FUTUREX

WHITEPAPER

KMES Series 3

Enterprise Certificate Authority

TABLE OF CONTENTS

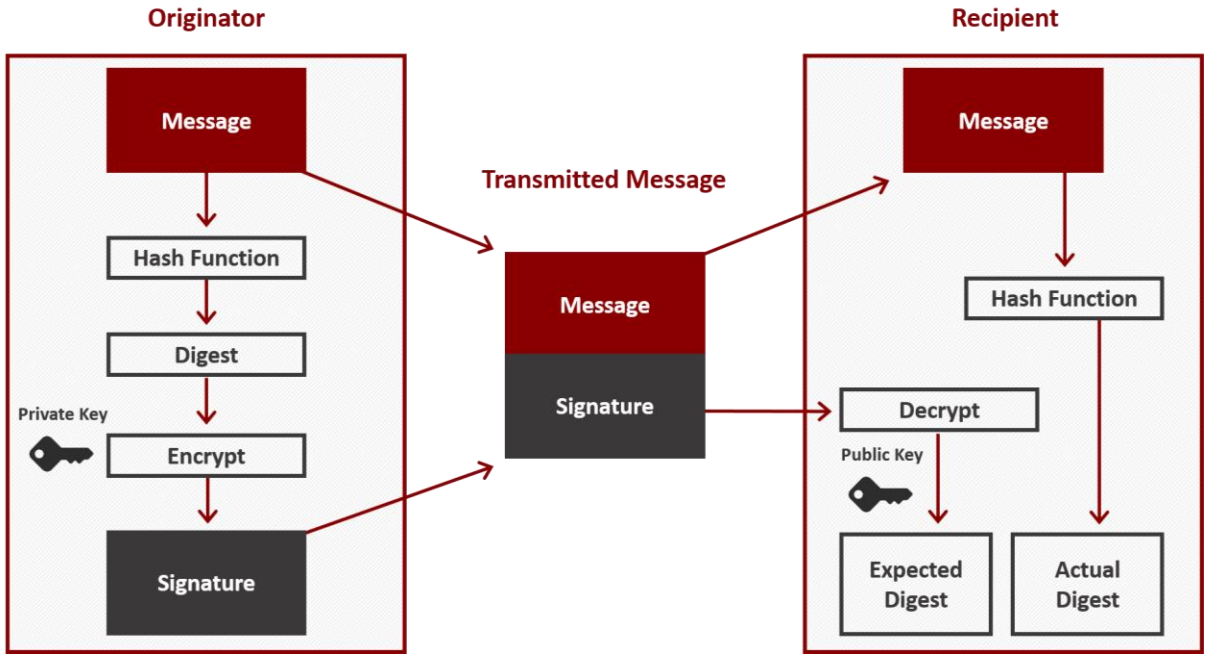
FUTUREX'S ENTERPRISE CERTIFICATE AUTHORITY

Digital communication is a staple of the modern business world, and as such, that communication often involves sensitive data. Businesses must protect this data by building a strong framework for safe communication, typically through building and expanding a robust public key infrastructure (PKI) to secure devices, documents, emails, and users. The KMES Series 3 does just this, serving organizations as an Enterprise Certificate Authority. This whitepaper will review several applications of the KMES Series 3 and will describe, in depth, the diverse functionality and integration capabilities of a PKI infrastructure built with Futurex technology. This includes a wide-ranging number of use cases including: certificate management, Certificate/CA Management, the Certificate Lifecycle, Windows Client Certificate Enrollment (WCCE), Registration Authority (RA), OCSP/Online CRL, SCEP, Authentication (Local, LDAP), Automation, Third Party CA Integration, and more, which can all be implemented with the Futurex KMES Series 3.

CERTIFICATE/CA MANAGEMENT

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 is capable of managing entire trees of keys, along with the certificates which validate those keys. The root of the certificate tree 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.

