cpl.thalesgroup.com

THALES
Building a future we can all trust

Best Practices for Cloud Data Protection and Key Management

White Paper

Contents

Introduction

Digital transformation is a persistent trend that has resulted in fundamental shifts in storage, access and management of digital assets. These shifts are particularly noticeable for the most prized asset: an organization's sensitive data. Sensitive data used to reside in controlled, on-premises enterprise data centers protected by both physical and logical security controls. Although, until recently it was unthinkable to trust a third-party with such data, organizations are now accelerating the migration of their workloads and data to the cloud. According to the Thales 2021 Global Data Threat Report [1], 50% of respondents said that more than 40% of their data is stored using infrastructure (IaaS), platform (PaaS) or software (SaaS) services of public CSPs such as Amazon Web Services, Microsoft Azure and Google Cloud Platform. This change, though initially driven by economics, has delivered greater flexibility and elasticity in management of computing and storage resources. A clear casualty of increased cloud consumption has been the traditional method of data security that relied on well-defined network perimeter to protect data.

Once particularly attractive to startups and small to medium size enterprises, cloud has now become a global transformation embraced by all enterprises. At the same time, consumers expect data and services to be available from anywhere, at any time, and from any device. Anything less degrades user experience creating a drag on productivity. No wonder businesses look to the cloud to meet such demanding requirements. However, amid this rush to the cloud, data security is often neglected [2]. Cloud deployments can considerably increase the attack surface, especially in case of multi-cloud use, providing more options for fraudsters to get access to sensitive assets [3]. Instead of protecting a single known network perimeter, the cloud introduces new cybersecurity challenges as environments in which sensitive data resides may no longer be trusted.

One example of sensitive data is the user personal identifiable information (PII). Protecting PII and consumer privacy is making headline news these days. Politicians, government officials and privacy advocates are demanding that all entities holding customer data be held accountable for protecting the data and consequently the privacy of end customers. Data privacy regulations such as the European Union's General Data Protection Regulation (GDPR) [4] and the California Consumer Protection Act (CCPA) [5] require strict compliance and impose stiff penalties for data breaches that result in loss of consumer sensitive data and privacy. Many other countries are following up with their own data sovereignty regulations. With the Schrems II ruling of June 2020 [6], Europe is further asserting their existing GDPR regulations. Digital transformation must be done within the context of such regulations. According to Gartner [7], by 2024, the increasing impact of international data residency and privacy requirement will result in more than 40% organizations adopting multicloud Key Management Services (KMS) over native CSP KMS service up from less than 10% today.

Recognizing the importance of data protection, CSPs now offer data encryption and key management services. These services can be used across the different types of infrastructure offered by the respective service providers. However, while the native encryption and key management services offer good-enough protection, many organizations, especially those in highly regulated industries such as finance, banking, insurance and health care, need higher levels of assurance for risk management and compliance. An important tool for risk management is the ability for an organization to be the custodian of data encryption keys instead of delegating key ownership to service providers. Many security-conscious organizations have an additional requirement that all data encryption keys must be created stored and managed using a FIPS 140-2 certified key manager. In response to such higher assurance requirements, CSPs offer features such as Bring Your Own Key (BYOK) and Hold Your Own Key (HYOK).

This paper describes security best practices for protecting sensitive data in the public cloud, and explains concepts such as BYOK, HYOK, Bring Your Own Encryption (BYOE), key brokering and Root of Trust (RoT). It explains the level of data protection that can be achieved by using the cloud native encryption and key management service, and how it can be augmented by allowing customers to take more responsibility for and control over their keys.

Security Principles

It is critical to adopt business practices that strike the right balance between security of data, assets, and user identities, and the cost associated with offering such security.

