Solution Brief

appviewX

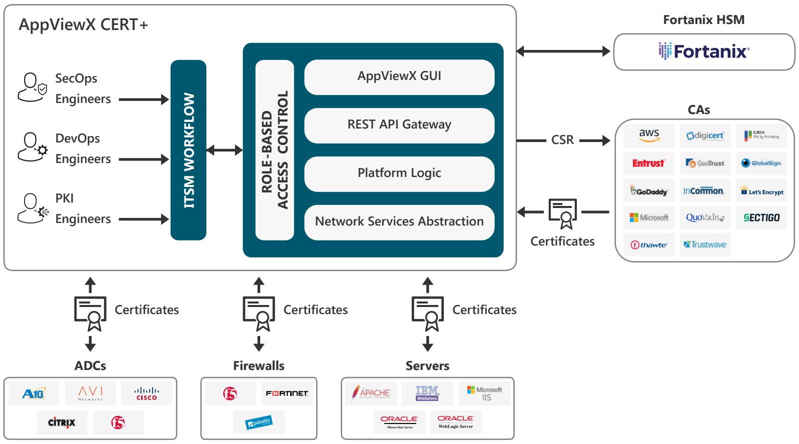
Automating Certificate Management and Secure Key Orchestration with Fortanix and AppViewX

Business Case

Public Key Infrastructure (PKI) has become standard for enterprises trying to secure data and authenticate machines on the move. X.509 certificates, often leveraged in the form of SSL/TLS certificates, are just one of the many PKI systems widely adopted by enterprises. All these systems operate on the principle of private and public encryption keys, which are used to encrypt and decrypt information flows respectively. This makes a private key the single most important asset of any security infrastructure. When a private key is uncovered by malicious actors, valuable data is compromised through the impersonation of an enterprise’s servers. And unfortunately, many enterprises are still using faulty, and often non-compliant key management processes that leave their most valuable data susceptible to theft and misappropriation. There is a need for certificate management systems that integrate with key security structures such as HSMs, in order to ensure that key circulation remains a closed-loop process.

AppViewX - Fortanix Joint Solution

The partnership between AppViewX and Fortanix helps enterprises overcome the challenges brought by managing private keys in a complex infrastructure. For enhanced security and compliance, private keys must be encrypted before they are stored in an enterprise’s infrastructure. Our combined solution gives the enterprise multiple options that cater to the specific needs of that infrastructure. AppViewX acts as the automation and orchestration engine for the lifecycle management of X.509 certificates, and Fortanix Self-defending KMS ensures the security of the private keys associated with those certificates in the cloud, on-premises or as a hybrid solution.



Fortanix

Challenge

Private keys are the most important assets in any network infrastructure, and the valuable data they safeguard can be compromised if they fall into the wrong hands. However, current management practices do not provide the protection demanded by these keys.

Solution

The AppViewX and Fortanix joint solution provides a single-pane-of-glass for managing, automating and protecting certificates and their keys. It combines AppViewX's certificate management suite with Fortanix HSM’s capabilities, allowing enterprises to harness unparalleled efficiency in key security and orchestration.

