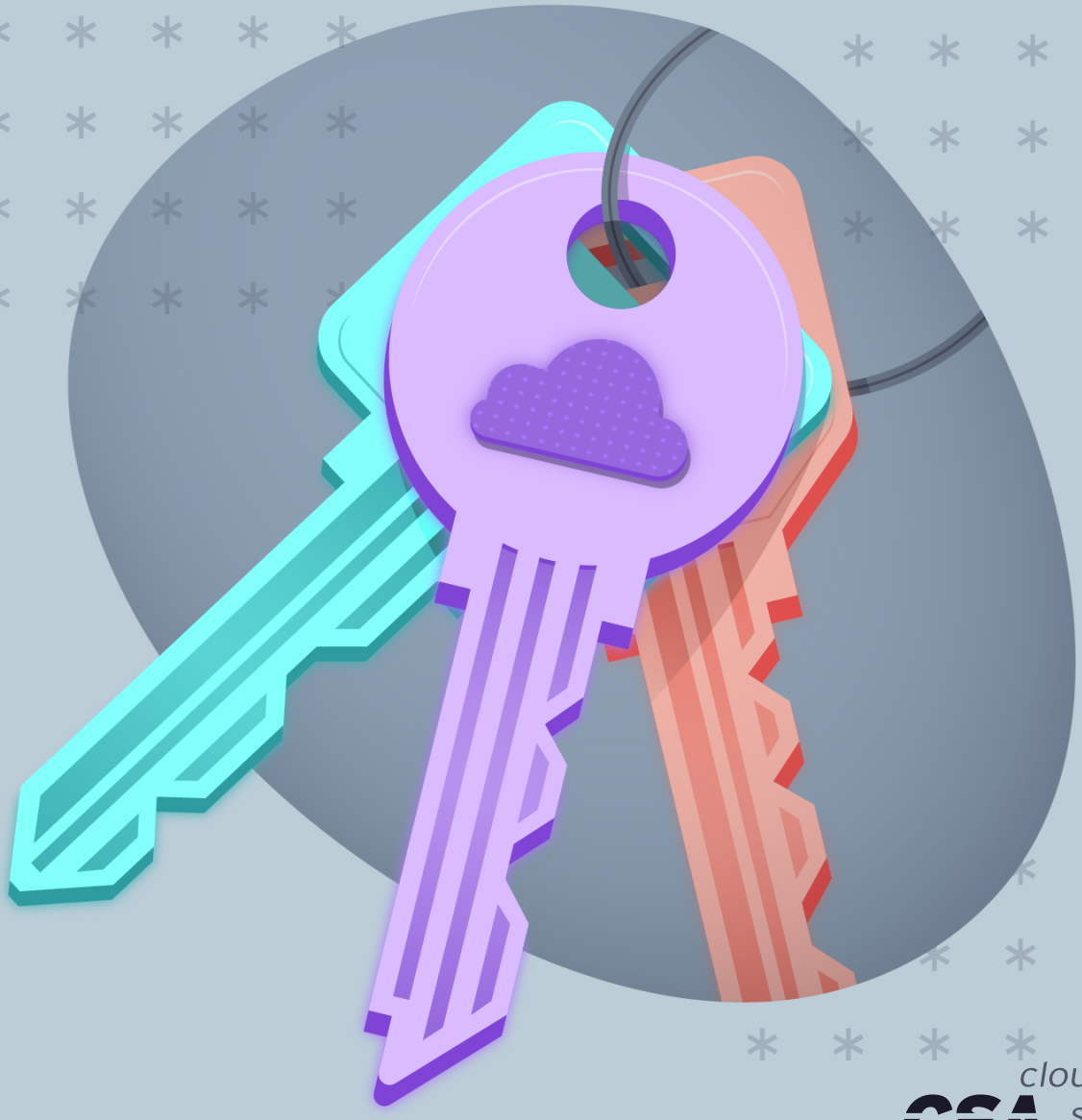
Recommendations for Adopting a Cloud-Native Key Management Service with an External Key Origin



cloud security alliance®

The permanent and official location for Cloud Security Alliance Cloud Key Management research is https://cloudsecurityalliance.org/group/CKM.

Acknowledgments

Working Group Co-Chairs:

Paul Rich
Mike Schrock

Lead Authors:

Paul Rich
Michael Born

Contributors:

Marina Bregkou
Michael Roza
Mike Schrock
James Underwood

Reviewers:

Damian Crosby
Iain Beveridge

CSA Staff:

Marina Bregkou
Claire Lehnert (Design)
Stephen Lumpe (Cover)

Table of Contents

1. Introduction

Before reading this document, readers are encouraged to review Key Management in Cloud Services, which provides the foundation for the choice of Cloud KMS pattern and general guidance for using KMS whether the KMS is native to a cloud platform, external, self-operated, or yet another cloud service. Also worth reading is "Recommendations for Adopting a Cloud-Native KMS," which provides more specific guidance for choosing, planning, and deploying Cloud-native key management systems (KMS).

Cloud-native key management systems offer organizations of any size and complexity a low-cost option for meeting their needs for key management, particularly for cloud services within the same provider. The cloud-native KMS operates as a Platform-as-a-Service (PaaS), where the provider operates all hardware, network, and software platform resources, and the customer provisions KMS artifacts (e.g., keys, vaults, secrets, policies) and directs applications to leverage the cloud-native KMS artifacts. Where a cloud-native KMS supports the import of key material, we refer to the pattern as *Cloud-Native KMS using External Key Origination (EKO)*. This document provides recommendations for adopting this pattern once the decision to do so has been made. For guidance on the choice of pattern to adopt, refer to the aforementioned CSA document Key Management in Cloud Services.

A cloud service provider's key management system (KMS) often has strong ties to its other cloud services. This same cloud-native KMS using EKO can also be used with a customer's [on-premises] technologies and cloud services from other providers. Integrating a cloud KMS with an organization's assets spanning traditional private data centers and private and public cloud services in various geographic locations presents multiple challenges: technical, operational, legal, regulatory, and financial.

As a general rule, the confidentiality and integrity of major cloud service providers are considered strong and well-attested. Because of this, when an organization or customer selects a cloud-native KMS using EKO, simplicity and availability are typically the overriding concerns. This is because key management systems are often fundamental to the availability of other technology systems. Therefore, downtime can have a catastrophic, cascading business impact. Though legal and regulatory obligations are undoubtedly important, operational reliability should not be sacrificed for these obligations unless there is a clear understanding and acceptance from both IT and business leadership.

Key management systems typically have a low cost of ownership relative to most information technology systems. With the use of a well-established, top-tier cloud vendor, security could likely be as good as, or better, than most on-premises key management systems for most organizations. With the advent of cloud-based key management systems, the cost of deployment and operation can be further reduced. Therefore, financial considerations will likely be of the least concern to organizations regarding a business driver/benefit. However, the cost is not an area to ignore when using cloud key management systems because the cost is typically a function of transactions. For that reason, an understanding of transaction volume and the drivers of transactions will be necessary to estimate service cost and perform charge-back where warranted.

1.1 Purpose

The purpose of this document is to provide general guidance for choosing, planning, and deploying cloud-native key management systems (KMS) where there is a desire or requirement to import key material from an external source. The guidance will provide recommendations that address technical, operational, legal, regulatory, and financial aspects of leveraging a cloud-native KMS using EKO. The goal is to optimize business outcomes, including security, agility, cost, and compliance.

The use of an external source for key origination does present the customer with some challenges. Minor challenges include researching the compatibility of key types/lengths/algorithms and the import process. The most significant challenge is reaching clarity on the purpose of using external key origination and ensuring that the purpose is going to be achieved. It is strongly recommended that customers eliminate all assumptions regarding their desire to use this cloud KMS model. It is strongly advised to use the guidance contained within Key Management in Cloud Services to identify and address assumptions.

It is important to note that adopting the guidance provided herein cannot ensure that business information is adequately protected when stored, processed or transmitted using public cloud services. This document provides guidance on how to assess and implement cloud key management services concerning an organization's needs for key management — it is up to the customer to then use encryption keys (or other artifacts, such as secrets) in ways that follow encryption best practices.

1.2 Scope

This paper addresses the "Cloud Native KMS using External Key Origin" pattern, first described in the CSA Working Group paper "Key Management in Cloud Services: Understanding Encryption's Desired Outcomes and Limitations," published in November, 2020. We address the considerations of the cloud-native KMS as well as the key material that will be imported, but the system(s) used to generate the key material are out of scope.

