appviewX

Deploying and Managing Cloud PKI with Google Certificate Authority Service and AppViewX

Problem Statement

PKI has conventionally been the de-facto means by which digital identities and network communications are secured. Efforts are being continually made to simplify large-scale deployment and ease compatibility with modern paradigms like DevOps and the IoT. However, traditional PKI deployments that leverage on-premise private CAs have not evolved to meet the status quo – some major concerns surrounding them are:

- **Deployment**: Setting up, maintaining, and deploying certificates are all time-consuming tasks, courtesy of the complexity surrounding the configuration and operation of each instance.
- **Compatibility Issues**: Standard PKI processes do not work or scale well with use cases for IoT, DevOps, containerization etc.
- **Cloud Applications**: Conventional on-prem private PKI does not demonstrate ease of compatibility with cloud platforms, which might force teams to leverage insecure public CAs.
- **Cost and Expertise**: Teams require a high level of PKI expertise to set up and manage the infrastructure backend, while the complexity of the setup adds to maintenance costs.

Managed PKIs are considered an alternative to on-premise deployments, as they abstract the PKI backend. However, a lack of control over the infrastructure and private keys is a potential security risk that administrators might not be willing to take.

There is a pressing need for an easy-to-deploy PKI solution with low to zero maintenance requirements, that can be managed end-to-end by internal teams.

Google Cloud

Certificate Authority Service

Solution Highlights

- Rapidly create a private CA and start issuing certificates in bulk, with zero infrastructure setup required.
- Store keys in FIPS 140-2 (Level 3) certified cloud HSMs
- Manage end-to-end certificate lifecycles and execute tasks like discovery, renewal, revocation, and so on.
- Integrate with DevOps tools like Kubernetes, Istio, and Ansible to perform certificate tasks.
- Auto-enrol certificates on a range of endpoints using ACME, EST, and SCEP.

AppViewX-Google Cloud Platform Integrated Solutions

AppViewX has crafted an integrated solution, with Google Cloud Platform's Certificate Authority Service to fill the market gap outlined above: a need for easy PKI deployment and maintenance, end-to-end control of the certificates and keys, rapid upward scaling, and compatibility with modern technology.

Google Cloud Platform is globally trusted for its security, and provides the Certificate Authority Service: A highly scalable and available private CA that can rapidly issue certificates in bulk and securely facilitate key and certificate operations by integrating with FIPS-140-2 Level 3-compliant HSMs. It is also conducive to DevOps- and cloud-application use-cases by means of enabling easy integration via APIs and short-lived certificates. Teams can easily set up PKI from scratch since there is no infrastructure setup involved.

The AppViewX platform helps securely manage the certificates and keys involved in this deployment via its single-pane-of-glass management layer for key and certificate lifecycles. It simplifies certificate acquisition, renewal, revocation, and installation for the end-user by allowing one-click execution of these tasks – AppViewX supports industry-standard protocols like SCEP, ACME, and EST, which allow the user to auto-enrol Google-CA-issued certificates on endpoints. Furthermore, the reporting, analytics, and notification capabilities assist administrators in maintenance of certificate lifecycles. AppViewX also has the ability to act as a Registration Authority for certificates issued by the Google CA that would allow for the implementation of secure issuance policy across the board.

