FUTUREX

WHITEPAPER

IoT Security in Manufacturing

Futurex Solutions for Modern and Secure Manufacturing Processes

TABLE OF CONTENTS

OVERVIEW

Whether it be a watch, computer, vehicle, or medical device — consumers and businesses alike benefit from the data sharing, data management, and new-age technologies that accompany smart devices. These devices dominate the global technology landscape, with an estimated 9.9 billion Internet of Things (IoT) active device connections worldwide in 2020.[1] Just through sheer numbers, these interconnected devices have made and will continue to make a significant global impact. If left unsecured, every IoT device has the potential to have its technology, information, and communication hacked. Therefore, organizations must understand this significance and take on the responsibility of securing and protecting this data. There are several challenges when building out an IoT security infrastructure. These include:

- Securing device identities
- Securing code deployments
- Establishing trusted communication and licensing
- Future-proofing the cryptographic functionality

This whitepaper will review each of these IoT challenges and addresses and how organizations can tackle these challenges head-on.

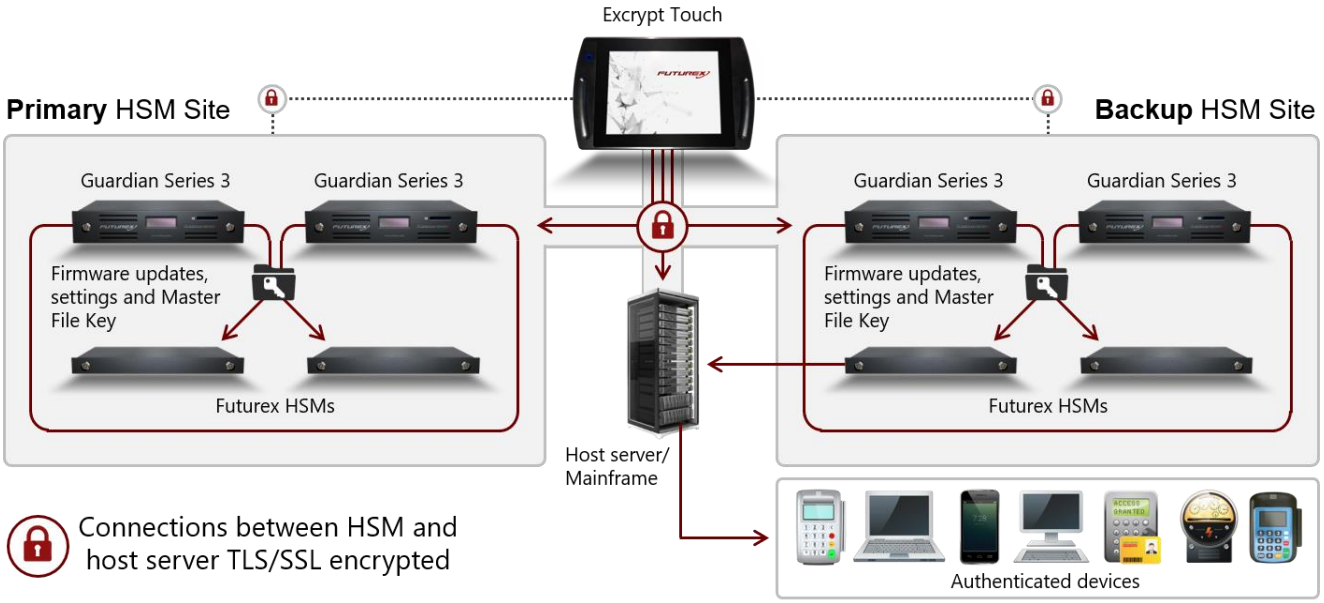
INTRODUCTION TO THE HARDENED ENTERPRISE SECURITY PLATFORM

To mitigate the risks associated with IoT devices, many device manufacturers put extra security measures in place before the product even hits the store shelves. Using a PKI (Public Key Infrastructure) and mutual authentication, device manufacturers set up a framework for encryption and authentication that restricts access only to authorized individuals and devices. This environment can be built out, from top-to-bottom, using the Futurex Hardened Enterprise Security Platform. This platform provides a complete hardware-based infrastructure featuring security, versatility, automation, scalability, disaster recovery, and remote administration of a cryptographic environment. Beyond the robust security of Futurex's FIPS 140-2 Level 3-validated Secure Cryptographic Devices (SCD), the Hardened Enterprise Security Platform enhances security by maintaining data integrity across every endpoint.