Coverage includes mainstream business and Information technology (IT) usage of hybrid and cloud technologies. We will not address more specialized patterns such as high-assurance military or intelligence community scenarios, as the recommendations made in this document should benefit organizations of any kind.

1.3 Target Audience

The audience for this document includes program and project managers, requirements or business analysts, architects, systems integrators, cloud customers, developers, as well as security and compliance staff concerned with the selection of, as well as the secure and reliable implementation and operation of, cloud-native key management services using external key origin.

A primary use of this document is as an aid to the program or project manager who leads an organization through the lifecycle stages covered here. The goal is to provide content that is clear and conveys enough explanation that the project manager can identify how to map the considerations to their organization.

2. Cloud-Native KMS using EKO Overview

In the cloud KMS patterns identified in the CSA paper "Key Management when Using Cloud Services,"[1] the cloud-native KMS using external key original pattern reflects the scenario where a customer has chosen to use a [public] cloud-hosted KMS that is designed and operated as a multi-tenant cloud service, including hardware-based key protection, and has also chosen to use one or more keys from an external source[2].

To achieve hardware-based key protection, typically, the cloud provider leverages a shared array of Hardware Security Modules (HSM) exposed as an Application Programming Interface (API). This model allows abstraction of the hardware and has tremendous potential to scale relative to traditional private data center deployments. Additionally, the cloud provider's architecture offers very high fault tolerance and transactional performance while maintaining confidentiality, integrity, and availability of keys during the lifetime of its cryptographic operation.

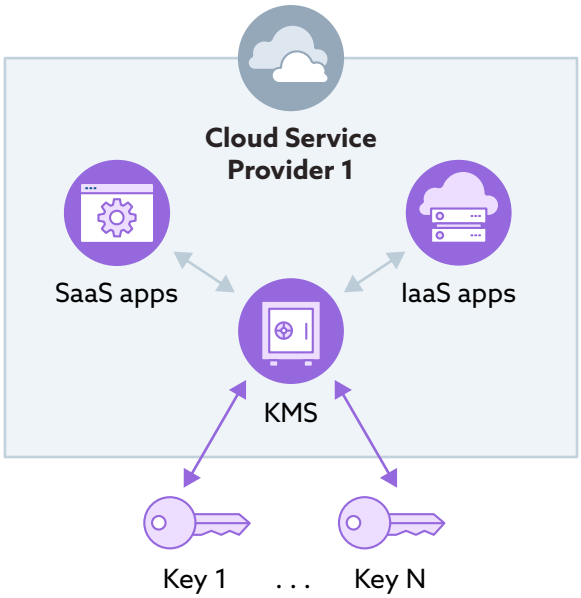


Figure 1: Leveraging the services of a cloud-native KMS and importing key(s) from an external source.

The scenarios that will be covered for this pattern are as follows:

- Choosing a cloud-native KMS using EKO
- Planning a cloud-native KMS using EKO
- Deploying a cloud-native KMS using EKO

[1] https://cloudsecurityalliance.org/artifacts/key-management-when-using-cloud-services/

[2] See https://cloudsecurityalliance.org/artifacts/key-management-when-using-cloud-services/ for the reasons a customer may choose an external key source, as well as the pros and cons of choosing this model.

Within each of the above scenarios, the following considerations are addressed:

1. Technical considerations, examples of which include

a. Development and systems configuration work necessary for adoption
    i. Typically, with this pattern, there is no development work required (or possible) within the cloud.
    ii. The cloud-native KMS using EKO typically cannot be modified or extended through software development by the customer, and co-resident cloud applications are typically written to fully integrate with the provider's KMS.
    iii. Therefore, development work refers to any software that needs to be written to integrate customer systems, including customer KMS with the cloud-native KMS using EKO.
    iv. Examples of customer applications and systems that may need software development done for integration include (a) custom applications, (b) asset management systems, (c) change control and/or ticketing systems, (d) log collection, and (e) reporting/analytics.
b. Development platform(s) supported by the cloud service provider
    v. The ability to integrate with internal systems and the ease with which staff can adapt software can impact both the cost of adoption and the degree of automation possible.
    vi. Additionally, automation has many downstream effects, including incident response dynamics, change management, and speed of adoption.
c. Scalability requirements, including any transaction limitations or surcharges as well as elasticity in geography
d. Provider documentation
    vii. Newer services often have less depth of documentation, and this may necessitate a paid support contract to obtain technical information.
e. Provider roadmap and track record of delivering change/features
    viii. The cloud KMS market is relatively new and rapidly evolving, and providers that give a view into the future give customers an ability to adapt to change more rapidly and thus take advantage of innovation as new features are introduced.

2. Operational considerations, examples of which include

a. Policies governing the use of the cloud KMS, which can range broadly across the goals of confidentiality (e.g., authentication mechanisms), availability (e.g., key escrow policy), and security (e.g., periodic auditing of events and actions);
b. Change management, with considerations for both the integration capabilities and the amount of notice from the CSP regarding service changes, as well as the methods of notification (email, text, portal);
c. Business continuity and disaster recovery options and configurability, including provider playbooks and customer testimonials of real-world experiences;
d. The CSP identity and permissions model for administering the service, including the granularity of supporting roles, just-in-time elevation, automated removal of permissions, periodic assessment of permissions granted, and integration with external identity systems;

e. The CSP track record with service level agreement violations and penalties;
f. The extent of scenarios to be used by the customer. In particular, a cloud-native KMS using EKO is (or may be) used in conjunction with applications not natively supported and with services and systems external to the CSP;
g. Geographic diversity, keeping in mind latency sensitivity of the organization's applications that will, or may in the future, leverage the KMS;
h. Provider quota/rate-limiting controls. Some providers have rate-limiting on KMS operations, and some have limits on collecting log data. Organizations should inquire about any capacity or rate limitations and ensure the provider's service-level agreement defines and specifies any limitations.
i. Provider logging, notification, and incident response capabilities; organizations should ensure that logging verbosity is sufficient and timely enough to meet downstream operational commitments.

3. Regulatory considerations, examples of which include

a. Changes/configuration necessary to comply with regulations applicable to the customer;
b. Whether or not the CSP offers a template or direct configuration option to enforce particular regulatory compliance;
c. Existing regulatory compliance certifications mapped to the customer's requirements and any provision for the failure of the CSP to maintain the certification.

4. Legal considerations, examples of which include

a. Contractual or external legal authority mandates
b. Contractual representations and warranties

5. Financial considerations, examples of which include

a. Factors that may drive cost increases or decreases are rate-limiting and quota features, provider billing features, provider service menu options, and SLA penalties.

Cloud-native key management systems using EKO are relatively new to the world of computing, and thus the set of best practices available is necessarily small[3]. Therefore, the guidance provided combines best practices drawn from experience with traditional key management systems, cloud services in general, and cloud-native key management systems.

[3] Reader feedback is welcomed and can be submitted via https://circle.cloudsecurityalliance.org/home.

3. Choosing a Cloud-Native KMS using EKO

When choosing a cloud provider for a cloud-native KMS using EKO, the organization should create a list of technical, operational, legal, regulatory, and financial requirements that the provider must meet. It is unusual to find significant differences in the legal, regulatory, and financial aspects of cloud service providers (CSPs), so typically it is the technical and operational considerations that are the main differentiating factors.

3.1 Technical Considerations

The following technical considerations will help determine whether a particular cloud-native KMS using EKO offering provides the functionality needed by a specific organization. It should be noted that PCI DSS, along with GLBA/FFIEC and FISMA, requires NIST-certified AES encryption and FIPS 140-2-compliant key management.

3.1.1 Hardware Security Module (HSM) Backed Keys

Consideration	Justification/ Rationale
Is the cloud-native KMS using EKO capable of protecting keys using a Hardware Security Module?	HSM-backed keys may help meet compliance requirements such as FIPS 140-2 levels 2[4] and above or provide additional physical security of keys.[5]
Is the cloud-native KMS using EKO capable of importing keys generated from an external source?	This is the fundamental requirement for this pattern, and an inability to accept keys from an external source will rule out the use of that cloud-native KMS using EKO.
Can the cloud-native KMS using EKO accept keys from the customer's local KMS software/ hardware configuration?	A cloud-native KMS using EKO may have limited support for external key sources. For example, a provider may be capable of accepting keys from only a limited set of HSM manufacturers. The customer may need to acquire compatible hardware/software.