Security Basics

Since data is no longer confined within traditional network perimeters, it can reside in a diverse set of environments during its lifecycle; from the time it is created until it is deleted. Each environment brings its own challenges that must be addressed using specific technologies. Three of the more commonly considered environments are:

- **At-Rest.** Data is predominantly in this "inactive" state, when it is stored physically in any digital form (e.g., databases, files, tape-backups, etc.) and remains unchanged.
- **In-Use.** In this state, data is "active" and being manipulated (e.g., operation on a row in a database, processing of data in a CPU, etc.). Most often, data protection mechanisms applied during at-rest state are removed before data is operated upon. However, there are emerging technologies that can also prevent exposure of data during its use [8].
- **In-Transit.** This state implies that data is transported from one physical location or medium to another, e.g., transmitted across the network or transferred from persistent memory to the CPU, etc.

Data security principles require that data is protected in each of these states. Security controls must defend against all threats applicable to the medium, including side-channel attacks where information is gleaned from valid operation of the device, rather than from exploitation of a weakness. Table 1 summarizes the building blocks of data protection.

Table 1. Data protection fundamentals

Concept	Description
Confidentiality	Keep information secret and private
Integrity	Prevent unauthorized changes to information
Availability	Keep system/data available for use
Accountability	Hold users/system accountable for actions
Auditability	Keep verifiable records of activities

Separation of Duties

It is essential to ensure that fundamental principles of both separation of duties and least privilege access are followed for data protection. This involves enforcing separation of duty between entities processing and storing data from the ones providing security services. In other words, ideally, data storage provider and encryption service provider should be separate entities, a distinction that is often overlooked. For example, cloud storage providers do encrypt data both during transmission and before storage. However, since they also hold the encryption key for stored data, they have direct access to all data that resides on their servers. For enterprises that own the data, this provides little comfort since trust must be placed entirely in the hands of cloud storage providers. Such encryption merely protects against data breaches in case attackers get access to the encrypted data stored on the server. However, even in this case, there is a possibility that if data is breached due to a configuration error or a security flaw at the cloud storage provider, the keys that encrypt the data may also be compromised.

As such, a growing number of enterprises have started to investigate solutions that encrypt data and files before sending them to cloud storage providers. Similarly, CSPs advocate security, in particular data security, as being a shared responsibility between the customer and the storage provider. Figure 1 illustrates this shared responsibility where CSP handles security of infrastructure and the customer handles security of data.

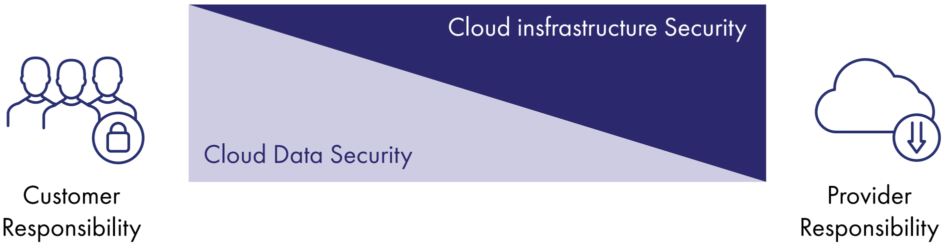

Figure 1: Shared responsibility model for cloud storage

The customer responsibility can be achieved in two ways:

- Third-Party encryption. In this model a third-party server encrypts data before sending it to cloud storage provider. This encryption server sits between customer and the storage provider, like a Cloud Access Security Broker (CASB). In the event of encrypted data being breached at the storage provider, no damage is done since keys are kept in a separate server and cannot be accessed.
- Data-Origin encryption. In this model encryption is done entirely on the customer side as close as possible to the origin of data, for example by using an agent in the browser, deploying file/folder encryption or in an application that generates the data. Several cloud storage providers support this model [9,10].

Authentication

Authentication is a mechanism of determining if a person requiring access to a resource is the same person he or she claims to be. This is a basic requirement for any system that manages access control to application or data resources. Methods to verify the authenticity of a user can be divided into three broad categories: what-you-know; what-you-have, and what-you-are. Any combination of two or more of these categories is referred to as multi-factor authentication (MFA). Good data protection demands that access to both data and keys be controlled by stronger authentication methods.

