appviewX

Certificate Management and Secure Key Orchestration with Thales and AppViewX

The Challenge

Public key infrastructure (PKI) has become standard for enterprises trying to secure data and authenticate machines on the move. X.509 certificates, such as TLS, are just one of the many PKI systems widely adopted by enterprises, all of which include both private and public keys. The public key, as the name suggests, is open to public data encryption, while the private keys are kept confidential for decryption purposes. This makes a private key the single most important asset of any 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 – manual key management processes that leave their most valuable data susceptible to theft.

AppViewX - Thales Joint Solution

AppViewX and Thales's partnership 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 Thales Data Protection On Demand (DPoD) Cloud HSM or Luna HSM ensures the security of the private keys associated with those certificates in the cloud, on-premises or as a hybrid solution.

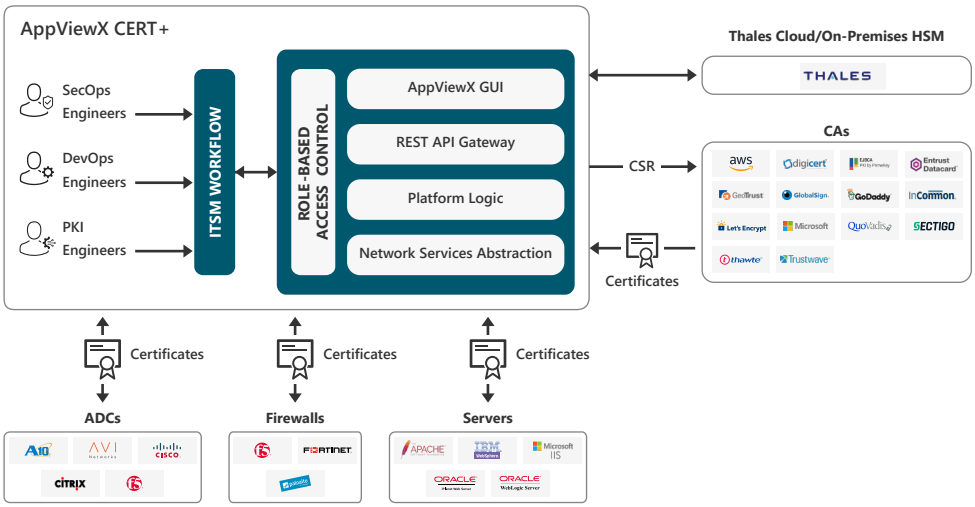

Figure 1 : AppViewX – Thales Integration Overview

THALES

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 Thales 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 Thales 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 Level 3 certified HSMs with the flexibility of either on-premises 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 inside AppViewX and limit their encryption to the DPoD Cloud HSM service or on-premises Luna HSM for optimum resource utilization. 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. This solution is suitable for all ADC and server devices.

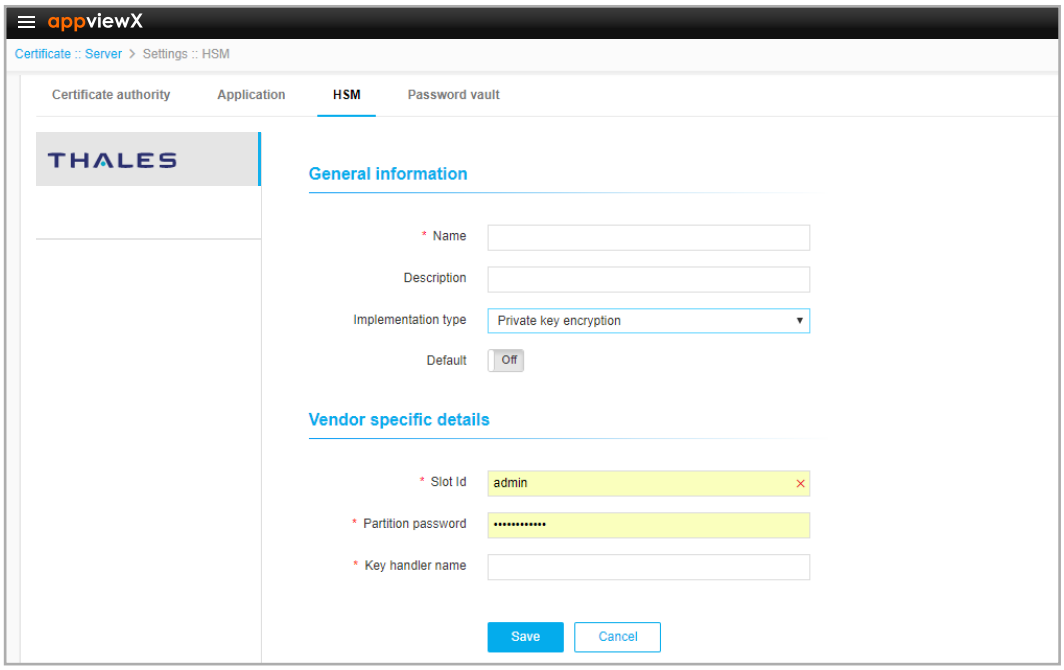

Figure 2 : Private Key Encryption Setup Screenshot

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.