[4] For additional information see https://csrc.nist.gov/publications/detail/fips/140/2/final

[5] To verify if the components of a cloud-native KMS using EKO may be validated to meet FIPS cryptography standards the Cryptographic Module Validation Program (CMVP)# provides the necessary information.

3.1.2 General Technical Considerations

Consideration	Justification/ Rationale
Does the cloud-native KMS using EKO provide the ability to migrate to one of the other cloud KMS patterns?	The flexibility to move to a more complex cloud KMS pattern may be required when the customer's needs change.[6]
Does the cloud-native KMS using EKO support the types of secrets (key types and lengths; passwords or passphrases, connection strings or other blobs) planned for use?	Customers can leverage a cloud KMS for many types of secrets, and ensuring support for these types is fundamental to the choice of CSP.
Does the cloud-native KMS using EKO support creating or importing keys and secrets without the key being active or enabled?	The capability to create keys without immediate use/ activation is primarily used for key rotation functions. Creating a key before activation allows for time to plan the cutover, and in some cases, the re-encryption of data using the new keys.
Does the cloud-native KMS using EKO offer labeling functionality for keys and secrets (e.g., tags, metadata, etc.)?	The capability to label keys allows an inventory-based system to understand the key's usage and allows for potential internal processes to take action on the keys. Labeling keys is helpful in the event of key exposure. For example, if application X is exposed, having all keys used in application X tagged allows for easy identification and automation to replace those keys.
Does the cloud-native KMS using EKO enforce secure transport using modern standards?	Ensuring that proper (secure/latest version) TLS protocols are used when accessing the cloud-native KMS using EKO provides the necessary security such as Transport Layer Security (TLS) 1.2 or higher) when accessing the KMS, keys, or secrets.
Does the cloud-native KMS using EKO ensure/support a key transfer method that supports FIPS compliance throughout the transfer process?	For customers with FIPS compliance obligations, the key transfer process must not degrade the protections afforded a key while it is transmitted from the external KMS to the cloud-native KMS using EKO.

[6] For more information about migrating to one of the other KMS patterns, please see https://cloudsecurityalliance.org/artifacts/key-management-when-using-cloud-services/

Does the cloud-native KMS using EKO provide API functionality to access and manage keys and secrets?	Having API functionality allows for automation of activities in the cloud-native KMS using EKO. Automation is critical in larger organizations where cloud-native KMS using EKO providers can have many thousands of keys. Also, APIs allow the customer to more easily integrate key management operations into the business applications that leverage keys more easily.
What forms of access control does the cloud-native KMS using EKO provide?	Providing access to certain users, roles, etc., ensures that only authorized members of the organization access the cryptographic keys in accordance with their specific knowledge and function. Examples of access control include policy-based, role-based, attribute-based, and application-based.
Does the cloud-native KMS using EKO provider meet the organization's software security standards?	Each organization may have specific requirements that code and API must meet. Organizations should review the terms of service with the cloud provider for this assurance.
Does the cloud-native KMS using EKO offer granular network access controls to limit inbound traffic sources to the KMS?	In many scenarios, only certain IP ranges relevant to the organization will need access to the cloud-native KMS using EKO. The capability to limit inbound network access to those IPs increases the security of that KMS against access from malicious actors. This is a form of attack surface reduction.
Does the cloud-native KMS using EKO support cryptographic keys and secret lifespan and expiration settings?	As keys are used, a good rule to follow is that the longer a key is in use, the greater the chance that the key has been exposed. Having a key expiration or rotation capability allows for the regeneration of keys, thus ensuring that any exposure of keys is limited in timeframe and impact.
Does the cloud-native KMS using EKO offer the capability to back up and restore individual keys and secrets?	Cryptographic keys used in the encryption of data are critical not only to encrypt the data but also to decrypt the data. Should a cryptographic key be lost or destroyed, the data protected using that key is no longer accessible. Having the capability to back up keys protects that data. Backup copies of keys should be protected with controls that are as strong as the controls used for online keys.
Does the cloud-native KMS using EKO offer the capability to transfer backed-up keys or secrets from another cloud-native or on-premises KMS?	When backing up keys, the organization should consider where the backups will be placed. Using another KMS allows for a greater capability to "fail over" in the event of a disaster.

Does the cloud-native KMS using EKO offer multiple geographic locations for the KMS service to achieve redundancy?	As with any cloud service, customers should examine the provider's service resilience characteristics. This includes not only the geographic regions the provider operates from, but also the ability for the customer to choose the geographic placement of objects within their tenant. This allows customers to choose geographical pairings that optimize for the customer's own geographical operations.
Does the cloud-native KMS using EKO offer the capability to set a mandatory retention period for content before deletion (i.e., "recycle bin" or "soft delete")?	Soft delete provides recovery capability in the event a key is accidentally or maliciously deleted from the KMS.
Does the cloud-native KMS using EKO support secure key distribution (i.e., only accepting connections from authenticated endpoints such as mTLS)?	Keys should be distributed only to known endpoints that can be verified. The cloud KMS should, therefore, be able to interact with identity providers as required.
Does the cloud-native KMS using EKO offer reporting functionality, providing a dashboard of operational activities?	Many cloud-native KMS using EKO providers charge based on utilization. Having the capability to review operational activities in the KMS in an easy-to-view manner assists the organization in understanding and anticipating costs.
Does the cloud-native KMS using EKO integrate into asset management systems, e.g., CMDB, so it, along with the keys it creates, can be tracked as assets?	Cryptographic keys, as an integral part of an organization's security, should have the capability to be tracked as an asset. Ensuring their operation, availability, and lifecycle (creation, renewal, destruction, etc.) is essential to the health of the cryptographic functions.
Can the cloud-native KMS using EKO support just-in-time (JIT) access?	Ensuring proper access to the KMS is foundational to the security of the cryptographic keys within. Just-in-time access is the capability to provide access when needed, avoiding the use of persistent highly-privileged accounts. JIT access can be manually or automatically approved through policy actions.

3.2 Operational Considerations

The choice of a KMS provider has a significant impact on existing technology, people, and processes in the organization. Integrating the KMS into the overall architecture, processes, and procedures can be daunting. Given that the cloud-native KMS using EKO is either new or replacing an incumbent in the architecture, achieving appropriate implementation or uplift ensures that timely and consistent access to organizational data is maintained. The following operational considerations will help determine whether a particular cloud-native KMS using EKO can be supported by an organization.

Consideration	Justification/ Rationale
Does the cloud-native KMS using EKO provide an SDK/ API that can help to automate routine processes?	Automation of routine operations minimizes human interaction and produces reliable and repeatable results. An SDK/API provides an interface to achieve this. This can then be leveraged as part of robust, auditable, and consistent application development.
Does the cloud-native KMS using EKO provider's staff require access to the KMS as part of the provider's duties?	As part of operating in a public cloud, it is expected that the cloud provider will need to perform operations on infrastructure backing many of the Platform-as-a-Service (PaaS) solutions such as a KMS. As part of those operations, the cloud provider personnel may, at times, require access to the infrastructure housing the KMS. Some organizations may have concerns about the risk of exposure to cryptographic material or the use of persistent and highly privileged credentials. Organizations with these concerns should review the terms of service with the cloud provider to assess these risks.
Can some or all operations be required to use two-person integrity?	Requiring two or more persons to complete any operation helps protect against malicious insiders and mistakes.
Does the cloud-native KMS using EKO integrate with existing security controls such as a Security Information Event Management (SIEM) Platform for security monitoring?	The operations and activities within a KMS are sensitive and should be appropriately monitored to ensure no undue or malicious access or use.

3.3 Regulatory Considerations

Regulations and regulatory agencies typically do not specify implementation details for technology, and encryption is an area where regulators typically stay far away from specifying operational requirements. Regulators seek to guide or constrain behavior and outcomes, not technology. In fact, constraining technology can be counterproductive to regulators' intentions because doing so can hamper an organization's ability to innovate in ways that advance the regulators' objectives — usually risk reduction, improved privacy, and stronger security. Typically, if technology constraints are included in regulatory language, it is to set a minimum acceptable value[7] or compel the use of a technology[8] but not the specific implementation of that technology.

Regarding compliance with a regulation, the CSP can claim (and present documentation as proof) to be compliant with a regulation, but it is ultimately the customer's responsibility to ensure compliance to applicable regulations. Stated differently, a CSP can violate or support an organization's compliance with a regulation, but it cannot ensure its compliance, only that of its own systems and processes. For this reason, the customer needs to know what regulatory regimes it is subject to and ensure that the cloud KMS does not violate any of those regimes. An example of this is ISO 27001. A customer of Azure, for example, can obtain all Microsoft cloud service certifications for ISO 27001 at the Microsoft Service Trust Portal or via public Microsoft documentation.

