enclaive

Whitepaper

Who Holds the Keys? Exploring GYOK, BYOK, and HYOK for Cloud Sovereignty

Executive Summary: A Strategic Overview of Cloud Key Management

In the digital landscape, the security of encrypted data is intrinsically linked to the protection of its cryptographic keys. As organizations increasingly migrate sensitive workloads to the cloud, a critical challenge emerges: how to leverage cloud-native services while maintaining a robust security posture for the keys that protect their most valuable information. This whitepaper examines three primary strategies for cryptographic key management—**Get Your Own Key (GYOK), Bring Your Own Key (BYOK) and Hold Your Own Key (HYOK)**—to provide a comprehensive framework for strategic decision-making. These models do not represent a simple choice of one over the other but rather a spectrum of control, enabling organizations to align their key management strategy with their specific risk tolerance, compliance requirements, and operational capabilities.

The analysis within this document reveals several key findings. The GYOK model exemplified by major cloud providers, offers unparalleled convenience, deep integration, and high availability. However, it necessitates a high degree of trust in the cloud service provider and their internal security protocols. In contrast, the BYOK model represents a shared-control paradigm where the customer generates and owns the key but delegates its custody and use to the cloud. This approach enhances compliance and provides a clear audit trail but introduces added responsibility for the user and requires a continued reliance on the provider's infrastructure. At the far end of the spectrum, HYOK provides a sovereign security posture, with keys never leaving the customer's security perimeter. While this delivers the highest level of data confidentiality and legal protection, it comes at the cost of significant operational complexity and potential limitations in cloud application functionality.

The landscape of key management is evolving with the advent of technologies like virtual Hardware Security Modules and Confidential Computing. These innovations are reshaping the spectrum by offering a hybrid approach that combines the security assurances of on-premises hardware with the agility and scalability of cloud services.

This whitepaper concludes with a detailed comparative analysis to assist security professionals and business leaders in selecting the most appropriate key management model for their specific needs, thereby navigating the complex balance between security, convenience, and control.

Table of Contents

Executive Summary: A Strategic Overview of Cloud Key Management 02

1 Introduction: The Evolution of Cryptographic Control in the Cloud 05

1.1 Foundational Concepts in Cloud Key Management 05

2 Get Your Own Key: The Convenience-Centric Model 07

2.1 Concept Definition and Core Functionality 07

2.2 Security and Access Analysis 07

2.3 Hybrid Multi-Cloud Architecture for KMS 07

2.4 Strengths and Weaknesses 08

2.5 What organization should use GYOK? 08

3 Bring Your Own Key (BYOK): The Shared-Control Compromise 10

3.1 Concept Definition and Purpose 10

3.2 The BYOK Operational Flow 10

3.3 The Critical Nuance of Ownership vs. Possession 10

3.4 Hybrid Multi-Cloud Architecture for BYOK 11

3.5 Security and Access Analysis 11

3.6 What organizations should use BYOK? 11

4 Hold Your Own Key (HYOK): The Sovereign-Centric Model 13

4.1 Concept Definition and Core Principle 13

4.2 Operational Mechanics and the Role of Modern Enablers 13

4.3 Security and Access Analysis 13

4.4 Single-Cloud Architecture for HYOK 14

4.5 Hybrid Multi-Cloud Architecture for HYOK 14

4.6 Strengths and Weaknesses 15

4.7 Which organization should use HYOK? 15

5 Comparative Analysis: Navigating the Key Management Spectrum 16

5.1 The Three Models: A Side-by-Side Comparison 16

5.2 The Role of Modern Solutions: Virtual HSMs and the Future 16

5.3 Summary Table: Key Management Concepts: A Strategic Comparison 17

6 Conclusion: Choosing the Right Strategy for Your Organization 19

Notices 20

Glossary of Terms 21

Further Reading from Multiple Sources 22

1 Introduction: The Evolution of Cryptographic Control in the Cloud

The shift to cloud computing has fundamentally altered the security paradigm for organizations worldwide. While the cloud offers immense benefits in scalability, cost-efficiency, and global reach, it presents a core security dilemma: relinquishing physical control over data and its encryption keys. The integrity of an organization's most sensitive data is only as robust as the security of the keys that protect it. Without a strong strategy for key management, an organization's cloud data remains vulnerable to insider threats, legal mandates, and sophisticated cyberattacks.

To address this challenge, a number of key management models (KMS)[1] have emerged, each offering a distinct approach to balancing control with convenience. This whitepaper focuses on three prominent concepts:

- **Get Your Own Key (GYOK):** A model in which the cloud service provider manages the entire key lifecycle, from generation and rotation to storage and destruction.
- **Bring Your Own Key (BYOK):** A hybrid model where the customer generates a key outside of the cloud environment and then imports it into the provider's KMS for use.
- **Hold Your Own Key (HYOK):** The most secure model, where the customer maintains absolute, sovereign control over the key, which never leaves the customer's security perimeter.

The core of this report is to provide the clarity necessary for secure and informed decision-making by correctly defining and analyzing each of the cryptographic key management strategies.

