Securing the Industrial IoT Market

ABIresearch THE TECH INTELLIGENCE EXPERTS

GlobalSign by GMO

Michela Menting, *Research Director, ABI Research*

TABLE OF CONTENTS

INTRODUCTION

The industrial market is undergoing a transformation using new technologies such as Artificial Intelligence (AI), digital twins, and robotics. The foundation of this evolution is connectivity where legacy siloed and airgapped networks are becoming internet connected exposing a broad industrial device ecosystem. Industry 4.0 and the industrial Internet are terms describing industry transformation with new technology investment expected to grow from **US$41 billion in 2022 to nearly US$200 billion by 2030.**

But greater Internet accessibility to the critical machines powering industry means that security is a top concern to both limit data loss and prevent operational disruptions. **By 2030, connected machines and production systems within factories will exceed 1.2 billion.**

The security challenge in the industrial market is the high degree of device heterogeneity, which varies in form, function, and intelligence across

markets, each with very different operational processes and production requirements. Legacy infrastructure is part of the security challenge, as it was not designed for modern security tools. But legacy infrastructure also presents an opportunity because digitizing these assets uses the latest processor and connectivity hardware. In both cases, new network approaches for Internet accessibility of both legacy and new devices are needed to secure the burgeoning Industrial Internet of Things (IIoT).

Securing the industrial Internet starts with providing identities to myriad industrial devices. With unique identities, operators can build security policies starting with authentication and access control, and then extend to monitoring, threat detection, and lifecycle management.

This whitepaper sets out the key drivers creating a more Internet-connected industrial market. It identifies the primary Internet networking approaches expected for industrial settings and lays out primary connectivity needs in the top industrial markets. It concludes by recommending Public Key Infrastructure (PKI) as a critical technology for securing the industrial Internet and its benefits for industrial organizations.

INDUSTRIAL INTERNET

INDUSTRIAL INTERNET DRIVERS

There are many reasons why the industrial market is becoming more connected, not only due to advancements and availability of technology, but also due to competitive and macroeconomic trends.

Innovation, Standards, and Supplier Expansion: To meet the vision of Industry 4.0 requires re-inventing who gets to play in the industrial Information Technology (IT) domain, and reimagining the role of technology. One way to do this is to de-silo the communication architectures. Traditional communication architectures use fieldbus and industrial Ethernet protocols. These protocols were originally proprietary, often proprietary to the controller equipment manufacturers. While many of these protocols have become standardized, it is easier for customers to maintain use of the same manufacturer's equipment to avoid interoperability issues and leverage internal knowledge on equipment programming.

One major innovation is the Time Sensitive Networking (TSN) standard. It is designed for industrial Ethernet communications, typically between Programmable Logic Controllers (PLCs) and even between PLCs and smaller equipment controllers. This standard enables greater interconnectivity between other Ethernet-connected industrial equipment, with the benefit of enabling more competition in the controller market. TSN is also the protocol incorporated into 5G networking standards, known as 3GPP Release 16, for communications in 5G private networks.

Industrial Process Efficiency, Uptime, and Maintenance: Trade wars, pandemics, and now supply chain disruption are causing a decoupling of the traditional logistics activities for building products. All these variables are driving more Internet of Things (IoT) connectivity into the operations of industrial companies to improve their industrial efficiency and uptime. More capabilities to monitor production equipment using IoT applications provide industrial operators three benefits:

1) **Preferred Supplier:** As enterprises diversify their supply chains, they will seek out manufacturers that can meet their needs for delivery and product quality. One crucial element of proving strong uptime and product quality is the extent to which IoT applications play a role in improving your operations and limiting downtime.

2) **Supply Chain Challenges:** Limiting downtime through the use of connected IoT applications has become even more critical due to disrupted supply chains. If a critical machine needs repairs, but the part is not available due to supply chain issues, operations can be severely disrupted, increasing both costs and lost revenue.

3) **Maintenance Activities:** More connected industrial processes greatly improve maintenance operations. Not only does the IoT allow the detection of machines on the cusp of failure, avoiding unplanned downtime, but the IoT in industrial markets can limit the amount of planned maintenance.