The what-you-know category represents knowledge-based authentication and is the oldest, most widely used but the weakest method of identifying users. An example of this is the password. The what-you-have techniques base their security on possession of a unique hardware token such as a smart card, Universal Serial Bus (USB) token or a mobile device. This device is paired with the user and can then perform some cryptographic computation on behalf of the user to attest his identity. Examples of such devices are One Time Password (OTP) token or Public Private Infrastructure (PKI) tokens such as smart cards. Finally, what-you-are, places its security on the natural habits or biological characteristics of the user. The user does not have to remember any secret nor carry any dedicated device. Examples of this category can be biometric characteristics like a fingerprint, iris scan, or facial recognition.

Access Management

Access Management (AM) is the next phase of robust security framework that builds on strong authentication. It adds fine-grained control to all user interactions with a system. For example, instead of authenticating credentials once at the perimeter, user's security posture should be continuously monitored using checks such as:

- What applications and data does the user have access to? This sets the high-level authorization scope for the user, which is further refined dynamically based on additional AM policy rules.
- For how long is the access granted?
- From what locations is the access allowed?
- During what times is the access allowed?

The goal is to manage access to data and restricted resources based on policies that are set by an administrator and enforced by real-time or near real-time monitoring of user activities.

Data Encryption

Many CSPs offer encryption and key management that are used with their own compute, storage, database and other services. Choosing the right type of encryption and key management with each of the services requires a deep understanding of the service providers' service offerings. Furthermore, one must understand the level of risk associated with the choice of an encryption and key management approach. Each of the service providers implements encryption and key management differently but many of them offer customers a choice of being the custodian of keys. Most providers refer to this service using some form of the expression Key Management Service (KMS). KMS enables not only creation and management of keys, but also provides control over the use of these keys in services and applications supported by the CSP.

Table 2 summarizes the encryption and key management services of major CSPs. It is worth noting that there are two types of encryption models offered:

- Server-side encryption: The encryption is done by the service provider using encryption keys that are:
  - Created and managed by the CSP, transparent to the user.
  - Customer provided keys that are managed by the CSP.
  - Customer hosted keys stored in customer's repositories on their premises and outside the control of CSP.
- Client-side encryption: Data is encrypted in the customer data center or by a customer-provisioned application running in the service provider infrastructure, using customer-provisioned keys. In this model, the service providers do not have access to the encryption keys and therefore cannot decrypt the data. Certain forms of client-side encryption may be referred to as "Bring Your Own Encryption" or BYOE.

Table 2. Data protection options offered by CSPs

CSP	Service	Data Encryption Option	Key Mgmt.	Comments
Amazon Web Services	S3	Server side, Client side	AWS KMS	Encryption keys can be provided by customer or by KMS
	EC2	Server side, Client side		
	RDS	Server side, Client side		
Microsoft Azure (IaaS/PaaS)	Virtual Machines, Containers	Disk encryption	Key Vault	Transparent data encryption for server side. Keys can be provided by customer.
	Databases: SQL Server	Server side, Client side		
Microsoft 365 (SaaS)	Microsoft Information Protection	Double Key Encryption		One portion of the key is stored in Azure Key Vault, while the second portion is provided by customer controlled Key Management System.
Google Cloud (IaaS/PaaS)	Storage, Compute Engine, Platform	Transparent multi-layered encryption	Cloud KMS	Allows customer provided and customer hosted keys
Google Workspace (SaaS)	Workspace Client-side encryption	Client-side encryption	Customer KMS	Encryption performed by browser; keys are created by browser and wrapped by the customer

Root of Trust

Root of Trust (RoT) refers to a source that can be trusted within a cryptographic system. Because cryptographic security is dependent on the actual security of the keys used to encrypt and decrypt data and perform functions such as generating digital signatures and verifying signatures, RoT schemes generally include hardened and trusted physical devices.

Entropy

Modern cryptography techniques rely on keys to mathematically transform data. These techniques require that keys are unique, have a low probability of collision and are not predictable. Consequently, the key generation algorithms require a high degree of randomness, known as high entropy. Since keys transform data so that confidentiality is maintained even in the event of data exposure, they are of exceptionally high value. Keys thereby require special handling to ensure only authorized people and systems use them. This service is provided through specialized and hardened devices.