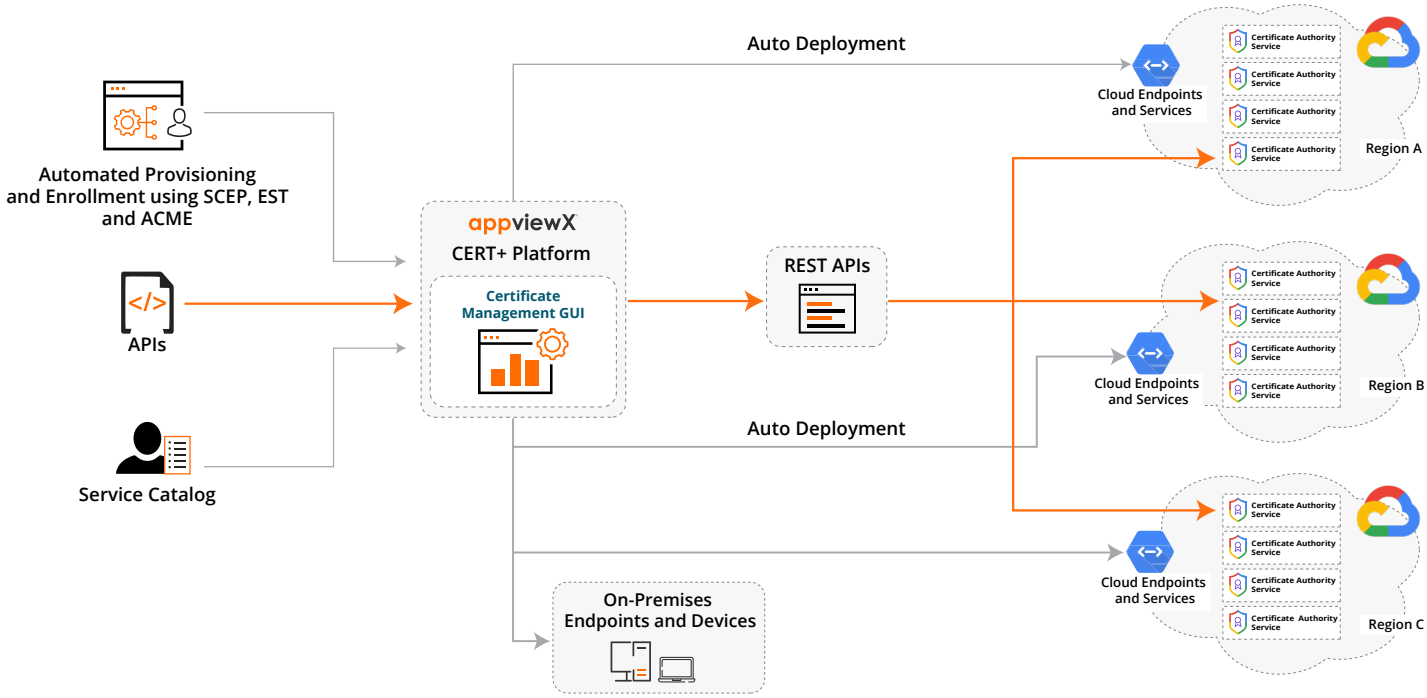

Diagram 1: Integration Overview

The integrated solution accomplishes the objective of making PKI easy to configure, deploy, and use, while also ensuring that the user retains complete control of their infrastructure and keys.

The benefits of being DevOps-, IoT-, and cloud-compatible notwithstanding, security teams can manage and monitor the entire PKI from within the AppViewX console. Teams looking to scale up their operations, minimize reliance on manpower to manage PKI, and optimize maintenance costs can realize significant benefits by migrating to the joint solution for PKI and certificate management.

Solution Highlights

PKI-as-a-Service

The Google Certificate Authority Service allows for the rapid creation of a custom private CA that can instantly start issuing high-volume certificates in bulk, with no infrastructure setup required. Private keys are stored in highly secure FIPS-140-2 (Level 3) certified cloud HSMs, and audit logs are available to gain full visibility into PKI modifications. The AppViewX platform can be used to automate key rotations as well.

Access control to the PKI can be implemented and enforced across the board, with both Google and AppViewX providing integrations with IAM services.

Certificate Lifecycle Management

Once the AppViewX platform is linked to Google Certificate Authority Service via an API-based connector, it becomes capable of accessing and executing all certificate issuance capabilities, renewals, revocations, and enrolment of new certificates. Hence, CERT+ acts as a Registration Authority with the requisite compliance policies, enabling users to manage the Google PKI from within the AppViewX platform. This simplifies the execution of issuance-related operations.

The following functions will be available to users once the integration is online:

- Discovery of certificates issued by Google Certificate Authority Service
- Discovery of certificates located on various endpoints
- Certificate Renewals
- Certificate Revocations
- Certificate Provisioning via Self-service
- Certificate Enrolment using Enrolment Protocols
- Reporting, Analytics, and Expiry Notifications
- Lifecycle Automation of DevOps certificates

Integration with DevOps tools

The AppViewX platform integrates with several DevOps and containerization tools to perform and automate certificate tasks:

- Deployment automation via Terraform, Ansible etc.
- Ingress certificate automation via Kubernetes, OpenShift etc.
- Service mesh security and east-west traffic security using mTLS via Istio

Import of Google Certificate Authority Service Certificates

AppViewX's discovery engine scans multi-cloud deployment environments to locate Google-issued certificates. These certificates are automatically mapped to the end-points they're tied to, and are presented in a AppViewX's Holistic View, featuring the CA, the certificate issued, and the end device that is leveraging the certificate. As part of the scanning process, all orphaned, stale, or unused certificates are reported.

Key Certificate Automation Use Cases

Auto-Enrolment of Certificates on Endpoints

AppViewX supports ACME, EST, and SCEP protocols for certificate auto-enrolment. AppViewX acts as the ACME/EST server to automate certificate enrolment from the Google Cloud issuance platform, onto a variety of endpoints. AppViewX automates the enrollment process for IoT devices by listening to the request generated by the IoT device, submitting the CSR, obtaining the certificate from the Google CA Service, and sending it to the IoT device while maintaining a copy of the certificate in its inventory.