Manufacturing Flexibility: Manufacturers that are serving markets where product introductions are frequent or where personal product customization adds value are constantly seeking technologies and approaches that make their manufacturing lines more flexible. Flexibility comes with greater implementation of connectivity. Fortunately, the 5G technology features of lower latency and Gigabyte (GB) bandwidth enable manufacturers to replace fixed-line connections with wireless connections using private 5G networks. This, in turn, enables more configurability of production operations.

Electrification and Energy Use: More and more products are moving away from Carbon Dioxide (CO_2)-generating fuels to electricity to power their functions, with the most obvious example being the automotive industry. Industrial markets are also moving toward replacing more production equipment that use gas and diesel engines with electric motors. Example markets include mining, textile production, and the chemical industry. As electrical motors become more common, they are being connected via augmentable or embedded means to not only monitor their performance, but also to monitor their energy use. Monitoring energy usage is particularly important in Europe today, as sky-high energy costs require improving the energy consumption of inefficient industrial equipment.

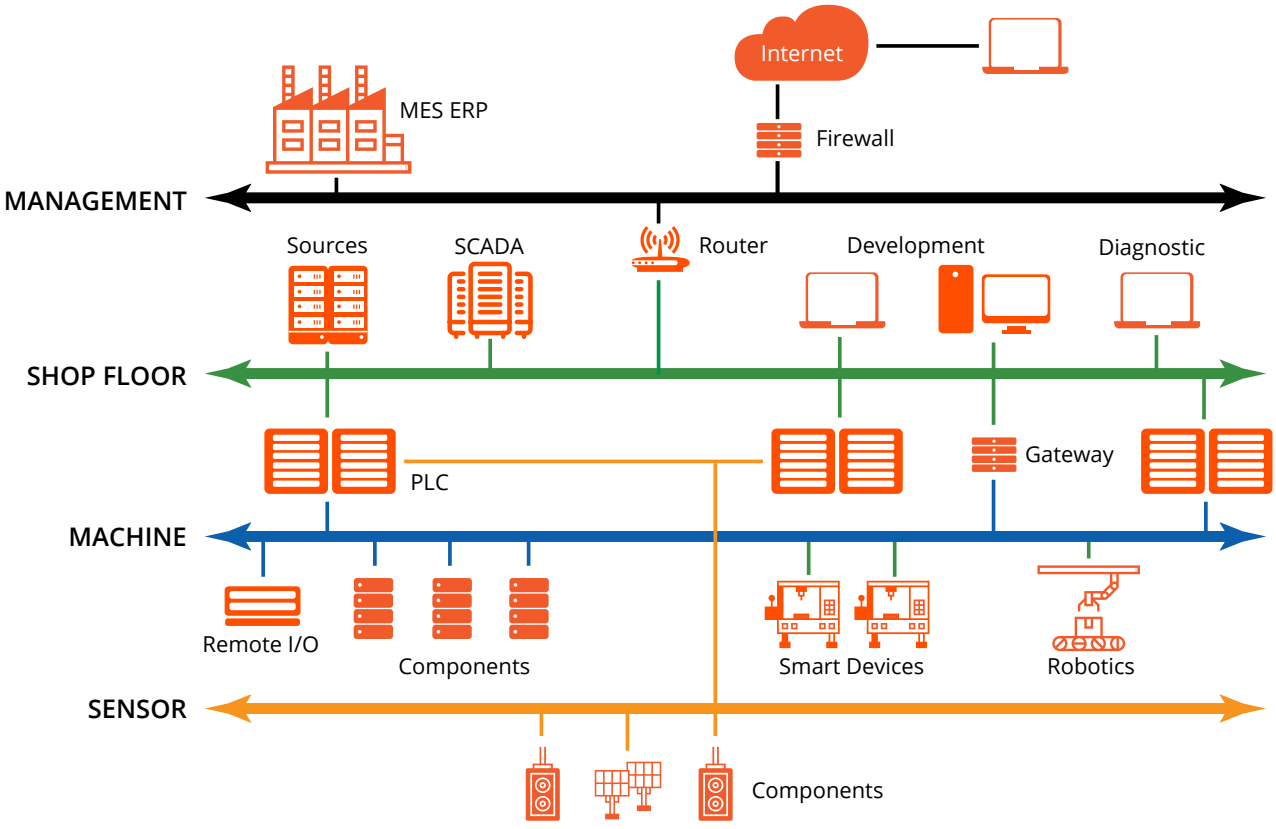
Digital Twins: Industrial organizations are increasingly turning to digital twin technologies to optimize their overall production processes. Digital twin analysis helps optimize capacity utilization, test for electrical equipment replacement, and reduce