Hardware Security Module

A Hardware Security Module (HSM) is a hardened physical computing device that specializes in key creation, key storage and execution of cryptographic processes, thereby acting as RoT and bringing much-needed entropy to cryptographic operations. These modules can be FIPS 140-2 [11] certified, and traditionally come in the form of a plug-in card that is inserted directly into a device, or as a network accessible appliance. In both cases, the goal is to deliver a trusted computing environment that protects confidential materials such as keys and uses these keys to securely perform cryptographic operations on sensitive data.

The need for such dedicated devices arises because typical servers cannot guarantee conformance to the goals mentioned above for trust, entropy, and performance. For example, an application running on a server which may also be providing keys, may contain database access code, user interface code, business logic and cryptographic calls. For mission critical applications this is a dangerous approach as an attacker can use exposed application endpoints to access cryptographic material, steal keys, and even alter output of cryptographic operations. To prevent such a scenario, applications must be segregated into two parts. One part does business logic, database access, and user interface. The second part does the more sensitive tasks such as key storage and cryptographic operation. It is this second part that should run inside the HSM. Trust can be achieved because an HSM typically offers most of the following security features:

1. It is built using specialized hardware that is manufactured in controlled facilities, is well tested and is certified.
2. It has a security-focused OS, that ensures no virus or malware is present.
3. It has limited and controlled access (both physical and logical) via network interfaces that can be managed by internal firewall and network rules.
4. It actively hides and protects cryptographic material, so that this sensitive material cannot be accessed by probing the silicon.
5. It offers true, high entropy random number generation, which forms the foundation of secure cryptographic operation.

In addition to these security safeguards, HSMs are built for performance. Since they are dedicated appliances, they can perform cryptographic operations faster than the more general-purpose servers. Furthermore, several providers of HSM have also started to evaluate support for post-quantum cryptography [12]. The goal is to support cryptographic algorithms that are considered secure against an attack by a quantum computer. Currently this is not true for the most popular public-key algorithms, which can be broken by a sufficiently strong quantum computer.

An HSM can also be built to either address a range of application types, or purpose built for specific use cases. As the name suggests, a general purpose HSM can support any application. It has a basic cryptographic command set that offers primitive cryptographic operations. Because its command set is primitive, applications that use such HSM must write the additional logic themselves. This increases development effort. Of course, the advantage is that the same HSM can be used in a wide range of applications that serve different industries and markets.

Cloud HSM

While HSMs offer a high level of security for cryptographic operation, they do come with overhead: they must be procured, configured, and administered by a dedicated team. Organizations also must forecast their needs ahead of time to allow for the latency of getting an HSM up and running. Cloud HSMs allow this burden of infrastructure overhead to be shifted to CSPs. All major CSP have a Cloud HSM infrastructure that they maintain for internal cloud security and many of them also sell Cloud HSM services to their customers. Applications that use a Cloud HSM interface with it through a web service endpoint, completely unaware of the physical HSMs powering the service. This allows enterprises to adapt in real-time to changes in usage patterns. The same allure of elasticity and cost saving that has attracted countless enterprise applications to move to the cloud, has begun to appeal to the HSM market as well.

Confidential Computing

Since software by nature can have security weaknesses, dedicated hardware has helped to counterbalance these weaknesses and improve the overall security posture of a system. Examples of such hardware include smart cards and secure elements in mobile phones. Even an HSM can be considered a specialized hardware dedicated to cryptographic operations and storage of keys.

In the context of the cloud, confidential computing is a technology that encrypts data in use, while it is being processed. The goal is to improve the trust in cloud environment, and it is achieved by ensuring the following two tenants of trust:

1. Any application operating in a cloud environment should be the same application that the developers intended and the end users expect. This means that the application should not be vulnerable to code injection attacks during execution by other co-hosted applications, or even from the OS layer itself. It should also be possible to provide assurance and verification that such claims. **This can be referred to as trust at runtime.** There are several technologies that offer this trust by providing a trusted execution environment ni hardware. Examples include Software Guard eXtention (SGX) from Intel, Secure Encrypted Virtualization (SEV) from AMD, AWS Nitro from Amazon, and Confidential VM from Google.

