Guide to Implementing and Managing PKI in Hybrid and Multi-Cloud Environments

Prologue

Setting up and managing internal PKI for multi-cloud or hybrid services has always been a subject of much confusion and debate because of the complexity in it. For a hybrid deployment model, enterprises need to set up separate PKIs for on-premise and cloud deployments. For multi-cloud, they use the security services offered by each cloud provider with no or limited interoperability. PKI isn’t set-and-forget; it needs constant monitoring and dynamic management, a pot of milk that’ll boil over in no time if you aren’t watching it close enough. Multiple PKIs in varied environments are a management nightmare - a tiny oversight is all it takes for an enterprise-wide outage. But simple PKI in complex environments isn’t all that tough to achieve. With a few steps in the right direction, you can set up a robust PKI for multi-cloud and hybrid with just your existing crypto resources such as CAs, KMS, vault, etc., without sinking heavy investments into new security infrastructures.

What's Inside

Introduction

There's never a discussion on the cloud without touching upon its security features, which are generally perceived as inadequate. While the distributed nature of multi-cloud and hybrid deployments makes them highly available and resilient, it also takes away a good deal of control over data security from in-house IT teams. Enterprises are reluctant to have their root certificates and keys, the "Keys to their Kingdom," taken away from them and stored in a remote cloud. Multi-cloud further exacerbates these concerns. With each cloud provider having its own set of security services and policies, it's difficult to gain overall visibility and control from a single pane of glass.

However, digital domination of multi-cloud, hybrid, and containers is imminent and inevitable, so enterprises need to come up with viable solutions to maneuver their PKI into the cloud. PKI needs to be scalable, agile, and resilient to support the crypto requirements of cloud-hosted and containerized applications, such as an enormous number of short-lived certificates, frequent protocol and policy upgrades, and compliance to industry regulations.

PKI Implementation Models for Multi-Cloud and Hybrid Deployments

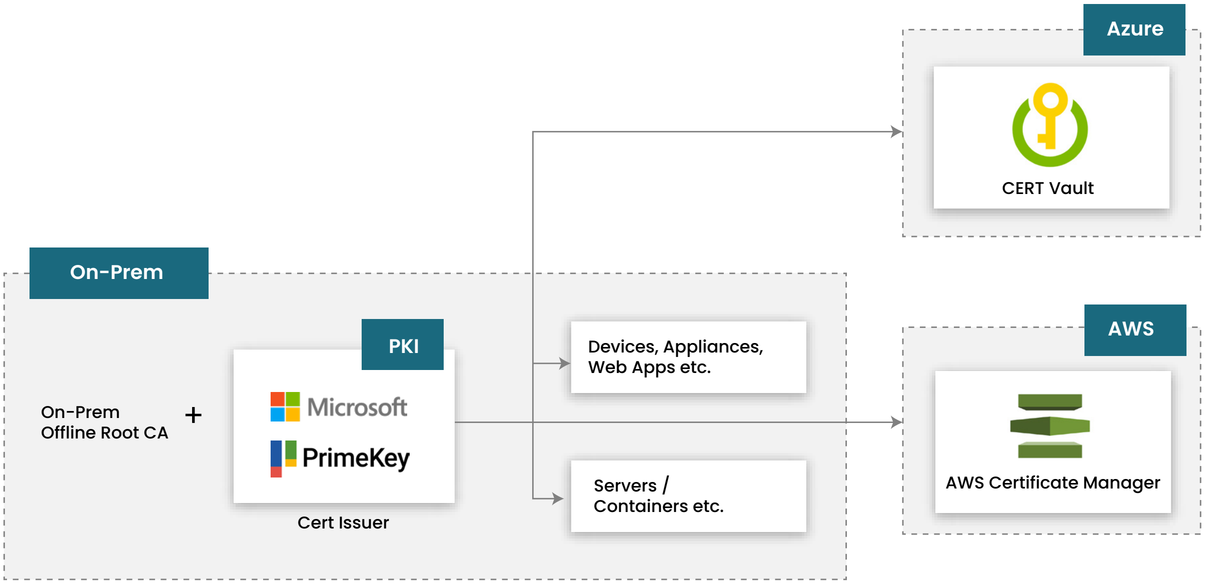
When adopting a multi-cloud or hybrid model, enterprises face a lot of dilemmas on how to deploy and manage their internal PKI. For applications hosted on-premise on physical or virtual machines, enterprises house their root and issuing CAs on-premise, along with an HSM and a KMS (also on-prem). Setting up private PKI(s) for applications hosted on multiple clouds or part on-premise and part cloud (hybrid) isn't as cut and dried. In the following sections, we explore the different methods by which enterprises can configure and manage PKI for cloud deployments and the potential downsides with each method.