1.1 Foundational Concepts in Cloud Key Management

The security of data in the cloud is a shared responsibility, a concept where the cloud service provider (CSP) secures the underlying infrastructure, while the customer is responsible for securing their data, applications, and access control. This division makes key management a critical customer-side responsibility, as the chosen model defines the level of trust placed in the CSP's control over sensitive cryptographic assets. The decision about which key management model to adopt is therefore a strategic one that directly impacts an organization's security posture.

A nuanced understanding of key terminology is essential for navigating the complex landscape of cloud key management. The terms „Bring Your Own Key“ (BYOK) and „Hold Your Own Key“ (HYOK) are often used interchangeably or inaccurately, leading to confusion. A more precise framework is to differentiate between three distinct concepts: key ownership, possession, and control.

- **Key ownership** refers to the legal right to the cryptographic key, which remains with the customer in all three models. This, however, does not guarantee physical or logical custody.
- **Key possession** is the physical or logical custody of the key material, which is the most critical differentiator. With a cloud-native Key Management Service (KMS) or BYOK, the CSP takes possession of the key to perform cryptographic operations. With HYOK, the customer retains sole possession, and the key never leaves their environment.
- **Key control** is the ability to manage the key's lifecycle, including generation, rotation, revocation, and destruction, and to define who can use it. All three models offer some level of control, but the scope varies dramatically.

1 The abbreviation „KMS“ is frequently used in the provided research material, but it is important to distinguish between a „Key Management Service“ and a „Knowledge Management System.“ Several research snippets refer to „KMS Lighthouse,“ which is a knowledge management platform unrelated to cryptographic key management.

A foundational cryptographic pattern common across all three models is **envelope encryption**. This two-tiered key hierarchy separates a master key, known as the Key Encryption Key (KEK), from the keys used to encrypt the actual data, known as Data Encryption Keys (DEKs). The process works by first encrypting the data with a unique, ephemeral DEK. The DEK is then encrypted, or „wrapped," by the KEK. Both the encrypted data and the wrapped DEK are stored together, while the plaintext DEK is immediately purged from memory. This approach provides significant performance benefits, as only the much smaller DEK needs to be transmitted over the network for cryptographic operations, rather than the entire data block. This architectural pattern is a critical security-by-design feature that balances high performance and scalability with strong key security. It minimizes the number of times the master key is used, isolating the data encryption process from the master key management process and thereby reducing the attack surface.

Central to traditional cryptographic security is the **Hardware Security Module (HSM)**. These are specialized, tamper-resistant physical devices designed to securely generate, store, and manage cryptographic keys and provide a root of trust for all cryptographic operations. A new concept based on Trusted Execution Environments allows the virtualization creating **virtual HSMs (vHSM)** that provide most of the HSM functionality with significantly increased flexibility. All three models leverage (v)HSMs in some form. Cloud providers use them to protect their native KMS keys, with many offering HSMs that are FIPS 140-2 validated to different security levels. Customers also use on-premises HSMs to generate keys for BYOK or to serve as the core infrastructure for the entire HYOK model. For organizations in regulated industries, HSMs are often a non-negotiable requirement for compliance.

2 Get Your Own Key: The Convenience-Centric Model

2.1 Concept Definition and Core Functionality

Get Your Own Key is designed to simplify the lifecycle management of key management. It provides a centralized service for generating, storing, distributing, and managing keys used for encryption and decryption purposes. The primary appeal lies in its deep integration with other cloud services, often providing a „plug-and-play“ solution where encryption can be enabled with minimal effort, sometimes without the user even being aware of its use.

Major cloud providers, such as Google and Amazon Web Services (AWS), offer various key types within their KMS offerings to cater to different levels of control and responsibility. These include:

- **Provider-owned keys:** The most automated option, where the CSP owns and manages the keys entirely, with no user configuration or control over policies or audit logs.
- **Provider-managed keys:** The CSP manages key rotation and other lifecycle events, but the customer can track key usage and access some audit logs.
- **Customer-managed encryption keys (CMEKs):** These keys are created and controlled by the customer within the KMS. This level offers granular control over key rotation schedules, Identity and Access Management (IAM) roles, permissions, and destruction schedules.

2.2 Security and Access Analysis

The security posture of a KMS is dependent on the level of customer engagement. For default, provider-managed keys, security is a „black box“ where the customer must fully trust the CSP's internal controls. However, for customer-managed keys (CMEKs), the user can enforce granular permissions and role-based access controls. This allows for the separation of key management and key usage permissions, providing a strong defense against insider threats or compromised accounts. The use of robust auditing tools, such as AWS CloudTrail, provides a detailed log of all key usage, which is essential for compliance and regulatory needs.

A critical aspect of the GYOK model is the inherent trust in the CSP. Despite FIPS 140-2 validation and robust security protocols, the keys reside within the provider's infrastructure. This means that CSP administrators and internal teams might have privileged access to these systems, creating a potential attack vector. While some providers offer features like Cloud HSM where keys are not accessible by the provider, the general KMS model still relies on a level of trust that may not be acceptable for all organizations.

2.3 Hybrid Multi-Cloud Architecture for KMS

When a GYOK-centric model is extended to a hybrid or multi-cloud environment, a critical architectural challenge emerges. Each cloud provider's native KMS is a distinct, isolated service. A workload running in Azure cannot, by design, use a key stored in AWS KMS. This lack of key portability creates a fragmented key management landscape. Organizations must manage and audit a separate set of keys and policies for each cloud. This can lead to vendor lock-in, as migrating data from one cloud to another requires decrypting the data with the original key and then re-encrypting it with a new key from the target cloud's KMS. The result is an environment with multiple, independent “key silos” that are not interoperable.