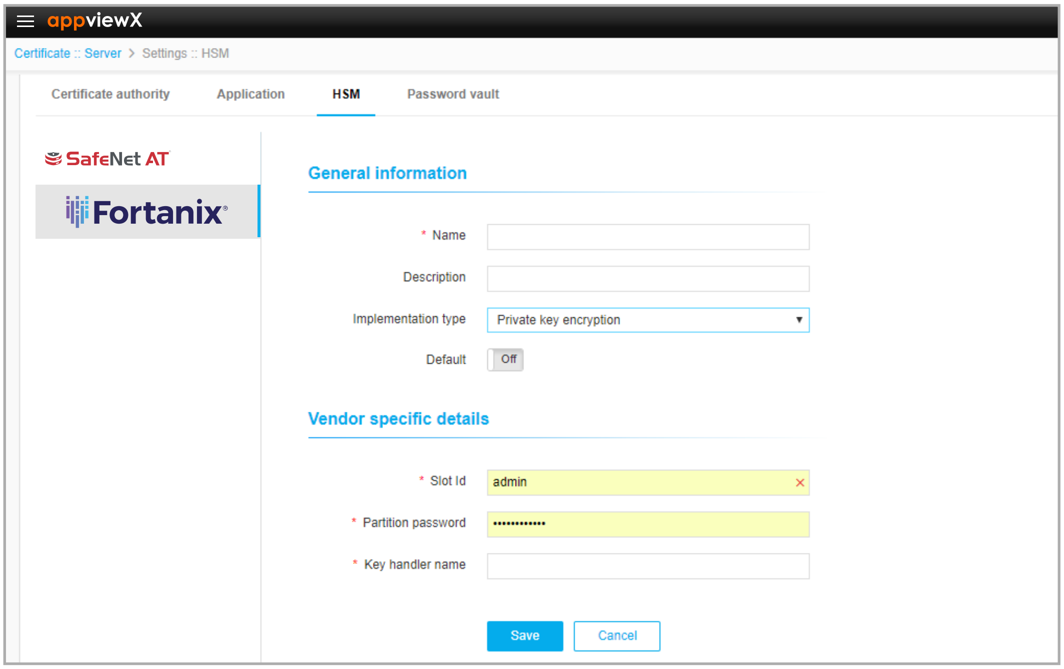
Benefits

- Encrypt and protect private keys using industry-standard, FIPS 140-2 certified HSMs with the flexibility of either on-premise or cloud-based services.
- Manage and automate multi-vendor X.509 certificates across multiple devices
- Gain visibility and control across all certificates and its keys
- Enforce policies and ensure compliance across the network
- Deliver secure, encrypted communications faster by reducing certificate deployment time by up to 70%

Solution Highlights

Certificate Management with Encrypted Private Key Storage in AppViewX

This solution is useful for enterprises seeking to generate and store private keys within AppViewX and limit their encryption to the Fortanix Self-defending KMS for optimum resource utilization – this is accomplished via Transparent Data Encryption (TDE). Before being stored in an AES-256 encrypted database, the private keys undergo multiple layers of encryption by Data Encryption Key (DEK), Key Encryption Key (KEK) and Master Encryption Key (MEK). While the encrypted private key, encrypted DEK, and encrypted KEK reside inside AppViewX, the MEK is stored inside the HSM and cannot be retrieved. Furthermore, the keys are securely backed up in a FIPS 140-2 Level 3 Fortanix HSM. This solution is suitable for all ADC and server devices.



General information

* Name:
Description:
Implementation type: Private key encryption
Default: Off

Vendor specific details

* Slot Id: admin
* Partition password: ••••••••••••
* Key handler name:

Figure 2 : Private Key Encryption Setup Screenshot

AppViewX provides a single pane of glass for managing and automating multi-vendor X.509 certificates on multiple devices. Once the AppViewX instance is up and running, the user opens the Settings page and inputs the HSM details. The implementation type is then set to “Private Key Encryption” to limit the utilization of HSM accordingly. After the configuration, the HSM is triggered to generate the Master Encryption Key (MEK) and designates a key handler to uniquely identify this key. From that point forward, every encryption/decryption request to the HSM is sent along with its corresponding handler. Next, a Key Encryption Key (KEK) is randomly generated within AppViewX and is encrypted with the MEK. Whenever a new CSR is generated within the platform, the associated private key is immediately encrypted with another randomly generated, unique Date Encryption Key (DEK). And, in the final layer of protection, this DEK is encrypted again with the KEK.