FUTUREX KMES SERIES 3 HSM

Certificates add validity to a trove of critical organizational structures, procedures, and information. As such, protecting this infrastructure is essential. The KMES Series 3 is Futurex's enterprise certificate authority solution, giving organizations a cryptographic solution for managing high volumes of symmetric and asymmetric keys across every step of the key management and certificate management lifecycle. The KMES is compliant with all major security standards for HSMs, including PCI HSM and FIPS 140-2 Level 3. The KMES Series 3 is powered by a high performance cryptographic module and has the capability to rapidly generate tokens through its easy-to-use interface and REST API. The process of creating tokens can be fully automated, so once the functionality is set up within the host system, an organization can be on its way to secure data storage and reduced PCI compliance scope and cost.

CERTIFICATE AUTHORITY CAPABILITIES

It is recommended that organizations who elect a self-managed PKI support a hierarchical PKI deployment. This is recommended for a number of security reasons and allows organizations to more easily expand the infrastructure to support additional scenarios or use-cases in future projects and deployments.

The hierarchical PKI deployment most commonly consists of the Offline Root CA and Issuing CA(s). This hierarchy increases security because roles are separated, allowing the private key of the Root CA to be better protected. Because the KMES Series 3 is a turnkey solution, it can take on either of these roles through the management of certificate trees, individual certificates, private keys, signing requests, and more through import, export, generation, tracking, storage, and revocation.

OFFLINE ROOT CERTIFICATE AUTHORITY

The Offline Root serves as the trusted anchor for the entire system. The Offline Root CA is the foundation of the entire PKI infrastructure and as such, the consequences of a *compromised* root CA is astronomical.

The security and integrity of this system is commonly ensured by keeping the unit in an offline state with no network connectivity. When the KMES Series 3 is used as an offline root, it is only brought online to complete very infrequent, and very specific tasks, such as signing an intermediate CA or issuing CA. In the interim, the device is powered-off, and stored in a secured, access-controlled environment.

ISSUING CERTIFICATE AUTHORITY

Issuing CAs are the lower tier of the hierarchical PKI deployment. Issuing CAs are subordinate to the Root CA, but are much more flexible. They can exist for different organizational or project silos, in different geographic regions, and with unique security levels in a more manageable environment. The issuing CA is used to provide certificates to applications, users, devices (i.e. phones, computers, etc.), and more. and other services. The KMES Series 3 is built for complete lifecycle management to meet this use case, in addition to integrating with or serving as a dedicated registration authority.

Futurex also integrates with other certificate management tools, helping to guard against key compromise, reduce fraud risk, and protect insider attacks. For example, the KMES Series 3 integrates with Venafi's Trust Protection Platform, enabling enterprises to expand Machine Identity Protection with secure key generation and storage and integrated private PKI with FIPS 140-2 Level 3-validated HSMs.

USB BACKUP HSM

Back-ups are important for any data security infrastructure, but with critical PKI infrastructures it is essential. Integrating directly with the KMES Series 3, Futurex offers a small, form-factor USB Backup HSM to store Futurex device backups on-premises or remotely, with a FIPS 140-2 Level 3 validated USB device.

The device is a software-free, 100% hardware-based 256-bit AES XTS encrypted USB key, with onboard keypad PIN authentication and ultra-fast USB 3.1 (3.0) data transfer speeds. Equipped with on-the-fly encryption, PINs and other important data remain encrypted while the drive is at rest. Meanwhile, device backups stored on the device are double-encrypted using source and USB HSM keys plus multi-user authentication. Secured with a passcode number pad, the FIPS 140-2 Level 3 validated USB device can be directly connected to the KMES Series 3 to take and restore back-ups and can be securely stored in a safe when not in use.

FINANCIAL CERTIFICATE AUTHORITIES

The Futurex KMES Series 3 also supports non-X509 certificates, also known as the EMV standard. The EMV secure payment process is possible entirely through a cryptographic microchip embedded directly into the card. EMV-enabled smart cards support public key infrastructure (PKI), a two-key encryption system that provides trusted authentication for objects such as devices, users, documents, and more. When the card is activated for a payment transaction, the Point-of-Sale terminal issues a command to the chip embedded in the card, requesting verification that the transaction is authentic. The card uses an HSM to process validation using secured PKI information, and that response is sent back to the reader. To set up the PKI that will allow EMV transactions to occur, the KMES Series 3 can be used to generate, store, and manage the public and private keys that encompass this process.