2.4 Strengths and Weaknesses

The GYOK model offers a compelling set of advantages and disadvantages for organizations to consider.

Strengths:

- **Operational Ease:** GYOK is exceptionally easy to set up and use, often requiring no setup to get started. It offers automatic key rotation for symmetric keys and is deeply integrated with a wide range of cloud services, simplifying the encryption process.
- **High Availability and Resilience:** GYOK is designed to be highly available, with keys stored by region to provide redundancy and resilience against data center outages.
- **Lower Operational Burden:** The CSP handles the complexities of key lifecycle management, including durability, availability, and security, reducing the overhead for the customer.
- **Cost-Effectiveness:** Compared to dedicated hardware solutions, GYOK is relatively inexpensive, with a low monthly cost per key.

Weaknesses:

- **Trust in the Provider:** The model requires a high degree of trust in the CSP's security controls and internal personnel, who may have privileged access to the key management systems.
- **Vendor Lock-in:** Keys are typically tied to a specific region and provider's ecosystem, making it challenging and costly to migrate data to another CSP.
- **Limited Control:** While customer-managed keys offer greater control, the customer still lacks full, sovereign control over the key's location and the underlying hardware it resides on.
- **Performance Bottlenecks:** While envelope encryption mitigates many performance issues, high-traffic services with a large number of objects can still create a burdensome amount of KMS activity, requiring specific optimizations like S3 Bucket Keys to reduce latency and cost.

2.5 What organization should use GYOK?

When encryption keys are fully managed by the cloud provider (with no customer control), this approach is suitable for several types of organizations.

- **Startups and small businesses** benefit when compliance requirements are minimal. They value simplicity and prefer to let the cloud provider handle security operations.
- **Organizations with a low regulatory burden**—such as those in media, gaming, or certain SaaS sectors—can rely on provider-managed keys since there is no legal obligation to control encryption keys directly.
- **Companies early in their cloud adoption journey** often start with provider-managed keys for effortless, default encryption, with the option to transition to customer-managed or Bring-Your-Own-ey solutions later as compliance demands increase.
- **Internal and non-production environments** like development, testing, or analytics systems are also well-suited, as they require encryption but do not justify the overhead of managing keys manually.

- **Cost-sensitive organizations** can avoid the expense of operating their own Key Management System (KMS) or Hardware Security Module (HSM) by using provider-managed keys as a cost-effective baseline.
- **Organizations that trust the cloud provider's compliance posture** may rely on the provider's certifications (e.g., ISO 27001, SOC 2, HIPAA-ready) to meet baseline requirements—for example, a small healthcare SaaS leveraging AWS HIPAA-eligible services with AWS-managed keys.

3 Bring Your Own Key (BYOK): The Shared-Control Compromise

3.1 Concept Definition and Purpose

Bring Your Own Key (BYOK) is a key management strategy that empowers organizations to generate and maintain control of their own cryptographic keys for use in public cloud environments. The central purpose of BYOK is to provide a user with greater control and assurance over their data's security without forgoing the benefits of cloud services. Under this model, the organization creates its own high-quality master key on-premises, often using a FIPS-certified hardware security module (HSM), and then securely transfers it to the CSP's KMS.

3.2 The BYOK Operational Flow

The BYOK process involves a series of critical steps that ensure a secure transfer of control from the customer to the CSP's environment.

- **Step 1: Key Generation:** The customer generates the encryption key within their own controlled environment, typically using a dedicated key management system or a Hardware Security Module (HSM). This step ensures that the key is created and stored in a secure, tamper-resistant location before it is ever exposed to the cloud.
- **Step 2: Key Import:** The newly generated key is then securely imported into the cloud service provider's Key Management Service. This transfer is often a complex process that may be required by specific regulations and often involves cryptographic wrapping of the key to maintain its integrity during transit.
- **Step 3: Key Usage:** Once imported, the CSP's services use the customer-provided key to encrypt and decrypt data at rest within the cloud. The customer maintains control over the key's lifecycle, including rotation and revocation, but the CSP now has possession of the key to perform cryptographic operations.

3.3 The Critical Nuance of Ownership vs. Possession

The term "Bring Your Own Key" is often considered more of a marketing term than a precise technical definition due to a lack of standardization across the industry. A fundamental distinction that must be made is between key "ownership" and key "possession." While the customer owns the key and controls its lifecycle, the CSP now has possession of it to perform the required encryption and decryption tasks. This is a crucial detail because, for many cloud applications, the provider must have access to the unencrypted data or the key to provide their services.

This shared possession has significant security implications. Once the key is imported, the customer must trust that the provider's administrators and internal teams will not misuse or gain unauthorized

access to it, a risk that BYOK itself does not fully mitigate. The integrity of the BYOK model relies on the CSP's internal security and the assurance that its operational processes, such as maintenance and backups, do not expose the plaintext data. This is why the security benefit of BYOK (auditable key usage and revocation) is directly tied to a trade-off: a user's increased responsibility and reliance on the CSP's internal integrity. While BYOK provides a clear audit trail and the ability to revoke access, it also introduces risks if keys are mishandled or compromised by rogue employees, which could undermine the very purpose of data backups in a disaster recovery scenario.