energy costs, which all support enterprise sustainability initiatives. The fidelity of the digital twin models is dependent on the ability to gather information on equipment utilization and performance. Enterprises are adding connectivity to the machines that drive industrial processes in order to gather performance data that facilitate better simulation analysis.

Sustainability: Sustainability in the environmental context covers the choices made to limit CO2 emissions, limit waste, and encourage reuse for more circular supply chains. Connectivity has a major role in facilitating all these activities. For industrial organizations, connectivity allows monitoring equipment to ensure they are operating efficiently, limiting energy use. Connectivity also provides a means to update firmware, software, and the recipes that drive control of the equipment, including the use of Artificial Intelligence (AI) that can improve equipment performance and detect conditions leading to downtime. As noted, monitoring equipment for energy use is particularly relevant today due to high energy costs. Finally, connectivity enables monitoring and tracking the flow of goods to improve efficiencies in supply chains.

INDUSTRIAL NETWORK ARCHITECTURE EVOLUTION

Industrial market network connectivity has heavily relied on fixed-line connections in a very layered approach. As shown in the figure below, connectivity extends from the management layer to the controller layer to the final layer of fieldbus-connected components. Typically, the only connection to the Internet was into the Personal Computers (PCs) that contained the recipes for controlling equipment.



However, with the dawn of the industrial Internet and a less siloed approach to industrial automation, more and more equipment at different layers is becoming Internet connected. Connectivity serves not only the factory or enterprise owner of the industrial process, but also the OEMs providing the machines that drive the industrial process.

Industrial automation components and network architectures connecting to the Internet in the industrial domain fall into three main categories:

IoT-Connected PLCs and Controllers: PLCs receive the operational recipes that control the machines driving industrial processes and equipment. They are effectively the gateway to the machines that enable industrial transformation. They have been one of the first Industrial Control Systems (ICSs) to have more direct Internet connectivity, typically sending operational data from the controllers to enterprise systems and other IoT applications.

PLCs range from large cabinet size boxes that control multiple production lines to smaller units that attach to, and control, a single machine. Connectivity is typically an Ethernet connection, but will increasingly become cellular connectivity via gateways that are either standalone or in a cellular private network.

Gateways for Custom Machine Connections: PLCs often do not provide the granularity of data to understand performance of the machines they control. In addition, there is much value in sensorizing and monitoring industrial processes beyond the controlling machines in the process. The connectivity of these smaller machines that include compressors, pumps, and low-voltage step motors is usually by an augmentable sensor to the machine, although many of these devices will eventually include embedded connectivity. Sensors can also be fitted to pipes and electrical equipment within an industrial process. In both scenarios, sensors are connected to a gateway that backhauls data to an application in a data center or in the cloud. Sensor connections to the gateway can be a simple wired connection or use various wireless technologies, such as Wi-Fi, Bluetooth, and even proprietary Low-Power Wide Area (LPWA) technologies.

As noted, connectivity at this level provides more fidelity to the condition of the assets driving and controlling the process. Gateways are the primary means for the collected data from these industrial sensors to be transported over the Internet. Gateways also act as a key control point for delivering the data, including securing the data on the gateway and in transit.

Private Networks: Wireless technologies have always offered value over fixed-line technologies for their ability to connect things and machines that are mobile and portable. This value proposition is becoming more attractive for industrial companies when considering newer wireless technologies, such as 5G, that offer more deterministic communications (lower latency) and higher data throughputs. 5G cellular technologies are the first alternative to traditional fixed-line connections, but there are others as well, such as DECT 2020, a non-The 3rd Generation Partnership Project (3GPP) wireless standard approved by the European Telecommunications Standards Institute (ETSI) in June 2020.