In the realm of key management systems, few regulatory bodies have promulgated guidance or constraints. Known instances include the following:

> - In the USA, the Defense Information Systems Agency publishes the Cloud Computing Security Requirements Guide (commonly referred to as the DISA SRG), which in Section 5.11, "Encryption of Data-at-Rest in Commercial Cloud Storage," constrains the use of cloud KMS services as follows: "Mission systems at all impact levels must have the capability for DoD data to be encrypted at rest with exclusive DoD control of encryption keys and key management."[9]
> - The Bank of Israel (Supervisor of Banks) promulgated Memorandum 15LM2087 on 29/06/2015, constraining key management with cloud services as follows: "Cryptographic keys must be stored in the corporation Banking and not at the cloud service provider."

It should be noted that the regulatory bodies referenced above are authoritative in determining if their regulations are addressed using the cloud-native KMS using EKO pattern covered in this document.

---

[7] For example, the number of bits of entropy in an encryption key.
[8] For example, the use of encryption with certain data specified by the Payment Card Industry Security Standards Council, or the requirement to use encryption for data-in-transit.
[9] Note, however, that DISA SRG Section 5.11 includes a provision for exceptions to this constraint: "For cloud applications where encrypting DAR with DoD key control is not possible, Mission Owners must perform a risk analysis with relevant data owners before transferring data into a CSO." https://dl.dod.cyber.mil/wp-content/uploads/cloud/SRG/index.html#5.11EncryptionofData-at-RestinCommercialCloudStorage

Because regulations can and do change, the customer should understand the potential for "vendor lock-in" and determine the associated risk. Should applicable regulations change, the customer must consider the following possibilities: (a) the ability to move from the cloud-native KMS pattern to another pattern or an on-premises solution; (b) the CSP's ability and willingness to comply with the new regulation; and (c) the ability to obtain a temporary or permanent waiver for the regulation.

It should be noted, however, that "vendor lock-in" is something that may not be avoidable when an organization implements a cloud-native KMS using EKO. This might be the case if, for example, the decision to use a particular KMS using EKO was driven solely because the organization chose to adopt an IaaS, PaaS, or SaaS offering from the same CSP as the cloud-native KMS using EKO and the only KMS supported by the IaaS, PaaS or SaaS offering is the cloud provider's own cloud-native KMS using EKO. In this case, there is no way to avoid vendor lock-in.

It is also worth keeping in mind that regulators have not typically created constraints on using particular technologies, including KMS products and services. As a general rule, regulators keep away from these constraints because they do not concern themselves with *how* a regulation is complied with and focus only on *whether* a regulation is complied with.

3.4 Legal Considerations

When an organization chooses a cloud-native KMS using EKO, legal considerations fall into two categories: (1) the acceptability of the warranties and representations in the contract and (2) the likely outcome of any legal demand or lawsuit brought against the cloud service provider. The contract should include clear language that addresses the second consideration, but there are other factors that a customer may also want to consider.

Consideration	Justification/ Rationale
Does the contract define customer data and specify that ownership of that data resides with the customer?	Customers need assurances regarding the handling of content, including clear boundaries, for several reasons. Thus, the following considerations should be addressed: (1) any intersection with CSP personnel activities and obligations regarding safeguarding customer data; (2) the dynamics of how the CSP handles third-party data requests; (3) data deletion handling; (4) data portability. The contract should state that any data that the customer creates within, or imports to, the service is the sole property of the customer. The cloud service provider may require that the customer grant a license to permit the lawful processing of data stored in the cloud. This may be appropriate. However, if the processing of data stored in the cloud is a concern, the customer should contact a qualified attorney for further consultation.

Does the contract define log data and specify its availability, including latency?	The contract should, at a minimum, state that the service provides the customer with a means of obtaining log data for all activities within the customer's tenant for a reasonable period of time (e.g., 90 days is often a good starting point). The customer should seek to obtain warranties regarding the availability of the logging service (if it has its own SLA, which it should if it is excluded from the general service SLA) as well as the expected time delay for the availability of logging data following activity within the tenant. It is common for logging data not to be provided in real-time since the provider typically makes available the same log data that the provider itself consumes, but with some processing performed within the provider. For example, the provider may be aggregating the logs of many different systems or service components to produce log data for customers that is more immediately useful and coherent. However, it is worth keeping in mind that key management systems can have a widespread impact if incorrectly configured, operated, or breached. Therefore, customers are advised to insist on a low number of minutes as a reasonable upper boundary (perhaps 15 as the maximum but ideally no more than 3-5).
Does the contract describe how the cloud service provider will process third-party demands for customer data?	All cloud providers should represent how any third-party demands will be processed. Customers should expect that providers will follow all laws where they operate. Customers should also expect that the provider has a policy of informing the customer of any access to customer data for purposes of fulfilling a third-party data request, unless prohibited by law from doing so. Customers may also wish to inquire about any differences in this process between private sector and government or law enforcement requests.
Does the contract describe the physical and logical security measures taken to protect the service and its contents?	The contract should identify or provide a reference to another document considered part of the contract, which outlines what physical and logical security measures are taken to protect the service and its contents. Customers should expect physical measures to include secure facilities with man-traps, biometric authentication and authorization, video and audio surveillance, fail-secure mechanisms, and armed guards if warranted by physical location. Logical security measures should be appropriate for a company of the cloud-provider's size and sophistication, considering the sensitivity of stored data.
Does the contract include content retention policies?	The contract should specify representations regarding the minimum and maximum time that the provider will retain customer data once the customer has deleted the data within the service and ceased to continue the customer-provider relationship. These policies should ideally include default data destruction timelines and specify whether the deletion process meets any necessary "secure" requirements (e.g., disk shredding or multiple overwrites).

Does the contract include a Data Protection Addendum or equivalent, stating data security and processing terms including disclosure, security incident notification, data transfers, use of subprocessors, compliance with data privacy regimes[10] (e.g., GDPR, CCPA, et al.)?	This is often a regulatory requirement, and in any case, it is good practice for any customer to eliminate ambiguity with respect to customer data handling. Moreover, much of the content described throughout this section is often included in a DPA and nowhere else.
Does the contract define acceptable parameters for customers performing penetration testing or similar activities?	The contract should inform customers of what penetration testing is allowed, if any, and any limitations in the customer's actions.
Does the contract define and describe any regional availability, including service partitioning?	Contracts should include language representing the geographic characteristics of the service that may impact the customer's operations, as well as any warranties regarding geographic boundaries. For example, the contract should state any geofencing that results from using any feature of the service that intends to accomplish that goal. The customer should also note whether the contract allows for cross-border transfers, which should be further addressed in a DPA.
Does the contract specify when and how changes to the service are performed? Does the contract include any provision for the customer to control changes or the timing of changes?	All cloud services are constantly evolving — the code itself is likely taking changes on a daily basis — but service changes that impact the customer should require at least reasonable notice. Ideally, the contract represents that a customer has the option to delay the implementation of a service-impacting change for some period of time (up to 60 days, for example) if a change is scheduled for a particularly business-critical time. Additionally, the contract should spell out terms under which the provider may deprecate a feature and what remedies are available to the customer if any.

[10] It should be noted, however, that typically a KMS will not contain privacy-sensitive data and so GDPR, CCPA, etc. are not likely to be applicable.

Does the contract define and specify Service Level Agreement guarantees and penalties, including Recovery Point Objective (RPO) and Recovery Time Objective (RTO)?	The contract should spell out the provider's Service Level Agreement commitments, including any penalties and conditions of penalties (e.g., the customer remains a customer; the customer can show harm, etc.). The service should have Recovery Point Objective and Recovery Time Objective identified as a representation, and it is beneficial for the provider to identify what conditions are necessary for identifying RPO and RTO starting points.
Does the contract include representations regarding the screening of employers, contractors, and third parties?	The contract should represent that all personnel have been examined for criminal background, previous civil law findings of a character nature, any required drug testing, nationality, and any other personal attributes required by the customer. The contract should also describe the frequency with which background checks are performed.
Does the contract define and describe the CSP's incident and breach notification policy?	Customers should ensure that the KMS provider's policies and incident response commitments meet the customer's requirements. Breaches of a key management system can have widespread effects and can be difficult to remedy quickly, so it may be prudent to consider requesting reduced notification time. Customers may also wish to specify that even *suspected* incidents be reported as swiftly as possible owing to the sensitivity of a key management system.
Does the contract define and describe termination rights?	Customers should ensure that termination does not infringe upon any representations already established in the contract.
Does the contract include Indemnification and Limitation of Liability?	These "purely legal" concerns are essential components of any business contract. They should be carefully reviewed in the context of the sensitivity and relative importance of a cloud-native KMS using EKO. Legal should always review these sections to ensure that the contract supports claims made by the cloud provider's marketing and sales departments.

