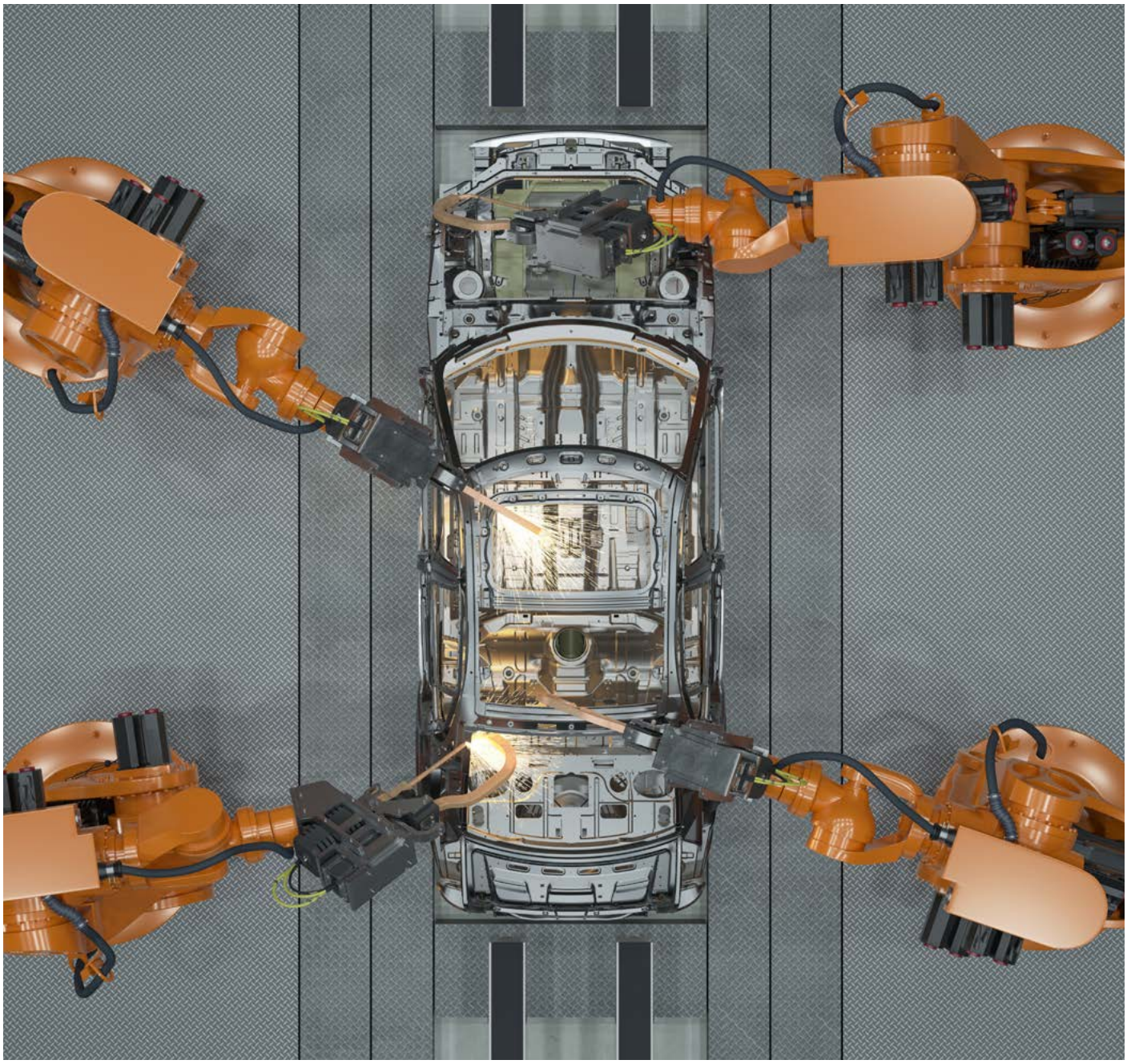
OTPaaS and ZTO – How PKI protects IT and OT

EVIDEN



Contents

1. Foreword

This white paper is a result of Eviden's Digital ID team participation to the roundtable "Securing data sharing in end-to-end industry (OT/IT): challenges and solutions" organized at SIDO IOT conference in Paris, December 2023. As our Digital ID team encountered a lot of interest and many questions arose, we decided to publish this document to a broader audience.