1. On-Premise PKI for Cloud and On-Premise Use Cases

These implementations involve a traditional on-premise PKI controlling and managing security for the cloud. There are two ways to implement them:

a) Extending On-Prem PKI to the Cloud

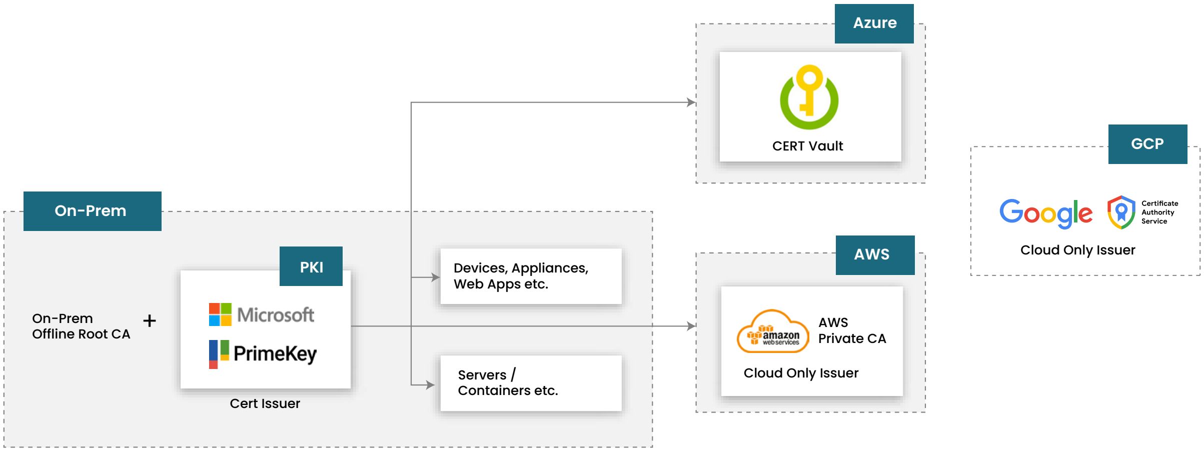
Here, the root CA (say, Microsoft AD CS) and the issuing CAs (like Microsoft or Primekey) are kept on-premise. The on-premise issuing CAs issue certificates to cloud services as and when they are spun up.



Downsides: The on-premise PKI might find it difficult to scale up to the certificate demands of cloud services. Cloud-hosted applications typically have a shorter certificate lifespan, so they need to be renewed more frequently. Moreover, some on-prem CAs may not support certain certificate auto-enrollment protocols (Microsoft AD CS for example, does not support ACME or EST), or vice-versa.

b) Having Multiple PKIs for On-premise and Multi-Cloud Deployments

Enterprises that have some applications on-premise and others in the cloud can follow this implementation. Here, the applications hosted on-premise are supported by traditional PKI with the root and issuing CAs residing on-premise, while the cloud-native applications have a cloud PKI (such as Google CA or AWS Certificate Manager) issuing and managing certificates on them.



Another method is where the on-prem issuing CA signs the certificates issued by the cloud service provider. In this case, the trust anchor stays on-premise.

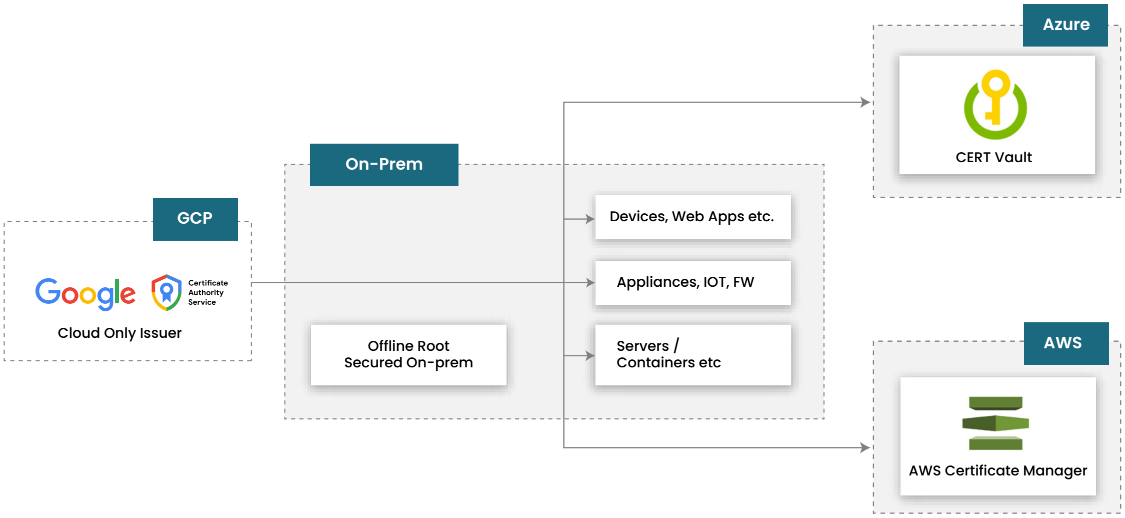
Downsides: Implementing separate PKIs for on-premise and cloud and multiple PKIs for different clouds (in a multi-cloud scenario) makes management convoluted. The setup and management costs go up. Security teams lose holistic visibility over the PKI implementations and cannot control them from a single pane.