2. Any data that is stored in the cloud should be persisted in such a way that its integrity and confidentiality is maintained. The owner of the data should have control over the data, and the storage provider should not be able to view the data in clear unilaterally. The ability to separate storage of encrypted data from the corresponding cryptographic key is central to achieving this trust. This can be referred to as trust in cloud storage. Emerging protocols enable multiple key management systems to ensure, for example, that only a confidential computing instance may be permitted to encrypt or decrypt stored data, by adjudicating access to the use of data encryption keys using such factors as confidential computing attestations and other known computing instances.

Key Management

Security services such as encryption and decryption of data, are based on cryptographic mechanisms that in turn rely on cryptographic keys. These keys must be generated, distributed, stored, rotated and eventually discarded in a secure and protected manner. Secure management of keys is one of the most critical elements when integrating cryptographic functions into a system. A security framework will be rendered ineffective if the underlying key management is weak.

Key management refers to management of cryptographic keys used for cryptographic operations. Good key management starts by having strong entropy, establishing a root of trust to store these keys, and then offering choices regarding how and where these keys are used. The scope of key management is broad, covering topics such as key generation, storage, usage operations (e.g., encryption, decryption, signing, and verification etc.), lifecycle management (e.g., key rotation, backup, revocation, suspension and deletion), along with logging and report generation capabilities. As keys control access to cryptographically protected data, key management becomes an important aspect of the overall security posture.

Federal Information Processing Standard (FIPS) 140-2 [10] is the benchmark for validating effectiveness of cryptographic solutions. Although FIPS 140-2 is a U.S. Federal standard, its compliance has been widely adopted around the world in both governmental and non-governmental sectors as a practical security benchmark and realistic best practice. There are four different levels (Level 1-4) specified by FIPS 140-2. Depending on regulatory requirements, an organization can choose a key management system (KMS) meeting the relevant level. Good key management systems must be FIPS 140-2 certified.

The adoption of cloud-based data storage has led to an evolution of key management services to enable data encryption and decryption. Some noteworthy corresponding evolutions that have emerged are cloud-based native KMS, BYOK, HYOK and cloud-based key brokering services. The sections below capture the main options available for such systems.

CSP Managed Key Management Service (KMS)

Cloud key management is the capability provided by cloud infrastructure providers to create and manage keys and control the use of encryption across a wide range of their cloud services as well as customer applications. Depending on the implementation by the CSP, Cloud KMS supports CSP managed keys along with customer managed keys. Main features and variations of these two options are listed below:

1. CSP Managed Encryption Keys in CSP KMS: Some CSPs like AWS, enable automatic key generation when encryption is invoked by a service, such as Amazon S3. These keys are referred to as CSP managed keys, and typically do not incur any added cost for the customer. While customers can monitor the key usage, they have little control over these keys.

2. Customer Managed Encryption Keys in CSP KMS: Many cloud KMS offerings by CSPs support customer managed keys (CMEK). This capability allows customers to create keys, control access to the keys (leveraging CSP's IAM solution) and manage the key lifecycle. The following options enhance security for customer managed keys in CSP KMS:

    a. **CSP KMS with Hardware RoT** (HSM): Some CSPs provide this capability to offer key management services with hardware protected keys. This addresses compliance use cases and best practices that need keys to be protected in FIPS 140-2 Level 3 compliant key store.

    b. **CSP KMS with BYOK:** Most CSPs support customer generated key material to be imported into the CSP's cloud KMS. This key material can be generated at a customer managed on-premises solution (e.g., an HSM) or at a cloud-based key brokering vendor. An important differentiator in this approach is that the customer owns, operates, and controls the key creation. This helps customers with regulatory or internal requirements for key entropy.

    c. **CSP Support for HYOK:** Some CSPs go one step further than traditional BYOK. They allow master keys to be hosted in the customer-controlled environment at all times. When the CSP needs access to the data encryption keys, they make an API call to the customer-controlled system. The customer-controlled keys are temporarily accessed by the CSP and never stored. This provides an additional control to the customer, where they can deny access to their encrypted data in the cloud at any time. Depending on the CSP's implementation, CSP's native KMS may or may not be needed in addition to customer controlled third-party KMS.