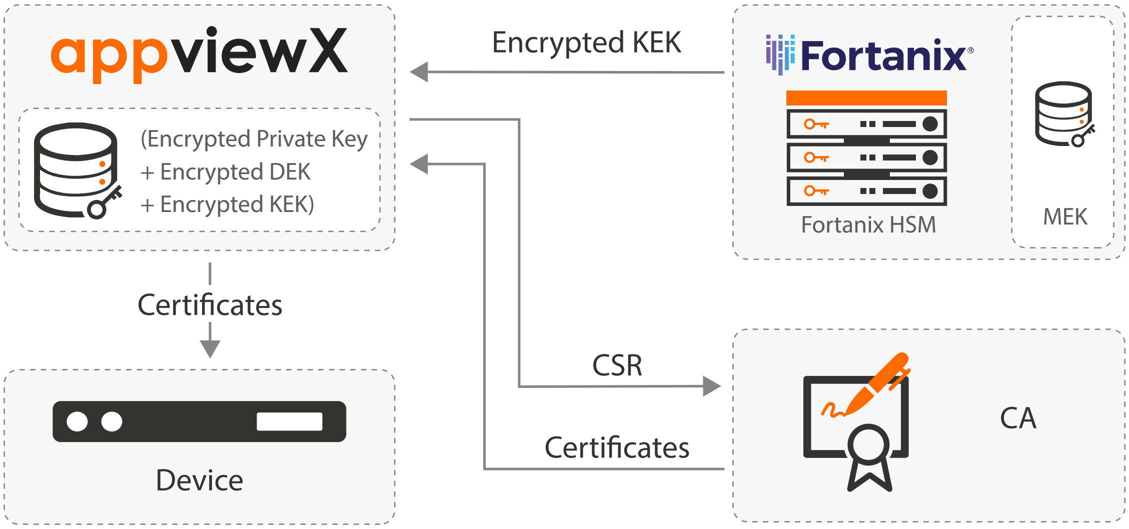
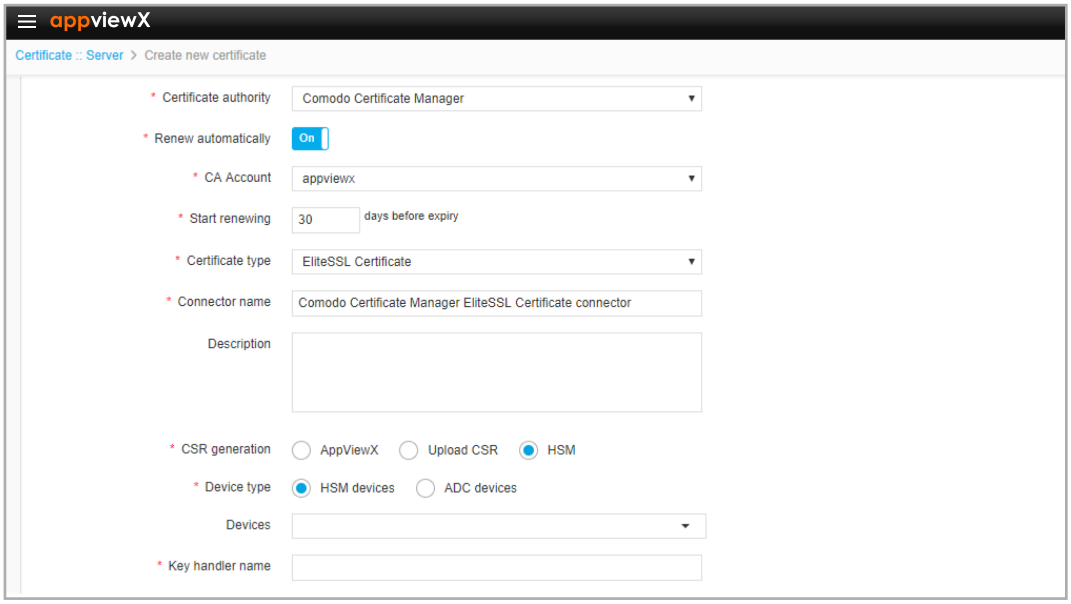


Figure 3 : HSM Private Key Encryption Workflow

Certificate Management in AppViewX and Private Key Storage in Fortanix

Enterprises can use this solution to assign AppViewX to certificate management activities while the HSM is used to both generate and store private keys in the name of added security. The private key generated using the Fortanix HSM cannot be removed and is completely shielded from tampering. This particular solution is suitable for all supported devices that can initiate direct communication with the HSM and use a key identifier to access private keys.