3.4 Hybrid Multi-Cloud Architecture for BYOK

In a hybrid multi-cloud environment, BYOK provides a compelling solution for avoiding key fragmentation and vendor lock-in. Instead of creating and managing multiple isolated key management systems, a single, centralized on-premises or external HSM becomes the single root of truth for all cryptographic keys. This central HSM is used to securely provision copies of the master key to the KMS instances of multiple cloud providers, such as AWS, Azure, and Google Cloud. The key import process is repeated for each cloud, with the centralized HSM acting as the common source for all key generation and wrapping. This enables a consistent and auditable key management strategy across the entire multi-cloud estate.

3.5 Security and Access Analysis

BYOK offers distinct security strengths and weaknesses that must be weighed carefully.

Strengths:

- **Enhanced Compliance:** BYOK facilitates compliance with regulations such as GDPR, HIPAA, and PCI-DSS by providing the customer with clear ownership and a detailed audit trail of key usage. This allows organizations to demonstrate they are independently managing their encryption keys.
- **Data Sovereignty:** Organizations can maintain control over where their encryption keys are stored and who can access them, which is critical for meeting data residency requirements.
- **Key Revocation:** The ability to revoke a key at any time instantly renders data in the cloud unreadable, providing a rapid response capability to security incidents.
- **Mitigation of Vendor Lock-in:** By owning the master key, organizations can avoid some of the difficulties associated with migrating data between different cloud providers.

Weaknesses:

- **Shared Trust Model:** A significant security weakness is the shared-trust model. The customer must still trust the CSP's internal controls to prevent unauthorized access to the keys and data.
- **Increased User Responsibility:** The customer bears the responsibility for securing the key against loss, compromise, or deletion. If a key is lost, the data becomes irretrievably inaccessible.
- **Infrastructure and Management Overhead:** BYOK requires an organization to invest in and maintain its own on-premises key management infrastructure, such as HSMs, which can increase cost and complexity.

3.6 What organizations should use BYOK?

BYOK is a suitable choice for organizations that need a balance between cloud convenience and enhanced data control.

- **Regulated Industries:** It is ideal for organizations in highly regulated sectors that need to meet compliance standards and demonstrate clear control over their encryption keys for audit purposes.
- **SaaS Providers:** Software-as-a-Service (SaaS) providers can use BYOK to offer cryptographic separation of tenant data, isolating each customer's data using their own unique key. This builds trust and enhances their security posture.

- **Multi-Cloud Strategies:** Organizations implementing a multi-cloud or hybrid strategy can use BYOK to maintain consistency in key management across different environments and avoid being locked into a single provider.
- **Specific Service Examples:** Several major cloud services support BYOK, including Microsoft 365, Azure Information Protection, and Power BI Premium.

4 Hold Your Own Key (HYOK): The Sovereign-Centric Model

4.1 Concept Definition and Core Principle

Hold Your Own Key (HYOK) is a key management model that provides the highest level of protection against unauthorized access to sensitive information. The fundamental principle of HYOK is that the cryptographic keys are exclusively generated, managed, and stored within the customer's security perimeter. The key material never leaves the customer's environment and is, therefore, completely inaccessible to the cloud provider or any other third party. This ensures that sensitive data is encrypted before it is even transmitted to the cloud, guaranteeing that it remains in encrypted form and that the CSP has no access to the plaintext data.

4.2 Operational Mechanics and the Role of Modern Enablers

In the traditional HYOK model, all cryptographic operations—encryption and decryption—must occur on-premises or within a customer-controlled environment. This approach, while offering unparalleled security, often limits the functionality of cloud-native applications that require access to unencrypted data to perform their services.

Modern solutions, such as the virtual Hardware Security Module (vHSM), are changing this dynamic by enabling HYOK principles in a cloud-native, hybrid environment. This new approach leverages advanced security technologies to create a secure, isolated execution environment for key management within a confidential virtual machine (cVM). The core technologies that enable this are:

- **"Buckypaper" Virtualization:** This atomic execution environment shields the workload and ensures both the confidentiality and integrity of the execution. It achieves this through a three-dimensional encryption strategy:
  - **Data at rest encryption:** Encrypts data on disk and cloud storage from within the buckypaper VM.
  - **Data in transit:** Protects data as it moves between systems to prevent interception.
  - **Data in use:** A critical advancement that ensures data remains encrypted even while being actively processed in memory, a vulnerability that traditional methods fail to address.
- **Attestable Boot:** This process verifies the integrity of the system's boot sequence by using cryptographic hashes to confirm that every component, from firmware to the operating system, has not been tampered with. This provides cryptographic evidence that the machine has booted from a trusted, untampered software stack, which is crucial for enforcing a zero-trust policy in the cloud.

These technologies allow an organization to achieve a new form of HYOK by maintaining control over keys and data within a private/public/hybrid cloud environment, effectively bridging the gap between absolute security and cloud functionality.

4.3 Security and Access Analysis

HYOK provides an uncompromising security posture but requires a full acceptance of the associated responsibilities.

