EQUINIX

KEY MANAGEMENT SECURITY CONTROL FUNCTION

DISTRIBUTED SECURITY SOLUTION BRIEF

Equinix.com

SOLUTION BRIEF

KEY MANAGEMENT SECURITY CONTROL FUNCTION

Executive Overview

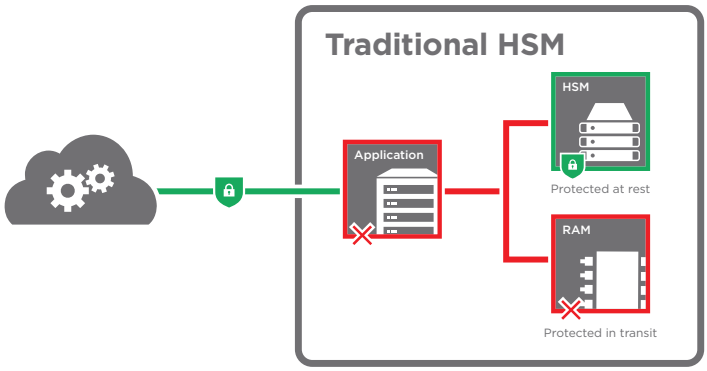
Enterprises seeking to realize the full potential of the cloud are on a digital transformation journey that requires shifting infrastructure from a siloed and fixed state to one that is agile and dynamic. The **IOA® Playbook** offers a compelling strategy for how to do this by establishing a hybrid or multicloud architecture on Platform Equinix®. Doing so allows enterprises to solve a host of scale and integration challenges.

A key to success, however, is to place security controls at the digital edge at the beginning of the journey. Key management, or the management of cryptographic keys in a cryptosystem, is one of the first security controls an enterprise must implement at the beginning of this journey. Doing so allows enterprises to support critical use cases including key management for SSL/TLS certificates, site-to-site VPN scenarios, for data encryption in databases and more.

However, secure management of keys across an enterprise's data centers and private/public, hybrid and/or multicloud environments presents a unique challenge. Until now, enterprises have been forced to use multiple key management solutions to match the various parts of their architecture. These can include traditional Hardware Security Modules (HSMs) for on-premises needs and/or key management services (KMS) within each cloud environment. As one could expect, the complexity of managing multiple key management solutions is significant.

HSMs for On-Premises Encryption Key Management

HSMs have historically been used to securely manage encryption keys within an organization's data centers. These hardware appliances are designed to be tamper-proof, providing the highest level of physical security. Encryption keys are stored in the HSM, and cryptographic operations are securely executed within the module.



As the de facto standard for encryption key management, HSMs provide a full complement of features and administrative functionality, including:

- **Life cycle management:** An HSM will guard encryption keys through every stage of the life cycle, including generation, import, export, usage, rotation, destruction and auditing.
- **Centralized management:** Desktop administrative tools remotely manage key life cycles and support separation of administrative duties for added security.
- **APIs:** HSMs allow for application and service integration as well as custom application development via APIs.

But, as enterprises transition to multicloud architectures, key management via traditional hardware-based HSMs is no longer the ideal solution. An enterprise that hosts applications and services with multiple cloud service providers will experience increased operational complexity and risk, as a different set of key management tools will be required for each cloud service provider. Additionally, in some cases connections between on-premises HSMs and encrypted data stored in the cloud can introduce unacceptable latency in key generation and retrieval. This could impact the encryption and decryption process within the cloud and therefore general performance.

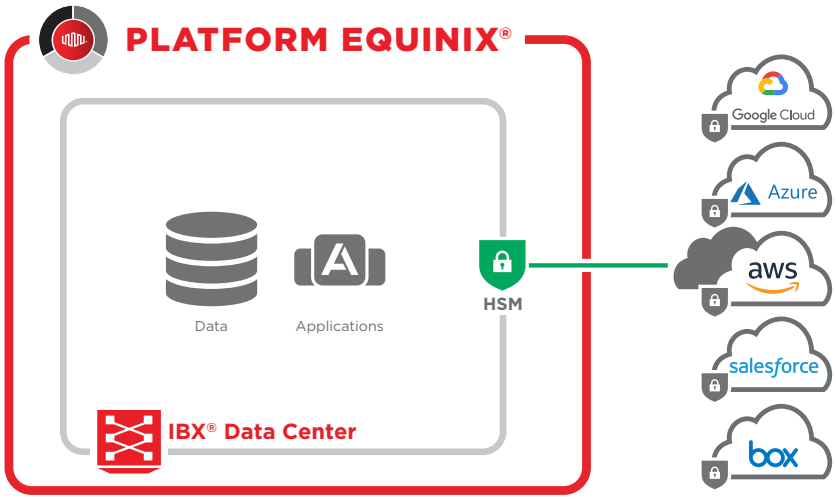
An alternative approach to traditional HSMs is Key Management Services within cloud environments.