The EMV Certificate Authority and Issuer certificates work with the banks, the issuers, and the acquirers to validate EMV transactions at the Point-of-Sale terminal. The KMES Series 3 supports generating EMV certificates for all major card brands, including American Express, Japan Credit Bureau (JCB), Mastercard, and Visa. Any issuer, or an organization that provides services on behalf of an issuer, can use the KMES Series 3 to securely generate and manage EMV certificates to implement an EMV certificate authority, with PKCS#7, EMV, ISO Formats, and more.

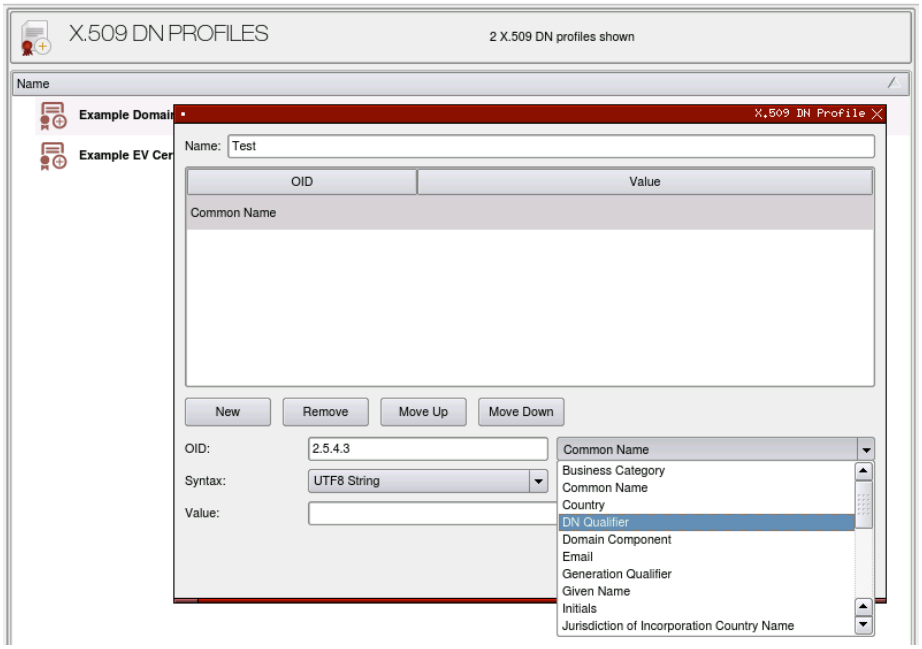
CERTIFICATE LIFECYCLE

X.509 PROFILES

X.509 public key certificate standards include a number of fields that are identifiable within a certificate. These fields make up the X.509 profile and include: the version, serial number, signature algorithm identifier, issuer name, validity period, subject name, public key information, issuer ID, subject, ID, and extensions. The CA will refer to these fields to confirm the validity of incoming certificates and certificate requests. Futurex contains these standard profile descriptors, and more.

DOMAIN NAME PROFILES

The KMES Series 3 also enables users to create and manage X.509 domain name profiles through an easy to use interface. These profiles operate as a subnet and identifies authority within an organization. Through the KMES Series 3, users can set up these profiles and customize features such as the object identifier (OID), syntax, and value.



WINDOWS CLIENT CERTIFICATE ENROLLMENT (WCCE)

The Windows Client Certificate Enrollment (WCCE) protocol was built by Microsoft to perform a variety of tasks which integrate directly with widely used Active Directory services. This protocol allows users to manage their X.509 certificates and request tasks from a certificate authority, including full certificate management in regard to certificate enrollment, issuance, revocation, and deletion. In dealing with a PKI to manage these keys and certificates, this protocol also complies with X.509 recommendations and standards for storage and complete certificate lifecycle management.