The focus is giving insights on our involvement in the "OT Platform as a Service" (OTPaaS) research project, which aims to ensure continuity between field data and IT data. A major building block within OTPaaS represents the "Zero Touch Onboarding" (ZTO) concept for the protection of IOT devices and the automatization of their lifecycle management, for which Eviden Digital ID has developed a combined software and hardware solution.

2. Introduction

IoT (Internet of Things) and OT (Operational Technology) cybersecurity risks can represent significant threats to companies, if not identified and analyzed in advance.

In IoT, the proliferation of connected devices increases vulnerabilities, potentially leading to unauthorized access and data breaches. Meanwhile, OT, which controls industrial processes, faces unique challenges with legacy systems often lacking robust security measures. Both realms are susceptible to malware, ransomware, and unauthorized control, jeopardizing critical infrastructure. The interconnectivity amplifies the impact, making it crucial to address vulnerabilities promptly, implement strong authentication, encryption, and regularly update systems to safeguard against evolving cyber threats in the rapidly advancing landscape of IoT and OT.

Given the fact that many companies dispose of limited resources and lack expertise, insufficient investment in robust security measures can make them vulnerable to phishing attacks, ransomware, and data breaches, third-party dependencies and supply chain vulnerabilities amplify risks.

Additionally, the evolving threat landscape and regulatory challenges pose significant obstacles for all companies striving to protect sensitive data, emphasizing the critical need for affordable and tailored cybersecurity solutions to safeguard their digital assets and maintain business continuity.

Three major risk categories can be identified, which are in particular:

- Data confidentiality:

It's important to take stock of the data available within the company and define its criticality. Data may be in the company's internal network or made available to customers or partners. Moreover, one has to define who needs access to what and set up access rights accordingly.

- Data theft and loss:

Every piece of company data has a value that could be consequent and jeopardize the business if it were to be stolen. The right level of security must be put in place for each piece of data to protect against industrial espionage, data theft and blackmailing, becoming increasingly popular amongst hackers.

- Mass attack on the company's computer network:

DOS/DDOS type (Denial-of-Service or Distributed Denial-of-Service) aim of damaging a company's reputation by making its service inaccessible and can lead to negative consequences on production and financial situation. This risk is increasingly present with the massive deployment of connected objects.

3. IT-OT Differences and Interdependencies

Information Technology (IT) and Operational Technology (OT) are distinct but interconnected domains. IT focuses on data processing, networking, and software, managing administrative tasks. In contrast, OT oversees industrial processes, controlling machinery and physical systems. While IT emphasizes confidentiality and data integrity, OT prioritizes reliability, safety, and real-time control in critical infrastructure.

Interdependencies arise as modern systems integrate IT and OT for streamlined operations. However, this convergence introduces cybersecurity challenges, as vulnerabilities in one domain may impact the other, emphasizing the need for comprehensive security strategies to protect both information systems and operational processes.

Also, one has to bear in mind, that the constraints of IT and OT environments are very different.

In IT, development cycles are relatively short. We are talking about software that is easy to develop and update. A new functionality or security update can be implemented rapidly and deployed on customer environments in just a few days.

In OT environments on the other hand, cycles are much longer. We are dealing here mainly with hardware, which has to be designed in the factory and maintained over several years. Updates are not easily deployable, and hardware upgrades are virtually out of question.

In this OT context, it is therefore very important to design product security right from the initial factory stage, what we call “security by design”.

Otherwise, adding security after this phase is neither effective nor necessarily feasible. Security and safety must be seen as an investment, not a cost, and must be built into the product right from the start. Experience in-the-field shows that failure to do so could cost 10 to 100 times more later on.

4. OTPaaS and ZTO – PKI technology as the security backbone

Device provisioning in manufacturing industries is a key challenge today, as manual processes are still applied everywhere in shipping control, commissioning, and domain registration and profiling. Therefore, research is ongoing to establish automated and intrinsic secure concepts that increase reliability of device management especially with respect to IT and OT deployments.

Public Key Infrastructure (PKI) is crucial for securing the Internet of Things (IoT) by providing a robust framework for authentication, encryption, and data integrity. As IoT devices proliferate, PKI ensures secure communication by issuing and managing digital certificates, enabling trusted interactions among devices, users, and servers.

This trust framework safeguards sensitive information, prevents unauthorized access, and mitigates the risk of data breaches. PKI's role in establishing a secure foundation for IoT ecosystems is paramount, fostering confidence in the integrity of interconnected devices and promoting the reliable exchange of data, essential for the seamless and safe operation of diverse IoT applications across various industries.