The second method is once again subject to demand (on-premise PKI not being able to keep up with cloud certificate demands) and protocol mismatches. Also, in this case, if the on-premise root or issuing CA gets compromised, it impacts cloud applications as well.

2. Cloud PKI for Cloud and On-Premise Use Cases

These implementations involve a cloud-native PKI, such as Google Certificate Authority Service (Google CAS) or AWS Certificate Manager, issuing and managing certificates for both on-premise and cloud deployments.

This implementation is an excellent option for enterprises that have invested heavily in multi-cloud, hybrid, or container-based deployment models, as the cloud PKI can easily handle the volume of certificates that these deployments require. Cloud PKI is the best bet for next-gen technologies such as IoT, virtualization, and DevOps because of its high scalability and hassle-free pay-as-you-go model.



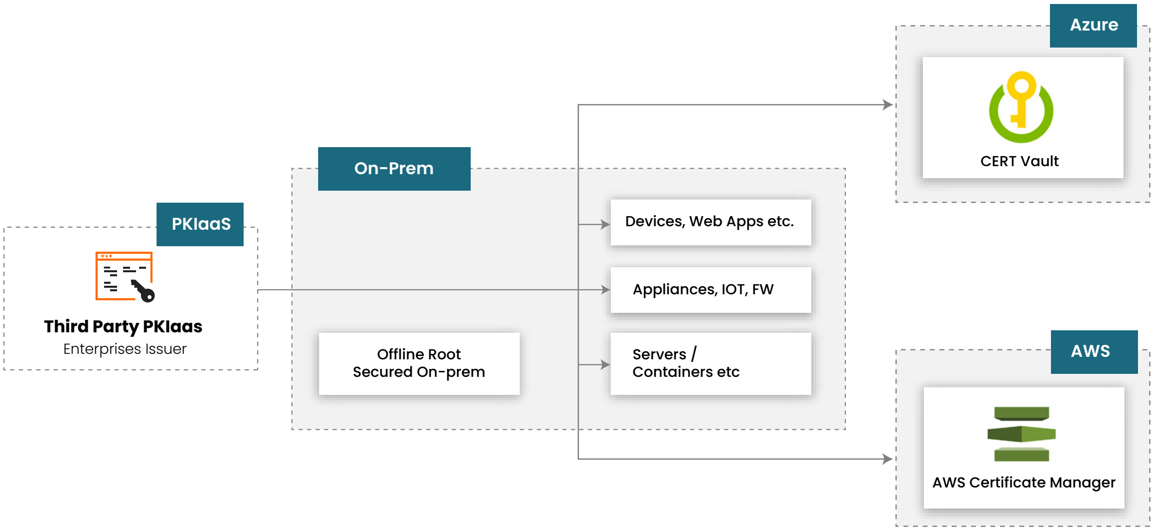
In this model, root PKI (which is as usual kept offline) signs the cloud CA, making it a trusted issuing CA. The cloud CA can now issue certificates to both on-premises and cloud applications. A significant advantage of this approach is that enterprises can leverage the built-in security services and policies that come with the cloud PKI for on-premise applications as well, thereby modernizing legacy systems and practices without a complete overhaul.

Downside: This implementation engenders the need to have multiple issuing CAs (the pertinent CA for each cloud - for example, Google CAS for GCP) in a multi-cloud model, causing management hassles.

For both the above implementations (using on-premise PKI for cloud or cloud PKI for cloud and on-premise deployments), one common downside is that on-premise or cloud applications cannot interchangeably use the security services that come built-in with individual cloud platforms. This leads to service duplication, management silos, and data sprawl; for example, GCP, AWS, and Azure each have their own IAM (Identity and Access Management) solution, along with the Active Directory services of on-premise deployments. One way to get around this problem is to use a third-party solution that works across clouds. However, using a third-party solution for each individual service can turn out unwieldy and costly. The next implementation focuses on how enterprises can come up with a sustainable, economical solution for the multi-cloud PKI conundrum.

3. Using a PKI-as-a-Service (PKIaaS) Solution for On-Premise and Cloud Deployments

Here, a third-party PKIaaS solution acts as the certificate issuer for both on-premise and cloud services. The root is again kept offline, and it authorizes the PKIaaS solution to issue certificates.



