Futurex-Signed Certificates Service

TABLE OF CONTENTS

FUTUREX-SIGNED CERTIFICATES SERVICE

Mutual authentication is the process by which two devices verify one another's identity so communication between them can be trusted. In order for mutual authentication to occur, the devices must be digitally signed by a trusted certificate authority (CA). This is often required in order for companies to remain compliant with regulatory standards, internal audit requirements, and industry best practices.

While organizations have the option to either sign the devices themselves using their own CA or outsource the signing to a third-party company, multiple standards and regulations must be followed by any company performing digital signing, which can be costly and time consuming. Instead, organizations can take advantage of the Futurex-Signed Certificates service, the process by which Futurex digitally signs devices in a TR-39 and PCI PIN-certified secure facility.

MUTUAL AUTHENTICATION AND THE KEY MANAGEMENT ENTERPRISE SERVER

Authentication occurs when users are required to prove their identity in order to access information using passwords, smart cards, fingerprints, or other identifiers. Authentication ensures that a user is who he or she claims to be, which reduces the risk of fraud and potential data compromise.

In the same respect, mutual authentication is the process by which electronic devices, often a client and a server, authenticate one another's identity by verifying digital certificates.

These digital certificates are issued by a trusted certificate authority. Digital signing ensures the integrity of electronic communication as well as files that are transmitted, certifying that the data has not been tampered with and devices have not been substituted. Certificate authorities are considered trusted devices because they are compliant with regulatory standards and are housed in secure, independently audited environments. For the financial services industry, applicable regulatory standards include TR-39, a standard published by ANSI Accredited Standards Committee X9 which ensures the security of electronic transactions, and PCI PIN, which governs the secure management of PINs during card-based transactions. These rigorous standards are often regarded as best practices in a wide range of additional industries.

Through this process, devices such as hardware security modules, management servers, and host applications can be certain that all other devices attempting to gain access are doing so for legitimate reasons, preventing outside intruders from communicating with and accessing protected devices. Users will also be confident that the information they receive is valid and genuine.

In this model of relationships and communication, the CA is a third party that is trusted by both the owner of the certificate and the party relying upon the certificate. CAs are required components of many public key infrastructures.

The certificate authority's purpose is to generate, manage, and store those certificates, which contain asymmetric key pairs used for encrypting, decrypting, signing, and validating data in a public key infrastructure.

In addition to creating and managing new certificates, the KMES Series 3 can also monitor when certificates expire or are no longer valid by utilizing a certificate revocation list (CRL), which prevents the use of invalid certificates. CRLs are crucial in maintaining the integrity of an organization's public key infrastructure.

THE FUTUREX ADVANTAGE

Organizations have three options for digitally signing their devices:

- Using a third-party CA to sign their devices
- Implementing their own certificate authority to digitally sign their own devices
- Using Futurex-Signed Certificates, which are automatically preloaded during the manufacturing process

Third party certificate authorities often have frequent expiration dates, which allows them to charge recurring fees to digitally sign devices. This can be costly, time-consuming, and logistically difficult.

Organizations can choose to purchase and implement their own CA and sign their devices themselves but, depending on the size of the organization, this might not be the most cost-effective solution. Smaller businesses will not have the volume necessary to justify the steep hardware and compliance costs.

Companies who maintain their own certificate authority must comply with regulatory mandates such as TR-39 and PCI PIN. These regulations require organizations to follow strict standards, including building and maintaining their own secure facility and undergoing regular audits.

Organizations spend considerable time and money complying with these regulations in addition to the manpower required to issue digital signatures. Digital signatures must always be issued under dual control, so at least two people will always be required to dedicate time to digitally signing devices, which will take them away from other duties.

The Futurex-Signed Certificates service offers many advantages for organizations of all types and sizes, including:

THE CORE CRYPTOGRAPHIC INFRASTRUCTURE WILL BE DIGITALLY CERTIFIED BY THE MANUFACTURER THAT BUILT IT.

Companies can rest easy knowing that their device is compliant, effective, and secure. Rather than spending time researching reputable third party companies, organizations can have their complete and customized solution digitally signed by the company they trusted to build it.

DEVICES ARE SIGNED IN FUTUREX'S TR-39 AND PCI PIN-CERTIFIED SECURE FACILITY.

Futurex's secure facility has undergone rigorous external audits to ensure its compliance with regulatory standards such as TR-39 and PCI PIN. These audits are performed on a regular basis, ensuring continuous compliance and security.

PRELOADED SIGNATURES SAVE CUSTOMERS VALUABLE TIME, EFFORT, AND RESOURCES.

Organizations can implement their Futurex solutions immediately, rather than waiting while they are signed, either internally by their own CA or externally by a third party CA. This increases both security and productivity. This also results in cost savings when compared to the typical expense of contracting a third-party provider of device signing services as well as the time that would be spent by the multiple administrators required to generate signing requests, load certificates, and other aspects of the process.

DIGITAL SIGNATURES ARE MADE AVAILABLE WITH LONG-TERM VALIDITY DATES AND NO RECURRING SERVICE CHARGES.

Third party companies may charge high fees to digitally sign devices, sometimes including recurring fees. The Futurex-Signed Certificates service is made available without annual fees.