Table 3 provides an overview of the various key management and encryption options supported by AWS.

Table 3. Options offered by AWS based on target data for encryption

What is Encrypted?	How?	Where?	Storage	Comments
Volume or Disk Block	OS/Kernel	Compute instances e.g. AWS EC2	Local volumes (e.g. AWS EBS)	Entire disk volume is encrypted
Files or File Folders	OS/Kernel	Compute instances e.g. AWS EC2	Local file systems (e.g. AWS EFS) or external storage service (e.g. AWS S3)	Used for encrypting unstructured data
Application Data	Application	Compute instances e.g. AWS EC2	Local volumes (e.g. AWS EBS) or external storage service (e.g. AWS S3)	Used for encrypting structured data such as a column of sensitive data in a database

Customer Managed Key Management Service (KMS)

Customer-managed KMS can be used to enable encryption independent of the cloud infrastructure provider's capabilities. Examples include application-level tokenization and encryption of cloud data such as Amazon Elastic Block Storage (EBS), Amazon S3 buckets, and Azure Files etc. This is referred to as Bring Your Own Encryption (BYOE). Typically, a third-party KMS vendor's solution is deployed as an on-premises or cloud-hosted appliance and managed by the customer. Some vendors also provide additional encryption tools to transparently protect data for certain cloud services and offer tools for extraction, transformation, and loading (ELT) of data. These third party KMS solutions also work seamlessly with many popular applications and databases, such as SAP-HANA, Teradata, Oracle etc. Customers deploying these applications or databases can benefit from the existing integration with the third party KMS solution.

In addition to BYOE, third-party vendor KMS can also be used to support BYOK and HYOK use cases for cloud encryption. HYOK offers greater customer control on keys as compared to BYOK. While BYOK enables customer to control only the key creation process, HYOK offers customers full control on the keys used for data encryption and decryption processes managed by CSPs. With HYOK, there is greater separation of duty between encryption provider (i.e., CSP) and encryption key manager (i.e., customer- managed third-party KMS), thereby giving customer the ability to deny access to encrypted data in the cloud. Depending on the third-party KMS vendor's implementation, highly automated ways to manage keys used for BYOK and HYOK are available for multiple CSPs and SaaS providers.

Key Brokering

Key brokering refers to a third-party vendor solution used by an enterprise for cloud key management. Key brokers are available as cloud services or customer owned solutions independent from the cloud infrastructure provider. They enforce separation of duty between key management and data stores. Depending on the set of services provided by the vendor, key brokering could be used to enable BYOK, HYOK or BYOE use cases.

Organizations use multiple CSP and hybrid clouds to meet requirements for different applications, to avoid lock-in, to maintain competitive pricing across vendors, and for high availability. Key brokering solutions also greatly simplify key management for multi-cloud and hybrid environments by creating consistent interfaces, centralizing management, automating key lifecycle tasks like key rotation, enabling audit and logging support, and enforcing compliance requirements such as FIPS 140-2.

Approaches for Cloud Data Protection

This section describes how principles of key management can be combined with security best practices to deliver key management and encryption solutions for the cloud. These solutions are illustrated in Figure 2 and represent a range of approaches with varying degrees of customer control. Each approach should be picked based on the value of data being protected, and the level of control desired to achieve a given level of security and/or regulatory compliance. Attention should also be given to routine tasks that need automation and are difficult to achieve across different providers. If done incorrectly these tasks can lead to loss of compliance or service availability.

CSP Managed Encryption Keys		Customer Managed Encryption Keys (CMEK)		
Default CSP Protection	**Managed CSP Protection**	**Bring your own Key (BYOK)**	**Hold your own Key (HYOK)**	**Bring your own Encryption (BYOE)**
CSP transparently handles key management and encryption of data without any consumer involvement or control.	CSP handles key management and encryption of data; with some customer monitoring, but no control.	Customer generates and rotates keys using entropy and security policies of choice and then hands these keys to the CSP.	CSP handles encryption of data but the key management is under customer control; directly or through third party key broker.	CSP only stores encrypted data. Encryption and key management done by customer, directly or through third party.

