EVIDEN

Zero Touch Onboarding

Automated and Secure Digital Identities for OT Systems

Operational Technology (OT): Threatened by Cyberattacks

Operational Technology (OT) controls industrial processes in critical sectors such as energy, manufacturing, transportation, water treatment, and utilities. From power grids to water supply systems, systems of this kind are integral to national security.

Many OT systems are not equipped to handle the current threat landscape. Initially designed with limited cybersecurity features, these environments prioritized functionality and uptime over security. The lack of cybersecurity in legacy systems makes them easy targets for cyberattacks, and the trend towards increasingly connected systems and convergence with IT has resulted in a larger attack surface.

OT Attacks: Present and Future

74%

Proportion of OT attacks

with commercial background

+9900%

Growth rate

of OT attacks between 2022 and 2027

15,000

Industrial shutdowns

caused by OT attacks expected for 2027

In recent years, cyberattacks have caused widespread outages at automobile manufacturing plants, tire factories, a leading food company, and a publishing giant. Additional OT security breaches have led to severe flight delays affecting tens of thousands of passengers, production halts in metals and mining, equipment fires and damage, as well as malfunctions in cargo containers and fuel supply systems.

Eviden predicts continuing growth of direct and indirect OT attacks, a problem made worse by the shortage of well-qualified and experienced OT security specialists.

Figure 1: OT attacks are a major challenge for the years to come. Sources: Gartner[1], SecurityIntelligence[2]

[1] https://www.forescout.com/gartner-market-guide-for-operational-technology-ot-cybersecurity
[2] https://securityintelligence.com/news/high-impact-attacks-on-critical-infrastructure-climb-140

Digital Identities: The Key to the Solution

Improving the security of OT systems is not just a voluntary concern but a regulatory requirement. Security standards, such as IEC 62443, provide a comprehensive framework for securing industrial control systems, with a strong focus on risk management and lifecycle security. Additionally, the NIS2 Directive imposes cybersecurity obligations on operators of essential services in critical sectors, mandating robust risk management, incident reporting, and security measures. NIS2 will lead to including more sectors and extending obligations already part of national law such as KRITIS (Germany) or OIV/SIIV (France). The EU Cyber Resilience Act (CRA) by the EU aims to further enhance cybersecurity for connected devices, including OT systems, by enforcing stricter security standards.

At the core of all OT security are secure digital identities.

By ensuring that every device or module in an OT system operates with a secure identity, devices can interact with one another safely: encrypted communications, passwordless mutual-authentication, data integrity. Each identity takes the form of a digital certificate and is anchored by a public/private keypair and follows a lifecycle that begins with onboarding and ends with decommissioning. Establishing secure digital identities forms the foundation for secure and efficient device management in OT environments.

Current Challenges in OT Digital Identity Management

Executives recognize the value of secure digital identities and are demanding adoption across OT environments. However, this is creating a headache for operational teams. Shipping control, record-keeping in commissioning tools, and domain registration and profiling are usually still performed by hand. On top, secure deployment and renewal processes are not always well known or implemented. When a digital certificate expires (after its validity period which is typically set at 2 years), it can lead to serious service outages, because of authentication failures. Without automation of certificate renewal, operators will have to manually renew the digital identity for each device. The limited remote access available in many OT systems further complicates these processes leading to operators having to physically travel to the system and connect it to an engineering workstation to perform the renewal.

Executives recognize the value of secure digital identities, but operational teams face significant challenges due to manual processes, limited remote access, and the risks of expired certificates causing service outages.

Zero Touch Onboarding – A Quick Introduction

Zero Touch Onboarding (ZTO) automates identity management in OT environments and is an approach that relies on standardized technology. It enables the simple and secure integration of new devices – represented by their unique digital identities – into an OT network without requiring direct human involvement. The ZTO process begins with the device manufacturer and ensures a smooth transition to the operator's environment through standardized protocols.

There are several ZTO standards: BRSKI (Bootstrapping Remote Secure Key Infrastructure) and FDO (FIDO Device Onboarding), which automate the initial authentication and key establishment for devices, as well as EST (Enrollment over Secure Transport) for secure device registration with a certification authority. However, many IoT devices currently lack compatibility with these standards, making them not yet ZTO-ready. Loading the Eviden ZTO Client on the device is the easiest path to making devices ZTO-ready.

ZTO drastically reduces the workload for operators and gives manufacturers a competitive edge by offering secure, ZTO-based solutions that enhance customer loyalty.

ZTO offers clear benefits for both operators and manufacturers. For operators, it drastically reduces the workload of operating secure device identities, while manufacturers gain a competitive edge in a market increasingly demanding secure, ZTO-based solutions. By supporting ZTO, manufacturers not only make their products more attractive to customers but also strengthen customer loyalty.

ZTO Compared with Manual Onboarding

The ZTO process automates steps currently done manually (Figure 2). Starting at the manufacturer where a component is assigned a manufacturer identity in the form of a digital certificate from the manufacturer's PKI. This temporary identity is later used at the customer's site to authenticate the device and generate a local identity and certificate. Once the onboarding process is completed, the device can securely communicate with other domain elements and autonomously renew its certificate before expiration, ensuring ongoing security.