Strengths:

- **Absolute Control and Data Sovereignty:** The customer has exclusive control over the keys, which never leave their environment. This ensures unparalleled security and protects against extraterritorial legal claims, such as those under the U.S. CLOUD Act, by making the data legally inaccessible to the CSP.
- **Mitigation of Insider Threats:** The cloud provider and its personnel have no access to the plaintext data or the key material, significantly reducing the risk of a breach due to insider threats or CSP vulnerabilities.
- **Total Key Revocation:** Since the key resides solely with the customer, access to the encrypted data can be instantly and permanently revoked by simply deactivating the key's URL.

Weaknesses:

- **Single Point of Failure (User):** The immense responsibility of managing and securing the keys rests solely with the customer. If the keys are lost or mishandled, the data can be irretrievably lost with no recovery process.
- **Hardware Vulnerability:** While HSMs are tamper-resistant, the on-premises hardware is still susceptible to physical theft or damage, which must be addressed through robust physical security protocols.

4.4 Single-Cloud Architecture for HYOK

The single-cloud HYOK architecture is characterized by a complete separation of duties and physical key possession. The cloud provider's environment, including the application and data services, contains no keys. All master keys are stored within an on-premises or separate secure environment containing a customer-owned EKM and HSM. When a cloud application needs to decrypt data, it initiates a synchronous API call to the customer's EKM, requesting a cryptographic operation. The EKM, which has sole possession of the master key, performs the operation (e.g., unwrapping the DEK) and returns the decrypted data to the cloud application. Some implementations, such as AWS's External Key Store (XKS) and Google's Cloud EKM, utilize a double-encryption process where the data is first encrypted with an internal key before being sent to the external key manager, providing an additional layer of security. This architecture enforces a true zero-trust model, as the cloud provider can never access the plaintext key material.

4.5 Hybrid Multi-Cloud Architecture for HYOK

The HYOK model's architecture is inherently well-suited for a hybrid multi-cloud environment. A single, centralized EKM/HSM located in the customer's on-premises environment acts as the sole root of trust for all cryptographic operations across multiple cloud providers. Applications in different clouds—such as AWS, Azure, and Google Cloud—make synchronous API calls to this centralized EKM to perform encryption and decryption. This design eliminates the key silos and vendor lock-in challenges of the native KMS model. The customer maintains a single, unified key management strategy and can instantly revoke access to all cloud data by disabling the EKM or severing the network connection to it, instantly rendering the data inaccessible.

4.6 Strengths and Weaknesses

The choice of HYOK represents a strategic philosophical trade-off between absolute security and operational agility.

Strengths:

- Unparalleled security and data sovereignty, providing peace of mind for the customer.
- Complete provider exclusion, ensuring the confidentiality of sensitive information.
- Ideal for handling highly sensitive, regulated, or classified data.

Weaknesses:

- **Operational Complexity and Cost:** HYOK requires significant investment in on-premises infrastructure, expertise, and management, making it costly to establish and maintain.
- **Limited Cloud Functionality:** Many cloud services and SaaS applications do not support HYOK, as they require access to plaintext data to function. This limits the range of cloud features available and can create friction for developers.

4.7 Which organization should use HYOK?

The primary strength of the HYOK model is that it is the only one that truly delivers a zero-trust security posture toward the CSP. The customer maintains absolute control and physical possession of the key material, which is a prerequisite for certain highly sensitive or government-classified workloads and is the gold standard for data sovereignty compliance.

This model is ideal for industries like government, defense, and finance, where legal and regulatory mandates are non-negotiable and outweigh the associated costs and operational burdens. However, the most significant challenge is the performance overhead. Every cryptographic operation requires a network call to the EKM, which introduces latency and can create a major bottleneck for high-volume applications. This is where upcoming vHSM offer an opportunity to bridge the gap between HYOK and Latency.

The choice of compatible cloud services is also limited, as not all cloud providers and SaaS solutions support HYOK.

HYOK is primarily suited for organizations with the most stringent security and compliance requirements.

- **Highly Regulated Industries:** It is essential for sectors like government, defense, and finance, where data confidentiality is paramount and legal jurisdiction is a concern.
- **Secure Storage and Archiving:** HYOK excels in applications that require secure data storage, archival, or backup solutions where data integrity must be maintained without any risk of exposure to a third party.
- **Cryptocurrency and Blockchain:** In the world of cryptocurrencies, HYOK is the foundational principle for self-custody wallets, where users hold their own private keys to maintain sovereignty over their digital assets.

5 Comparative Analysis: Navigating the Key Management Spectrum

5.1 The Three Models: A Side-by-Side Comparison

The choice between KMS, BYOK, and HYOK is not a simple one, as each model exists on a spectrum of control, convenience, and security. An informed decision must be based on a comprehensive understanding of the trade-offs involved across several key dimensions.