Advantages of Using a PKIaaS Solution

The main advantage of using a PKIaaS solution is that it provides complete management of certificates, keys, policies, etc. Some PKIaaS solutions are CA-agnostic; that is, they issue and manage certificates from an array of cloud and on-premise CAs such as Digicert, GlobalSign, GCP, ACM, etc. They eliminate the need for setting up multiple PKIs for multi-cloud and hybrid use cases and instead provide a single, unified PKI that breaks down management silos.

How AppViewX CERT+ Helps Simplify Multi-Cloud and Hybrid PKI Implementations

In this section, we'll look at how AppViewX CERT+ helps enterprises erase the downsides of cloud PKI implementations and provides a PKIaaS solution for enterprises looking to transform their multi-cloud PKI.

What is AppViewX CERT+?

CERT+ is a next-gen PKI management platform that manages and automates identities of network devices, applications, container workloads, mobile devices, and IoT endpoints. It manages and automates certificate and key lifecycles across multi-cloud, hybrid, and containerized environments. It is CA agnostic and supports all certificate auto-enrollment protocols such as ACME, EST, SCEP, and CMP, and also supports the symmetric key management protocol - KMIP.

What Makes AppViewX CERT+ the Ideal Solution to Manage Multi-Cloud PKI?

CA-agnostic lifecycle automation: CERT+ automates the lifecycle of keys and certificates end-to-end, from discovery to enrollment to renewal or revocation, irrespective of which CA issues them. It supports on-premise CAs like Microsoft AD CS, Primekey, etc., and also cloud-native CAs like Google CAS and ACM.

PKIaaS: CERT+ provides both protocol-based and non-protocol-based (REST API) management and automation of PKI for any device or endpoint in any environment. For instance, if an IoT device needs a Microsoft AD CS certificate to be enrolled on it, CERT+ acts as an EST server (Microsoft AD CS does not support EST), does the necessary verifications, and gets a Microsoft certificate auto-enrolled on the IoT device. This gives enterprises the flexibility to choose any CA(s) and make it work with any endpoint, however incompatible the CA and the endpoint are, anywhere.

Ability to act as a glue between incompatible or disjointed services: Applications hosted in one cloud can use CERT+ as an interface to consume another cloud's services. For example, applications hosted on GCP could use AWS Secrets Manager to store and manage their keys, allowing true best-of-breed solutions. Similarly, an application hosted on Azure could use Google CAS as their CA and get their certificates from it. This is possible because CERT+ fully supports all three popular cloud providers - GCP, AWS, and Azure. Besides, it has a containerized architecture and can easily be deployed in any environment.

Marketplace presence: AppViewX CERT+ is available across GCP, AWS, and Azure marketplaces, where enterprises using any or all of these cloud services can easily consume CERT+ for their multi-cloud PKI management and orchestration needs. The marketplace version includes all of the capabilities discussed above. CERT+ also supports Kubernetes natively.

Now, with all these capabilities, let's see how CERT+ helps eliminate the cloud PKI implementation downsides discussed previously:

Cloud PKI for Cloud and On-Premise Use Cases

As we've established already, this implementation is best suited for forward-looking enterprises that host most of their applications in the cloud, have applications deployed in containers on-premise, or a mix of both. The reason is that on-premise PKI cannot handle the certificate volume that cloud and containers require.

The primary downside with this implementation was management arising from incompatibility between different cloud CAs and the need to set up a separate PKI for each cloud. CERT+ simplifies and streamlines this implementation by allowing enterprises to have one issuing CA issue certificates to applications deployed on-premise and in multiple clouds. As an example, an application whose database is on-premise and has instances running in AWS, GCP, and Azure can get a certificate enrolled commonly from Google CAS through CERT+, as it breaks down incompatibility barriers between cloud service providers. Enterprises do not have to sink in time, effort, and cost to set up multiple PKIs, as one PKI covers both on-premise and multi-cloud use cases.

Sometimes, enterprises may wish to use multiple PKIs for reasons such as to lower the blast radius in case of planned maintenance, outages, or breaches. CERT+ simplifies the management of multiple PKIs by providing a centralized, single pane of glass from which security administrators can monitor the PKIs and implement policies.

Conclusion

mplementing PKI in multi-cloud and hybrid scenarios need not be a complicated affair if you have a clear strategy and the right tools to help you along. Cloud and containers are the future, and a simple but strong PKI is essential for ensuring airtight device and application security and cryptographic agility, which in turn come only with proper monitoring, management, and most importantly, automation. This is exactly what AppViewX CERT+ does - it simplifies management and automates 98% of PKI operations, paving the way for robust, agile PKI that can sustain any new technology without the slightest show of weakness.

Try AppViewX CERT+, or book a live product demo

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 crypto-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**