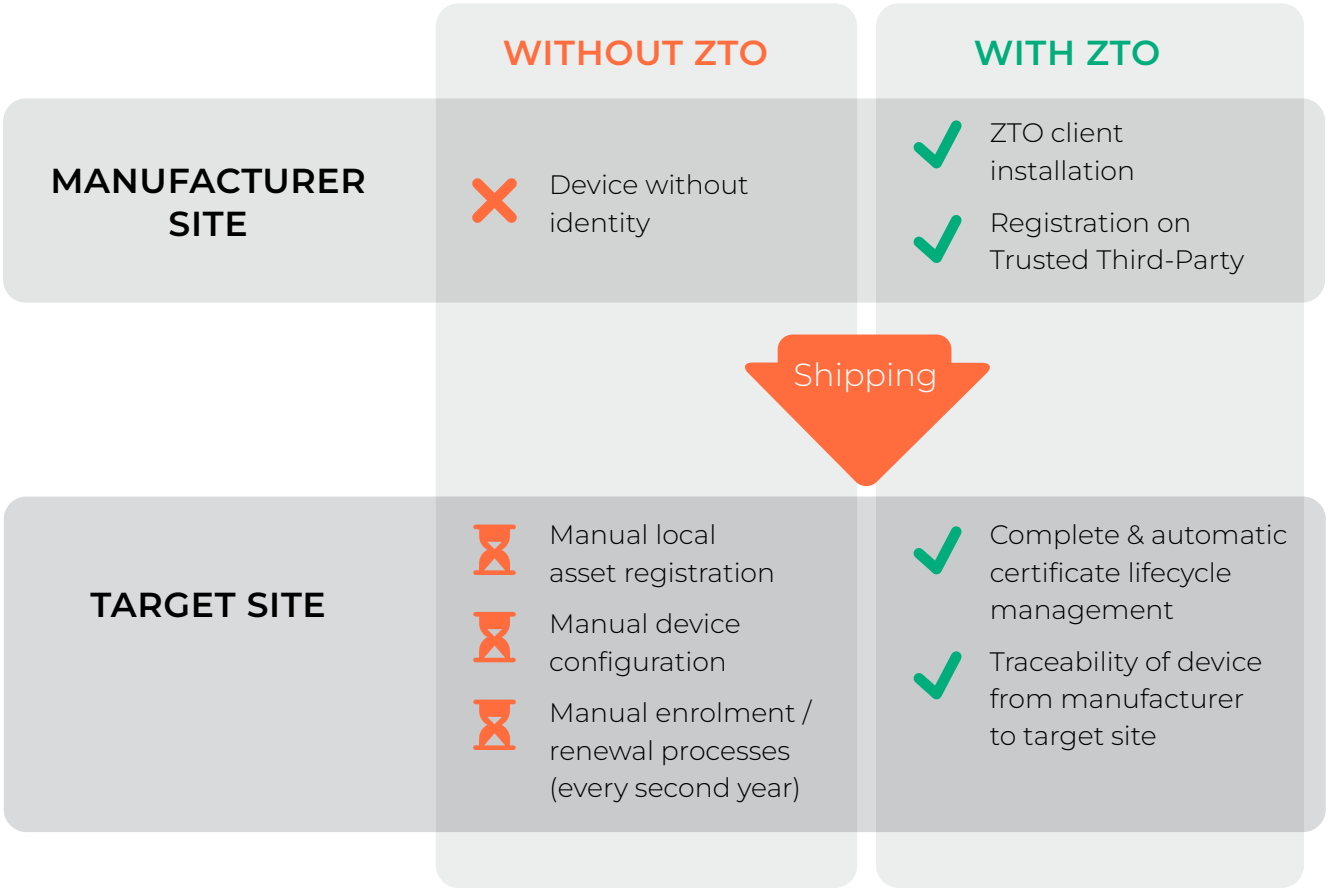

Figure 2: Device workflow from the manufacturer to the target site

Eviden Digital Identity Offering

Eviden offers a comprehensive suite of products and services for ZTO, including the Eviden ZTO Client, Eviden MASA (Manufacturer Authorized Signing Authority), and Eviden Domain Registrar. These components are fully compatible with any X.509-compliant PKI.

For those seeking turnkey solutions, Eviden offers the IDnomic PKI, a platform for creating custom PKI systems.

With over two decades of expertise and a proven track record of deploying numerous large-scale PKI systems, IDnomic PKI is a mature, secure and reliable solution.

These ZTO solutions are backed by Eviden‘s expertise in consulting. We support both operators and system integrators in deploying our solutions.

Contact us

Eviden encourages all operators managing large-scale OT deployments to explore the full potential of ZTO solutions. We invite device manufacturers to integrate our ZTO technology into their products and recommend that system integrators familiarize themselves with our offerings.

Let’s discuss how we can help streamline processes, reduce costs, and enhance overall system performance. We are happy to provide a demo – please don’t hesitate to contact us at:

cv-info@eviden.com

www.cryptovision.com

Our advisory team will be happy to get in touch with you.

cv cryptovision GmbH
Munscheidstr. 14
45886 Gelsenkirchen
Germany
Tel: +49 (0) 2 09 / 1 67 – 24 50
Fax: +49 (0) 2 09 / 1 67 – 24 61

About Eviden[1]

Eviden is a next-gen technology leader in data-driven, trusted and sustainable digital transformation with a strong portfolio of patented technologies. With worldwide leading positions in advanced computing, security, AI, cloud and digital platforms, it provides deep expertise for all industries in more than 47 countries. Bringing together 53,000 world-class talents, Eviden expands the possibilities of data and technology across the digital continuum, now and for generations to come. Eviden is a company with an annual revenue of c. € 5 billion.

1 Eviden business is operated through the following brands: AppCentrica, ATHEA, Cloudamize, Cloudreach, Cryptovision, DataSentics, Edifixio, Energy4U, Engage ESM, Evidian, Forensik, IDEAL GRP, In Fidem, Ipsotek, Maven Wave, Profit4SF, SEC Consult, Visual BI, Worldgrid, X-Perion. Eviden is a registered trademark. © Eviden SAS, 2025.

Connect with us

eviden.com