In a typical non-Futurex environment structure, a computer will reach out to an active directory server to pull the certificates needed for user management. This leaves these certificates vulnerable to attack, as the certificates are more easily assessable to manipulation or fraud by outside parties or threatening technologies. If a certificate authority is compromised, the validity of every single certificate and every single item previously validated will be questioned. It is not an understatement to suggest that a poorly secured PKI is completely detrimental to the security of an organization.

In a Futurex environment, the Windows client will, again, request a certificate from its Windows server as expected. However, this is where the process differs. The windows server connects using PKI authentication, issuing software (PKCS12) or hardware (PKCS11 tokens) to complete the PKI structure. This allows the Windows Server to connect to the Host-API port. It will then forward those certificate requests to the KMES Series 3 HSM, which will validate that request within the boundaries of the cryptographically secure machine. The KMES Series 3 allows the creation of user groups that require only one login, creates users for the Windows Server in that group, assigns the TLS PKI certificates to the user for PKI authentication, and lastly, gives that user's group use permission over the CA certificate(s) with the WCCE issuance policy. The KMES Series 3 issues the certificate, in addition to managing the entire lifecycle of the certificate, including generation, distribution, revocation, and expiration.

AUTOENROLLMENT

Another common use case of WCCE is autoenrollment. This is easily configured via the KMES Series 3. Futurex has developed a proxy installer which connects the windows server to the KMES Series 3, essentially enabling the autoenrollment WCCE command. Simply enable both the WCCE feature and command, and then configure an issuance policy for the specific type of certificate. The default of this issuance policy can be set to "autoenrollment" to allow enrollment of client computers under a windows domain. Joining a client on the domain will trigger autoenrollment and clients already on the domain already have a workstation certificate enrolled.

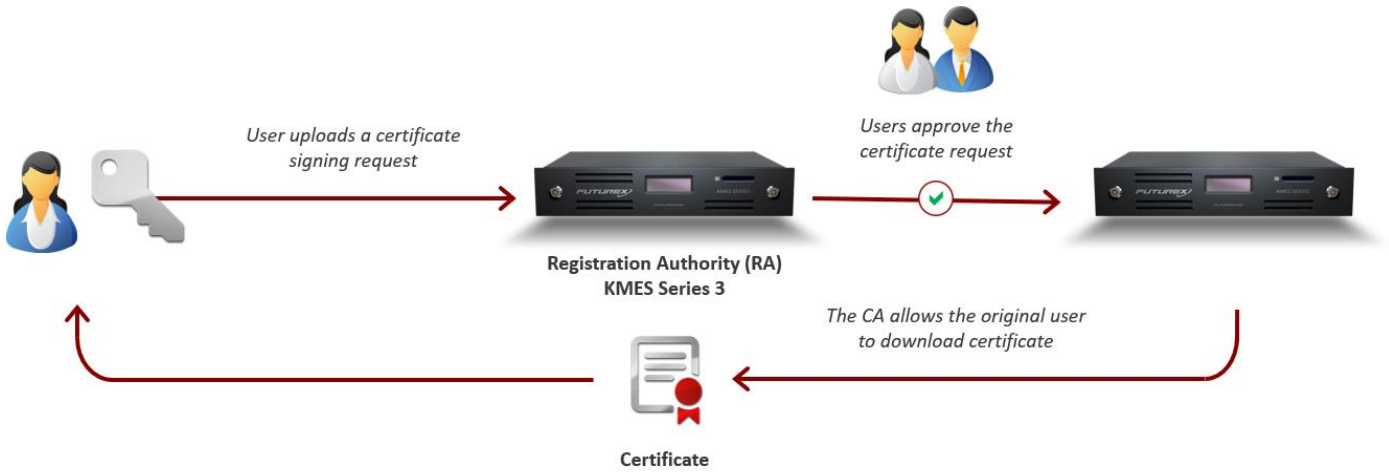
WCCE also handles enrollments that require approvals. This is done by creating a new PKI Template for certificates that require approvals and adding it to the issuance policy WCCE. The enrollment will be pending until it gets approved. Also, each certificate request is assigned a unique ID, under the approval group on the KMES. This ID is needed to check the enrollment state on the client machine. Then the administrator can approve the request via the KMES Series 3.