- **Key Ownership vs. Possession:** While a KMS key is owned and possessed by the CSP, a BYOK key is owned by the customer but possessed by the CSP, and an HYOK key is both owned and possessed by the customer. The implications of this are significant, as possession is critical to protecting a key and its associated data.
- **Trust Model:** KMS requires a high level of trust in the CSP's security and internal processes. BYOK introduces a shared-trust model, where the customer and CSP must both uphold their security responsibilities. HYOK operates on a zero-trust model, where the customer trusts no third party with The key material.
- **Operational Burden:** KMS places minimal operational burden on the customer, as the CSP automates key lifecycle management. BYOK increases this burden, requiring the customer to manage key generation, rotation, and protection. HYOK requires the highest level of operational complexity,demanding significant investment in infrastructure and expertise.
- **Integration and Agility:** KMS offers seamless integration and high agility, as it is a native service deeply integrated with the cloud provider's ecosystem. BYOK also offers strong integration but may require a specific setup. HYOK provides the lowest level of integration, as many cloud services do not support external key management, potentially limiting cloud functionality.
- **Compliance and Legal Risk:** All three models can facilitate compliance, but they address different levels of risk. KMS meets basic requirements. BYOK provides a clear audit trail and greater control for regulations like HIPAA and GDPR. HYOK offers the strongest legal protection by preventing the CSP from being forced to surrender keys or data under legal mandates.

The choice of a key management model is a direct consequence of an organization's core priorities. The highest security (HYOK) comes with the highest complexity and lowest functionality, while the highest convenience (KMS) comes with the lowest level of customer control. The highest-value outcome is achieved when the security posture is aligned with the organization's specific threat model, compliance needs, and risk appetite.

5.2 The Role of Modern Solutions: Virtual HSMs and the Future

New technologies are emerging that blur the lines between these traditional key management models. The provided research on virtual HSMs (vHSMs) highlights a new approach that combines the security of on-premises solutions with the agility of the cloud. By leveraging confidential computing and „bucky-paper virtualization," vHSMs create a secure, isolated execution environment where data can remain encrypted even while in use.

This paradigm shift allows an organization to achieve the core principles of HYOK—key material never leaves the customer's enclave—within a cloud-native architecture. The integrity of this environment is cryptographically proven through Attestable Boot, providing a zero-trust foundation. This new model offers a compelling middle ground, potentially enabling organizations to achieve the unparalleled security of HYOK without the substantial operational and functional limitations of a traditional on-premises solution. This innovation provides an alternative to the binary choice between security and functionality, opening up new possibilities for key management in the cloud.

5.3 Summary Table: Key Management Concepts: A Strategic Comparison

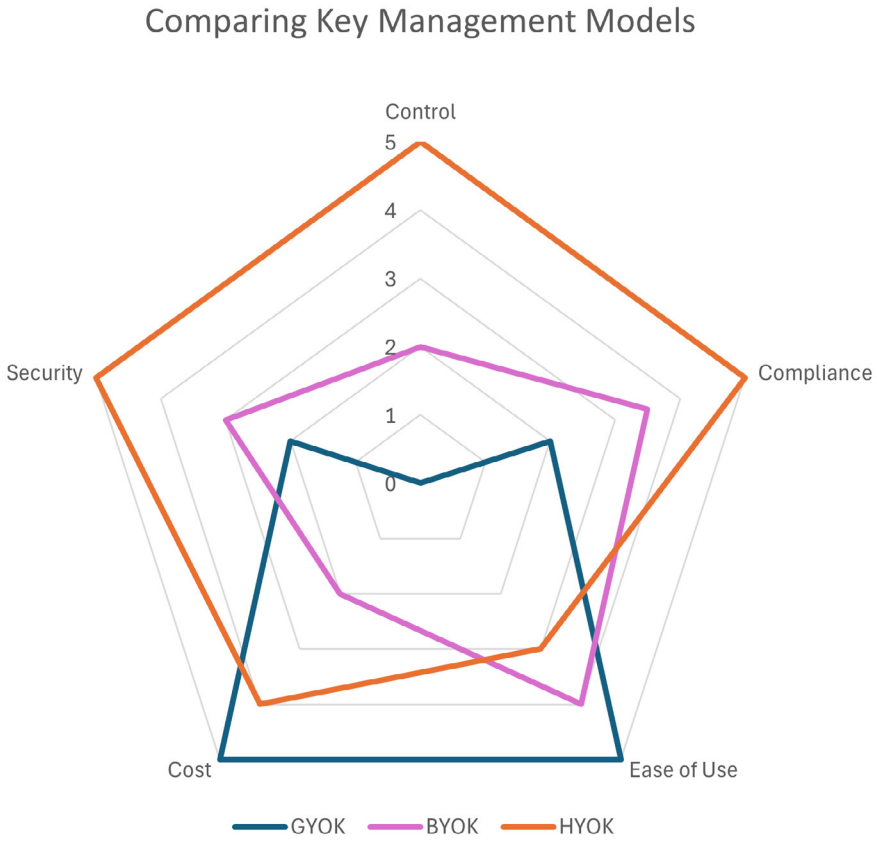
Feature	Key Management Service (KMS)	Bring Your Own Key (BYOK)	Hold Your Own Key (HYOK)
Key Ownership	Cloud Service Provider (CSP)	Customer	Customer
Key Possession	CSP	CSP	Customer
Key Location	Within CSP's environment (Cloud)	On-Premises (Original) and imported into CSP's environment	Exclusively within customer's environment
Primary Security Model	Provider-managed trust	Shared trust (customer owns, CSP possesses)	Zero-trust (customer maintains sovereignty)
Operational Complexity	Low	Medium	High
Trust Model	High trust in CSP	Partial Trust in CSP	Zero Trust
Integration with Cloud Services	Deep and seamless	Strong	Limited