Figure 2: Approaches for cloud data protection with varying degrees of customer control

The key management and encryption options, explained in sections below, are broadly classified into two categories; one in which CSP manages the encryption keys and the other in which this responsibility is handled by customers. The latter category of options is collectively referred to as Customer Managed Encryption Keys (CMEK) and gives customers greater control over protection of their data. BYOK, HYOK and BYOE are specific ways of enforcing CMEK, each with a different level of customer control.

Default CSP Data Protection

In this approach CSP transparently handles data protection for customers. This includes generation and management of keys, as well as use of these keys in encryption and decryption of the user data stored by CSP. Many CSPs offer this feature for their customers through mature solutions that can meet many low assurance data security compliance requirements. It can be an acceptable option for customers that either have relatively less critical data or do not want any additional responsibility related to protection of their data; they choose to fully trust their CSP. Different CSPs honor this trust in different ways. For example, some may deploy strong root of trust to protect keys using HSM, while others may not.

An example of default CSP protection can be AWS services like S3 that automatically create keys in AWS KMS for encrypting data stored in S3 buckets. The APIs that manipulate such data in S3 are completely unaware of how data is protected. Similarly, Google transparently encrypts all data at rest.

Managed CSP Data Protection

The managed CSP protection approach is similar to the default CSP protection but offers customers some limited control over their keys. These keys are still generated and stored using a key management system provided by the CSP, but instead of handling all operations unilaterally and without customer input, CSP exposes the key management interface to the customer. The customer therefore gets visibility into how their keys are generated, rotated, and used. Even though users do not fully control their keys, they can at least monitor them.

Bring Your Own Key (BYOK)

Bring your own key (BYOK) refers to services provided by some CSPs that allow customers to generate their own keys and then import these keys into the KMS managed by the CSP. Customers can also opt to rotate these keys and provide CSP with new versions. In the BYOK approach customers can enforce strong entropy and policy rules regarding key generation and rotation that may help meet regulatory compliance requirement. However, once these keys are handed to CSP, the key management and storage is done by the CSP. Most often the imported keys are used as key encryption keys (KEK). For greater control on management of keys customers can use HYOK approach if offered by the provider.

Hold Your Own Key (HYOK)

The hold-your-own-key (HYOK) approach offers the first real separation of duties between CSP and the customer. In this approach CSP still handles encryption and decryption of customer data but does not manage the keys. These keys are generated and managed by the customer; either directly or through an independent third-party such as a key broker. The CSP can request access to these keys when encryption and decryption operations must be performed. However, once these cryptographic operations are complete, and keys are no longer required, the CSP erases them from its cache. As such these keys are never persisted by the CSP. The customer can choose to host the keys in a KMS in its own data center or use a separate cloud service.

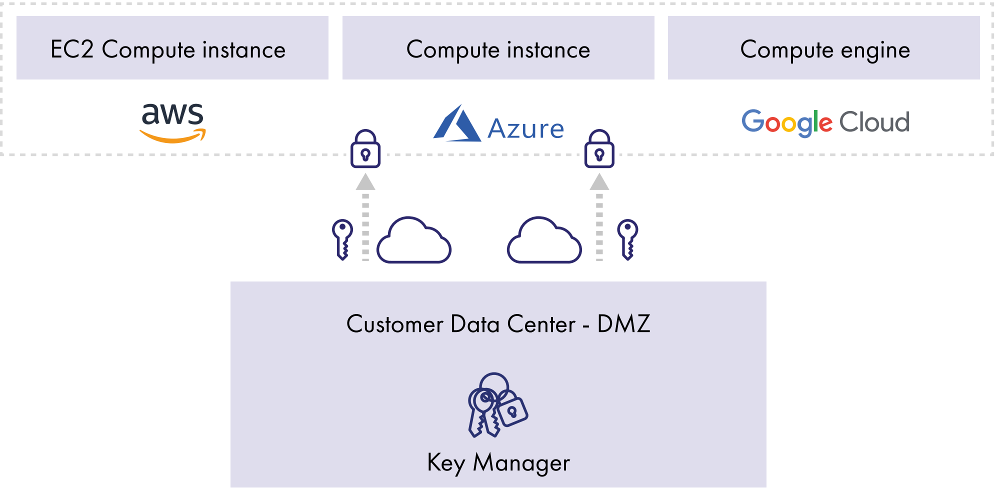

Figure 3: BYOK or HYOK approach with KMS in customer data center and encryption done in a CSP