REGISTRATION AUTHORITY (RA)

As discussed throughout this whitepaper, a PKI is a system of people, processes, and technologies used to manage, create, and revoke digital certificates. This allows multiple users to communicate privately, even on a public network. A registration authority (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 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 user's identity is validated using information stored within the CSR, including the user's public key and X.509 profile, as detailed previously in this whitepaper. Based on this information the CA will validate the user's identity, create a digital certificate with the user's public key, sign the certificate with the user's private key, and return the signed certificate to the user, 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.

HOW FUTUREX RA FUNCTIONALITY IS ACCESSED

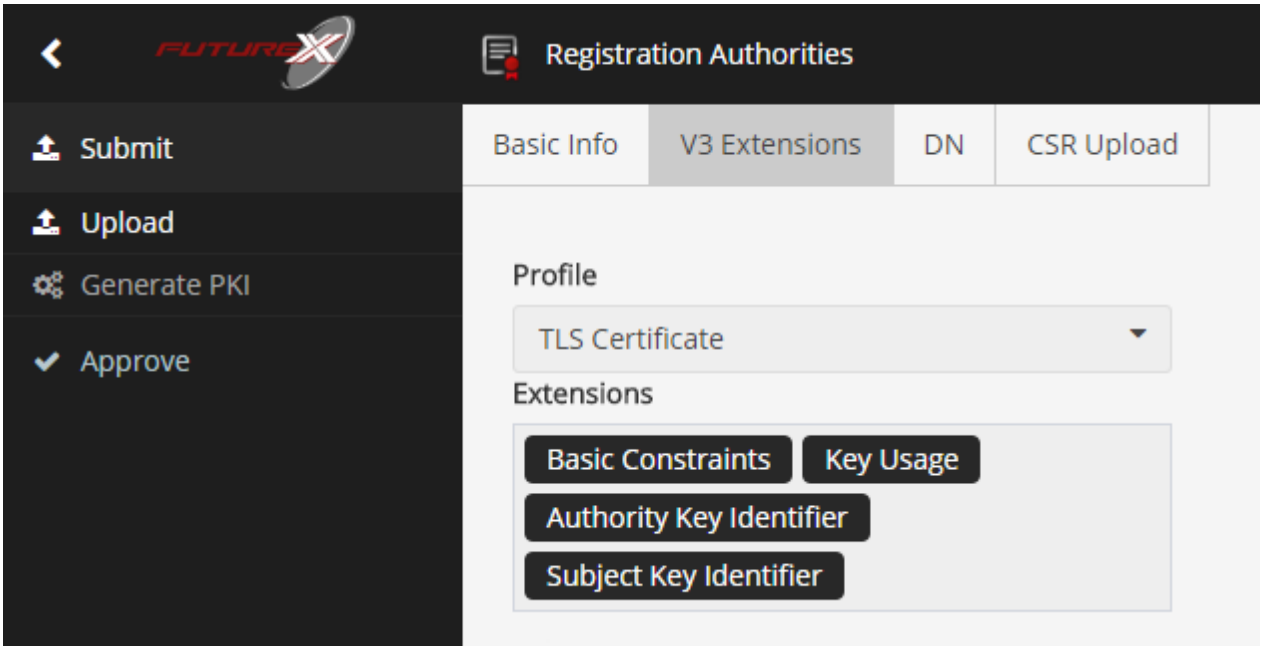
Futurex leverages RA functionality across multiple channels, including through a GUI, an API command set, and a secure web portal. All three options are intended to provide convenience and ease of use for the end user.