- The KMES Series 3 provides full key and certificate lifecycle management for enterprise applications as well as for the Futurex Hardened Enterprise Security Platform itself. It is the foundation for a secure PKI and enables organizations to establish trust with IoT devices and secure deployment of code and licenses.
- The Guardian Series 3, running in active-active mode, handles centralized configuration for groups of Futurex solutions. It routes transactions, eliminates single points of failure, deploys firmware updates, replicates settings between devices, and offers customized alerting and monitoring.
- Remote management, including initial device provisioning, is performed by the Excrypt Touch using FIPS 140-2 Level 3 and PCI HSM compliant technology to enable full control from virtually any location.

[1] "Internet of Things (IoT) active device connections installed base worldwide from 2015 to 2025." Statista. https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/

- The VirtuCrypt Hardened Enterprise Security Cloud operates from industry-certified data centers and provides services ranging from scalability for on-premises Futurex infrastructures to completely standalone cloud cryptographic services. Over 10 additional Hardened Enterprise Security Platform solutions integrate seamlessly using the base architecture model common code base, enabling functionality such as secure storage, tokenization, remote key management, TLS line encryption, trusted identity management, and more.

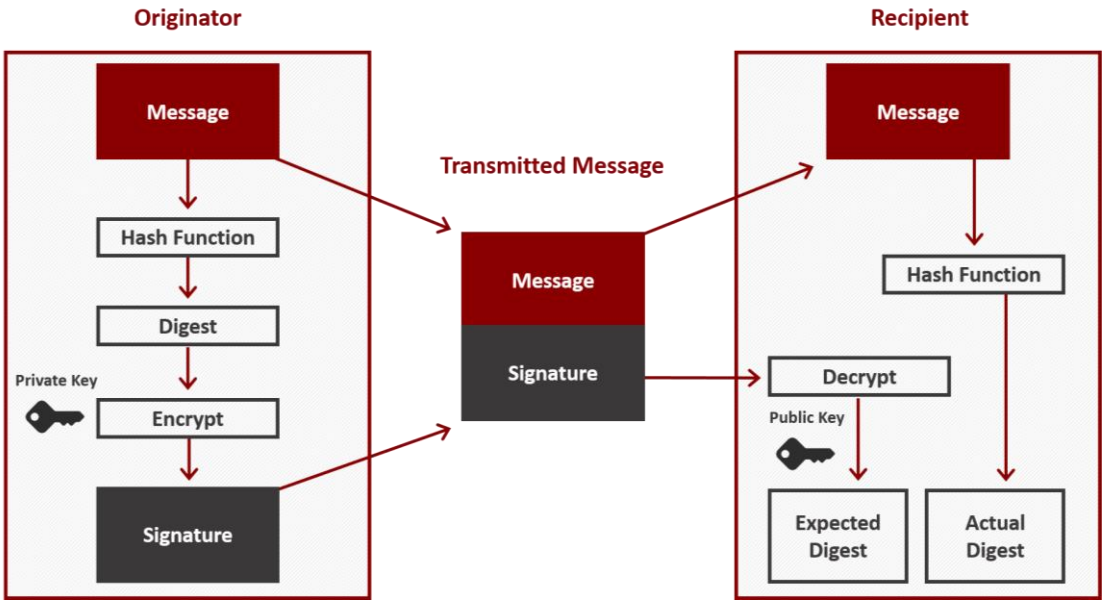


DEPLOYING IOT IDENTITIES IN THE HARDENED ENTERPRISE SECURITY PLATFORM

Just as an organization must identify and manage its people, organizations must also identify and manage its devices. A device identity is a way of identifying a device or object. In a physical form, this could be accomplished through a sticker with a serial number listed. But how would organizations manage these devices once out in the field? And how would one control how and with whom that device connects, interacts, and shares information with? This environment is controlled through a public key infrastructure.