Key Management Services (KMS) for Cloud Environments

A cloud-based KMS is a service rather than a specific appliance. As such, it enables clients to manage encryption keys without concern for HSM appliance selection, provisioning and management of on-premises hardware. A cloud-based KMS centrally manages the encryption key life cycle within the specific cloud provider. In addition, it can export and import existing keys and provide a software development kit (SDK) to enable third parties to perform application development and integration to customize the KMS as needed.

KMSs are offered by cloud service providers and provide distinct advantages. For starters, they build on the well-established strengths of cloud platforms, including:

- **Scalability:** Cloud platforms can easily accommodate large-scale data processing and geographic growth.
- **Availability:** Cloud service provider infrastructures ensure a high level of service availability.
- **Integration:** Native integration with other services such as system administration, databases, storage and application development tools are generally offered by cloud service providers.
- **Bring Your Own Key (BYOK):** An added level of security provided by some cloud service providers is the option, among others, to use an external HSM for storing master keys.



If an enterprise's cloud architecture uses a single cloud provider, the KMS encryption key approach may be the ideal solution. However, in a multicloud architecture, the benefits of the cloud are reduced by the complexity of administering multiple key management services. In addition, keys will be located close to the data, thus reducing the benefits of separation of duties security best practices recommend.

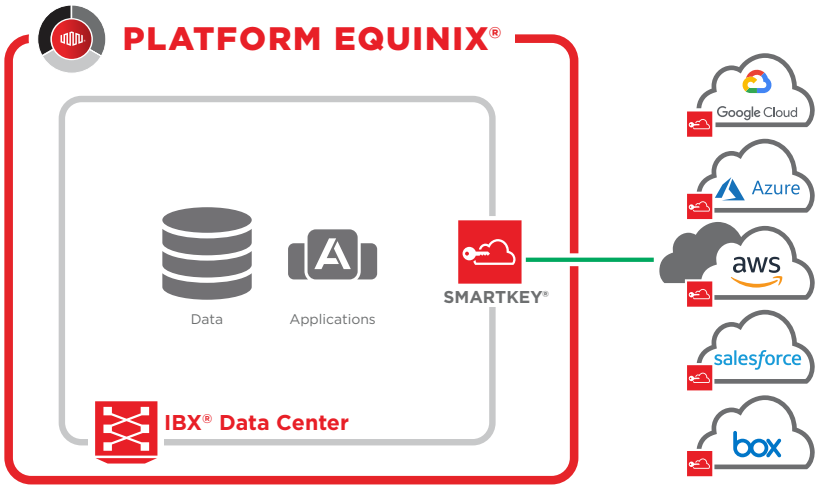
HSM as a Service

To reduce the burden and complexity of HSM and KMS key management approaches, enterprises can deploy key management at the digital edge, proximate to the clouds, SaaS applications, networks, enterprise data centers, branch offices and remote sites where they are needed.

This approach is ideal for enterprises that need both HSM-grade security for key management and the consistency of a single administrative environment, regardless of where encryption keys are used. HSM as a Service provides HSM-grade key storage with no need for cloud-based or on-prem HSM appliances. It's easy to implement and effortlessly scales to support data, processes and geographic growth as needed.