GUI:

Through the client GUI, users can leverage full control of RA functionality. From this tab, users can create, edit, delete, and filter registration authorities; or users could create, edit, delete, revoke, approve, deny, or renew certificate signing requests. Users can anonymously add certificate requests, making it easier for large organizations who do not have the time to create a user account for each user needing to upload CSRs. Additionally, users can oversee every aspect of X.509 extension profiles through creating, modifying, and applying templates. Once certificates have been signed, users can download them as .pem or .der files.

WEB SERVER:

This web portal is accessible from virtually anywhere, so long as there is an internet connection. This is especially beneficial for large organizations because administrators can be assigned to the RA without needing direct access to the HSM. Once two administrators have logged in, the portal is an easy to use web service where one can upload, submit, approve, or deny CSRs. Once the CSRs have been signed, the certificate is returned to the user who can then download the associated certificates, as shown in the prior diagram. Users can also anonymously upload certificate signing requests through the web portal.



API COMMANDS:

A complete set of API commands allows users to manage RAs, X.509 templates, and CSRs. The commands are provided through a technical reference that gives further details and examples of command usage.

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 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.

OCSP/ONLINE CRL

Part of the certificate lifecycle is the revocation of certificates. Revocation or deletion of certificates, prior to their expiration date, is necessary for a number of reasons: if a certificate is compromised, if user privileges change, if there is a cease of operations, among other reasons. A certificate authority manages this process through certificate revocation lists, commonly known as CRLs. A CRL contains information about the associated certificate that needs to be removed. An administrator must then regularly manage, review, and enforce the revocation of certificates on this list, to maintain a secure and up-to-date certificate environment.

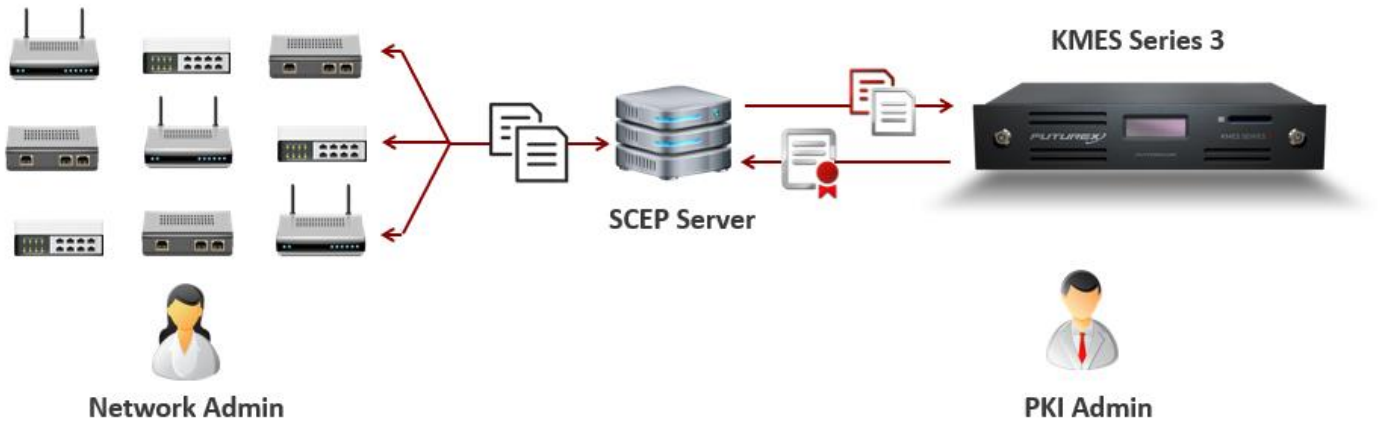
A common alternative to manually reviewing CRLs is through the Online Certificate Status Protocol (OSCP). OSCP is a web-based protocol, typically used over HTTP, which helps to manage CRLs and revoke private keys and certificates in real time. OCSP addresses latency issues associated with the traditional issuing and processing of CRLs. CRLs require administrators to manually check certificates and private keys for revocation. For example, if an employee quits and needs their private keys to be invalidated, their private key would remain in place until the pre-scheduled time that the CRL is pulled and processed by an administrator. OSCP however, operates through HTTP allowing CRLs to be

pulled almost instantaneously with the entire revocation process completed with almost immediate effect (or at least much quicker than traditional CRLs). OCSP responses contain less data than the typical CRL, meaning there is less data to parse through and the request can be processed much quicker because of this. Futurex's enterprise CA offering integrates with this protocol, offering customers essential security, ease of use, and agility in their enterprise CA environment.