For two reasons, these new technologies will offer the most value when used in private networks. First, they allow network owners to construct a network that meets their exact needs, which can vary greatly by vertical market. Second, the newer wireless technologies, such as 5G, can be used to control the equipment driving industrial processes, rather than solely monitoring machine health. Public network options for 5G do not provide the service levels to ensure meeting deterministic communication requirements for industrial processes.

INDUSTRIAL MARKETS

The industrial sector includes markets that extract and later convert raw materials into final products. It also includes energy distribution and production markets. Industrial markets fall into three primary market segments.

Extraction: The extraction industries are those that extract the raw materials used in the manufacturing industry or that extract oil, gas, coal, or other materials used in energy production. Important machines in these markets are earth moving equipment, such as excavators, backhoes, and trucks, along with oil & gas rigs located both on land and water.

Connectivity very much relies on cellular and satellite technologies communicating with gateways installed in mobile equipment and production environments. PLCs are very prevalent in oil & gas rigs. Secure communications are particularly critical in rig infrastructure for the safety of crew and continuity of operations.

IoT solutions are extremely important in these markets to extend asset life and reduce truck rolls for maintenance operations on assets that can be hundreds of miles from major population centers. As profitability is dependent on commodity pricing, the IoT has played a major role in lowering these markets' cost structures.
Capital expenditures on oil and gas assets in the United States reached nearly $145 billion in 2021.

Utilities: This market consists of power generation facilities that use coal, gas, and nuclear fission materials. It also includes green energy production facilities using hydropower, solar panels, and wind turbines. Also within this sector are gas, water, electricity, and sewer distribution networks, along with related infrastructure, such as electrical substations, pump stations, and water/waste treatment facilities.

PLCs are standard devices used to control machines in power generation facilities and have been the first to get connected for monitoring the health of the power generation process. IoT solutions have mainly focused on machines in power generation and critical distribution network facilities. These solutions typically use condition-specific sensors connected to IoT gateways. However, pipelines and other in-line distribution network infrastructure are getting connected, partly facilitated by LPWA network technologies. Low Earth Orbit (LEO) satellite technologies are also expected to play a role in future sensor-based IoT solutions.

Because utilities infrastructure is vital for supporting commerce and building services, communications security is becoming more critical as more assets in this segment are connected. **In 2020, capital expenditures on utility assets in the United States exceeded $180 billion.**

Manufacturing: The manufacturing segment is the largest of the three and can be segmented into two main markets—discrete manufacturing and continuous manufacturing. Discrete manufacturing is the building of a product through the assembly of many subcomponents. Automotive and aerospace are top discrete manufacturing markets. In a continuous manufacturing process, raw materials at the beginning of the process are transformed during a single non-stop activity into a final product. The chemicals and steel industry are representative of this manufacturing market.

Uptime, production efficiency, and product quality are the primary Key Performance Indicators (KPIs) for this market and IoT solutions are becoming important differentiators for manufacturers. Monitoring PLCs is a key focus for IoT solutions, but sensor-based monitoring of a large breadth of equipment continues to grow, particularly from equipment OEMs extending beyond pure equipment sales to both sales and services models.

Private wireless networks will see significant uptake in the manufacturing market due to the concentration of connected equipment, both for health monitoring and industrial operations. Communications security is a necessity for IoT solutions, but will become critical if private networks are also used for controlling production machine operations. **In 2020, nearly $260 billion was spent on equipment and infrastructure in the US manufacturing sector.**

SECURITY

CHALLENGES

Securing industrial operations is no easy feat; the heterogeneity of the ecosystem makes the task complicated as new smart devices and connected operational technologies, including virtualized assets, add to the fragmented body of proprietary and legacy systems already in place.

Spending on OT and IoT security represented about 6% of total cybersecurity spending in the industrial sector globally in 2022.

There are numerous challenges to implementing uniform security protections to devices:

- Highly constrained and low compute devices
- Strict bandwidth limits
- Ultra-low latency requirements for real-time operations
- Limited upgradeability of legacy devices
- Decade long life spans
- Air-gapped and offline systems, among many others

This makes it difficult to apply high-powered and resource-intensive IT cybersecurity solutions, as many industrial processes rarely tolerate such exigencies, even for something as important as security.

