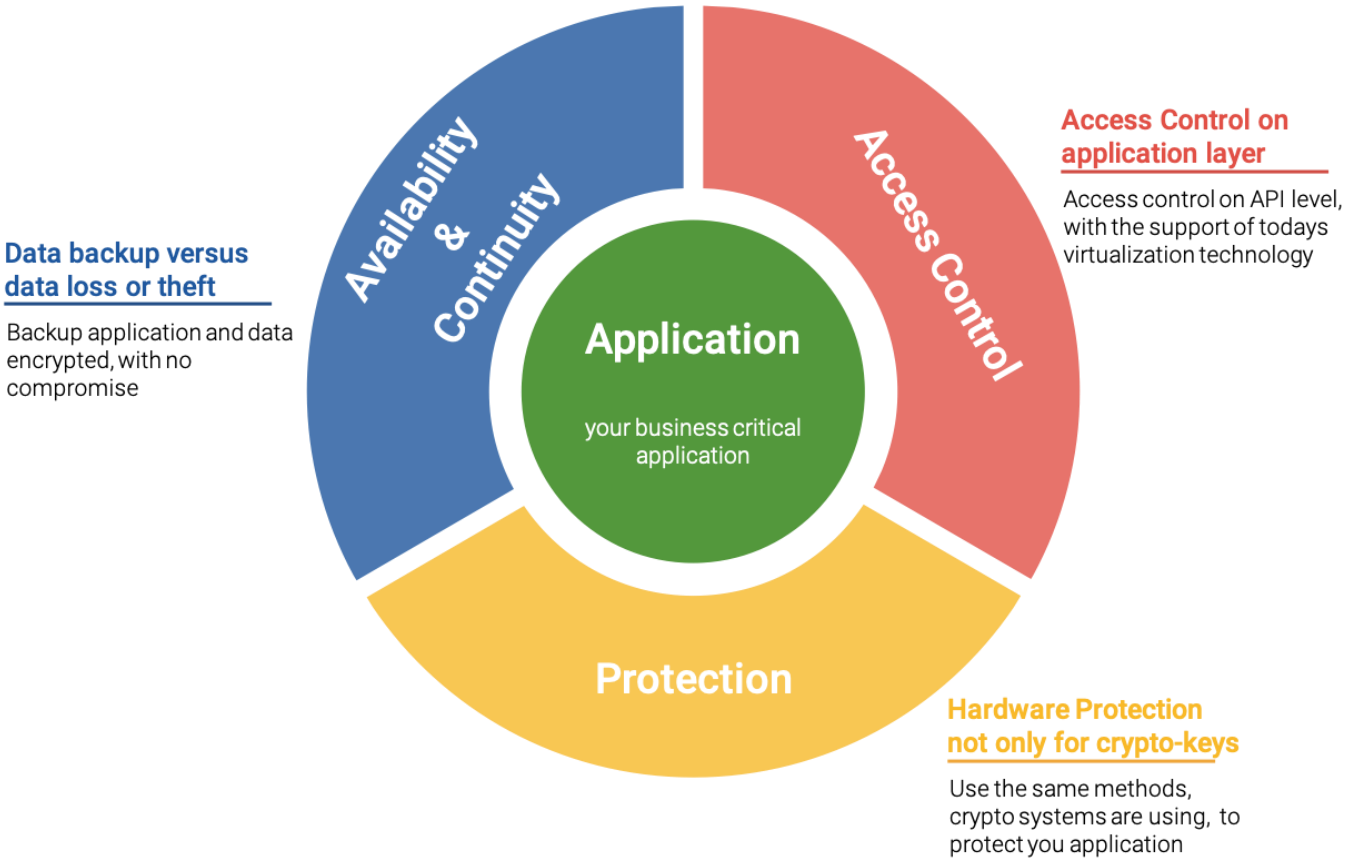
- A hardened housing that prevents tampering with hardware and software
- Security certifications, according to FIPS 140-2 Level 3
- A special protection of the boot process through a "Trust Anchor" (TA). This is an ARM processor that validates the boot images before the start and enables a reset (zeroization) of the image
- Support of FIPS-compatible encryption measures such as RSA, ECC, SHA-2
- Integrated hypervisor so that different system environments can be implemented
- Full control over the entire lifecycle of software and firmware including factory reset
- Access only via secure and limited interfaces, such as Ethernet and serial connections

## 4.3 Application-centric security strategy

What are the important building blocks?