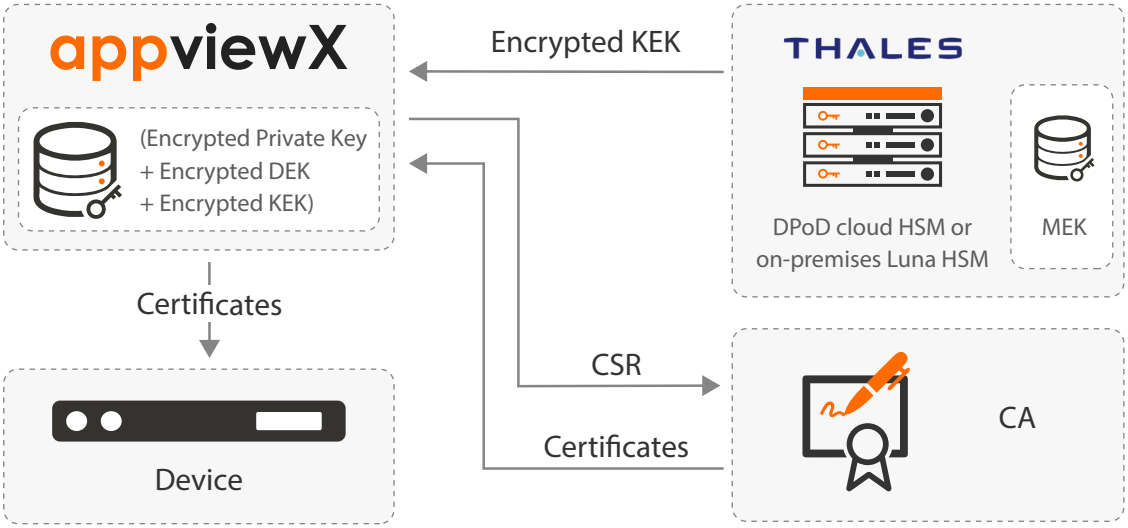

Figure 3 : HSM Private Key Encryption Workflow

Certificate Management in AppViewX and Private Key Storage in Thales

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 DPoD or Luna 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.

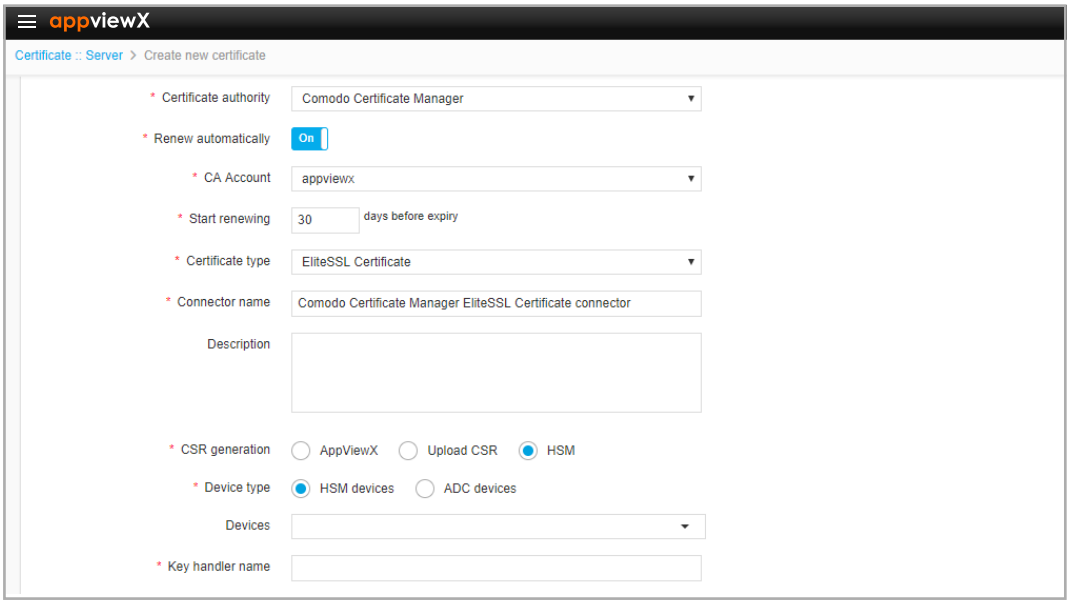

Figure 4 : CSR Generation Setup Screenshot

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.