Therefore, it is a significant challenge for an operator to enable cohesive security across their industrial infrastructure and requires an intimate understanding by cybersecurity vendors of the industrial environment, something that few have.

Cybersecurity must be adapted not just to legacy industrial systems, but it also must take into account the slew of newly connected industrial sensors and IoT devices. The key to successful security integration lies as much in minimizing friction between all those elements as in finding the most fitting solution.

In truth, there are not a lot of security technologies that can be easily applied without spending significant resources on retrofitting and customizing security for industrial assets. Most commercial off-the-shelf security solutions can only be implemented at the network level or above. However, industrial protection needs to be extended much closer to the endpoint for it to be truly valuable; therein lies the most pressing problem for industrial operators.

APPROACHES

One part of the solution is understanding that building an effective chain of trust requires the establishment of an identity first and foremost. Asset identification allows for asset management and the ability to set security policies. With machine identity measures, industrial operators can enable myriad functions, including authentication and access control, monitoring, threat detection and response, and lifecycle management.

The other part of the solution is to find an appropriate identification method that is both practicable and agnostic to the highly fragmented mass of assets present in the industrial space—one that is also easily scalable, as well as flexible.

Digital certificates are one such technology. Initially standardized in 1988 under the X.509 format, today they are well-established and ubiquitous. More than that, they are highly customizable, which makes them a good fit for a heterogenous environment. Digital certificates provide a trust anchor to establish a verifiable identity for any asset (individual, machine, application, etc.). Its popularity is due to its fundamental role within PKI, which has provided the foundation of digital trust for the last 30 years. It makes sense to leverage a tried and tested technology, especially one that has stood the test of time, in part because of its flexibility.

The global PKI market was estimated at just over $2 billion in 2022. Within that, IoT represented only about 5-10% of total revenues.

PKI is a uniquely pliable technology that can fit a variety of use cases, from public trust (such as Secure Sockets Layer (SSL)/Transport Layer Security (TLS) certificates for public-facing websites) to private trust (Secure/Multipurpose Internet Mail Extensions (S/MIME) for private use by organizations for encrypting emails). Digital certificates can be implemented in several ways, including Secure Shell (SSH) certificates, code-signing certificates, digital signatures, and digital identities, among many others.

BENEFITS

This malleability means digital certificates are particularly well suited to the diversity of IoT and industrial ecosystems, both physical and virtualized. Thus, PKI has become the primary credentialing platform for machine identity. There are several benefits that can be derived from using PKI for identifying and managing industrial assets.

First, PKI can be easily adapted for challenging and diverging industrial implementations. This means the certificates can be crafted to align with a range of varied requirements, from proprietary ones to established industrial security standards (such as International Electrotechnical Commission (IEC) 62443 and 62351).

Further, the impact of PKI on industrial operations is minimal, and limits the amount of friction during usage. A generic digital certificate file is already small (2 Kilobits (kb) to 4 kb), containing just the primary identifying information required, although the size depends on the algorithm used. Innovative modifications have been devised to suit different industrial capabilities. Adapted PKIs can use lightweight digital certificates with smaller memory footprints by using either lighter cryptographic algorithms or improved compression mechanisms. But it is also possible for the certificate management part to be offloaded completely to industrial gateways if the individual asset is extremely constrained.

A PKI's crypto-agility is a key requirement for these use cases, not only in providing choice for cryptographic algorithms, but also future-proofing certificate usage (and notably for enabling the eventual switch to new algorithms that will emerge from post-quantum cryptographic development).

Also, there are many ways to bend PKI technologies to the use case in terms of binding identities to the asset. Certificates can be injected into the device within a secure element at the point of manufacturing to create a hardware root of trust. But equally, they can be deployed as software clients on any number of varying form factors: sensors, smart devices, and gateways, and their virtualized counterparts. The format and size of the certificate will depend on the asset's technical capabilities.