Feature	Key Management Services (KMS)	Bring Your Own Key (BYOK)	Hold Your Own Key (HYOK)
Primary Advantage	Convenience, ease of use, high availability	Enhanced compliance and auditability	Unparalleled security and data sovereignty
Primary Disadvantage	Reliance on CSP, potential vendor lock-in	Increased user responsibility, shared-trust risk	High cost, operational burden, functional limitations
Data Sovereignty	Low	Medium	High
Ideal Use Case	General-purpose applications, non-sensitive data	Regulated industries, multi-cloud strategies, SaaS providers	Highly sensitive, classified, or legally exposed data, IP, PII
Performance	High	High	Configurable Very high to low
Compliance Suitability	Basic requirements	Strong for regulatory compliance (e.g., GDPR, HIPAA)	Exceptional for highest-level security and legal protection
TCO	Medium	High	Medium

6 Conclusion: Choosing the Right Strategy for Your Organization

The decision to adopt a specific key management model is a strategic one, not merely a technical one. The choice should be driven by a thorough assessment of an organization's threat model, regulatory obligations, and technical capacity. The analysis presented in this whitepaper demonstrates that GYOK, BYOK, and HYOK each serve a distinct purpose and offer a unique balance of security, access, and convenience.

- For organizations prioritizing **operational efficiency and seamless integration**, GYOK is the most suitable choice. It is ideal for general-purpose applications and non-sensitive data where a high level of trust in the cloud provider is acceptable.
- For organizations in **regulated industries** that need to demonstrate control and auditability without fully abandoning cloud-native functionality, BYOK provides a robust middle ground. It offers the ability to meet stringent compliance requirements while leveraging the benefits of a cloud ecosystem.
- For handling **highly sensitive, classified, or legally-exposed data**, HYOK is the only acceptable option. It provides the highest level of security and data sovereignty, ensuring that an organization's most critical information remains protected from third-party access and legal mandates.



Ultimately, the future of key management lies in innovative solutions that combine the best aspects of these models. New technologies like Virtual HSMs are enabling a hybrid approach that allows organizations to achieve the sovereign security of HYOK with the operational benefits and scalability of cloud computing. By carefully evaluating these options and aligning them with business objectives, an organization can create a cryptographic key management strategy that is both secure and agile, ensuring the long-term integrity of its data in the ever-evolving cloud landscape.

Notices

Customers are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) may represent or impact current enclaive product offerings and practices, which are subject to change without notice, and © does not create any commitments or assurances from enclaive and its affiliates, suppliers, or licensors. enclaive products or services are provided “as is” without warranties, representations, or conditions of any kind, whether express or implied. The responsibilities and liabilities of enclaive to its customers are governed by enclaive agreements, and this document is not part of, nor does it modify, any agreement between enclaive and its customers.

Glossary of Terms

- **AES (Advanced Encryption Standard):** A symmetric encryption algorithm.
- **CMK (Customer-Managed Key):** A key in a cloud KMS whose lifecycle and policies are controlled by the customer.
- **CSP (Cloud Service Provider):** A company offering cloud computing services, such as AWS, Azure, or Google Cloud.
- **DEK (Data Encryption Key):** A key used to encrypt the actual data.
- **EKM (External Key Manager):** A key management system (HSM or software) external to the cloud provider, used for HYOK.
- **FIPS (Federal Information Processing Standard):** A U.S. government computer security standard. FIPS 140-2 is a certification for cryptographic modules.
- **HSM (Hardware Security Module):** A physical, tamper-resistant computing device used for protecting and managing digital keys.
- **KEK (Key Encryption Key):** A master key used to encrypt other keys (DEKs).
- **KMS (Key Management Service):** A managed cloud service for key creation, storage, and lifecycle management.
- **PMK (Platform-Managed Key):** An encryption key whose lifecycle is fully managed by the cloud provider.
- **vHSM (virtual Hardware Security Module):** A logical, build on confidential computing, tamper-resistant computing environment used for protecting and managing digital keys and further services.
- **XKS (External Key Store):** AWS's specific name for its HYOK implementation.

Further Reading from Multiple Sources[2]