WHAT IS A PUBLIC KEY INFRASTRUCTURE?

A public key infrastructure, often referred to by its acronym PKI, is the most secure solution for ensuring that shared data is only accessible by authorized recipients. A PKI uses a key pair (a public and private key) to encrypt and decrypt data, through asymmetric encryption. The public key cannot decrypt data, only encrypt it, and so it can be widely distributed without fear of exposing sensitive data. The private key must be kept secure as it is used to decrypt the data that was originally encrypted by the public key. When users or devices wish to communicate securely, they begin by exchanging public keys. Each party uses the public key they received to encrypt the message, then sends that encrypted value to the other person. Once that value is received, it is decrypted with the corresponding private key. This process allows for information to be shared easily while maintaining full security, because if the message falls into the wrong hands, it cannot be read.



The exchange of public and private keys encrypts and decrypts messages; however, in this simplified environment, there is no authentication process to validate the origin or ownership of these shared keys. A certificate authority (CA) does just this, issuing certificates to create a larger circle of trust between keys. A CA can manage entire trees of keys, along with the certificates that validate those keys. The certificate tree root must be highly secure because as the root, all new certificates are created beneath it. It issues signed (encrypted) certificates that are distributed to users, individual devices, or objects. The CA creates and signs the asymmetric keys, which are used for data exchange, and when the same CA is used throughout a network, it further expands the circle of trust for that organization by verifying the authenticity of users, devices, communications, and the organization as a whole.

WHAT IS A DEVICE IDENTITY?

In the Internet of Things landscape, organizations need to be able to track devices, as well as manage device access to sensitive information. This is accomplished by giving each device a device identity. Similar to a serial number, devices can be uniquely and securely identified by a cryptographic certificate. Through a certificate authority, the device is issued a certificate, which in turn provides an unique identity for each device in the IoT ecosystem. Similar to how a person might present a driver's license to identify themselves, devices verify one another's certificates to authenticate other devices. It allows devices in a network to mutually authenticate each other as being part from the same system, which in turn: will enable devices to communicate securely; guarantees the authenticity of the information being transmitted; prevents attackers from tampering with the data, and ensures that data is not stolen or sent to an unauthorized device. Certificates provide a secure identity and protect each device in the ecosystem.

TRUSTED COMMUNICATION AND LICENSING

Device identities serve two purposes: providing secure communication and validating trusted sources. Beginning on the manufacturing line, organizations can establish the validity of software and data within a smart device by utilizing a hardened PKI environment. Before a device is deployed in the field, a manufacturer can inject encryption keys using a compliant and secure hardware security module (HSM). This establishes a framework for encryption and authentication that restricts device access only to authorized individuals. This framework also allows secure communication to manifest itself in a number of significant ways.

Once the product is in the hands of the consumer, organizations can pro-actively protect consumers, again through a PKI. While organizations regularly roll out software updates, bug fixes, and security enhancements, the average consumer does not always make a concerted effort to actively update the software on their connected IoT devices. Therefore, devices are susceptible to malicious outside activity or security threats. Manufacturers can protect both their technology and their consumers with cryptographically secure, over-the-air software updates or push notifications. A robust certificate authority, in conjunction with a PKI, verifies that the update and connection is from a trusted source. If an unauthorized connection is attempted, it will be rejected because it does not have the appropriate encryption keys to establish trust.