The secure execution hardware can protect the entire life cycle of an application. This means that the user has full control over his software at all times, including protecting dormant data, such as data backups.
This makes the secure execution hardware a central component of the application-centric approach. The strategy consists of the following elements:

- hardware-based protection of applications
- availability and business continuity through encrypted backups
- application-level access control, including support for current virtualization techniques



## 4.4 PKI and secure execution hardware use cases

The following example from the automotive industry shows how a public key infrastructure can be used in conjunction with IIoT. The terminal device is a controller for an engine with injection technology. It is already common today for the vehicle electronics and control elements to receive software updates. This is done in the workshop. However, there are approaches to carry out such updates "over the air" via mobile connections. In this case, the driver receives a message from his workshop and has the update carried out. This way, they save the visit to the workshop and do not need a rental car.

The engine control is connected to an IIoT platform, which in turn is linked to a PKI. This ensures that the correct software update is installed on the car, preventing operating errors and manipulation attempts.

Another security layer is the signing of the program code. Code signing, for example using PrimeKey SignServer, ensures that only software authorized by the manufacturer and only the version intended for the corresponding vehicle model is installed.

## 4.5 Secure execution hardware in practice

The following example shows how a secure execution hardware can be used: A supplier from the automotive sector has infotainment systems manufactured by a contract manufacturer, for instance in China or Korea. This means that the manufacturer has

to keep part of the production software and applications on servers on site at the offshore plant. On the one hand, these servers are responsible for uploading current firmware versions to the components produced there. On the other hand, they use a PKI to ensure that each infotainment system has its own digital identity.

A secure execution hardware can be used to prevent unauthorized access to the servers running the production software. The programs then run in a "data safe" for which only the manufacturer has the key. Employees of the partner on site have no possibility to read, analyze or copy the applications. Manipulation of the firmware installed on the infotainment systems is also ruled out.

After completion of the order, the supplier can reset the software environment in the secure execution hardware and replace it with a new version. This will allow another line of infotainment system to be manufactured at the same plant, which will be installed in vehicles from another manufacturer.

Another example can be found in the safeguarding of supply chains such as the production of toys, household goods or industrial machines, as well as in software or application programming, product plagiarism as well as software and hardware piracy are a significant area of economic crime that causes major economic damage. In its 2018 study, the German Engineering Federation (VDMA) [6] estimated the annual damage caused by product piracy at around 7 billion euros in the mechanical engineering sector. How can this be prevented? Certificates in combination with a secure SEE environment are an effective means of establishing a chain of trust and defending against product piracy.

Everything starts with the creation of a so-called birth certificate in the production process of PLC modules. Today, there are three possible proceedings: Either the device has a security anchor in the form of a TPM or Secure Elements (SE). If the device has the appropriate computing power, the cryptographic keys and certificate requests can alternatively be generated within the software of the device. In the third variant, keys and certificate requests are generated within an external unit. The integration process is as follows: The cryptographic key pair is generated on the external unit or within the device (onboard). A certificate signing request is then created and sent to the PKI. There, the certificate is issued, if the identification of the applicant is positive. After the certificate has been returned and installed on the terminal device, it is securely integrated into the industrial ecosystem or included and activated within the PKI hierarchy. The solution must take into account that the certificate can be switched, depending on the change of owner or application area.

By issuing the certificate, the end device can now activate a wealth of security parameters. In the first step, the secure connection establishment is of note. This enables Message Queuing Telemetry Transport (MQTT) or Constrained Application Protocol (CoAP) via TLS [10], for example, and provides the basis for working with the OPC Unified Architecture Certificate Tool. Furthermore, it is now possible to roll out mechanisms such as code signing or license management on the basis of the provided certificates and the integration of the device identity within the certificate hierarchy. Signed software updates or license data can now be checked within the end device. In addition, the manufacturer and sender can be clearly identified. This way, supply chains are protected against product piracy.

# 5 Requirements for the PKI and secure execution hardware solutions

Easy to handle, transparent and flexible – these are the central requirements that PKI and secure execution hardware solutions must meet for an effective use in the IIoT.