1. What is Bring Your Own Key (BYOK)? - Utimaco,
   https://utimaco.com/service/knowledge-base/encryption/what-bring-your-own-key-byok
2. What is a virtual HSM - enclaive,
   https://docs.enclaive.cloud/virtual-hsm/documentation/what-is-virtual-hsm
3. Why a HSM - Key Management Challenges - enclaive,
   https://docs.enclaive.cloud/virtual-hsm/documentation/why-a-vhsm
4. How does a virtual HSM work - enclaive,
   https://docs.enclaive.cloud/virtual-hsm/documentation/how-does-it-work
5. What is Bring Your Own Key (BYOK)? - Entrust,
   https://www.entrust.com/resources/learn/what-is-bring-your-own-key-byok
6. AWS KMS: Default vs. Custom Keys for Enhanced Security and Compliance - ElasticScale,
   https://elasticscale.com/blog/how-secure-is-aws-kms/
7. Pros and Cons of Amazon's Key Management Service - The IT Hollow,
   https://theithollow.com/2017/02/13/pros-cons-amazons-key-management-service/
8. Bring Your Own Key (BYOK): Pros and Cons - Clumio,
   https://web-dev.clumio.com/blog/byok-pros-and-cons/
9. What is Hold Your Own Key (HYOK)? - Utimaco,
   https://utimaco.com/what-hold-your-own-key-hyok
10. What is Bring Your Own Key (BYOK) Encryption? - Thales CPL,
    https://cpl.thalesgroup.com/faq/key-secrets-management/what-bring-your-own-key-byok
11. Case Studies - KMS Software,
    https://kms-software.com/resources/case-studies/
12. Case Studies - Knowledge Management - KMS Lighthouse,
    https://kmslh.com/case-studies/
13. Amazon Connect Customers - Amazon Web Services,
    https://aws.amazon.com/connect/customers/
14. KMS (Key Management Service) - securiti Glossary,
    https://securiti.ai/glossary/key-management-service-kms/#:~:text=A%20Key%20Management%20Service%20(KMS,for%20encryption%20and%20decryption%20purposes.
15. Cloud Key Management Service overview | Cloud KMS - Google Cloud,
    https://cloud.google.com/kms/docs/key-management-service
16. FAQs | AWS Key Management Service (KMS),
    https://aws.amazon.com/kms/faqs/
17. Decide on KMS Requirements | The Cloud Posse Reference Architecture,
    https://docs.cloudposse.com/resources/legacy/design-decisions/decide-on-kms-requirements/

2 The online sources listed were last accessed on September 30, 2025. Please note that the availability or content of the referenced websites may have changed after this date.

18. Why building your own BYOK is a trap - WorkOS, https://workos.com/blog/byok-with-vault
19. Bring Your Own Key (BYOK) details - Azure Information Protection - Microsoft Learn, https://learn.microsoft.com/en-us/azure/information-protection/byok-price-restrictions
20. Understanding the Basic Differences Between BYOK & HYOK - Fortanix, https://www.fortanix.com/blog/differences-between-byok-and-hyok
21. Understanding BYOK: Bring Your Own Key Explained - Cryptomathic, https://www.cryptomathic.com/blog/understanding-the-various-meanings-of-bring-your-own-key
22. BYOK Meaning: Key to Secure Cloud and Enterprise Data - Lark, https://www.larksuite.com/en_us/blog/byok-meaning
23. BYOK, CYOK, HYOK: Cloud Key Management Explained - Cryptomathic, https://www.cryptomathic.com/blog/what-is-the-difference-between-byok-cyok-hyok
24. Bring Your Own Key (BYOK) - Piwik PRO, https://piwik.pro/glossary/bring-your-own-key-byok/
25. Bring your own encryption keys for Power BI - Microsoft Fabric, https://learn.microsoft.com/en-us/fabric/enterprise/powerbi/service-encryption-byok
26. BYOK and HYOK in ASP.NET Core — Detailed Explanation with Use Cases - Medium, https://medium.com/@kirteshsuthar2605/byok-and-hyok-in-asp-net-core-detailed-explanation-with-use-cases-fd0c2f068463
27. BYOK vs HYOK: What's the Difference and Which Approach Is Right for You? - archTIS, https://www.archtis.com/byok-vs-hyok-whats-the-difference-and-which-is-right-for-you/
28. What is Hold Your Own Key (HYOK)? - EntropiQ, https://entropiq.com/hyok/
29. What is Cloud Security Architecture? Principles and Framework - Wiz, https://www.wiz.io/academy/cloud-security-architecture
30. Bring Your Own Keys (BYOK): explained - IronCore Labs, https://ironcorelabs.com/byok/
31. Hold Your Own Key (HYOK): explained | IronCore Labs, https://ironcorelabs.com/hyok/
32. Key Management Systems: Cloud-Based vs On-Premises KMS Solutions - Futurex, https://www.futurex.com/blog/key-management-systems-software-vs-hardware
33. Overview of Key Management in Azure | Microsoft Learn, https://learn.microsoft.com/en-us/azure/security/fundamentals/key-management
34. AWS Key Management Service Cryptographic Details - awsstatic.com, https://d1.awsstatic.com/whitepapers/KMS-Cryptographic-Details.7d90f34ba02a50805cefbafad3d35edba3b4cb29.pdf

35. Azure Key Vault - DEV Community,
https://dev.to/pedroignacio13/azure-key-vault-4i7b

36. Cloud Key Management Service encryption | Security,
https://cloud.google.com/docs/security/key-management-deep-dive

37. Multi Cloud Architecture: Tutorial & Best Practices - Multiplayer,
https://www.multiplayer.app/system-architecture/multi-cloud-architecture/

38. How to generate & transfer HSM-protected keys – BYOK – Azure ...,
https://learn.microsoft.com/en-us/azure/key-vault/keys/hsm-protected-keys-byok

39. External key stores - AWS Key Management Service,
https://docs.aws.amazon.com/kms/latest/developerguide/keystore-external.html

40. Cloud External Key Manager | Cloud KMS - Google Cloud,
https://cloud.google.com/kms/docs/ekm

41. Reference architectures for Cloud External Key Manager | Cloud KMS - Google Cloud,
https://cloud.google.com/kms/docs/ekm-architectures