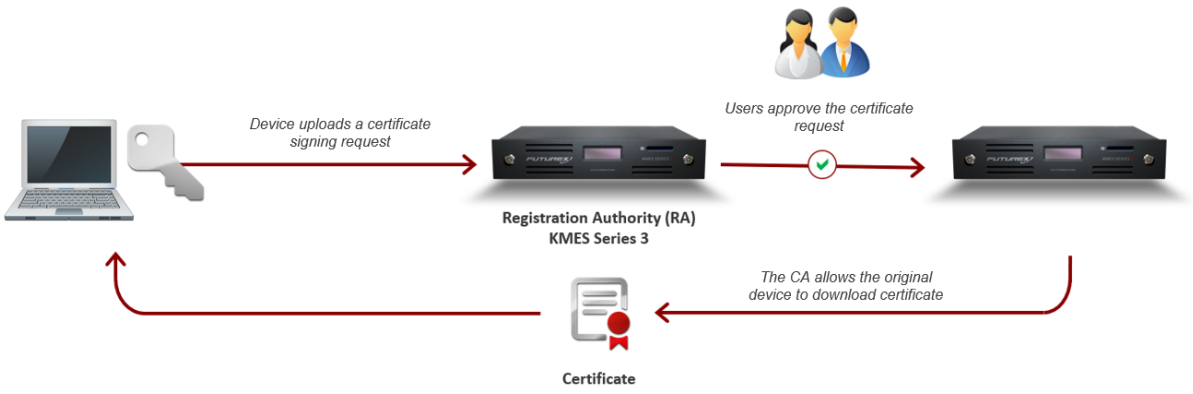
Hardware-based cryptographic solutions protect data regardless of the implementation by businesses or consumers. Encrypted device identities also protect the authenticity of intellectual property and help combat counterfeit or malicious devices. A digital signature cannot be replicated, protecting the brand from counterfeits and protecting consumers from inadvertently purchasing unsafe equipment.

MANAGING A CERTIFICATE AUTHORITY AND THE ISSUANCE OF IDENTITIES

A PKI is a system of people, processes, and technologies used to manage, create, and revoke digital certificates, which as discussed, is the foundation of securing device identities. This allows multiple devices to communicate privately, even on a public network. Futurex manages the PKI, the certificate authority, and the issuance of identities through the use of a registration authority (RA). An RA works with this system, as another integral part of building an enterprise PKI and CA infrastructure. In the simplest terms, an RA is a sub-set of a CA, and eases the process of submitting certificate signing requests, verifying these requests, and passing this information to the CA to issue the appropriate certificates.

HOW CAS AND RAS WORK TOGETHER

As stated above, an RA is a sub-set of a CA, with the CA serving as the trusted source for securely signing, issuing, revoking, and storing certificates. An RA helps filter information to the CA and serves as an intermediary between a certificate request and the CA, telling the CA which certificates can be issued. When users or devices place requests for digital certificates, RAs verify the identity of requesters before forwarding the request to the CA. Requests are then submitted to the RA through a certificate signing request (CSR). The device's identity is validated using information stored within the CSR, including the device's public key and X.509 profile. Based on this information, the CA will validate the device's identity, create a digital certificate with the device's public key, sign the certificate with the device's private key, and return the signed certificate to the device, completing the signing process.



The diagram above describes how the RA and CA work together to sign certificates within the cryptographic boundary of a FIPS 140, Level 3 hardware security module (HSM). A user applies for a certificate at the RA using their public key. The RA confirms the user's identity. Two approvers must log in to the RA to verify the request. After approval is granted, the RA subsequently sends this information to the CA for signing. The CA then returns the signed certificate to the original user for download.

RA, ALL WRAPPED UP

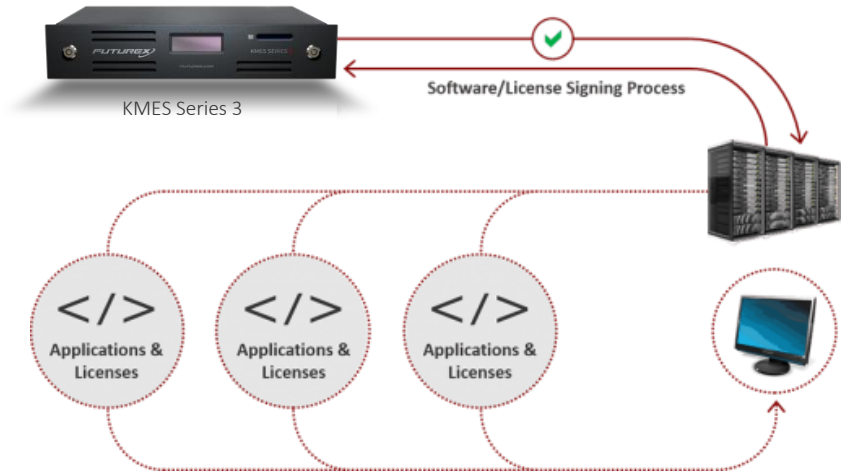
For enterprise-level organizations, the RA functionality can save time and resources by providing an accessible and robust channel for creating and verifying certificate signing requests. Since it is stored within the same KMES Series device as the CA, users benefit from the maximum level of convenience and functionality. Equally importantly, all functionality is displayed in an intuitive, easy-to-learn, and graphics-based interface, reducing training time.