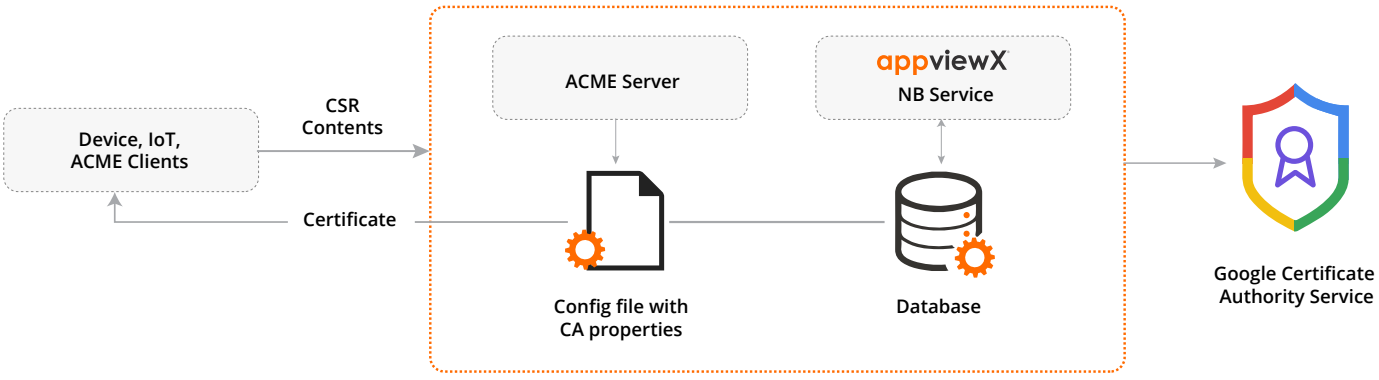

Diagram 2: ACME Support

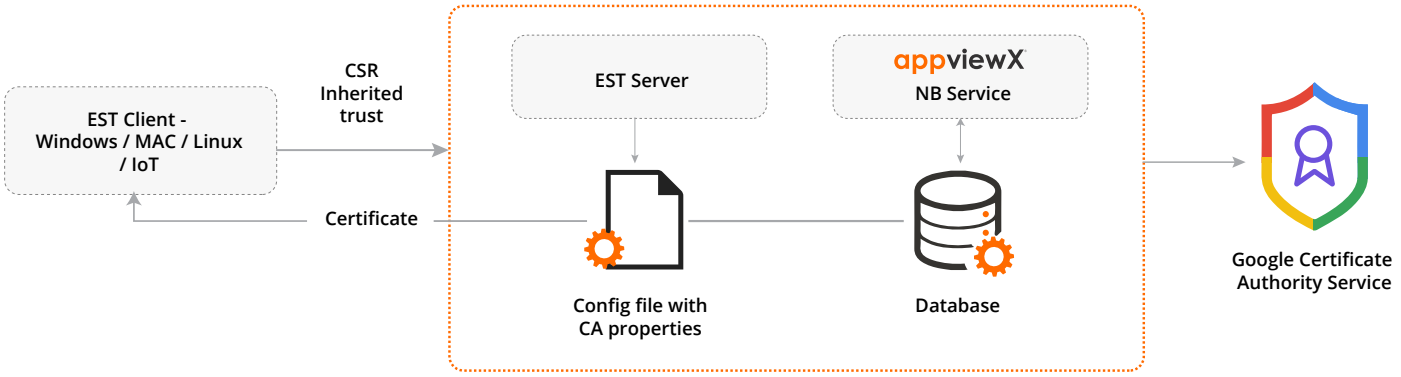

Diagram 3 : EST Support

Auto-Enrollment on Windows Servers using EST

AppViewX supports the EST protocol in order to enable automatic certificate enrollment on endpoints. AppViewX acts as the EST server and thus serves as a bridge between the Google CA Service and a windows server by submitting the CSR to the CA service, obtaining the certificate, and pushing it to the Windows server. AppViewX can also move auto-enrollment for domain-joined Windows machines to the Google CA.

Mobile And Network Device Auto-Enrolment via SCEP

AppViewX supports the SCEP protocol for auto-enrolment of certificates on a variety of network devices and mobile devices. In this role, it acts as the interface between those endpoints and the Google Certificate Authority Service. AppViewX integrates with Mobile Device Management (MDM) or Enterprise Mobility Management (EMM) platforms as well, so once a certificate is enrolled on a device, it can be continuously monitored, renewed, and updated via the MDM.