OSCP must communicate with a 3rd party to confirm certificate validity and unfortunately this can leave organizations exposed to attack or interference. If the OCSP server is not cryptographically protected there is no way to ensure that the HTTP server key is compromised, leaving organizations vulnerable to replay/playback attacks or other interference by malicious outside parties. Managing this process through the KMES Series 3 eliminates this concern, because instead of communicating with a 3rd party, certificate validation and processing occurs within the cryptographic boundary of the HSM. The diagram below depicts this process both with and without hardened cryptography:

SIMPLE CERTIFICATE ENROLLMENT PROTOCOL (SCEP)

With an enterprise CA being such a critical (and large) infrastructure for organizations, organizations are constantly looking for ways to simplify and streamline the certificate and key management process- with one popular integration being with the Simple Certificate Enrollment Protocol (SCEP). SCEP was designed by CISCO to get certificates onto a router or network switch. Most network switches do not have a documented identity that a CA can understand, process, or read. To address this, a SCEP server sits between the endpoint and the CA. The SCEP server requests a one-time password from the router, translates it into a format readable for the CA, and sends it to the CA for validation and certificate generation. The SCEP server then compares the one-time password from the unauthenticated side with the password issued from the trusted CA. This removes the manual translation of this information by a network administrator. Also, the KMES Series 3 requires that 2 administrators log into its CA system to approve the certificate issuance. These certificates give "permission" for the switch to be on the network.



Unfortunately, SCEP gained notoriety due to a major vulnerability which was announced in 2012, VU#971035. This notice states that "SCEP does not strongly authenticate certificate requests made by users or devices," particularly as it relates to bring your own device (BYOD) technologies such as mobile phones or laptops. Integrating Futurex's enterprise CA platform into one's environment helps address this vulnerability and allows organizations to maintain the benefits of scalable and simple operations.

THIRD PARTY CERTIFICATE AUTHORITY INTEGRATION

Futurex supports the orchestration of certificate deployment both through the KMES Series 3 as a certificate authority, and also through integrations with external certificate authorities. The primary purpose of these integrations is to incorporate third-party certificate authorities with a FIPS 140-2, Level 3, PCI-validated platform. This provides organizations the ability to generate self-signed certificates or their own root CAs, while also importing third party CAs.

The integration of third party CAs are managed through the registration authority process. As detailed earlier in this whitepaper, registration authorities (RAs) approve and deny requests for certificates, also known as certificate signing requests (CSRs). The RA presides over and assists the Certificate Authorities (CAs) by informing them of which certificates can be issued. Upon approving a CSR, the RA has validated the identity and registration information of the user, and permitted the CA to issue a certificate.

Integrating with third-party certificate authorities offers a number of key benefits, including the ability to:

- Automatically download successfully signed requests submitted by the RA
- Utilize Futurex approval requirements
- Revoke signed requests from the RA
- Resign requests from the RA
- Cancel pending orders
- Utilize rate limiting mechanisms

Cloud Credentials are used to allow the KMES Series 3 device to interface with third party services. The Cloud Credentials menu on the KMES Series 3 stores the imported API Key that authenticates the KMES Series 3 to the third-party service.

Enterprise Certificate Authority – What it can do for your organization?

An enterprise certificate authority can completely transform the way your organization processes and protects its critical information and infrastructures. This whitepaper reviews several KMES Series 3 use-cases, ranging from Certificate Authority Capabilities, Certificate Lifecycles, WCCE, Registration Authority, OCSP/Online CRL, SCEP, Third Party Integrations, and more. Futurex is available to answer any questions that you may have, discuss integration capabilities, or to provide a demonstration of the KMES Series 3 at any time.

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