* Certificate authority	Comodo Certificate Manager ▾
* Renew automatically	On
* CA Account	appviewx ▾
* Start renewing	30 days before expiry
* Certificate type	EliteSSL Certificate ▾
* Connector name	Comodo Certificate Manager EliteSSL Certificate connector
Description	
* CSR generation	○ AppViewX ○ Upload CSR ● HSM
* Device type	● HSM devices ○ ADC devices
Devices	▾
* Key handler name	

Figure 4 : CSR Generation Setup Screenshot

In this scenario, AppViewX maintains the single pane of glass that can be used to manage and automate multi-vendor X.509 certificates. Once the AppViewX instance is up and running, the user opens the Settings page and inputs the HSM details. The implementation type is then set to “CSR Generation”, to use the HSM for generating the private key. After the configuration, the platform passes CSR parameters to the HSM to generate the corresponding CSR file as well as a unique key identifier that will be used to identify the private key used to sign it. The CSR file and the key identifier are then sent back to AppViewX for use in additional certificate-related operations. Whenever a new certificate is required to be pushed to a device, the key identifier is also sent with it. This step in the process helps devices identify the corresponding private keys from HSMs.

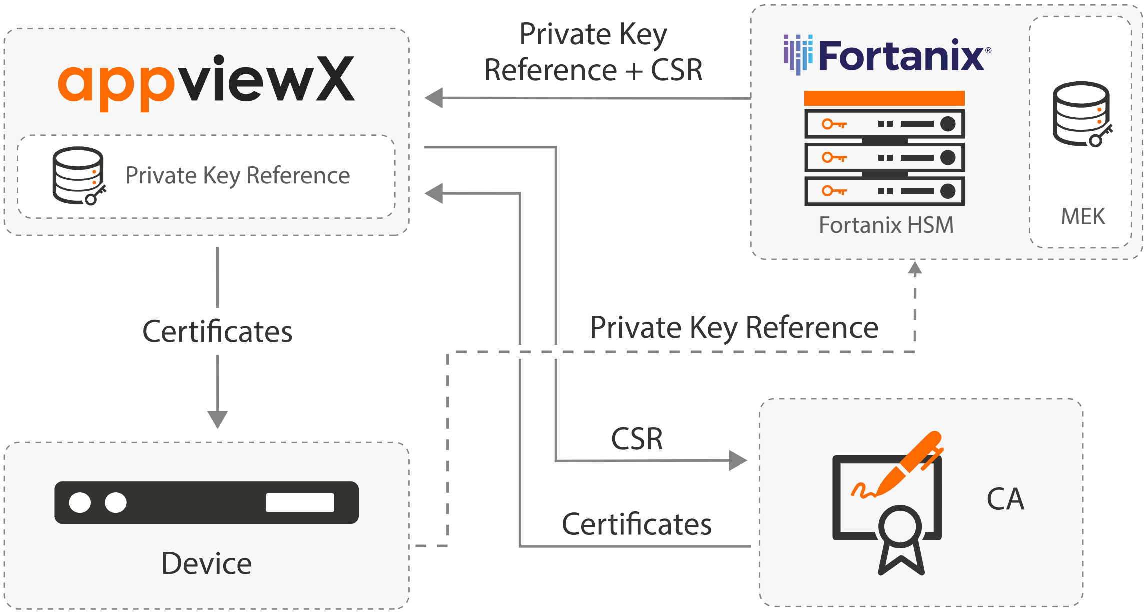


Figure 5 : HSM CSR Generation Workflow

Comprehensive Role-based Access Control

The first step in any access control process is having complete visibility into your certificate ecosystem. Sifting through the thousands of certificates in your inventory can be cumbersome. With our holistic view, CERT+ graphically represents important certificate information like chain of trust, associated devices and HSM. Users can also perform necessary lifecycle management tasks like issuing, renewing and revoking multiple certificates all within the holistic view itself.