Within this context, OTPaaS a research project led by the French CEA (The French Atomic Energy and Alternative Energies Commission) has been launched with the global objective to design and develop a complete software stack to administrate and use "Cloud to IoT" infrastructures.

Eviden's Digital ID BU participates to the research group through contribution of our innovation team. Our objectives are essentially to provide a cybersecurity solution to securely deliver digital identities to OT through "Zero Touch Onboarding" approach.

OTPaaS offers various hardware and software security bricks that manufacturers can use in the IoT environment, such as Zero-Touch-Onboarding, which secures industrial equipment right from the design stage.

Figure 1 shows how device management can be conceived in the near future:

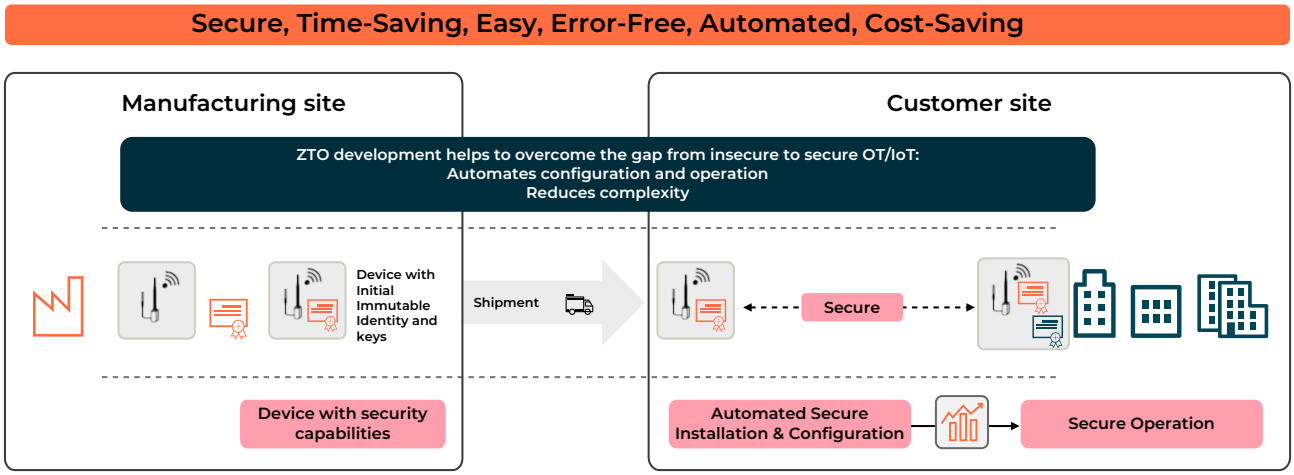
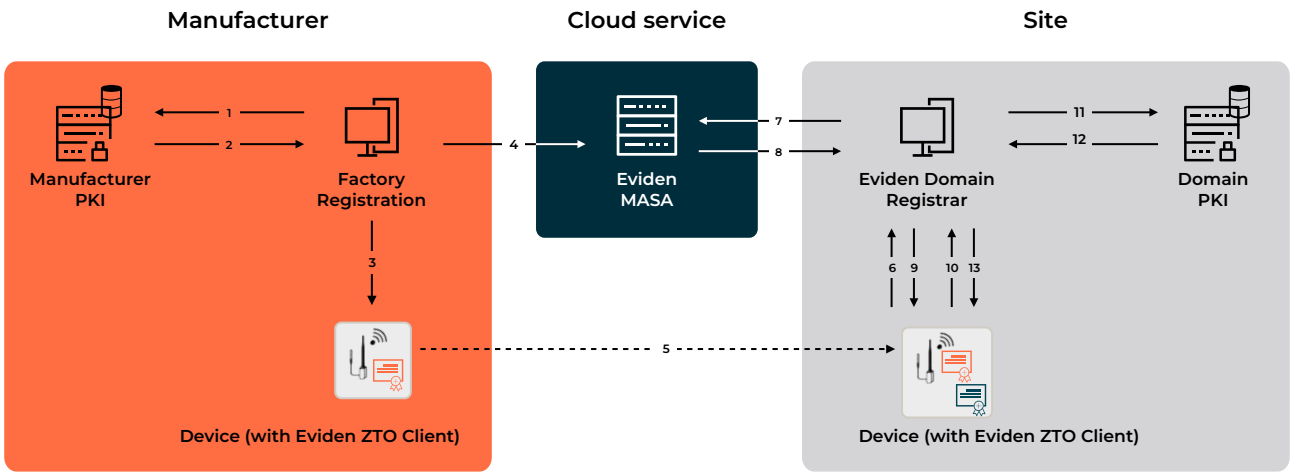


Figure 1 – Device Provisioning secured by ZTO

The Zero Touch Onboarding (ZTO) concept perfectly enables industries to manage securely device provisioning between manufacturing and customer site, by delivering digital identities to objects and managing their lifecycle. As a consequence, companies are able to connect without risk new industrial devices to their networks and automate their configuration and installation.