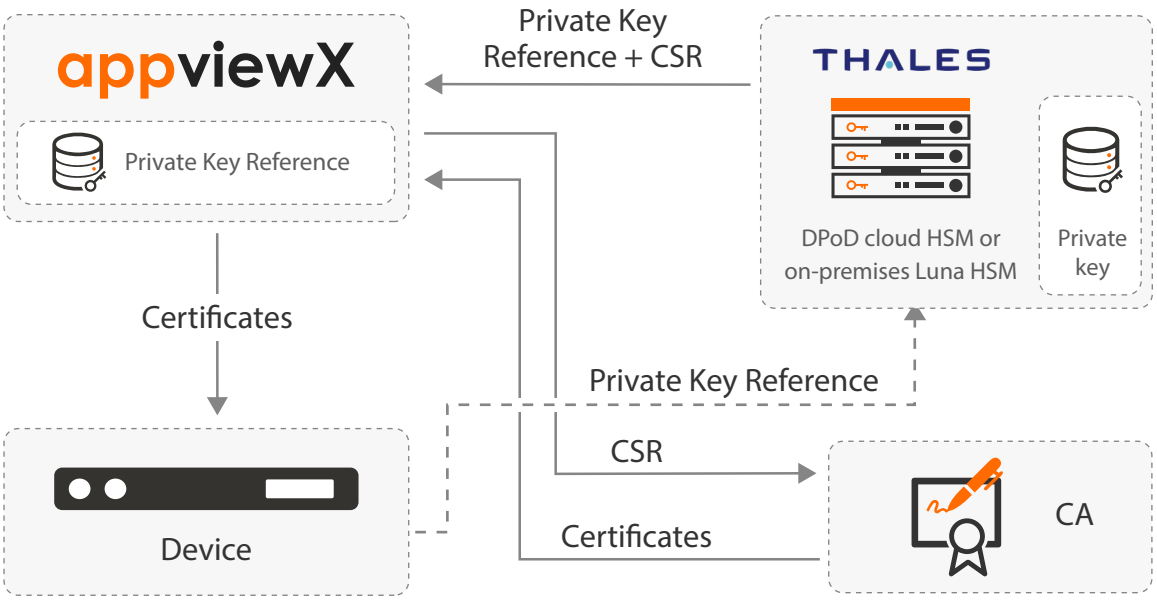

Figure 5 : HSM CSR Generation Workflow

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.

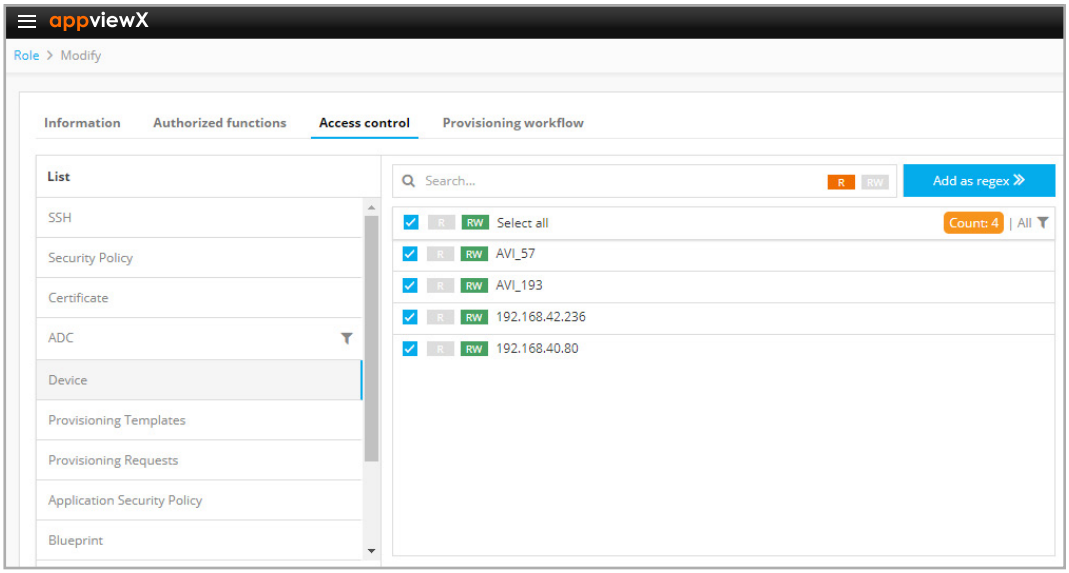

Figure 6 : Role-Based Access Control

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 AppViewX and Thales 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 answer to rapidly changing business needs. By leveraging the full-cycle certificate management suite of AppViewX and the cloud-based or on-premises Thales HSMs enterprises can maximize the efficiency of their certificate and key management programs.

Next Steps

To learn more about Thales and AppViewX joint solution,
visit www.appviewx.com or thalesesecurity.com/partners/technology-partners

Get more information about individual product lines here:

AppViewX CERT+ | Thales Luna HSM | Thales DPoD HSM

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

About AppViewX

AppViewX is revolutionizing the way NetOps and SecOps teams deliver services to Enterprise IT. The AppViewX Platform is a modular, low-code software application that enables the automation and orchestration of network infrastructure using an intuitive, context-aware, visual workflow. It quickly and easily translates business requirements into automation workflows that improve agility, enforce compliance, eliminate errors, and reduce cost. AppViewX is headquartered in Seattle with offices in the U.S., U.K., and India. To know more, visit **www.appviewx.com.**

AppViewX Inc.,
500 Yale Avenue North, Suite 100, Seattle, WA 98109

info@appviewx.com
www.appviewx.com

+1 (206) 207-7541
+44 (0) 203-514-2226