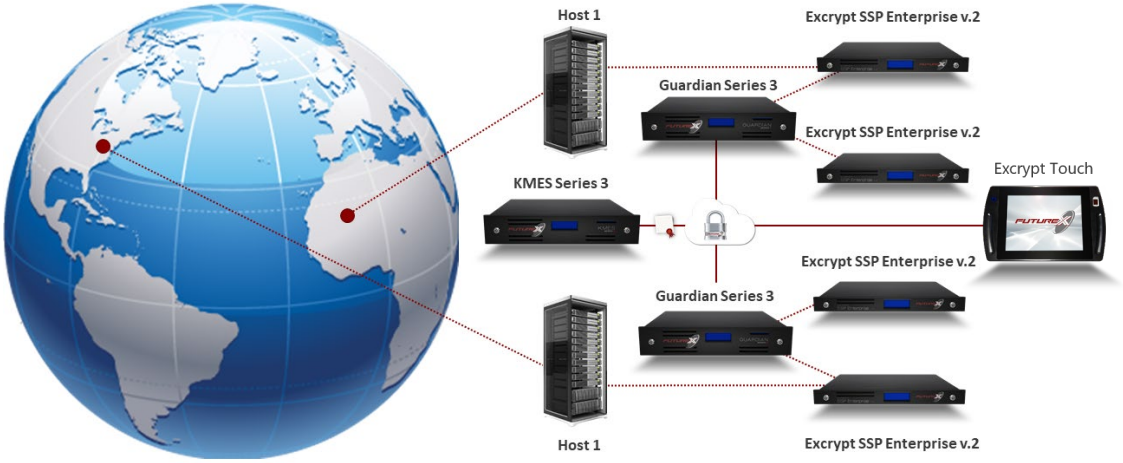
ORGANIZATIONS DO NOT HAVE TO PURCHASE THEIR OWN CA OR BUILD, MAINTAIN, AND AUDIT A SECURE FACILITY.

Purchasing a certificate authority and maintaining a secure facility is costly and time-consuming for businesses. By taking advantage of the Futurex-Signed Certificates service, organizations do not have to take on these financial burdens or expend the time and manpower required to digitally sign devices.

MUTUAL AUTHENTICATION USING THE FUTUREX ENTERPRISE SECURITY PLATFORM

Successful mutual authentication results in each device being able to verify the certificate of every other device with which it attempts to connect, thereby validating the identity of the device and the safety of the connection. Specifically, this prevents hackers and other malicious entities from unauthorized access to sensitive information or systems because they will not be able to communicate with the protected devices.

In the example below using the Futurex Enterprise Security Platform, the KMES Series 3 has digitally signed each of the devices in the infrastructure, including the Excrypt SSP Enterprise v.2 hardware security module (HSM), the Guardian Series 3 centralized management platform, and the Excrypt Touch remote access device.



The Excrypt Touch and the Guardian Series 3 are able to remotely connect with all other network-attached Futurex solutions in the infrastructure in order to perform tasks from remote locations such as key management, firmware updates, and device configuration.

Additionally, these connections are encrypted using SSL/TLS to ensure the security of sensitive data traveling over public communication lines. In order to securely communicate with the other devices, they must be able to successfully mutually authenticate with one another, which they accomplish by verifying the digital signature created by the KMES Series 3 in the Futurex secure facility.

HOW IT WORKS

In this example, there are two geographically separate data centers, each with one Guardian Series 3 managing two Excrypt SSP Enterprise v.2 hardware security modules. All Futurex solutions within this diagram can be managed remotely using the Excrypt Touch.

The use of multiple HSMs and Guardian Series 3s, all of which were signed in the Secure Facility, removes any single point of failure and eliminates any downtime due to both planned and unplanned outages.

This type of infrastructure can be set up in almost any industry with little difficulty, and it can save organizations time and money associated with maintaining disaster recovery and redundancy capabilities.

This infrastructure would not be able to function without the KMES Series 3. Every cryptographic device in this infrastructure received a digital certificate from it, allowing all other devices to communicate with one another securely and transmit data without risk of compromise.

THE FUTUREX SECURE FACILITY

To comply with regulatory requirements, all digital signing must be performed in a secure facility that has undergone a meticulous audit process.

The Futurex secure facility has received TR-39 and PCI PIN certifications, which are standards that address the security of electronic transactions containing sensitive data. TR-39 regulates the treatment of encryption, key management, and key protection while PCI PIN governs the secure management, processing, and transmission of PINs as well as devices that accept them during card-based transactions.

In order to receive these certifications, the Futurex secure facility underwent rigorous external audit processes. These audits must be performed on a regular basis to ensure continued compliance. For organizations that do not need to perform digital signing on a regular basis, the money and time required to maintain a secure facility is not always cost-effective.

The Futurex-Signed Certificates service incorporates hardware-based cryptographic technology contained within a physically protected environment, all managed according to industry standards and best practices.

Device signing enables trusted, mutually-authenticated connections between host applications, client endpoints, and Futurex solutions. By taking advantage of these Futurex's services, organizations are no longer required to undergo the cost and logistical burden of maintaining their own TR-39 and PCI PIN compliant secure facility.

SECURE FACILITY REQUIREMENTS

Mandatory dual access: requires that no one person be in charge of digital signing, ensuring the integrity of the process. Dual control is required for all tasks carried out within the secure facility.

No connection to outside networks: prevents unauthorized access by malicious parties, mitigating the risk of fraud and data compromise.

Auditable use and visitor logs: allows for tracking and auditing of all activity that takes place within the secure facility, assisting with day-to-day monitoring as well as TR-39 compliance audits.

Access restricted to authorized personnel: prevents unauthorized access by internal or external parties.

These requirements work together to ensure that all activity that takes place within the secure facility is valid and compliant. Consistent TR-39 audits ensure that these standards are always maintained, granting organizations confidence in the security of their core cryptographic infrastructure.

Compliance: PCI PIN and TR-39

TR-39 and PCI PIN compliance are two accreditations granted to the Futurex secure facility. These standards address the security of activity involving sensitive data.

While these specific standards were designed initially for the financial services industry, they have been widely recognized and informally adopted throughout other industries as representative of security best practices.

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