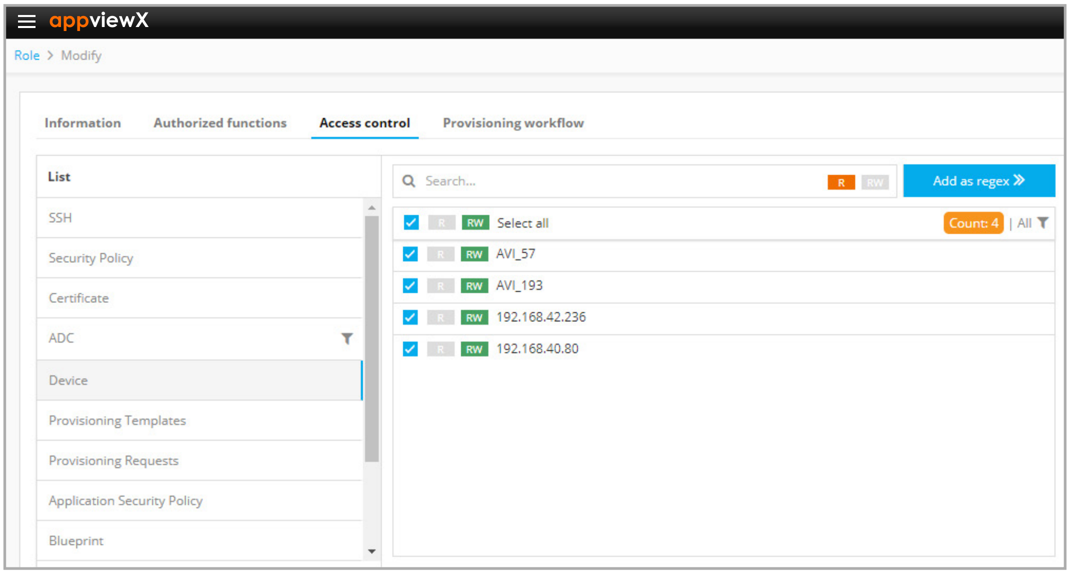


Figure 6 : Role-Based Access Control

While maintaining visibility can help to identify threats early, weak certificates and unregulated access can still compromise the security of your application infrastructure. With AppViewX, users can easily administer policies – such as recommended cryptographic techniques, CAs and workflows – to eliminate rogue certificates. Users can delegate access and apply granular visibility to either individual certificates or entire certificate groups to enable efficient provisioning. The certificates can then be grouped based on functionality or by their underlying policy group, all while being efficiently audited to ensure compliance.

Summary

Digital certificates are the face of your enterprise online. Given the high level of security associated with PKI technology, the need for digital certificates is only going to increase. This will inevitably leave enterprises with an abundance of private keys to safeguard and without an efficient mechanism to safeguard them with. Using the AppViewX and Fortanix joint solution, enterprises can apply the visibility and security that their private keys and certificates demand, all while maintaining the agility and compliance needed to adapt to rapidly changing business needs. By leveraging the full-cycle certificate management suite of AppViewX and the key security capabilities of Fortanix Self-defending KMS, enterprises can maximize the efficiency of their certificate and key management programs while protecting keys from theft or misuse.

Next Steps

To learn more about this joint solution,

visit **appviewx.com/partners/technology-integrations/** or **fortanix.com/partners/**

Get more information about individual product lines here:

AppViewX CERT+ | **Fortanix Self-defending KMS**

About AppViewX

AppViewX is revolutionizing the way DevSecOps and NetOps teams deliver services to enterprise IT. The AppViewX platform is a modular, low-code software application that enables the automation and orchestration of enterprise network infrastructure and certificate management using an intuitive, context-aware visual workflow. It is built to rapidly enable users to implement cryptto-agility, enforce compliance, eliminate errors, and reduce cost. AppViewX is headquartered in New York City with additional offices in the US, UK, and India.
To know more, visit **www.appviewx.com** or **info@appviewx.com**