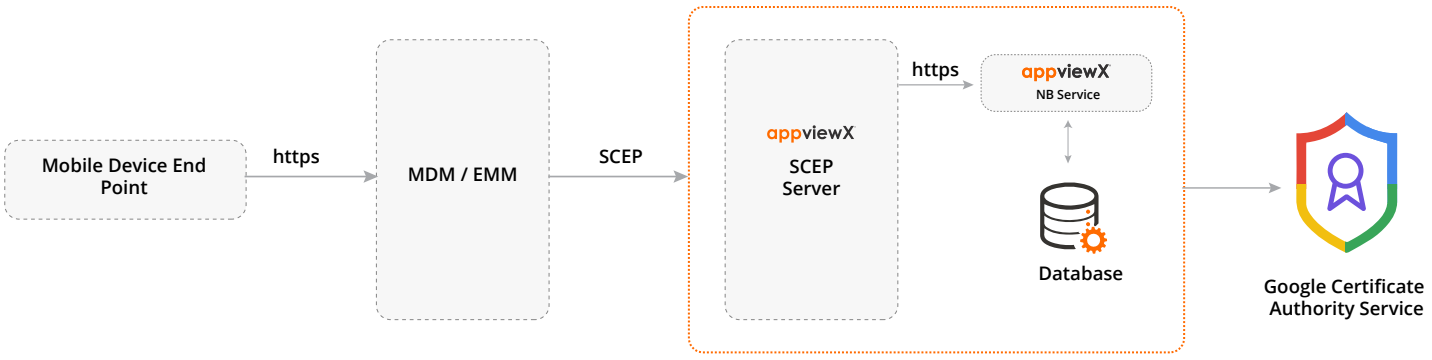

Diagram 4: SCEP Support for Mobile Endpoints

Self-service Certificate Provisioning and Bind to Servers and Services.

Through AppViewX's self-service forms, end users can request certificates from the Google CA Service that will automatically be provisioned on servers and other network services. AppViewX integrates with 100+ vendors and versions across cloud and on-prem deployments, including Apache, IBM HTTP/Websphere, Cisco, Arista, F5, and so on.

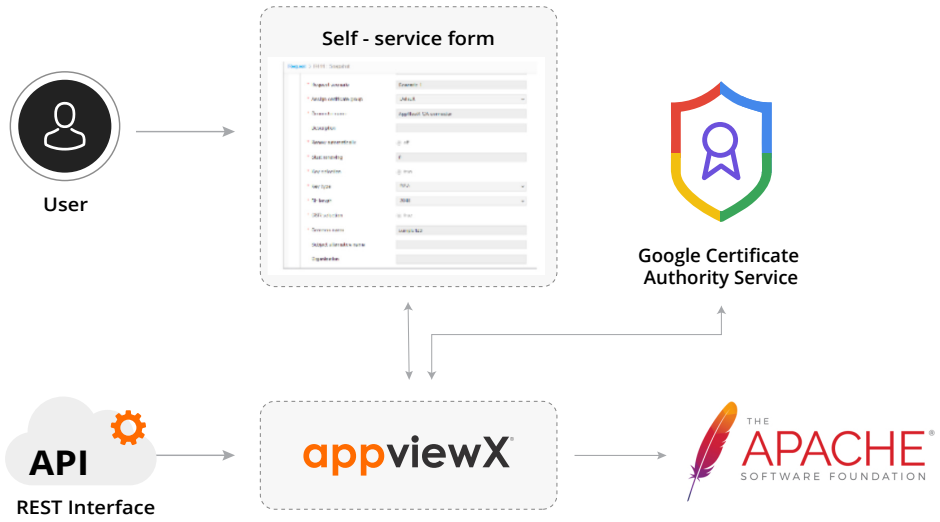

Diagram 5: Self-Service Provisioning on Apache

Summary

With the number of digital identities increasing by the second, it has become imperative to adequately protect them with PKI. For teams that cannot invest heavily in setting up and maintaining a PKI from scratch, the AppViewX-Google Certificate Authority Service Joint Solution is the best way to operate a secure PKI. Not only does it eliminate the expertise needed to maintain the PKI, it is also conducive to modern implementations like DevOps and IoT. The joint value delivered by a cloud-hosted PKI and an end-to-end lifecycle management platform will enable admins to rapidly scale up on-demand and maximize the efficiency of their certificate and key management programs.

Next Steps

To gain access to the AppViewX integrated solution and Google Certificate Authority Service, register for early access,

or contact us for a **demo**

Learn more about individual product lines

AppViewX CERT+

Google Certificate Authority Service

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**