Figure 2 depicts the typical ZTO architecture:



By combining different cryptovison and IDnomic products from our Digital ID BU, such as secured cryptographic microSD token and PKI software, Eviden has set up a ZTO solution, consisting of following building blocks:

- Middleware applications
- MASA (Manufacturer Authorized Signing Authority) – a trusted authority to check that device comes from reliable, recognized manufacturers.
- Domain Registrar – which operates as a local entity allowing the device to retrieve a certificate in an automatic and secure way.
- Domain PKI to issue to device digital certificates and ensure full compliancy with IETF standards, such as RFC 8995, RFC 7030.
- Provision of electronic certificates used for firmware code signing via a signature application.

From a security point of view, it's vital to secure the entire chain, from equipment production to deployment and updating.

As part of the OTPaaS project, the ZTO (Zero-Touch-Onboarding) solution makes it possible to integrate security into industrial equipment right from the design phase in the factory, and to automate the deployment of this equipment in the target customer product site, removing all manual intervention which is a source of errors and security problems, and all in a totally secure way.

5. How to move forward concretely?

As the very first item, one has to establish a risk analysis, identifying real and potential threats and their possible consequences.

In conjunction with the risk analysis, a clear security policy based on the company's operational objectives and needs has to be defined. You also need to give value to your data, products and services. Not all elements have the same sensitivity and require the same level of security.

It is therefore of utmost importance to define and implement a security policy, based on an objective assessment of company's sensitive data and processes and adapted to its working and business environment. The security policy for instance will indicate which elements will need to be equipped with trusted digital identities and how.

To implement a security policy, you also need to base it on standards. They ensure that the world's leading experts agree on a solution that meets the highest security standards. Relying on standards is also the assurance that information exchange between companies or between equipment will be possible and secured in a uniform way and with the same level of security.

Several standards and frameworks have emerged in the recent years, such as the European Cyber Resilience Act, the EU Directive NIS2, and the IEC 62443 standard.

A major breakthrough represents the EU Cyber Resilience Act, which introduces mandatory cybersecurity requirements for hardware and software products.

This Regulation, announced in the 2020 EU Cybersecurity Strategy, will guarantee harmonized rules for products or software with digital components, a framework of cybersecurity requirements governing the planning, design, development and maintenance of such products, and an obligation to provide duty of care for the entire lifecycle. Moreover, security updates have to be made available for at least five years. The Regulation will apply to all products connected directly or indirectly to another device or network and is expected to enter into force in early 2024. Manufacturers will have to apply the rules 36 months after their entry into force.

The Cyber Resilience Act completes the NIS2 Directive, which in essence aims to achieve the following goals:

- Require national governments to pay due attention to cybersecurity.
- Strengthen European cooperation among cybersecurity authorities.
- Require the main operators in key industries of our society to take security measures and report incidents.

The NIS2 Directive (an EU directive is a process that needs to be transposed into national law) has a strong impact on network infrastructure and will de facto enforce security-by-design as a global development concept.

On the industry side, IEC 62443 sets the reference as international standard for industrial cybersecurity, providing guidelines to assess, mitigate, and manage cybersecurity risks in industrial automation and control systems, enhancing the resilience of critical infrastructure.

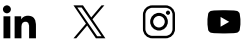
IEC 62443 describes the rules for component manufacturers, system integrators and operators. Component manufacturers for example must ensure the safety of products, whose safe interaction must be taken into account by machine and plant manufacturers. Operators on the other side are ultimately responsible for safe procedures.

“When it comes to defining and implementing corporate security, services, products and business, it’s essential to rely on cybersecurity specialists like Eviden, whose core business it is. Security is not something you can invent or develop yourself.”

Sebastien Defrance, Senior R&D Engineer, IT Security specialist at Eviden

For more information, please visit:
https://eviden.com/solutions/digital-security/digital-identity/
https://www.cryptovision.com/en/solutions/iot-and-industry/ot-security

Connect with us



eviden.com