Bring Your Own Encryption (BYOE)

The bring your own encryption (BYOE) approach offers the ultimate separation of duty by allowing customers to use their own encryption as well as key management tools instead of the corresponding solutions offered by CSP. This gives customers highest level of control over their data since the data and keys are never exposed to the CSP. Instead, data is encrypted before sending it to the CSP for storage.

Tasks Approaches	Key Monitor	Key Generation	Key Management	Data Encryption	Key Monitor	Key Generation	Key Management	Data Encryption
Default CSP Protection	●	●	●	●				
Managed CSP Protection		●	●	●	●			
BYOK			●	●	●	●		
HYOK				●	●	●	●	
BYOE					●	●	●	●
Responsible Party	CSP				Customer			

Figure 4: Approaches for separation of duties between CSP and Customer

Figure 4 illustrates how the approaches described in this section address separation of duties between CSP and customer for four independent operations: key monitoring, key generation, key management, and use of these keys in cryptographic operations such as data encryption/decryption. Key management implies complete key lifecycle management, including key rotation.

Conclusion

Recognizing the need for data protection, CSPs such as Google, Amazon Web Services and Microsoft Azure offer native encryption and Key Management Service with many of their services. Applications can use the encryption and KMS to protect data at rest. While the native encryption and key management services are robust, separation of trust between the CSP and the customer is not only a good security practice but is often necessary for compliance. This separation of duties enables the customer to be the custodian of encryption keys and thereby achieve higher levels of assurance and risk management. Recognizing this important need for separation of trust, CSPs offer several approaches to allow a customer to be the custodian of keys. These approaches are Bring Your Own Key (BYOK), Host your Own Key (HYOK) and Bring Your Own Encryption (BYOE). While BYOE is the best option for separation of trust between the customer and the CSP, BYOK and HYOK are good choices that meet many of the high assurance and regulatory compliance requirements.

References

[1] Thales 2021 Global Data Threat Report

[2] 2019 Thales Cloud Security Report

[3] Gruschka, Nils & Jensen, Meiko. (2010). Attack Surfaces: A Taxonomy for Attacks on Cloud Services. 276 - 279. 10.1109/CLOUD.2010.23.

[4] Rules for the protection of personal data inside and outside of EU, European Commission

[5] California Consumer Privacy Act (CCPA), https://oag.ca.gov/privacy/ccpa

[6] The Court of Justice of the European Union in Schrems II: The impact of GDPR on data flows and national security

[7] Select the Right Key Management as a Service to Mitigate Data Security and Privacy Risks in the Cloud, https://www.gartner.com/en/documents/3997032/select-the-right-key-management-as-a-service-to-mitigate

[8] Victor Costan and Srinivas Devadas. "Intel SGX Explained." IACR Cryptology ePrint Archive 2016 (2016): 86. https://eprint.iacr.org/2016/086.pdf

[9] Amazon Simple Storage Service (S3), https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingClientSideEncryption.html

[10] Azure date encryption at rest, https://docs.microsoft.com/en-us/azure/security/fundamentals/encryption-atrest

[11] NIST Security Requirements for Cryptographic Modules, FIPS 140-2, https://csrc.nist.gov/publications/detail/fips/140/2/final

[12] Post-Quantum Crypto Agility, https://cpl.thalesgroup.com/encryption/post-quantum-crypto-agility

THALES

Building a future we can all trust

Contact us

For all office locations and contact information,
please visit cpl.thalesgroup.com/contact-us

> cpl.thalesgroup.com <