HSM as a Service offers features and functionality equivalent to a KMS, yet possesses several additional capabilities that complement the strengths of cloud service providers. These include:

- **Hybrid and multicloud capabilities:** Consistent, centralized control and management of keys regardless of where data resides.
- **Accessibility:** Keys can be utilized by on-premises or cloud service provider applications or services.
- **BYOK support:** Enterprises can use existing encryption keys.
- **Cryptographic protection:** Only authorized users can access encrypted keys.
- **Cloud-friendly APIs:** Both legacy and cloud-native APIs are supported.
- **Separation of duties:** Following security best practices, keys are stored separately from the data that utilizes the keys, ensuring a potential data breach does not also breach the keys.
- **Latency:** Keys can be stored proximate to data, reducing latency for key generation and retrieval.
- **Connectivity:** Access to multiple cloud service providers and network service providers is available via the public internet and/or a private interconnection across global data centers.



Determining Optimal Key Management Strategy

Choosing the optimal encryption key management strategy can be a straightforward process. If an enterprise is running a private or hybrid cloud environment within its own data center, it likely already has HSMs with established encryption keys in place. Many enterprises will choose to maintain the environment for the foreseeable future, leveraging their existing HSMs. Similarly, if the enterprise is transforming to a single cloud services provider and has no immediate plans to expand beyond that sole provider, then a cloud service provider's KMS should be suitable for its needs.

If, however, an enterprise is designing a hybrid or multicloud architecture, it may wish to select an HSM as a Service. Doing so can eliminate the cost and overhead of provisioning HSMs in its data center as data and processing demands grow. In contrast to a cloud service provider's KMS, a cloud-neutral HSM as a Service enables enterprises to manage their keys separate from the platform where their data is located, while enabling encryption keys to be used across the cloud service provider's platforms.

The chart below offers recommendations for the best encryption key management solution based on an organization's cloud strategy:

PRIVATE CLOUD		SINGLE CLOUD SERVICE PROVIDER	HYBRID OR MULTICLOUD
Recommendation	HSMs already provisioned in the enterprise data center	Cloud service provider's KMS or KMS enhanced by cloud service provider	HSM as a Service
Advantages	HSM security	Ease of management (optional BYOK)	Ease of management, HSM-level security, more granular control of key life cycle management
Alternatives	HSM as a Service to eliminate the ongoing cost and overhead of provisioning and managing HSMs	HSM as a Service to separate encryption keys from data for additional defense	

Key Management at the Digital Edge

When evaluating these different key management approaches, you should also consider where to deploy this capability. Due to the fact that various services that leverage key management must constantly fetch credentials and encryption keys, and those services may be located anywhere, key management services need to be deployed at the digital edge, near users, data, applications and clouds.

This is described in more detail in design pattern 4 of Equinix's **IOA Security Blueprint**.

To fulfill this need, Equinix offers its own HSM as a Service solution called **Equinix SmartKey®**. Equinix SmartKey is a global SaaS-based secure key management service.

Conclusion

As data is increasingly distributed to multiple digital edge locations, the traditional, centralized data center model is becoming increasingly obsolete, unable to provide the security controls needed for digital business. New IT infrastructure and security paradigms allow for control, visibility and segmentation of cloud resources and enable cloud agility. A service-based approach to key management ensures security control functions apply to hybrid multicloud environments.

How to Get Help

For more information on how key management applies in your environment, please contact **securityteam@equinix.com**.

EQUINIX

WHERE OPPORTUNITY CONNECTS

Corporate HQ

Equinix, Inc.
One Lagoon Drive
Redwood City, CA 94065
USA

Main: +1.650.598.6000
Email: info@equinix.com

EMEA

Equinix (EMEA) BV
Rembrandt Tower
Amstelplein 1
1096 HA Amsterdam
Netherlands

Main: +31.20.754.0305
Email: info@eu.equinix.com

Asia-Pacific

Equinix Hong Kong Limited
65/F International Commerce Center
1 Austin Road West
Kowloon, Hong Kong

Main: +852.2970.7788
Email: info@ap.equinix.com

About Equinix

Equinix, Inc. (Nasdaq: EQIX) connects the world's leading businesses to their customers, employees and partners inside the most-interconnected data centers. On this global platform for digital business, companies come together across more than 50 markets on five continents to reach everywhere, interconnect everyone and integrate everything they need to create their digital futures.

SB_Key Management IOA Control Function_v2_US-EN |6318| v080819 | 0419 | Q418

Equinix.com