SECURING CODE DEPLOYMENT

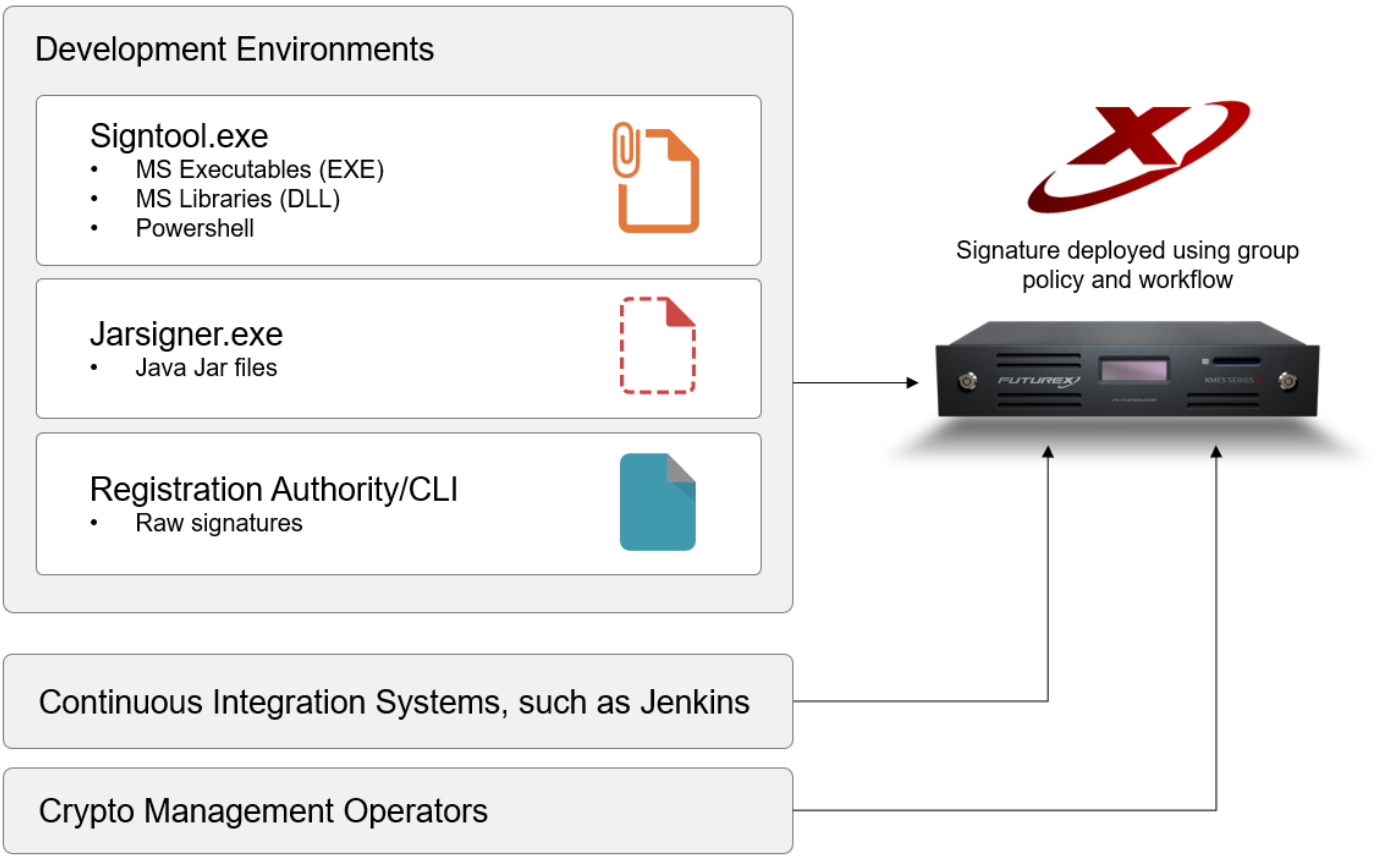
We've spoken throughout this whitepaper about the importance of securing device identities. A large portion of that security comes by protecting the code that runs on those IoT devices. Code signing provides considerable benefits, including:

- Using a PKI to generate a digital signature, from which trust can be established
- Preventing and detecting code tampering or counterfeit code
- Support for workflow management
- Protects IP, such as executables, by using a hardware security module (HSM) to secure a public key infrastructure (PKI)
- Prevents and detects code tampering or counterfeit code

Additionally, Futurex's IoT solution includes support for multiple embedded signature methods, ranging from Microsoft Authenticode (.exe/.dll), to Java, and includes general signature generation. With Microsoft Code Signing,



At a high-level, code-signing provides a centralized group policy for managing keys and certificates, as well as application tracking and policies for creating and distributing signatures. Futurex's code signing solution offers native support for commonly used embedded signature applications, as well as workflow automation using available Registration Authority or API/CLI to integrate with CI systems, such as Jenkins.



FUTURE PROOFING CRYPTO

A telecommunications satellite being sent to space to track and share data over the next 50 years. Whatever cryptographic algorithm it is currently using *will* be broken during that time. With the rise of quantum computing on the horizon, society faces a threat that will break PKI cryptography as we know it. Unlike classical computers that process bits of information in binary, quantum computers produce quantum bits, or qubits, enabling them to process data exponentially quicker. Quantum computers will be powerful enough to render many widely used cryptographic algorithms, such as RSA, Diffie Hellman, or ECC, completely useless. While industry experts predict this transition in the next five to ten years, long-lifespan IoT devices, such as satellites, automobiles, and critical infrastructure components, need to prepare now. These devices can be future proofed with quantum-safe cryptography through Futurex.

Futurex is developing a post-quantum hybrid certificate authority solution, delivered as a turn-key HSM-integrated appliance or HSM-integrated cloud service. With this technology, you can simultaneously sign code, IoT devices, or any other digital object with both classical and post-quantum algorithms. The quantum-safe certificates lay dormant, while conventional algorithms continue operating without impact to the existing ecosystem. When the organization is

ready, they can easily switch to the quantum-safe certificates, without having to migrate systems of issue new certificates. In the satellite example, it can be sent to space with both standard cryptographic measures and new quantum-safe method through hybrid certificates, protecting it both now and in the future.

While there is no current standard NIST approved post-quantum algorithm, the National Institute of Standards and Technology (NIST) says, "It is critical to begin planning for the replacement of hardware, software, and services that use public-key algorithms now so that the information is protected from future attacks."[2] NIST is currently in the process of selecting and establishing this standard now and plans to release the initial standard for quantum-resistant cryptography in 2022. Futurex, through our partnership with ISARA Corporation, the world's leading provider of quantum-safe and crypto-agile security, is deploying these quantum algorithms in our hardware so that organizations can start using those algorithms now.

CONCLUSION

The internet of things landscape is growing, with projections of 21.5 billion units worldwide by 2025. These numbers can be daunting, but with a secure PKI in place, each device coming off the manufacturing line can be easily protected and secured. This system of device identities and certificates provides cradle-to-grave protection for both the manufacturer and the consumer.

Through the Futurex KMES Series 3 HSM, a certificate authority provides a secure, full-service, and highly-available cryptographic solution, capable of meeting the demands of high volume IoT manufacturers. For more information and to schedule a demonstration of key management and the Hardened Enterprise Security Platform, contact Futurex today.

[2] "NIST's Post-Quantum Cryptography Program Enters 'Selection Round'". National Institute of Standards and Technology. July 22, 2020. https://www.nist.gov/news-events/news/2020/07/nists-post-quantum-cryptography-program-enters-selection-round

FUTUREX ENGINEERING CAMPUS
OFFICE: +1 830 - 980 - 9782 TOLL FREE: 800 - 251 - 5112
864 OLD BOERNE ROAD, BULVERDE, TEXAS, USA 78163