Importantly as well, PKIs already form an intrinsic part of IoT connectivity platforms and cloud applications; with many providers enabling PKI integration and management with their respective platforms (Azure IoT Hub, Amazon Web Services (AWS) IoT Core, Google Cloud IoT Core, Arm Pelion, etc.). Certificates are the de facto currency for identity management in these platforms, and the extension of PKI to industrial assets in the field is an expected development that cloud platforms are ready for. Moreover, there is an important and maturing market for IoT and industrial PKI services coming from these providers. The only missing piece is the extension down to the industrial edge, which needs to be driven by the operators themselves.

Finally, the other main advantage of using certificates for industrial asset identification is that they are well suited to high-volume environments and can, therefore, be very cost effective. A PKI scales well, and by leveraging RESTful Application Programming Interfaces (APIs), for example, the underlying infrastructure can integrate with other third-party services and applications for managing certificates, policies, assets (such as the devices and machines), and the Certificate Authority (CA). This uniformity is important, especially as industrial environments often require custom certificate formats, extensions, and management.

Certificate management still requires expertise in setup and management. The learning curve can be especially high for those operators that want to run their own in-house PKI. The market, however, offers an ever-growing range of PKI solutions—from consulting services to helping operators set up their own PKI, managed PKI solutions, or PKI-as-a-Service offerings. The choice of a solution will depend on the specific needs and capabilities of the industrial operator and requires careful due diligence. A startling amount of industrial PKI implementations fail because the operator has not been able to successfully implement and run the technology.

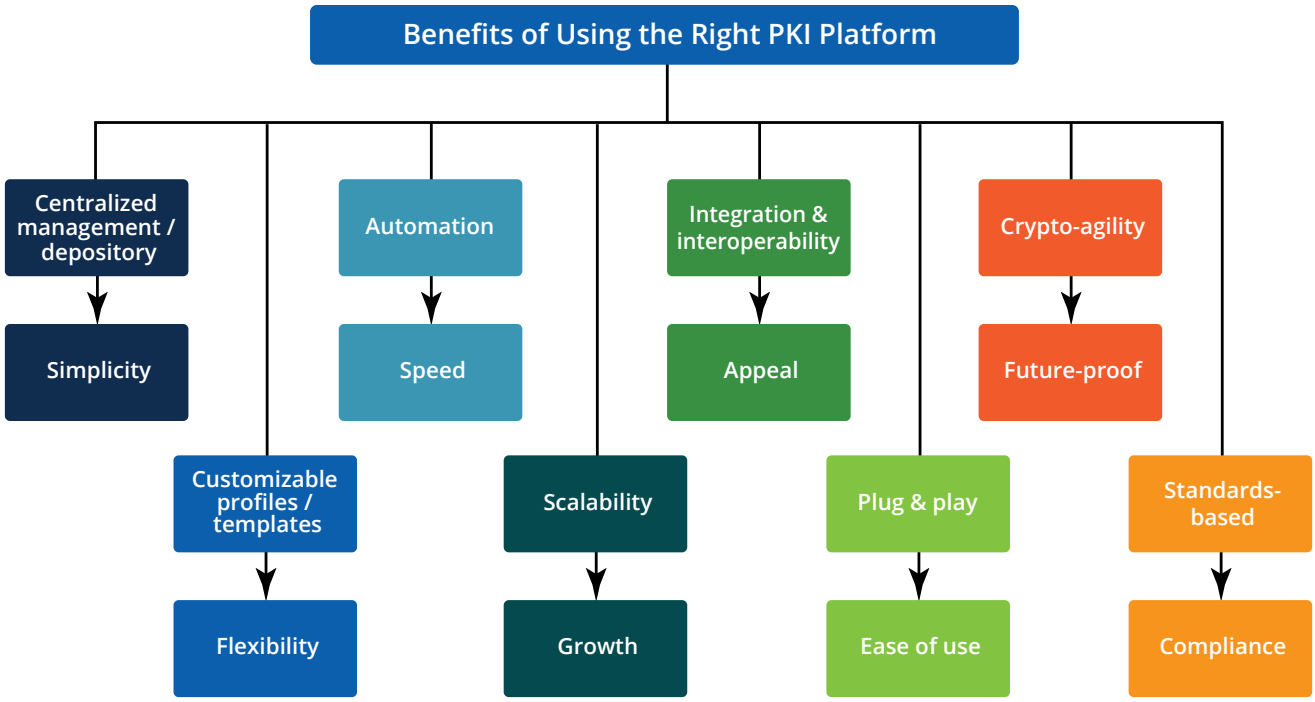
What is clear, however, is that the business case for industrial PKI is strong. The right PKI solution can go a long way toward alleviating some of the challenges associated with deployment and lifecycle management of industrial assets, providing much needed visibility into industrial operations at the very edge.