- **Simple operation** is important because there is only limited expertise in the information technology sector, especially among OT staff. Here, PKI appliances have proven helpful. They combine encryption, hardware security modules, clustering functions and databases in one system. This means that users do not have to assemble an equivalent solution from various components of different providers.
- Open source software ensures **transparency.** This, for instance, allows a company's IT professionals to understand

which encryption or key exchange procedures a vendor uses and how they have implemented them. In addition, open source solutions can be extended more flexibly than closed, manufacturer-specific approaches.

- A further criterion is the **high flexibility** of the PKI and secure execution hardware solutions. This is especially true for the deployment models. A provider should therefore offer several options:
    - **On premises and private cloud:** The installation of the solutions in the client's own data center. Support for private cloud is important, as a considerable proportion of companies still prefer this approach. Its advantage is that the organization retains full control over the PKI and secure execution hardware. However, this requires a great deal of effort, for example in terms of specialist personnel and data center equipment.
    - **PKI and** secure execution hardware **appliances:** This is important in order to be able to implement such systems at remote locations or at a contract manufacturer. In addition, integrated systems of this kind greatly simplify handling: they can also be implemented by employees who do not have dedicated expertise in areas such as PKI, encryption and certificates.
- **Support for public and hybrid clouds:** Security solutions in IIoT are moving towards the cloud as well. This means that a provider of PKI and secure execution hardware solutions should support the leading public cloud services such as AWS and Microsoft Azure. The advantage of public clouds is their high scalability and the possibility of expanding the stock of IIoT security components as required. However, users should be careful not to become dependent on individual cloud providers – the so-called vendor lock-in. As a result, many companies are now relying on several clouds (multi-cloud environments).
- **Option: PKI as Managed Service:** Not all manufacturing companies have the means to implement and operate their own PKI solution for their IIoT environment. In this case, the vendors are responsible for setting up and operating the security solution, thereby relieving the on-site IT and OT department.

## 5.1 Code signing and scalability

Solutions that support code signing are also recommended. The technology prevents unwanted changes to applications and firmware in IIoT systems. With a solution like PrimeKey SignServer, organizations can implement all kinds of signed software on IIoT

components. PKI-based signatures in conjunction with hardware security modules and certificates ensure the authenticity and integrity of the transmitted code.

Particularly in IoT and IIoT environments, another factor has to be considered: the scalability of the security solution. Currently, many industrial IoT implementations are limited to field trials using hundreds or even thousands of devices. It is foreseeable, however, that these first attempts will quickly develop into use cases in which millions of IIoT components are integrated. A PKI solution must be equipped for such scenarios and needs to be able to scale accordingly.

# 6 Conclusion and outlook

In many ways, digital transformation is still in its early stages. In particular, manufacturing companies are not yet giving due importance to security in IIoT environments. As-a-service models, cloud computing and applications will continue to thrive – also and especially in the IIoT environment. This development will sharpen awareness in companies and public institutions where trust, data protection and security have become business-critical factors. Application-centric security strategies need to be developed and implemented using solutions such as PKI, code signing and secure execution hardware.

## 6.1 The quantum menace

One issue currently occupying IT security professionals is the threat quantum computers may pose to traditional encryption. Cryptographically relevant quantum computers particularly threaten asymmetric encryption methods such as RSA and ECDSA. Although nobody knows today if and when quantum computers can break conventional asymmetric encryption, encryption standards of IoT and IIoT systems are considered at risk in the future.

Researchers are already working on post-quantum cryptography (PQC), with new algorithms that are resistant against future quantum computer attacks. The American standardization body NIST [11], together with experts from several countries, is currently evaluating PQC algorithms for standardization. Since the end of January 2019, the second round of the selection procedure has been in progress. Of the original 70 proposals, around 25 are still in

the running. Standardized quantum-safe algorithms are expected to be available sometime between 2023 and 2025.

However, the good news is that solutions such as PrimeKey's secure execution hardware, PrimeKey SEE, and PKI are already equipped for the age of quantum computers. The key word is crypto-agility, meaning that PrimeKey SEE supports protocols and upgrade technologies that allow a rapid transition to quantum-safe algorithms. In development environments PrimeKey has already issued PKI certificates using several of the proposed post quantum cryptographic algorithm. IIoT terminals, hardware security modules and code signing appliances can therefore be upgraded and equipped with quantum-ready encryption methods when needed.