Both technical and legal staff should rigorously examine the terms to ensure a thorough understanding and address all concerns or outstanding issues before making a commitment. In general, large and well-established cloud service providers will have similar contract language. However, variances do exist, and some may be of particular importance to any single customer.

Though possibly not in the contract, there may be a consideration made that customers of a particular kind (industry association, government, etc.) can either directly audit the CSP or have an intermediary (typically an independent auditor) perform audits. For companies that demand the right to audit a CSP, it should be confirmed whether the CSP allows for external auditing.

The primary legal aspect to consider is the contractual representations and warranties made by the provider. Of nearly equal importance is the ability of a CSP to pay damages or survive a lawsuit — representations, warranties, and indemnification rights are less valuable if a CSP is underinsured or an asset-poor startup. A secondary legal consideration is the history of the company and any public statements made by the company regarding its commitment to safeguarding customer data. Lastly, it is necessary/prudent to attempt to discover any litigation the CSP has been a party to and determine if the circumstances and outcome of litigation are a cause for concern.

3.5 Financial Considerations

Typically, the direct service costs of a cloud-native KMS using EKO are relatively low.[11] The overall cost is typically driven by indirect costs, particularly the retention of technical expertise necessary to administer and operate the KMS functions.

Consideration	Justification/ Rationale
What is the provider's pricing model, and how will the customer use the cloud-native KMS using EKO?	Though the cost of a cloud-native KMS using EKO is likely to be quite insignificant for many customers, understanding the pricing model will bring reasonable certainty to one's budget. Typically, cloud-native KMS using EKO providers charge a very small amount per transaction for most transaction types — on the order of one to fifteen cents per ten-thousand requests — and a fixed, low-dollar cost for the use of hardware (HSM) backed keys. However, there are higher costs for "premium" configurations, including the use of EKO. Customers should clearly understand not only the specific services/features to be consumed but the volume of transactions expected to achieve a reasonable degree of precision for budgeting. Particularly in the use of a cloud-native KMS using EKO for a very high volume of transactions, the pricing model of the CSP is worth considering. A typical pricing model for a cloud-native KMS using EKO is to charge nothing to provision the service (creating vaults, lockers, storage buckets, key rings, logging functions, roles, and permissions, etc.), a cost per volume of transactions, and a fixed cost per month for keys and premium features such as non-shared HSMs and external key management. In general, transactions are inexpensive, with millions of transactions per month equating to single or double-digit dollars. For this reason, one needs to have a broad understanding of the types of transactions the organization will perform as well as the expected volume of transactions. It is wise to bring this to the attention of the information technology architecture and planning teams across all lines of business and ask about existing KMS operations and costs. It may be that current KMS costs are quite high, and there is an opportunity to reduce costs by moving existing KMS operations to a cloud-native KMS using EKO.

[11] It is even possible for the direct service cost to be zero when used as a dependent service for other services offered by the same cloud service provider.

Will the customer desire or mandate billing granularity, for example, supporting the ability to charge back to business units based upon their utilization?	The customer may need the billing to be done such that different resources in the customer's tenant result in billing different entities (departments, divisions, etc.) within the customer's organization. Customers should examine the granularity of billing offered and how that might interact with the desired technical and operational design. For example, if billing can be done only at the vault or storage bucket and not individual keys, there may be a need to instantiate more vaults/buckets. This could potentially complicate operational support.

4. Planning a Cloud-Native KMS using EKO

After a cloud provider to host the cloud-native KMS using EKO is chosen, the next logical step is to plan the deployment. There will be many technical, operational, legal, regulatory, and financial concerns that must be addressed in this step. The outcome of this step should be a list of requirements that the user or organization will use when deploying the cloud-native KMS using EKO.

4.1 Technical Considerations

There are several categories of technical considerations for organizations planning to deploy a cloud-native KMS using EKO.

4.1.1 Identity and Access Management

With any commercial information technology system, identity and access management (IAM) is a fundamental component and significantly contributes to an overall security posture. It is the foundation of any secure and fully compliant public cloud architecture.

IAM systems serve as mechanisms that can reduce risks associated with cloud environments. Many organizations provide IAM systems to secure the information by controlling the access permission of each user. It is critical to plan how to govern the control and data-plane access to resources. Any design for IAM must meet regulatory, security, and operational requirements.

The process for identity and access management (IAM) involves planning for identity integration and other security considerations, such as blocking legacy authentication and planning for modern passwords, selecting business-to-business or business-to-consumer identity and access management. These requirements may vary from organization to organization, but there are common design considerations and recommendations to consider.

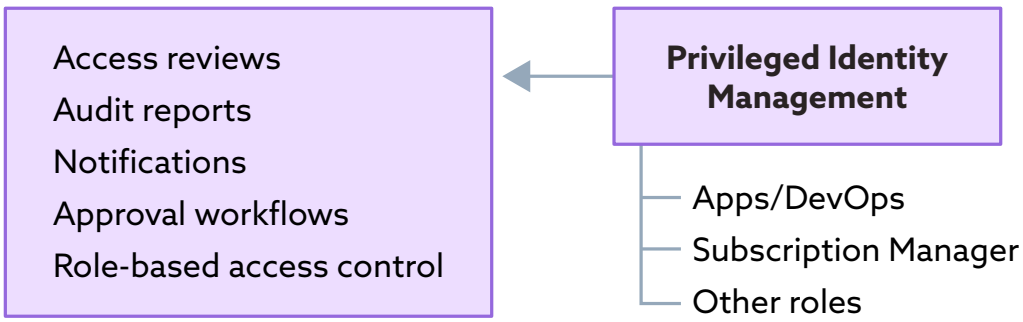


Figure 2: Identity and Access Management

Design considerations in key operational areas:

Consideration	Justification/ Rationale
Does the cloud-native KMS using EKO support granular and/or custom roles and role assignments?	Operating on the "principle of least privilege," users who have only the rights necessary to perform their role makes for the most secure access model. In some scenarios, there may not be a built-in role that works, and in these scenarios, consideration should be given to a custom role. Users should refer to the cloud provider's best practices for custom roles as they are not always possible or a recommended solution.
Does the cloud-native KMS using EKO support integration into existing authentication mechanisms, such as Single Sign-On (SSO) and federation with the organization's identity provider?	If the organization has an existing identity provider, ensuring that authentication occurs using these accounts via federation or SSO can increase security through the already in-use authentication mechanisms from the organization. Customers should not be required to perform password synchronization to a cloud provider, thus creating an exposure and threat to the enterprise.
Does the cloud-native KMS using EKO support the use of separate roles for read / write access?	Write access should be segregated to a privileged role that a user must escalate to safeguard against accidental changes from the user or malicious changes should the normal user account become exposed.
Does the provider offer notifications of privileged role use and trending/comparison metrics? Are those metrics configurable?	When Privileged Identity Management (PIM) is used in this fashion, it is essential to regularly audit the access logs to ensure that no undue access has taken place.

Does the cloud-native KMS using EKO support the use of conditional access policies through the organization's identity provider for providing access?	The use of conditional access policies can increase security by ensuring that access is only permitted only in certain use cases. An example is that a user must successfully authenticate from an IP within the organization's authorized IP ranges.
Does the cloud-native KMS using EKO support the use of Multi-Factor Authentication (MFA) for write access?	MFA is typically performed at the organization's identity provider instead of the cloud-native KMS using EKO. Using MFA strengthens security by providing further confidence that the person logging in is the correct and authorized person.
Does the cloud-native KMS using EKO allow the disablement, or non-use, of non-federated identities from the organization's identity provider?	Managing user credentials within an organization-managed directory service will help centrally enforce the same secure account management policies for user accounts with access to the cloud-native KMS using EKO.

4.1.2 Shared Responsibilities

Shared responsibilities recognize that while cloud providers are responsible for the security of the cloud, cloud customers are responsible for security in the cloud. However, shared responsibilities vary by service model (IaaS, PaaS SaaS) and cloud service provider. Regardless of the model or service provider, data and access to that data are, in the end, the customer's responsibility. It is up to the cloud customer to verify shared responsibilities and controls over data (at rest and in transit) and keys in the cloud-native and customer key management systems (CKMS).

Consideration	Justification/ Rationale
Are cloud-native KMS shared responsibilities considered in combination with separation of duties (SOD see 4.1.3), for example, key management and data access?	Responsibilities are identified and assigned to roles to enable performance and establish accountability. Separation of duties is considered when roles are assigned in order to protect against error or fraud.
Are cloud-native KMS shared responsibilities and separation of duties (SOD see 4.1.3) documented in writing in operational policies and procedures and other documentation?	Users should document responsibilities / SOD in writing to ensure a source for training, operational use, and contractual disputes.

4.1.3 Separation of Duties (SOD)

Separating job duties or privilege levels is an information security best practice. When planning the deployment of the cloud-native KMS using EKO, the organization should consider how user roles are separated and whether that will occur across CSP and CSC KMS groups, users, or accounts.

Consideration	Justification/ Rationale
Will the organization need service accounts with specific access to certain keys or secrets?	It is essential to document ALL accounts accessing the cloud-native KMS using EKO and customer KMS, especially accounts associated with applications accessing the KMS. Thorough documentation helps organizations with timely response to security incidents, separation of duties validation, and other security-related tasks pertaining to account management for the cloud-native KMS using EKO.
Does the cloud-native KMS allow the assignment of the typical roles?	Administrator: This role has full access to the cloud-native and customer KMS and will be the primary role responsible for day-to-day administration tasks. This role has read, write, delete, recover, backup, restore, import/ export, update, and purge permissions on keys/secrets. Break Glass Administrator: This role has the same privileges as the Administrator role and is used only if the other administrators cannot access their accounts. This role should be time-bound and should link to the user's unique id ID. Auditor: This role has read access to all keys and secrets within the cloud-native and customer KMS and should have enough privileges to review necessary metadata or log data associated with key or secret expiration, key or secret rotation activity, key or secret import or export activity, key or secret restore or recovery activity, and key or secret purge activity. Read-Only: Groups, users, or service accounts with the "Read-Only" access role should have this role assigned to specific keys or secrets appropriate for their job requirements. This role will allow read-only access to keys or secrets and will not allow users with this role to alter the keys or secrets in any way. Service accounts with this role serve a specific read-only purpose within applications interacting with the cloud-native or customer KMS. Encrypt/Decrypt: Groups, users, or service accounts with this role are allowed to interact with specific keys or secrets within the cloud-native or customer KMS. This role may also require that the group, users, or service accounts have read access to the same specific keys or secrets within the KMS. Assigning this role to a service account fulfills an application that needs to perform encryption/decryption.

4.1.4 General Technical Considerations

Organizations deploying a cloud-native KMS using EKO should consider the level of effort required to configure this pattern and integrate the KMS into the organization's information system architecture.

Consideration	Justification/ Rationale
Are systems accessing the cloud-native KMS using EKO capable of utilizing web (e.g., REST) protocols?	Each architecture may require additional, specialized security controls and/or configurations impacting the level of effort needed to support and secure the KMS. Solutions not capable of supporting web protocols will have a larger effort needed to utilize the KMS.
Are staff technically proficient with the chosen cloud-native KMS using EKO?	The time to achieve operational readiness will be significantly impacted by the staff's technical proficiency to integrate and operate the cloud-native KMS using EKO.
Will documentation and configuration procedures need to be developed prior to deployment?	It is necessary to allow sufficient time to thoroughly document configurations, architecture, and any steps taken to deploy the KMS. This will save time in the future as personnel changes and updates to the KMS or environment are made.
What systems integration work will be required to monitor and alert on security-related events within the cloud-native KMS using EKO?	Additional information systems may need to be configured to store security-related event logs, additional connections to support alerting facilities, and other systems to support automated responses to specific events.
How will encryption types, algorithms, and key lengths be determined?	Industry best practices, organization use cases, and compliance requirements, as well as the KMS configuration and the key material it supports, may shift over time.
Does the test environment have the same features as production, and does the organization have application representation sufficient to test features identified as business-critical?	It is necessary to consider the level of effort needed to properly configure and test network and application access to the KMS from the perspective of each environment and system.

Organizations should determine KMS deployment model requirements.

Consideration	Justification/ Rationale
What capacity planning needs to occur, and does the cloud-native KMS using EKO service provider offer capacity planning tools and documentation?	The organization may need to deploy a KMS solution in multiple geographical regions, may need to increase bandwidth to account for additional traffic between information systems and the KMS, and may need to monitor the additional potential performance impact to the organization's network.
What automatic scaling capability is needed, and does the cloud provider offer native configuration options for this purpose? Organizations should consider the cloud-native KMS using EKO's capabilities when determining configuration requirements, for example, auto-scaling, clustering, and back-ups.	Additional cloud services or configuration steps may be necessary for performing these tasks according to the organization's requirements.

Organizations should establish what cloud-native KMS provider documentation and support will be available during deployment using EKO.

Consideration	Justification/ Rationale
Is sufficient documentation available to troubleshoot issues that might arise during deployment?	A lack of documentation or outdated documentation may dramatically increase the time it takes teams to troubleshoot technical challenges that arise during deployment.
Will technical or engineering support be available from the KMS provider during the deployment process?	Additional costs may be associated with technical support from the KMS provider. Data privacy is a consideration when an organization is relying on the KMS support of the provider.

4.2 Operational Considerations

Most operational considerations are made during the planning of a cloud-native KMS using an EKO deployment. Ensuring that proper processes and procedures are in place prior to the deployment is the best way to realize the adoption and success of the cloud-native KMS using an EKO solution. The organization should consider the ways in which it plans to use the cloud KMS because different uses of encryption keys (or other KMS features such as storage of blobs, passwords, or connection strings) will have different levels of sensitivities to service outages. The operational considerations

described below provide guidance and considerations for users and organizations during the planning of a cloud-native KMS using an EKO solution.

Consideration	Justification/ Rationale
How will users request objects, as well as access to objects, in the cloud-native KMS using an EKO?	Without self-service, the operations team will have to handle all provisioning of KMS resources, and this could be costly and slow.
What security monitoring needs to be configured on the cloud-native KMS using EKO during deployment?	Examples of security controls that may require read access to the cloud-native KMS using EKO include controls such as centralized logging, privileged access management, and cloud security posture management.
How will access to the keys and secrets in the cloud-native KMS using EKO work in the event of an outage from the cloud provider?	Users and organizations should prepare business continuity plans for how applications would continue to function without connectivity to the cloud-native KMS using EKO in the event of an outage to the cloud provider or backing authentication services.
What personnel will monitor stored log data for potentially malicious activity?	The operational roles and responsibilities should be identified with runbooks or processes in place for actions to take on detected security events in the cloud-native KMS using EKO.
How will the organization manage roles while maintaining the principle of least privilege?	Without a proper plan or set of documented procedures to efficiently manage user roles and their level of access to the KMS, maintaining the principle of least privilege becomes a challenging exercise for an organization provisioning user accounts.
How will the organization assign roles to maintain separation of duties?	Without a set of documented procedures in place to help guide how user access to the KMS is provisioned, whether through RBAC via directory service (cloud, on-premise, or hybrid), or within the KMS privilege assignment functionality itself, maintaining a separation of duties between user accounts becomes nearly impossible.
How will the organization handle new account provisioning, stale account deprovisioning, and periodic role audits?	As with information system access, the organization will need to periodically review accounts with KMS access and determine whether that access is still needed. Maintaining policies and procedures with this information will help set the expectation for personnel responsible for performing these actions and ensure that they have the privileges necessary to do so within the KMS.

Does the cloud-native KMS using EKO offer the capability to log, monitor, and alert based on registrant activities (i.e., read, write, edit, delete, update, etc.)?	As part of a mature security program, logging, monitoring, and alerting on activity within the KMS helps track down whether the alerting activity was performed by malicious users or as part of planned maintenance. Another benefit of logging this activity is in the event of an accidental change made to the KMS. The more information captured, the more likely the organization will be able to revert any unintended changes.
Does the cloud-native KMS using EKO offer the capability to implement robust disaster recovery functionality?	Not all service providers can maintain a healthy level of service offering for their KMS, which introduces some level of risk associated with getting locked into a specific KMS. The ability to implement robust disaster recovery functionality helps an organization avoid getting locked into one service provider and provides the organization a way of recovering from an incident within the cloud-native KMS using EKO.
Does the cloud-native KMS using EKO provider enable high availability within their KMS service to prevent outages?	This functionality enables an organization to continue operating the KMS in the event of an outage as part of business continuity.

4.3 Regulatory Considerations

Consideration	Justification/ Rationale
What regulators, if any, need to be notified of the organization's use of cloud services?	For regulated businesses, notification of the use of public cloud services may be required before production usage. Not doing so can result in penalties or fines.

4.4 Legal Considerations

Consideration	Justification/ Rationale
Where will the signed service contract [with the cloud service provider] be stored, and who will need access?	Guaranteeing that the organization has stored a copy of the signed contract ensures that its legal counsel can examine the terms and conditions in the event of a dispute with the cloud service provider. It is prudent to assume that it is not possible to anticipate every person or role that will want access to the contract and err on the side of making it available broadly within the organization on a read-only basis.

What is the process for all personnel not associated with the legal department to raise concerns to legal counsel/the legal department regarding changes in design and/or operation of the cloud-native KMS using EKO?	Should a concern arise that is suspected of having legal ramifications, a process should exist whereby staff not associated with the legal department can raise a concern to legal counsel for evaluation.

4.5 Financial Considerations

Consideration	Justification/ Rationale
What steps are taken to prepare the organization to handle billing from the cloud provider?	The organization must avoid having services disabled or deprovisioned due to lack of payment of an invoice. Additionally, if the organization is performing chargeback of some kind to internal consumers of the service. The steps to prepare for this billing model must be taken before initiating production.
What steps are being taken to audit the CSP's invoices to ensure that unexpected costs are not being incurred due to a lack of oversight?	It is entirely possible that unexpected transaction volumes occur due to misconfiguration or poor application design, resulting in a potentially enormous discrepancy between the expected and actual invoice for services. Someone must be accountable to ensure that the delta between expected and actual costs can be accounted for and addressed, if necessary.

5. Deploying a Cloud-Native KMS using EKO

With the deployment of the cloud-native KMS using EKO planned, the next step is to perform the processes required to set up the KMS and start utilizing services. In this scenario, the financial and operational concerns are at the forefront as costs are accumulated for a user or organization as resources get deployed and initiated. Additionally, legal and regulatory matters become a reality as data starts to populate.

5.1 Technical Considerations

The following technical considerations provide guidance to users during the deployment of a cloud-native KMS using EKO solution. The primary focus for the user or organization should be on ensuring that proper access models are in place and that secure operation of the KMS solution can occur without impacting business functions.

Consideration	Justification/ Rationale
Are multiple instances of the cloud-native KMS using EKO warranted in order to ensure separation of development, test, and production uses?	It is often advantageous for a user or organization to deploy multiple instances of a cloud-native KMS using EKO so that testing of changes can occur in a non-production instance before enacting the change in production.
Do the cryptographic keys need to be backed by an HSM device?	An industry best practice is to use an HSM for production keys, but test or development keys may elect to use software protection. The option to use an HSM-backed key is often configurable during key creation processes in the cloud-native KMS.
Should the cryptographic keys be configured for automatic renewal with the cloud-native KMS using EKO?	Outages resulting from expired keys are all too common. Customers should consider using automatic renewal features, if available.
Does the cloud-native KMS using EKO need to be restricted from public Internet access?	A customer may have a requirement where all access to the cloud-native KMS using EKO originates from the customer's network, typically done via some form of Virtual Private Network connection with the CSP. This can also extend to blanket restrictions based on geographic (as represented by IP address space) location.
What configuration settings need to be enacted to reflect the organization's policy regarding key recovery following deletion?	Some cloud-native KMS using EKO solutions will offer the ability to enable a soft delete or versioning of keys at the point of KMS creation. If this ability is required, it should be considered during, or prior to, the deployment of the KMS as it cannot be enabled after in some cases.
Does the cloud-native KMS using EKO need to be deployed in a specific geographic location?	Cloud providers may allow the selection of a geographic location when a resource is created. Resources may be optimized to operate in certain regions for technical reasons such as connectivity to other resources or operational reasons such as disaster recovery.

5.2 Operational Considerations

The operational considerations described below provide guidance for users and organizations during the deployment of a cloud-native KMS using EKO solution. The operational aspects of deploying a cloud-native KMS using EKO are mostly driven by the need to ensure access, proper monitoring, and associated processes and procedures.

Consideration	Justification/ Rationale
If there were two-person-integrity steps that needed certification, have those been completed?	Any key-ceremony steps that have not been completed are potential compliance violations and may undermine the legitimacy of the KMS.
Have owners of all dependencies signed off?	Without sign-off from dependencies (e.g., SIEM, identity management, monitoring, HelpDesk), the decision to move to production implies the acceptance of significant risks.
Have all [planned] supported KMS activities (including key import) been end-to-end tested in both the cloud-native KMS using EKO?	Without standard change-management practices, the organization accepts the risk that the service may fail to deliver services/features as advertised.
Has logging been confirmed functional and calibrated for production use?	It is possible that prior to production use, logging configuration was set at a reduced or increased verbosity for testing and validation. So, confirming that the desired logging level is set for production addresses the risk of too much or too little detail being collected.
Has monitoring been tested?	Once integrated, the KMS is an instrumental component of an application, providing access to keys used by an application and, as such, may benefit from monitoring for service availability and connectivity.
Have disaster recovery scenarios been tested and validated with expectations?	Once integrated, the KMS is an instrumental component of an application providing access to keys used by an application. In the event of a service outage, this could mean downtime to an application that cannot access keys. Without plans for how the application will function in an outage, the user or organization may experience unexpected downtime.

5.3 Regulatory Considerations

Consideration	Justification/ Rationale
Does the organization maintain compliance documentation that should reflect the usage of the cloud-native KMS using EKO?	Any required documentation should be completed before using the cloud-native KMS using EKO in production.
Are the user or organization you prepared for an audit where the cloud-native KMS using EKO might be in scope?	Audit processes and documentation should reflect the use of the cloud-native KMS using EKO before the service is used in production.

5.4 Legal Considerations

Consideration	Justification/ Rationale
What steps have been taken to ensure that the organization has archived a signed contract with the service provider?	If there is a dispute regarding contractual obligations, the customer will want to produce a valid contract. The customer's legal department should store a copy of the agreement and all licensing terms.

5.5 Financial Considerations

Consideration	Justification/ Rationale
Has the accountability for the cost of completing deployment been determined, and is the billing routing planned accordingly?	Completing the deployment steps to enable a cloud-native KMS using EKO is going to incur some one-time and/or unusual charges. The CFO staff should be prepared to see new charges appear and ensure that these charges are expected.
What is the review process to examine the initial few months' charges for validity against expectations?	It is possible that a software process that is performing unexpected, high volume transactions will be caught through billing rather than monitoring settings, so a technical staff member reviews billing statements for at least several months after deployment has completed to get a sense of normal operations and charges. This should be done until monthly charges settle into a predictable pattern, at which point triggers may be used to warn of unusual charges.
What process is in place to handle new business units, applications, or other types of customers that begin utilizing the cloud-native KMS using EKO?	Without an intake process to support a charge-back model, the billing for services will likely not be appropriately allocated, possibly resulting in intra-organizational churn and conflict.

6. Conclusion

Adopting a cloud-native KMS using EKO need not be more complicated than adoption of any public cloud service. Because a KMS is often a core utility it warrants treatment similar to that of other systems of this kind like directory and other identity services. Like all information systems, ensuring that the necessary talent is available and given sufficient time to give great attention to detail will go a long way toward successful adoption. Additionally, customers must not take a "set and forget" approach to cloud key management systems, though this is a common mistake. Because keys frequently have periods of use spanning a year or more it is unfortunately common for organizations to neglect the underlying systems from which they are issued. One advantage of using a cloud KMS

is that the providers have learned this lesson and are doing more and more to help customers avoid shooting themselves in the foot through neglect. This does not imply, however, that customers no longer need to pay attention. The pervasive use of keys, and the scope of data that they often apply to, makes them attractive targets for cyber attacks. Customers are strongly advised to put robust systems in place for monitoring intrusions and misuse of cloud KMS systems and artifacts.

The choice of cloud KMS need not be a significantly greater burden on an organization than a traditional non-cloud KMS system. Key factors to consider are the service contract, particularly the RTO and RPO commitments, since those will be outside of the customer's control — in contrast with a non-cloud KMS. The impact of latency and any transaction volume limitations are of particular technical concern for customers with high utilization from many applications outside the vendor of the cloud-native KMS using EKO. On the plus side, cost is often negligible in relative terms, and most customers should find that premium features are available with very reasonable terms.

Assistance with adoption should be readily available, as both the cloud KMS vendors and a robust ecosystem of systems integrators are eager to assist organizations with successful outcomes. The cloud KMS vendors see adoption as inevitably leading to further penetration of that provider's other cloud services, and systems integrators see their involvement in adopting a cloud KMS as the foundation for future services engagements.

The cloud KMS landscape has begun to mature into distinct differentiation across providers, offering customers great choice at the commodity end of the spectrum and a variety of feature and pricing models at the premium end. With price as a lesser concern, customers should emphasize cloud vendor relationships and responsiveness to emerging customer scenarios. When choosing a provider, customers should also consider reliability and financial stability because of the long-lived natures of KMS artifacts. It is possible that consolidation will take place in this cloud service arena over the coming decade; therefore, customers should consider choosing a provider with a strong balance sheet and commitment to providing this service as a strategic part of the provider's business.

7. References

NIST SP 800 57 Part 2	NIST SP 800-57 Part 2 Rev. 1. Recommendation for Key Management: Part 2: Best Practices for Key Management Organizations, May 2019. https://csrc.nist.gov/publications/detail/sp/800-57-part-2/rev-1/final
CSA API Keys	Protect the API Keys to your Cloud Kingdom, Mark O'Neill, CTO, Vordel, April 2011. https://cloudsecurityalliance.org/blog/2011/04/18/protect-the-api-keys-to-your-cloud-kingdom/
Google Cloud KMS	Cloud Key Management Service>Documentation>Guides>Key Rotation, November 2020. https://cloud.google.com/kms/docs/key-rotation

NIST SP 800 57 part 1	SP 800-57 Part 1 Revision 5, Recommendation for Key Management: Part 1 – General, May 2020. NIST Publishes Special Publication (SP) 800-57 Part 1
IBM Cloud KMS	IBM. (2021). IBM Cloud Docs. Key Protect. *Rotating your root keys*. https://cloud.ibm.com/docs/key-protect?topic=key-protect-key-rotation
NIST 800:38b	NIST 800:38b, Recommendation for Block CipherModes of Operation: The CMAC Mode for Authentication, May 2005. NIST SP 800-38B - NIST Page
AWS Cloud KMS	AWS Key Management Service (KMS) https://aws.amazon.com/kms/ Importing key material in AWS Key Management Service (AWS KMS) https://docs.aws.amazon.com/kms/latest/developerguide/importing-keys.html
Google Cloud	Cloud Key Management https://cloud.google.com/security-key-management Customer-Supplied Encryption Keys https://cloud.google.com/security/encryption/customer-supplied-encryption-keys Key Import https://cloud.google.com/kms/docs/key-import
Microsoft Key-Vault	Key Vault https://azure.microsoft.com/en-us/services/key-vault/ Import HSM-protected keys to Key Vault (BYOK) https://docs.microsoft.com/en-us/azure/key-vault/keys/hsm-protected-keys-byok
Alibaba	Key Management Service https://www.alibabacloud.com/product/kms Import key material https://www.alibabacloud.com/help/doc-detail/68523.htm
CSA Security Guidance for Critical Areas of Focus in Cloud Computing V4.0	Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing v4.0, April 2017. Security Guidance for critical areas of focus in Cloud computing 4.0
Key Management in Cloud Services	Cloud Security Alliance, Key Management when using Cloud Services, November 2020. https://cloudsecurityalliance.org/artifacts/key-management-in-cloud-services/
Recommendations for Adopting a Cloud-Native KMS	Cloud Security Alliance, Recommendations for Adopting a Cloud-Native KMS, September 2021. https://cloudsecurityalliance.org/artifacts/recommendations-for-adopting-a-cloud-native-key-management-service/

Appendix A: Acryonyms

Acronyms and abbreviations used in this paper are defined below.

ACL	Access Control List
API	Application Programming Interface
AES	Advanced Encryption Standard
BC/ DR	Business Continuity/ Disaster Recovery
BYOK	Bring Your Own Key
CCMM	Caching Cyptographic Materials Manager
CCPA	California Consumer Privacy Act
CKMS	Cloud Key Management Systems
CMDB	Configuration Management Database
CMR	Code of Massachusetts Regulations
CMVP	Cryptographic Module Validation Program
CSC	Cloud Service Customer
CSO	Cloud Service Offering
CSP	Cloud Service Provider
DAR	Data-at-Rest
DFIR	Digital Forensics And Incident Response
DISA SRG	Defense Information Systems Agency Security Requirements Guide
DOD/ DoD	Department Of Defense
EKO	External Key Origin(ation)
FedRAMP	Federal Risk And Authorization Management Program
FFIEC	Federal Financial Institutions Examination Council
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
GDPR	General Data Protection Regulation
GLBA	The Gramm-Leach-Bliley Act
HIPAA	The Health Insurance Portability And Accountability Act
HSM	Hardware Security Module
IAM	Identity Access Management
IP	Internet Protocol
ISO	International Organization For Standardization
IT	Internet Protocol
JIT	Just-In-Time
KMS	Key Management System
mTLS	Mutual Transport Layer Security
NIST	National Institute Of Standards And Technology
PCI-DSS	Payment Card Industry Data Security Standard
PHI	Protected Health Information
PII	Personal Identifiable Information
RACI	Responsible, Accountable, Consulted, And Informed
RPO	Recovery Point Objective
RTO	Recovery Time Objective

SDK	Software Development Kit
SIEM	Security Information Event Management
SOC	System And Organization Controls
SOD	Separation Of Duties
TLS	Transport Layer Security

Appendix B: Glossary

Definitions for selected terms used in this paper are below.

Cloud-Native	Refers to systems and applications designed, developed, and deployed to and for the cloud to maximize cloud computing concepts and architectural advantages that include speed, scalability, resiliency, and agility.
External Key Origination	Refers to the Generation of cryptographic keys outside of a cloud KMS and subsequently importing the key(s) to a cloud KMS.
Cloud-Native KMS with an External Key Origination	Pattern in which a customer has chosen to use a [public] cloud-hosted KMS that is designed and operated as a multi-tenant cloud service, including hardware-based key protection, and has also chosen to use one or more keys from an external source.[12]
Cloud-Native KMS	The pattern where the KMS is built and owned by the same provider that delivers the cloud service the customer consumes, and all components of the KMS are in the cloud.[13]
Break Glass Administrator	Emergency access accounts that are highly privileged and not assigned to specific individuals. Emergency access accounts are limited to emergency or "break glass"' scenarios where normal administrative accounts cannot be used. https://docs.microsoft.com/en-us/azure/active-directory/roles/security-emergency-access
Hardware Security Modules (HSMs)	Hardened, tamper-resistant hardware devices that strengthen encryption practices by generating keys, encrypting and decrypting data, and creating and verifying digital signatures. https://cpl.thalesgroup.com/faq/hardware-security-modules/what-general-purpose-hardware-security-module-hsm
Security information and Event Management (SIEM)	This technology supports threat detection, compliance and security incident management through the collection and analysis (both near real time and historical) of security events, as well as a wide variety of other event and contextual data sources. The core capabilities are a broad scope of log event

[12] See https://cloudsecurityalliance.org/artifacts/key-management-in-cloud-services/ for the reasons a customer may choose an external key source, as well as the pros and cons of choosing this model.
[13] See https://cloudsecurityalliance.org/artifacts/key-management-in-cloud-services/ page 12

	collection and management, the ability to analyze log events and other data across disparate sources, and operational capabilities (such as incident management, dashboards and reporting). https://www.gartner.com/en/information-technology/glossary/security-information-and-event-management-siem
Separation (Segregation) of Duties	Fundamental building block of sustainable risk management and internal controls. The principle of SOD is based on shared responsibilities of a key process that disperses the critical functions of that process to more than one person or department. https://www.aicpa.org/interestareas/informationtechnology/resources/value-strategy-through-segregation-of-duties.html
Shared Responsibility	The customer security team maintains some responsibilities for security as the user or organization moves applications, data, containers, and workloads to the cloud. At the same time, the provider takes some responsibility, but not all. Defining the line between customer responsibilities and providers is imperative for reducing the risk of introducing vulnerabilities into public, hybrid, and multi-cloud environments. https://cloudsecurityalliance.org/blog/2020/08/26/shared-responsibility-model-explained/
IAM	IAM is the information security process of protecting how users and devices are identified in a system and can access resources based on these identities.