PKI solutions attuned to industrial workings will offer feature-rich certificate capabilities within a comprehensive identity platform that can simplify and streamline management from an operational perspective. A rich feature set can allow for fine-grained controls and tuning of asset behavior, optimizing industrial processes. Key features that operators should consider include:

- Choice of device identities
- Creation of a trusted root hierarchy (CA) for issuance
- Choice in communication and enrollment protocols
- Customization for defining appropriate rules and policies for enrollment
- Configuration and provisioning capabilities for certificates
- Offer of revocation services
- Maintenance of certificate inventories
- Integration with IoT platforms and cloud applications, among others

Ideally, an advanced solution prioritizes automation, especially considering that high volume and scale are key demands in industrial environments.

A suitable PKI platform will also be able to support custom development through various plug & play tools (e.g., certificate templates, APIs, Software Development Kits (SDKs)), as well as partner programs for integration with third-party solutions targeted at industrial environments and cloud services that can enable device lifecycle management. There are significant benefits to be obtained from a dedicated industrial PKI solution, such as offering a level of agility that is not readily matched by other security solutions.



CONCLUSION

Industrial transformation relies on connecting its broad and diverse base of assets. IoT connectivity and later production control will be facilitated by new networking approaches using PLCs, gateways, and private networks. Security is a top consideration for industrial actors to realize the benefits possible with digitization and implementation of new technologies.

For industrial operators, implementing machine identities offers considerable benefits. By delivering asset visibility, a machine identity can, through PKI, enable granular control deep within industrial processes. This ability is key to risk minimization and threat mitigation.

There is no question that PKI is the most suitable technology for delivering and managing machine identities. But more than that, PKI can deliver additional value beyond security: process optimization, operational flexibility, etc. At the heart of PKI, digital certificates are a valuable business asset and a key enabler for building trusted and resilient industrial infrastructure.

Implementing a PKI need not to be an overly complex and costly endeavor; a maturing market in this domain means many affordable solutions are increasingly available to operators. Solutions should be able to shoulder the technical burden, reduce the complexity, and provide dedicated support in PKI deployment and management. For operators, it is simply a matter of finding the right trusted provider to deliver on that promise.

Published January 2023
157 Columbus Avenue 4th Floor
New York, NY 10023
Phone: +1 516-624-2500
www.abiresearch.com

About GMO GlobalSign

As one of the world's most deeply rooted Certificate Authorities, GlobalSign is the leading provider of trusted identity and security solutions enabling organizations, large enterprises, cloud-based service providers and IoT innovators worldwide to conduct secure online communications, manage millions of verified digital identities and automate authentication and encryption. Its high-scale PKI and identity solutions support the billions of services, devices, people and things comprising the IoT. A subsidiary of Japan-based GMO Cloud KK and GMO Internet Group, GMO GlobalSign has offices in the Americas, Europe and Asia. For more information, visit https://www.globalsign.com.

GlobalSign US Office
Two International Drive, Suite 150
Portsmouth, NH 03801
Phone: 603-570-7060
Email: sales-us@globalsign.com

GlobalSign UK Office
Springfield House,
Sandling Road, Maidstone,
Kent ME14 2LP
Phone: 01622 766766
Email: sales@globalsign.com

GlobalSign EU Office
GlobalSign NV/SA
Diestsevest 14
3000 Leuven
Belgium
Phone: +32 16 89 19 00
Email: sales@globalsign.com

About ABI Research

ABI Research provides actionable research and strategic guidance to technology leaders, innovators, and decision makers around the world. Our research focuses on the transformative technologies that are dramatically reshaping industries, economies, and workforces today. ABI Research's global team of analysts publish groundbreaking studies often years ahead of other technology advisory firms, empowering our clients to stay ahead of their markets and their competitors.