# 7 About PrimeKey

PrimeKey is one of the world's leading companies for PKI and digital signing solutions. With EJBCA Enterprise, SignServer Enterprise and the PrimeKey SEE, we deliver the capability to implement an enterprise grade PKI system ready to support solutions such as IoT, e-ID, e-Passports, authentication, digital signatures, code signing, digital identities, and validation; all solutions where digital certificates would be a main enabler. Choose to deploy your solution as flexible software, in a robust hardware appliance, in the cloud, or in a hybrid deployment adapted to your business needs.

PrimeKey products are used in all types of industries where IT security and integrity is a priority. Our products are Common Criteria and FIPS certified. We have numerous Webtrust/ETSI and eIDAS audited installations, and our internal processes are ISO 9001, 14001, and 27001 certified.
PrimeKey has offices in Stockholm, Sweden; San Mateo, USA; and Aachen, Germany. Together with our global network of technology and resell partners, we are proud to count many of the industry leading companies and institutions within IT, Telecom, Banking, Industrial, Public CAs, and different branches of Government as our longtime customers.

## 7.1 PrimeKey SEE

The secure execution hardware solution, PrimeKey SEE, is a full-size rack-mount application server that comes with a patented FIPS 140-2 level 3 protected execution environment for any operating system and application. It ensures that the server runtime environment at all times only can be accessed by an authorized security administrator, making it impossible to access, to extract or to modify by an unauthorized party. By doing so it opens up new

possibilities where you can run mission-critical applications in uncontrolled environments.

## 7.2 PrimeKey EJBCA Enterprise

EJBCA Enterprise is a multipurpose PKI software that supports multiple CAs and levels of CAs to enable you to build a complete infrastructure (or several) for multiple use cases within one instance of the software. Different use cases have different requirements on how registration, initial enrollment and life-cycle management should be performed. EJBCA Enterprise enables multiple integration and automation possibilities and issues certificates to individuals, infrastructure components and IoT devices. This software is flexible, scalable and secure and is installed at numerous ETSI/eIDAS-, WebTrust audited and ePassport reference customers. EJBCA Enterprise offers Certificate Authority, Registration Authority and Validation Authority (OCSP and CRL) functionality.

EJBCA Enterprise can be deployed as software, hardware appliance (PrimeKey PKI Appliance), in the cloud (PrimeKey EJBCA Cloud) or a combination of these.

## 7.3 PrimeKey SignServer Enterprise

SignServer Enterprise is a server-side digital signature software used to sign any digital document, code, time-stamping or travel documents. This software provides built-in modules for fully controlled cryptographic processing. Signing can be done large-scale, guaranteeing both availability and speed. Additionally, one or several Hardware Security Modules (HSMs) can be integrated to secure signature keys. SignServer Enterprise can be deployed as software, hardware appliance (PrimeKey PKI Appliance), in the cloud (PrimeKey EJBCA Cloud) or a combination of these.

# 8 References

[1] https://www.daimler.com/innovation/case/connectivity/industrie-4-0.html
[2] https://www.iosb.fraunhofer.de/servlet/is/80215/
[3] https://iot-analytics.com/industry-4-0-and-smart-manufacturing/
[4] https://www.forbes.com/sites/louiscolumbus/2018/12/13/2018-roundup-of-internet-of-things-forecasts-and-market-estimates/#608fd16f7d83
[5] https://www.hilti.de/content/hilti/E3/DE/de/services/tool-services/internet-of-things.html#nav/close
[6] https://www.one-identity-plus.com/wp-content/uploads/2018/07/VDMA-Studie-Produktpiraterie-2018_FINAL-english.pdf
[7] https://lp.skyboxsecurity.com/rs/440-MPQ-510/images/Skybox_Report_Vulnerability_and_Threat_Trends_2019.pdf
[8] https://pages.nokia.com/T003B6-Threat-Intelligence-Report-2019.html
[9] https://www.heise.de/security/meldung/Neue-Vorwuerfe-zu-Spionage-Implantaten-in-Supermicro-Boards-4186462.html
[10] https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/mqtt-and-coap-security-and-privacy-issues-in-iot-and-iiot-communication-protocols
[11] https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions