亚马逊云科技

2021 Security Day

亚马逊云端应用安全增强方案

安全加密：如何选择，怎么选择?

硬件安全模块

托管服务

自建系统

集成度

自由度

数据保护：亚马逊云提供适用于不同场景的服务

Amazon Key Management Service

Certificate Manager Private Certificate Authority

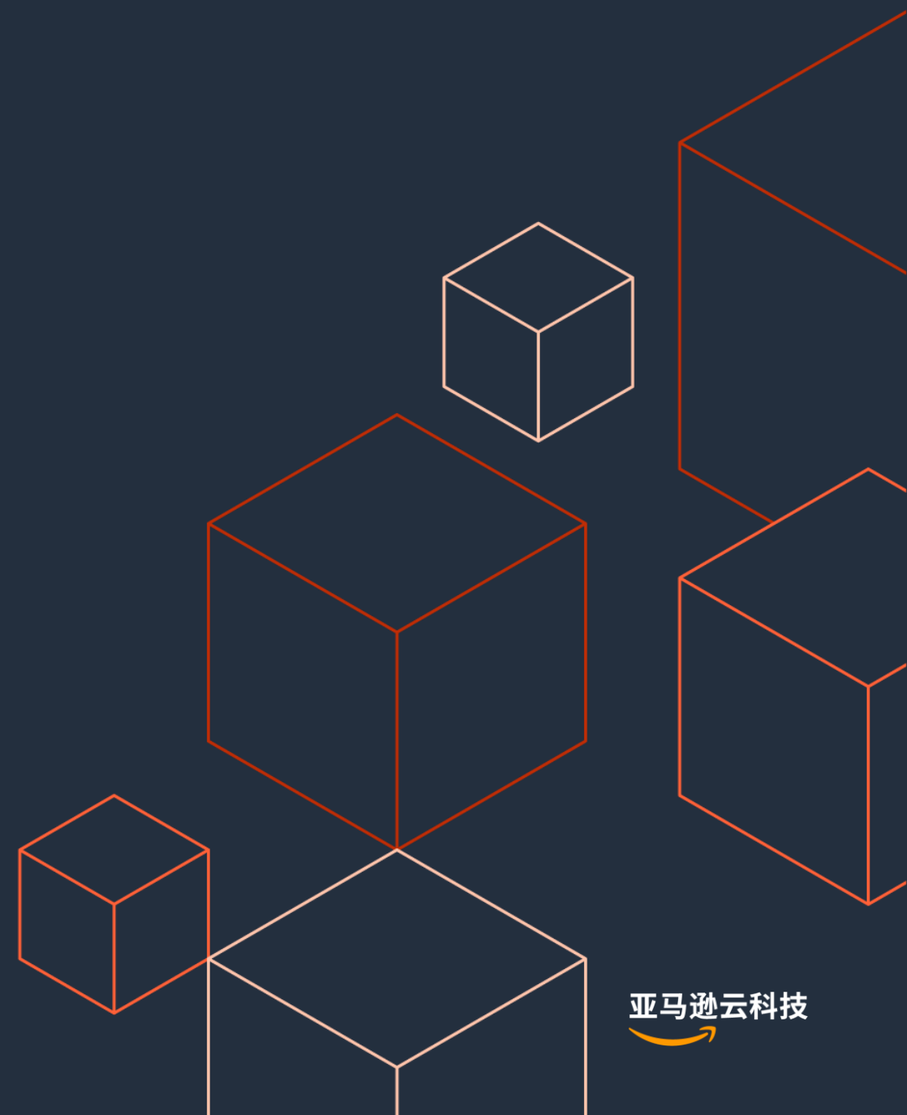
Amazon Secrets Manager

Amazon CloudHSM

每个服务都使用经过FIPS验证的硬件来保护密钥

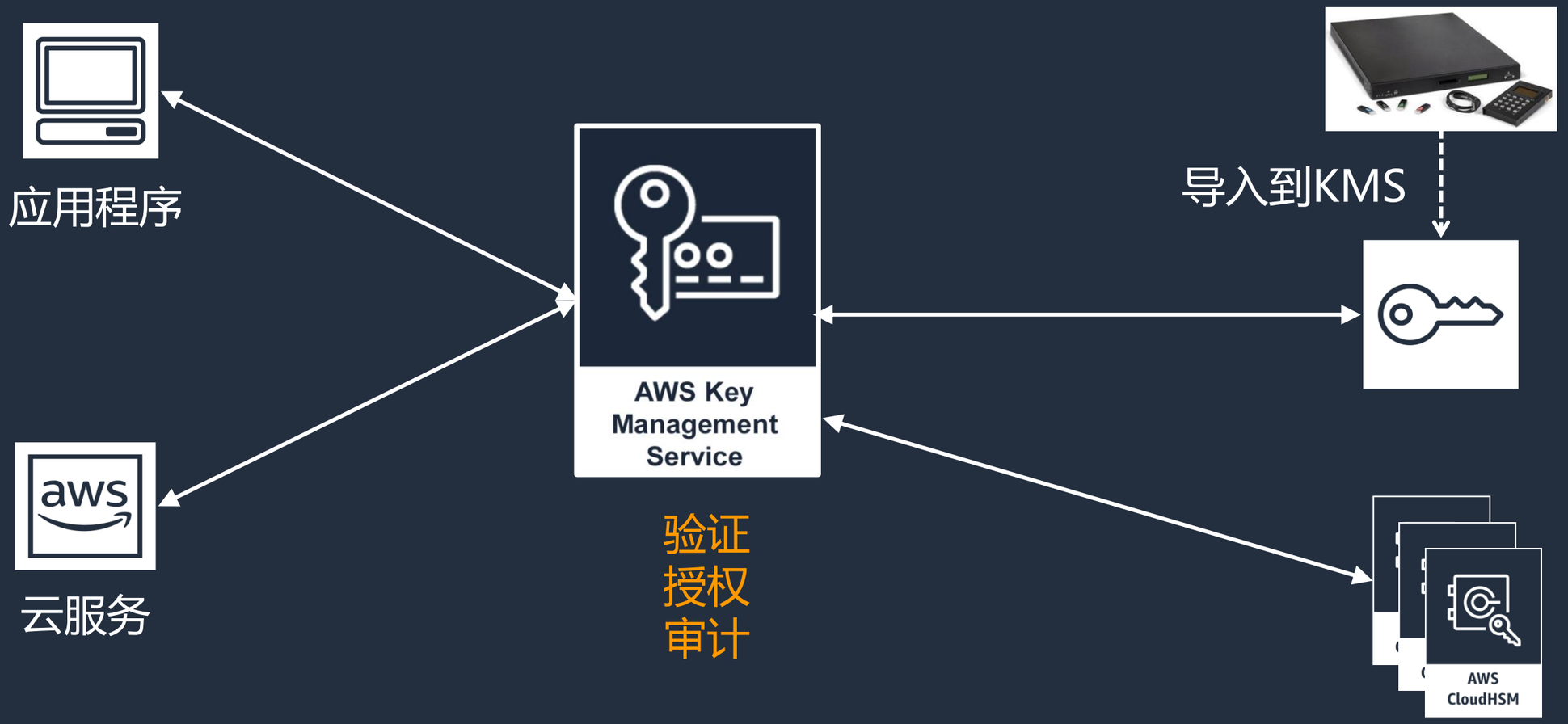
几种服务在同CloudHSM的集成上有所区别，包括控制维度，成本以及灵活性等方面

我想安全地使用密钥来加密数据

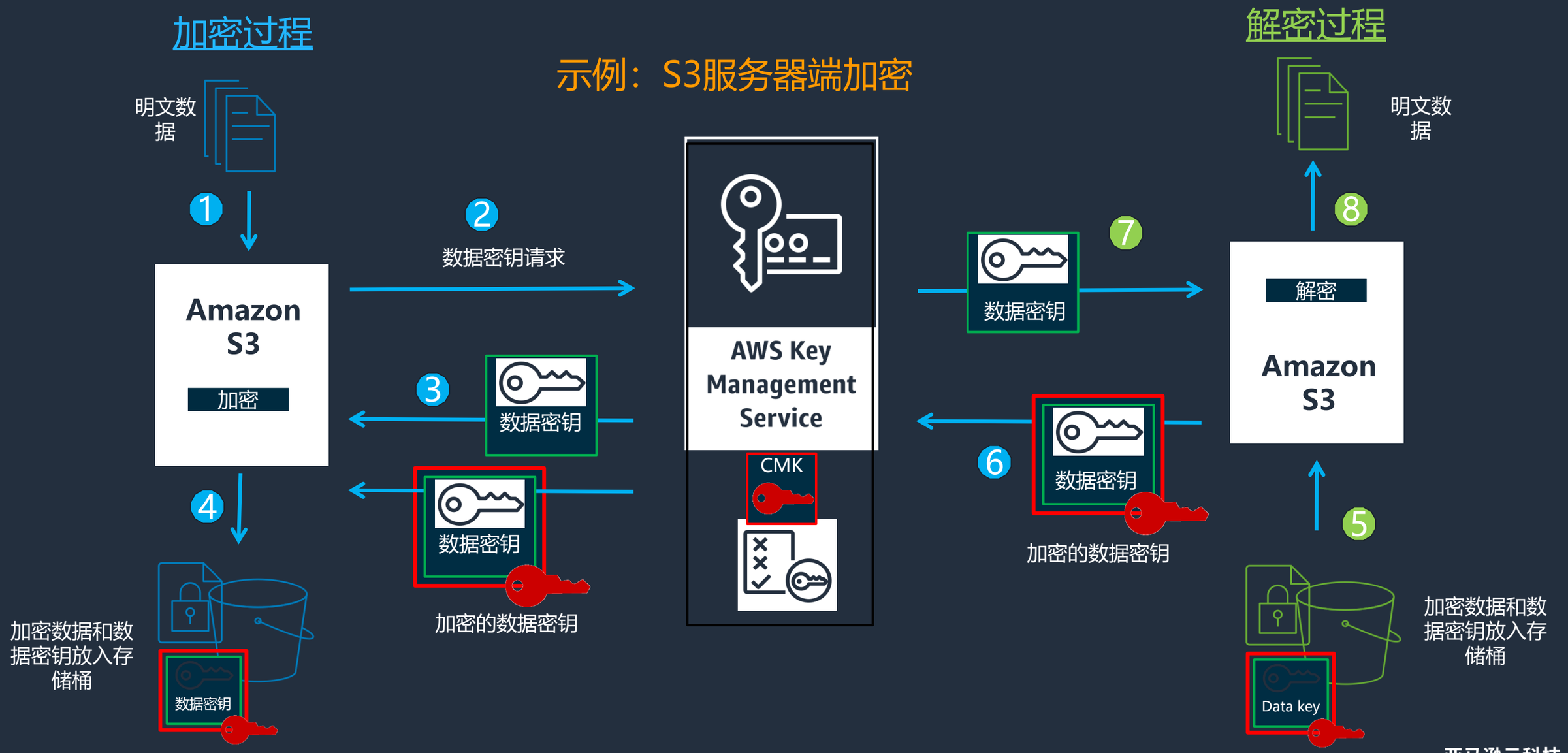


亚马逊云科技

亚马逊云 KMS



信封加密

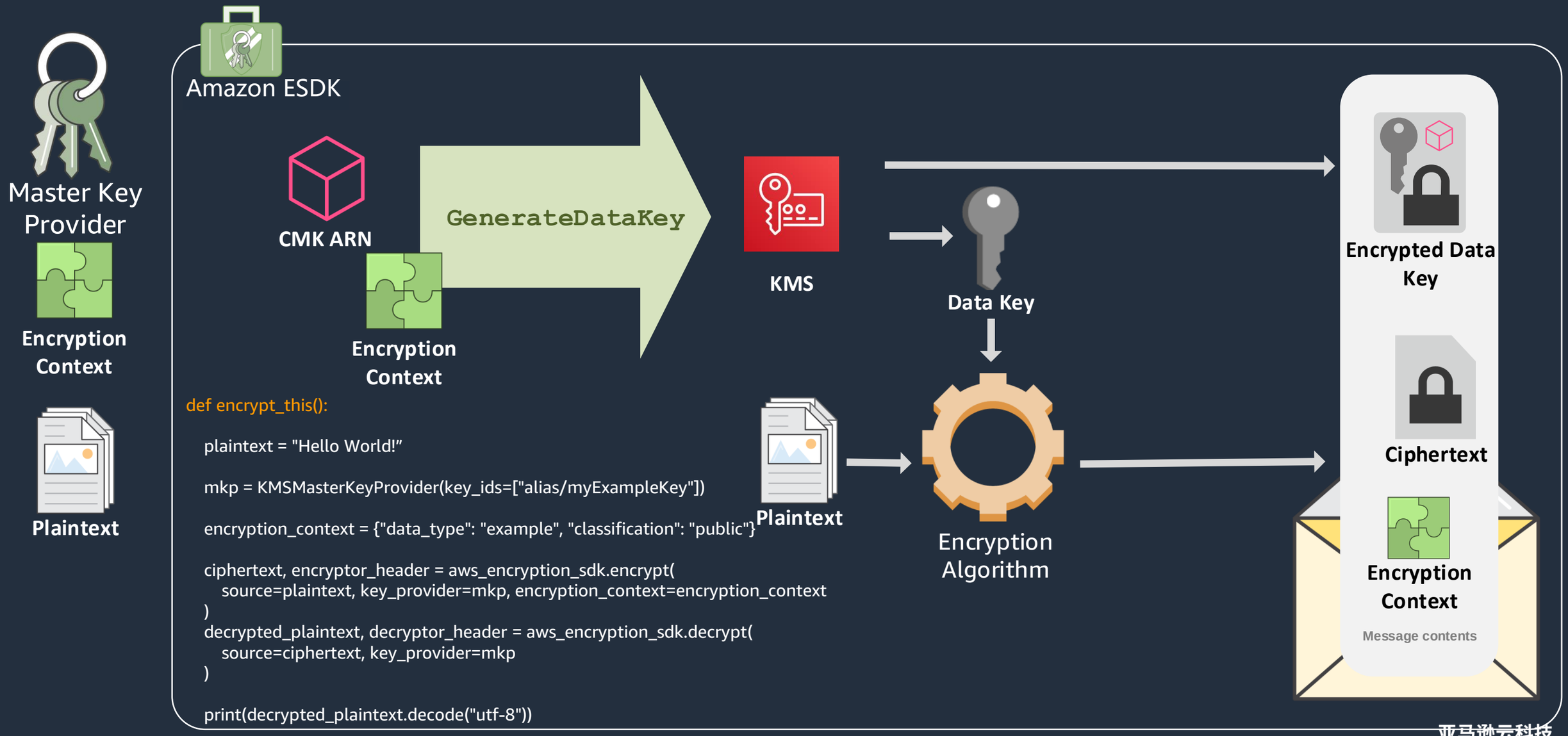


亚马逊云科技

亚马逊云加密SDK

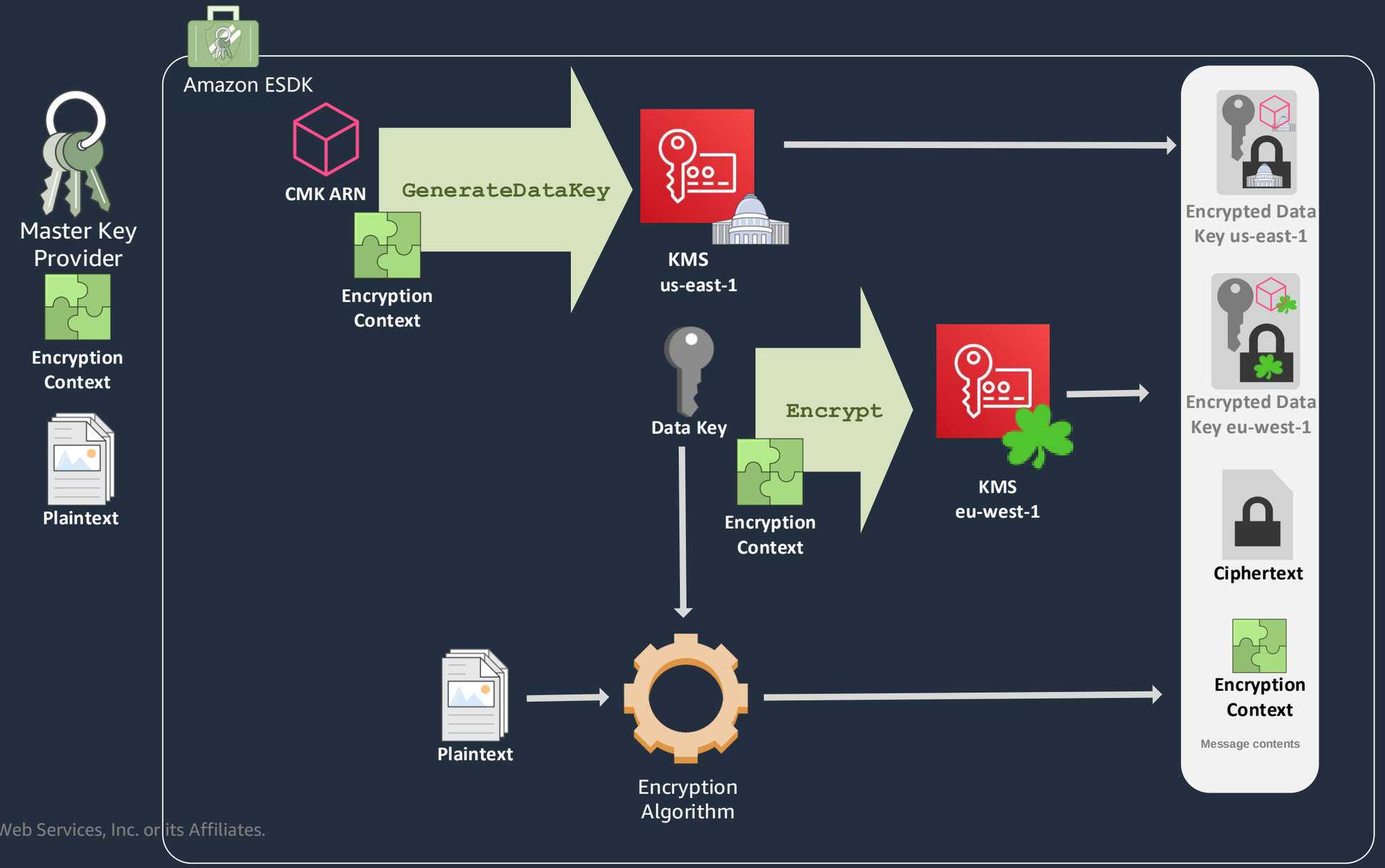
- 提供了客户端加密的框架和数据格式
- 为您提供经过验证的信封加密的库
- 可以支持KMS的主密钥也可以使用外部的密钥
- 适用于Java,C,Python和JavaScript的实现
- 如果您想使用其他语言来实现，则可以使用规范说明
- 支持数据密钥缓存
- 在Apache 2.0许可下开源
- 建立在特定于语言的加密基元上

使用Amazon Encryption SDK加密

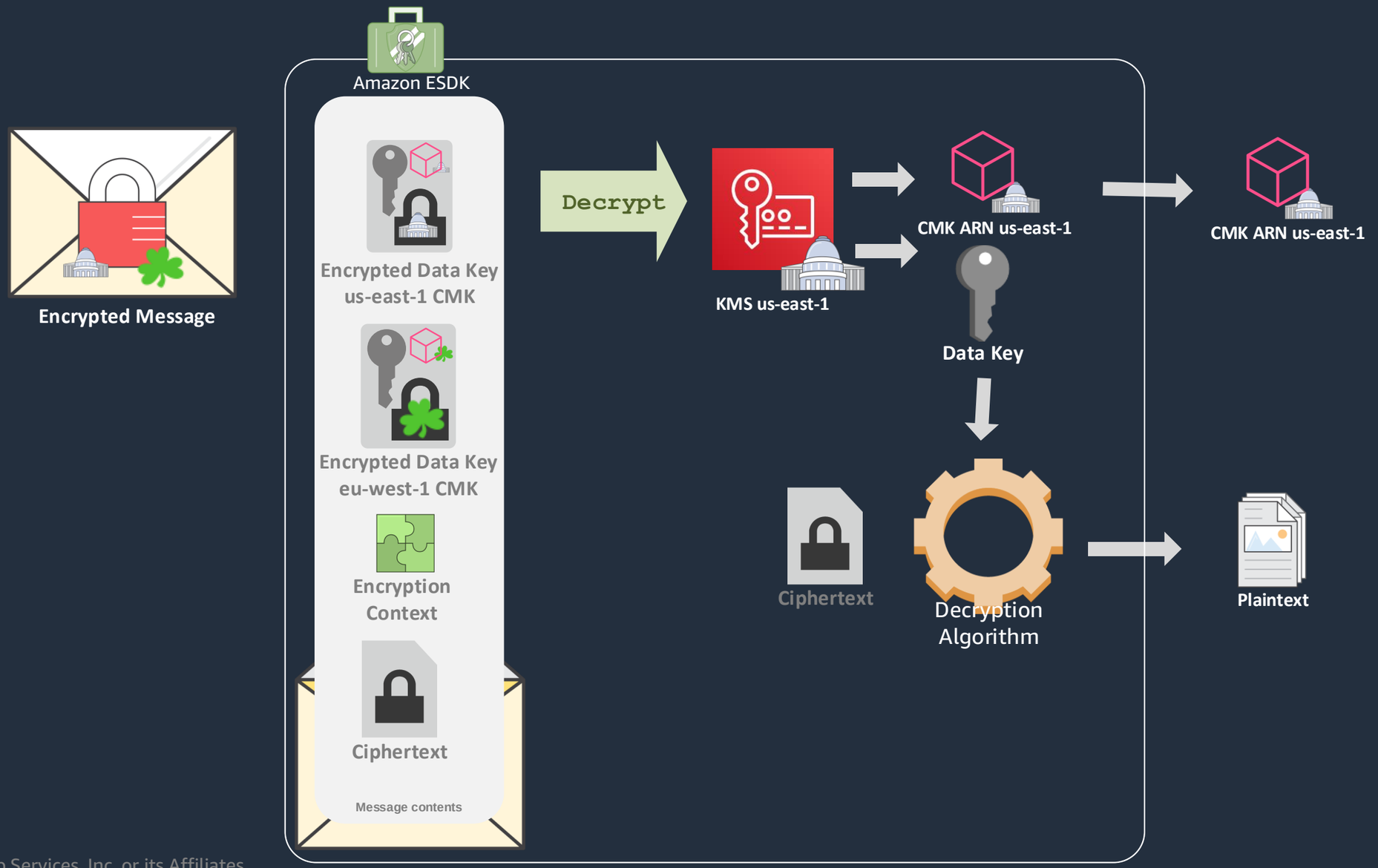



```
def encrypt_this():

    plaintext = "Hello World!"

    mkp = KMSMasterKeyProvider(key_ids=["alias/myExampleKey"])

    encryption_context = {"data_type": "example", "classification": "public"}

    ciphertext, encryptor_header = aws_encryption_sdk.encrypt(
        source=plaintext, key_provider=mkp, encryption_context=encryption_context
    )
    decrypted_plaintext, decryptor_header = aws_encryption_sdk.decrypt(
        source=ciphertext, key_provider=mkp
    )

    print(decrypted_plaintext.decode("utf-8"))
```

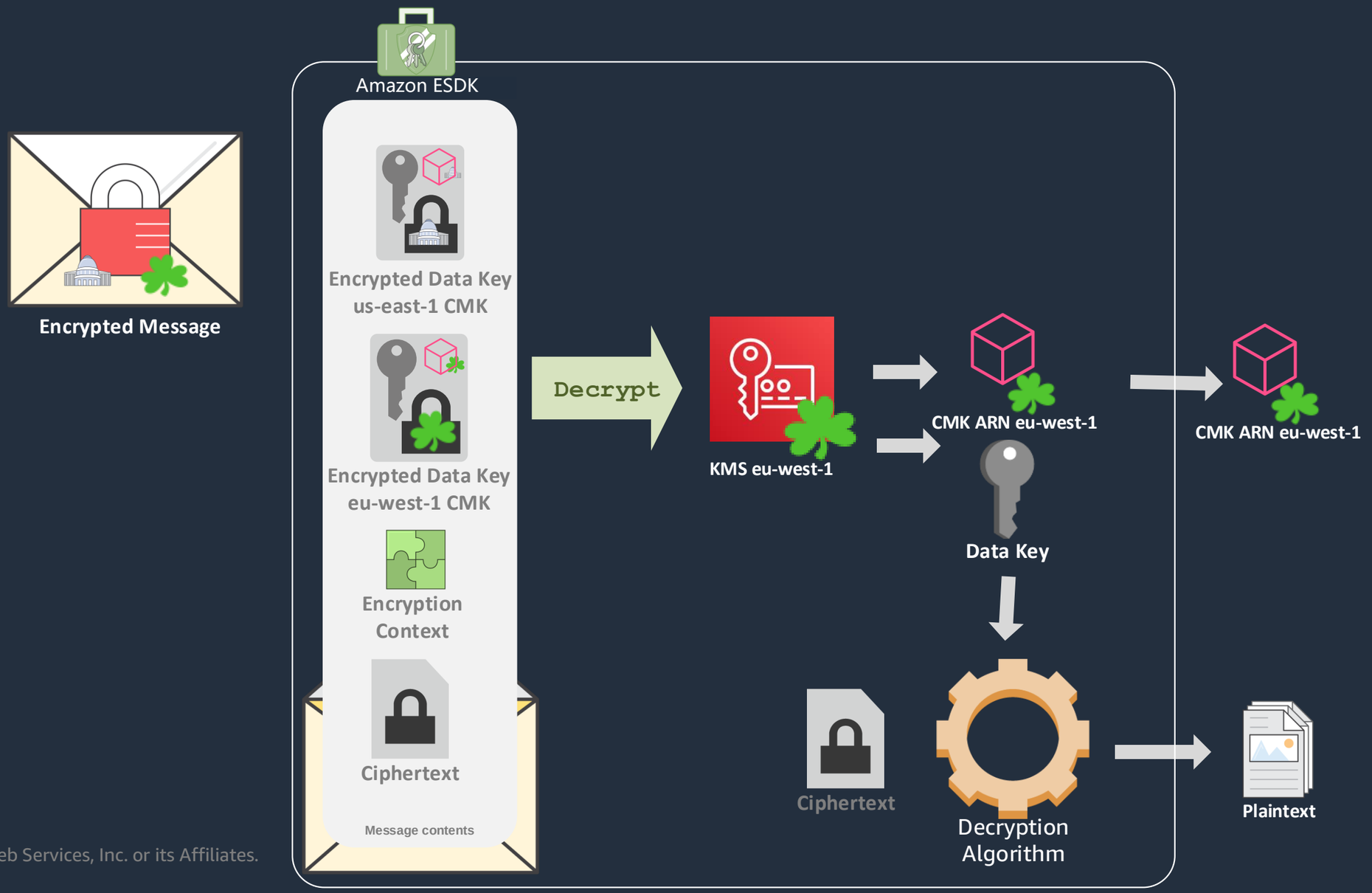
使用 亚马逊云 Encryption SDK 加密+ 多个 CMK



在us-east-1进行解密



在eu-west-1进行解密

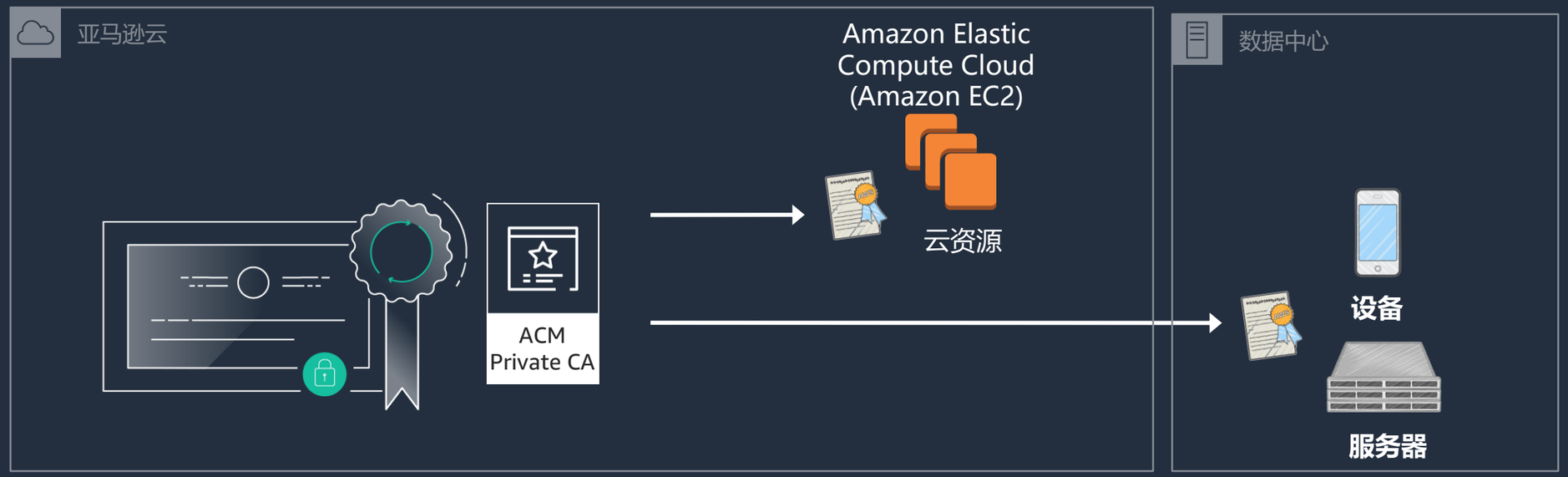


我想创建一个公钥基础架构（PKI）以对内部服务器或设备进行身份验证

亚马逊云科技

ACM 私有 CA

- ACM私有CA是完全托管的CA
- 避免了自己管理CA的复杂性
- 可作为独立的CA或与ACM一起运行以进行证书管理
- 证书在您的组织内是受信任的

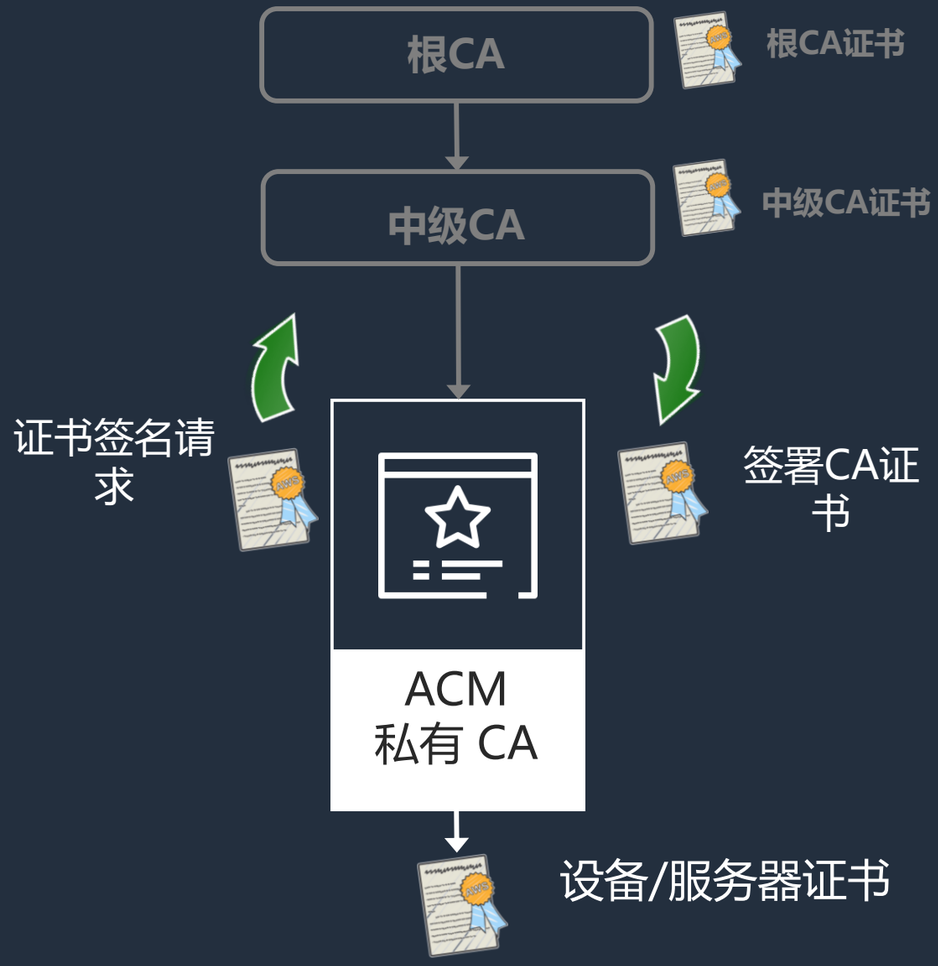


CA的相关词汇

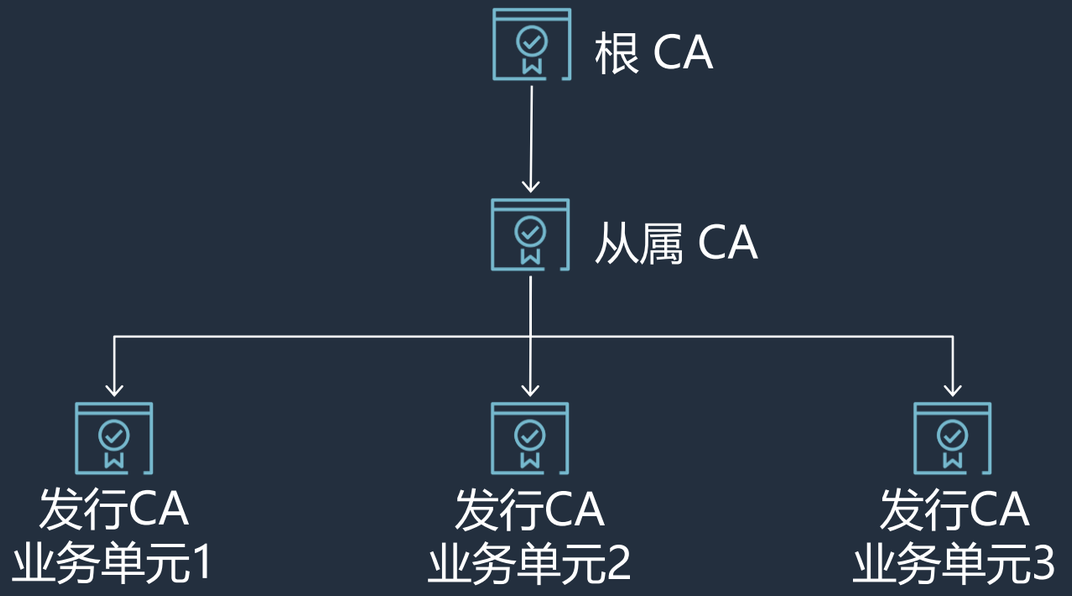
CA层次结构	证书颁发机构之间的信任链，从根到下级CA
根CA	用于在组织中建立对后续CA和证书的信任的CA
下级CA	由根CA或更高级别的下级CA签名并获得其信任的CA，用于实现灵活性或组织性
最终用户证书	颁发给服务，设备或个人的证书（不是CA证书）
有效期	证书将被信任的时间段
吊销	强制无效证书

ACM私有CA设置和层次结构

- 创建私有CA，完整的CA层次结构，包括根CA
- 第三方外部CA是可选的
- 建立对现有根CA的信任链
  - 导出CSR并与父CA签署
  - 导入签名的CA证书
- 颁发设备/资源/服务器证书



根CA和从属CA



- 经FIPS-140-2 L3验证的HSM中保护CA密钥
- 使用亚马逊 Identity and Access Management（IAM）控制访问
- 跨区域的场景中，通过将一个区域中的根CA作为外部CA来处理其他区域中从属CA

符合ACM的数据隐私和保护

- **HIPAA Eligible** - 敏感的患者数据保护标准
- **AICPA SOC 1, 2, and 3** – 深入了解ACM的安全流程和控制
- **PCI DSS** – 保护持卡人数据的技术和操作要求
- **ISO 9001, 27001, 27017, and 27018** – 在最受认可的全球安全标准中

私有CA层级结构设计考量因素

组织

如何隔离?

谁应该信任什么?

颁发

多少张证书?

在什么时间?

吊销

我可以负担得起吗?

在这种情况下会发生什么?

访问

谁需要访问?

访问频度? 从哪里?

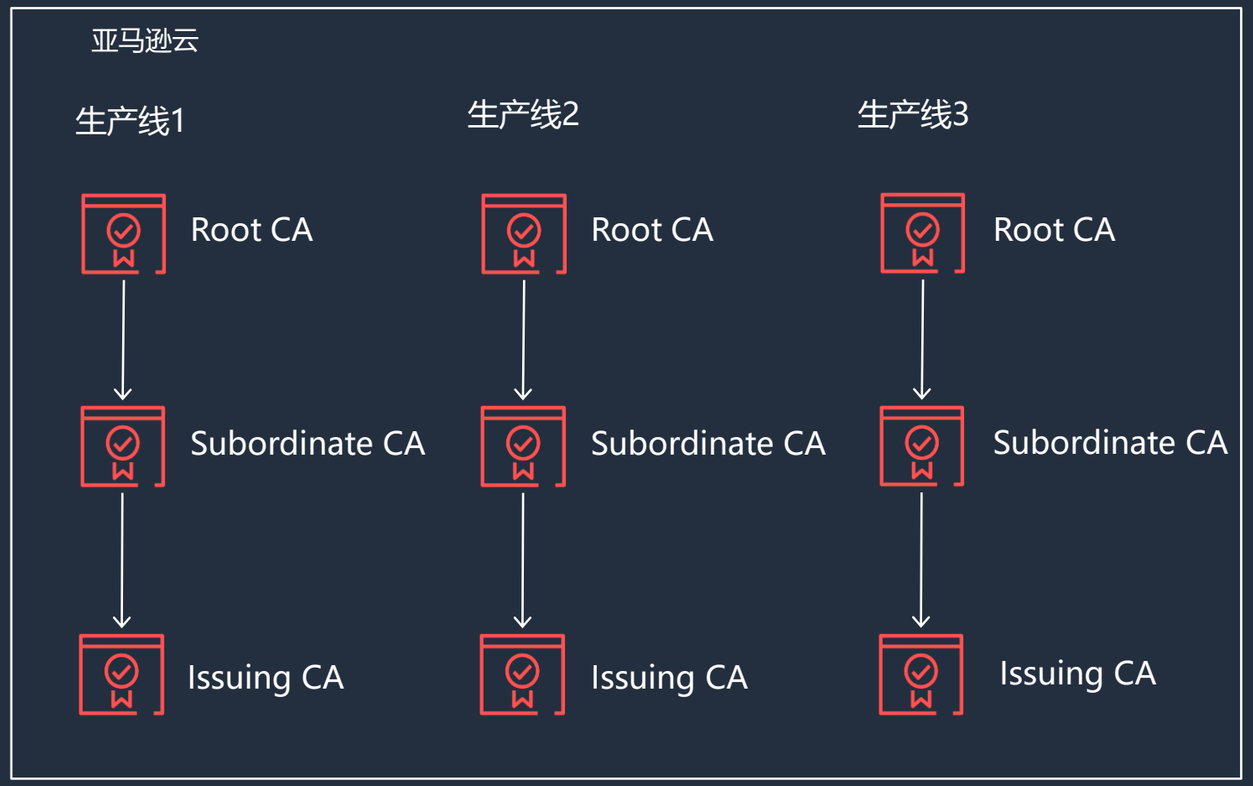
有效

必要的寿命?

如果证书签发不正确怎么办?

私有CA架构设计

生产线



服务网格

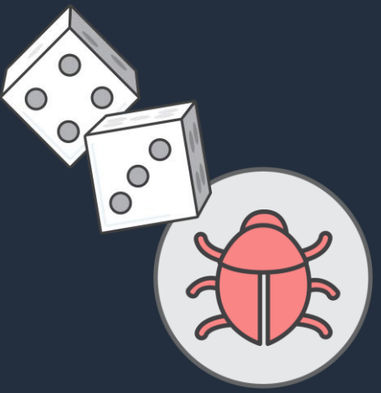
亚马逊云科技

我想管理应用程序使用的密钥的生命周期–存储，检索，轮换，审计和监视

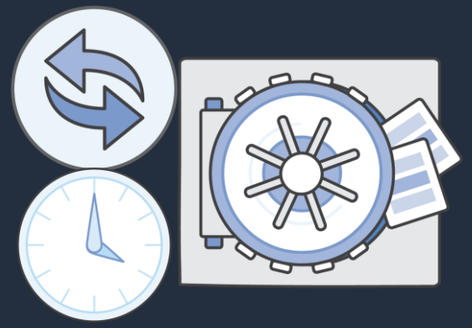
亚马逊云科技

亚马逊 Secrets Manager

- 密钥信息的生命周期管理，例如数据库凭证和API密钥
- 控制对密钥的访问通常与控制对数据的访问相同
- 与亚马逊 IAM和其他服务集成
- 太多的人处理密钥会带来风险和脆弱性；自动密钥轮换提供安全性和可用性
- 与Amazon RDS集成，以使用新凭证更新客户端和数据库服务器

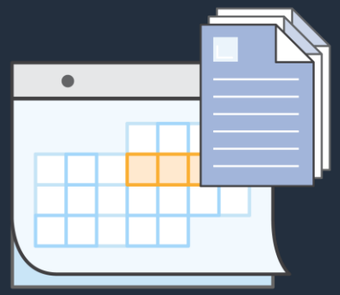


亚马逊 Secrets Manager: 功能特点



安全轮换
凭证

内置集成，可通过
Lambda扩展



带版本控制的按需或自
动轮换

细粒度
访问策略

加密存储

记录和监控

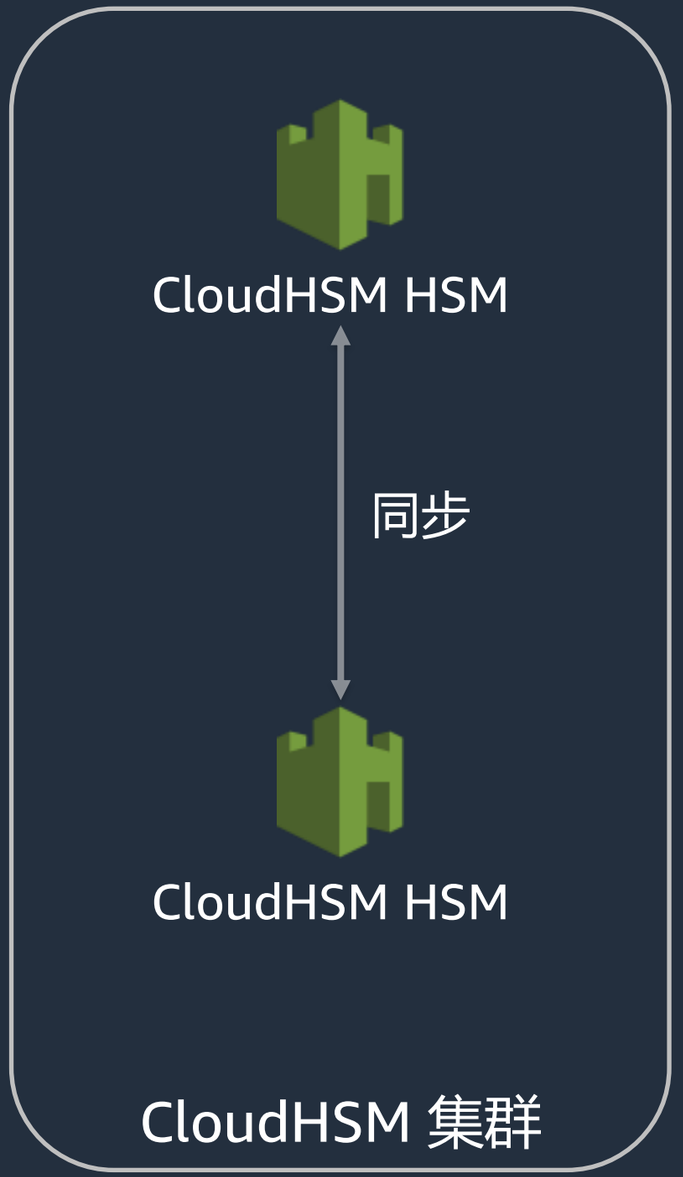
我想直接访问我所控制的FIPS 140-2 L3的HSM

亚马逊云科技

CloudHSM基本概念

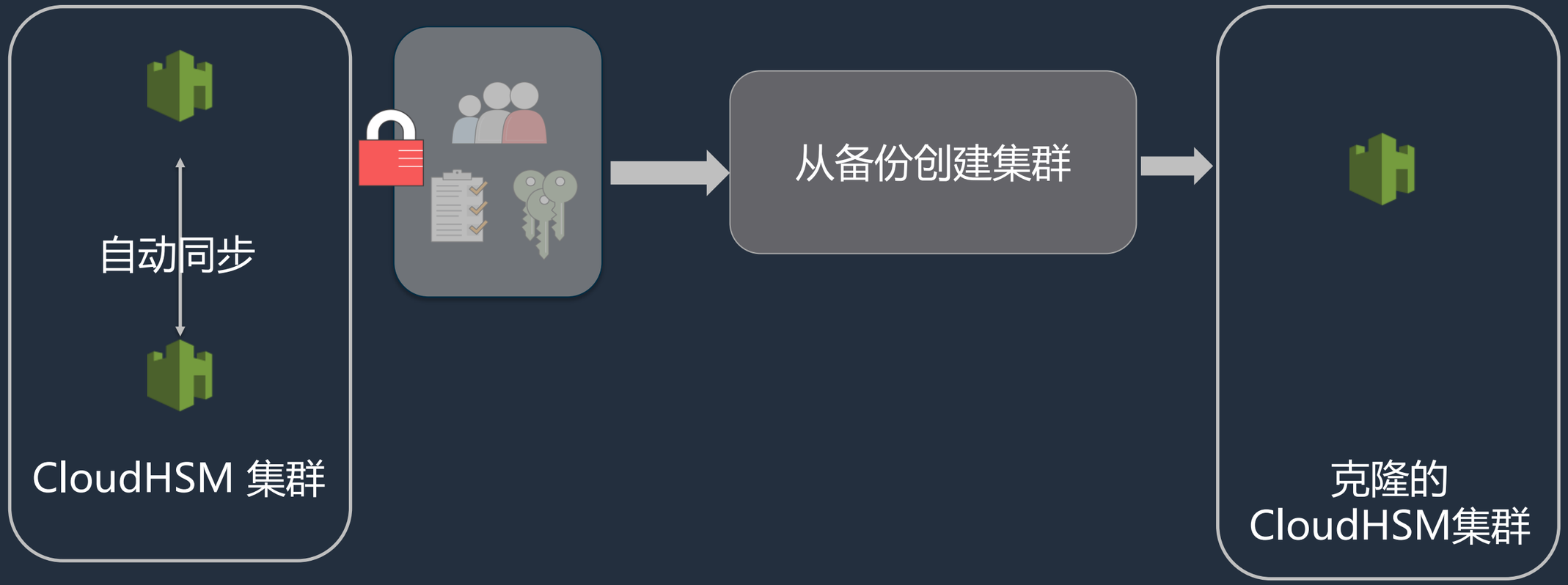
- 集群
- HSM
- 备份

- 更高的吞吐量：扩展集群
- 需要更多密钥：新集群

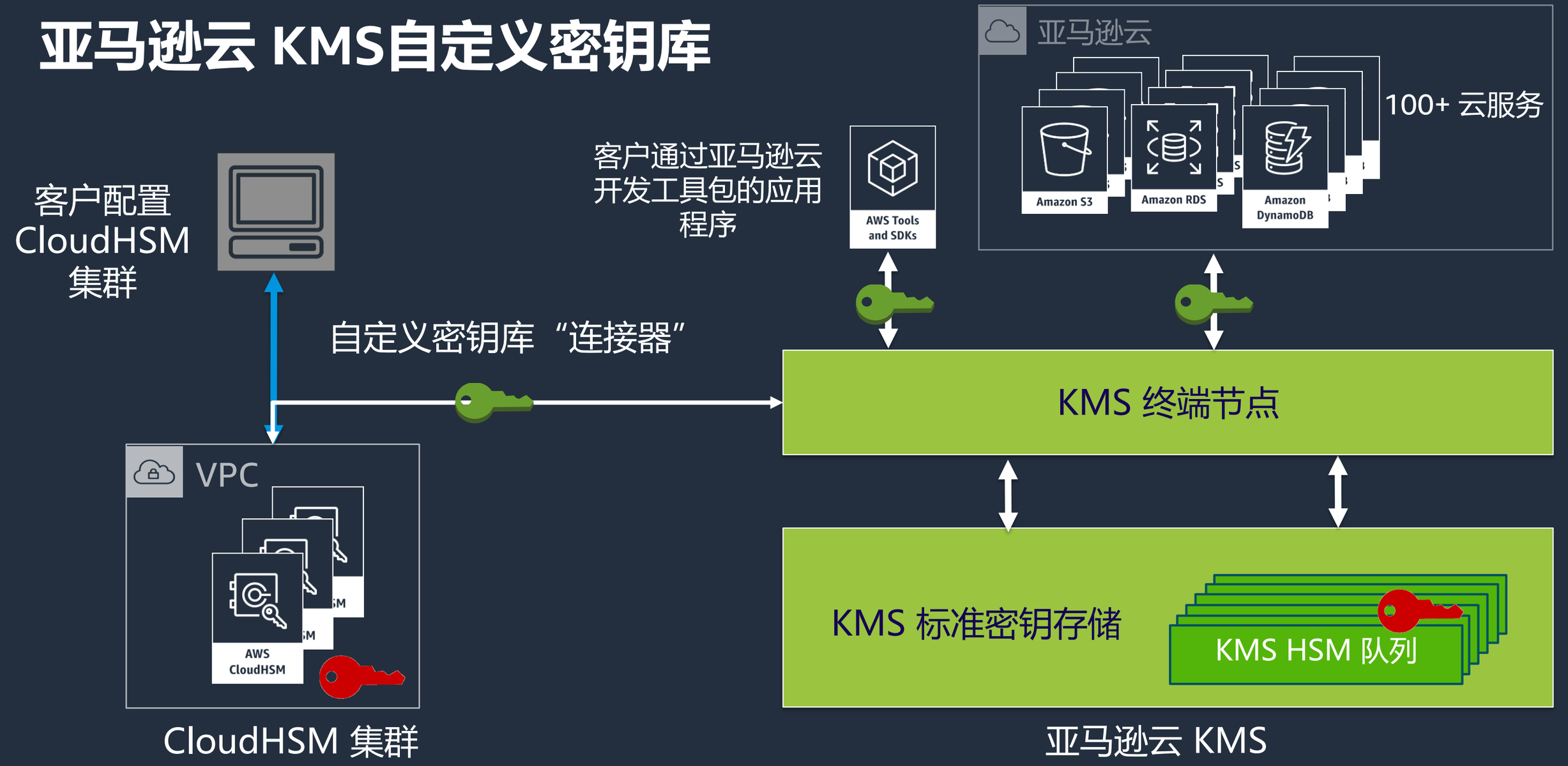


CloudHSM概念

- 克隆集群
    - 相同的信任层次结构和主密钥
    - 可以通过FIPS验证的信封加密同步密钥



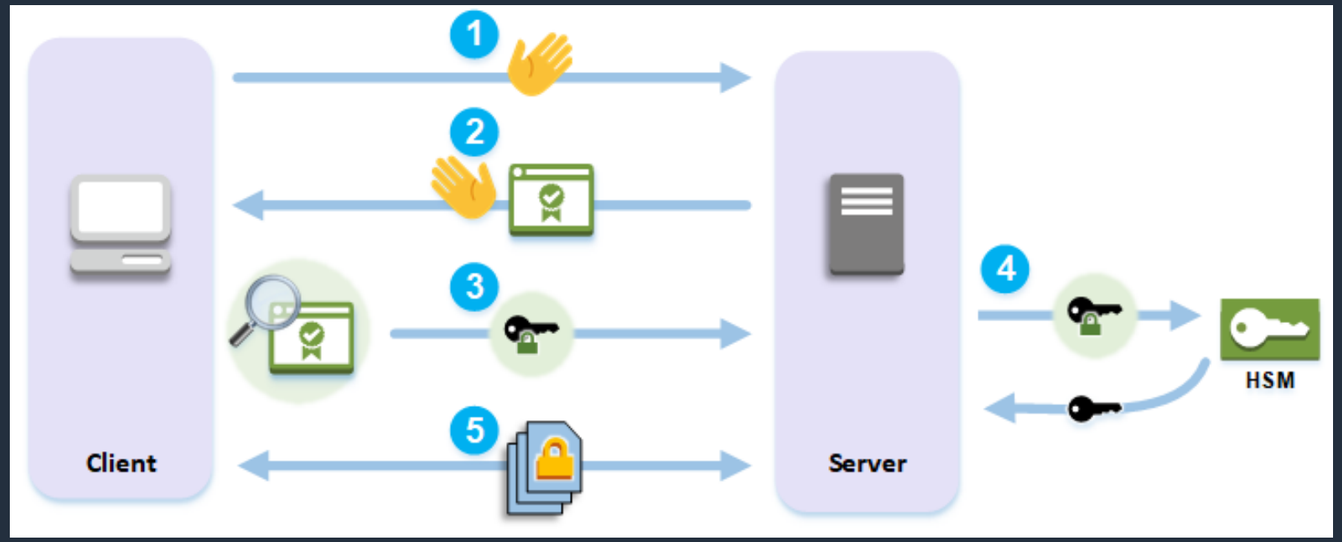
亚马逊云 KMS自定义密钥库



使用CloudHSM的两种方式

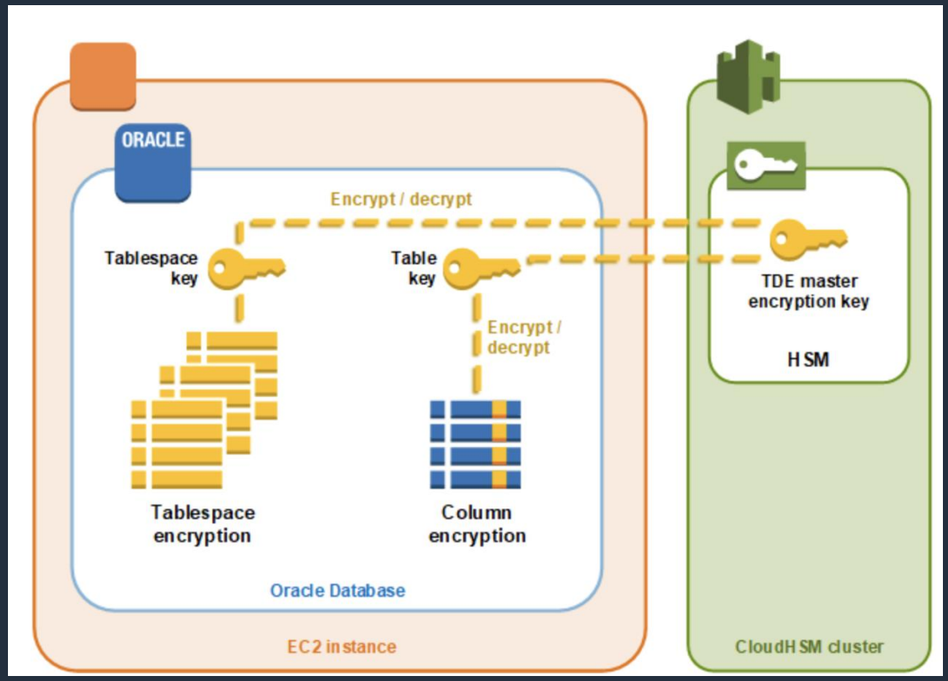
直接交互

- HSM位于每次交互的路径中（例如，SSLOffloading，自定义密钥存储区）
- 可用性和延迟至关重要

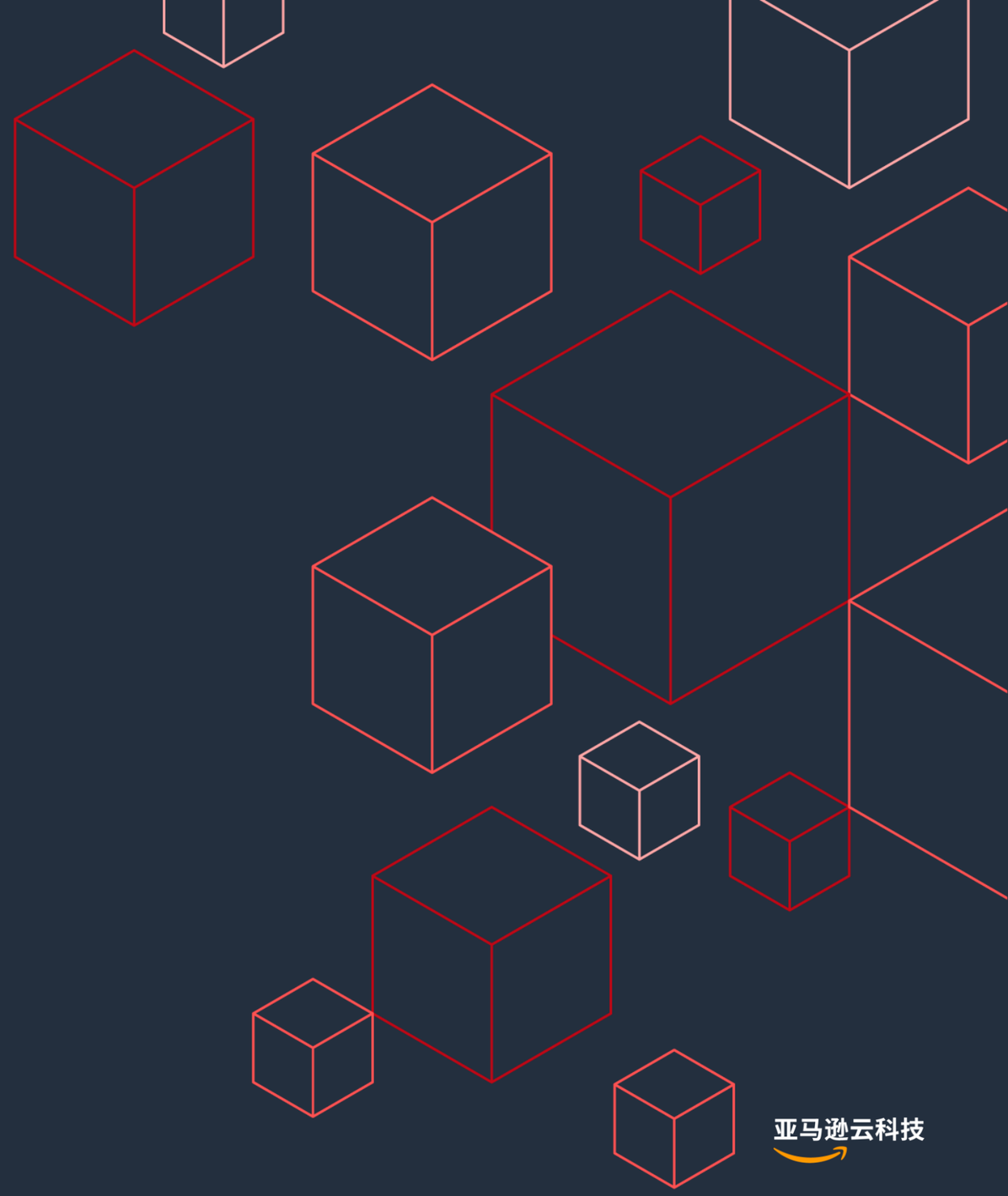


信封加密

- 基于HSM的主密钥可解锁数据密钥（例如，oracle TDE）
- 持久性是首要问题



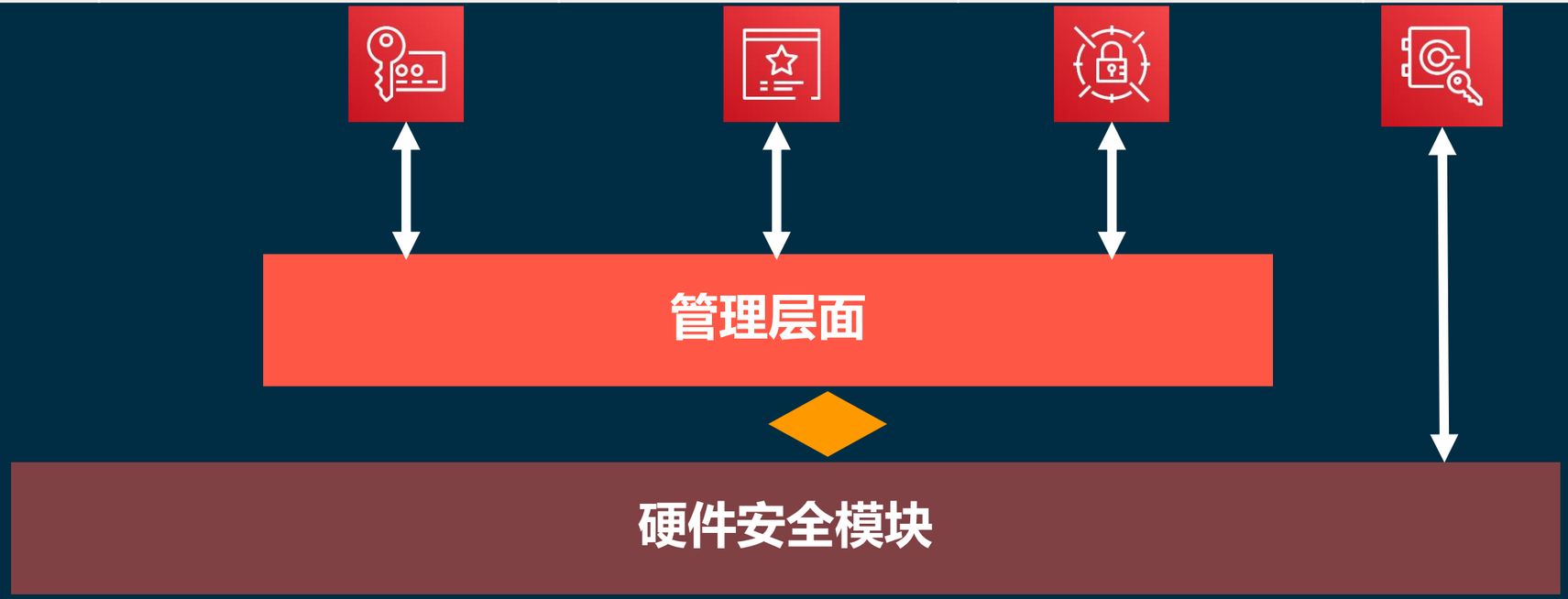
亚马逊云数据加密服务总结



亚马逊云科技

亚马逊云数据加密服务一览

	Amazon KMS	ACM Private CA	Secrets Manager	CloudHSM
范围	AES-256 & RSA 加密; RSA & ECC 签名	PKI 基础设施	生命周期的密钥管理	完善的通用HSM



亚马逊云数据加密服务一览

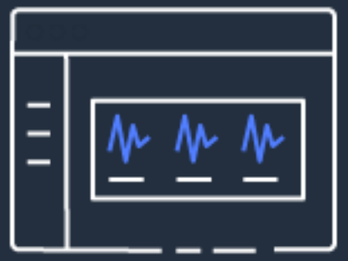
	Amazon KMS	ACM Private CA	Secrets Manager	CloudHSM
范围	AES-256 & RSA 加密; RSA & ECC 签名	PKI 基础设施	生命周期的密钥管理	完善的通用HSM
密钥/凭证存放位置:	共享的FIPS验证的HSM	共享的FIPS验证的HSM	由Amazon KMS管理的加密密钥	客户VPC中经过FIPS验证的HSM
HSM由谁控制:	亚马逊云	亚马逊云	亚马逊云	客户
如何访问密钥:	IAM /资源策略	IAM 策略	IAM 策略	客户自定义的密钥
同亚马逊云的其他服务集成:	是	是	是	否
通过何种方式实现密钥操作:	亚马逊云 CLI/SDK or 加密 SDK	亚马逊云 CLI/SDK	亚马逊云 CLI/SDK	客户自建系统
可扩展性管理:	亚马逊云	亚马逊云	亚马逊云	客户
密钥管理:	亚马逊云	亚马逊云	亚马逊云	客户
轮换:	亚马逊云 [not for BYOK & CKS]	亚马逊云	亚马逊云	客户
价格:	密钥/个，API/次数	证书/个，API/次数	凭证/个，API/次数	HSM/个/小时

我想要快速评估云端数据隐私和安全性并保持合规性

亚马逊云科技

Amazon Macie

大规模发现和保护您的敏感数据

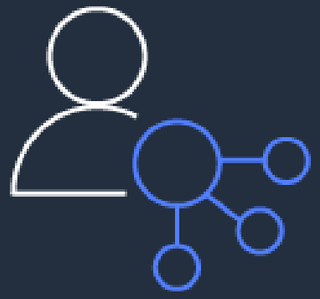


获得可见性并进行评估

- 存储桶可见性
- 存储桶策略变化

发现敏感数据

- 数据检测
- 灵活的范围



大规模集中管理

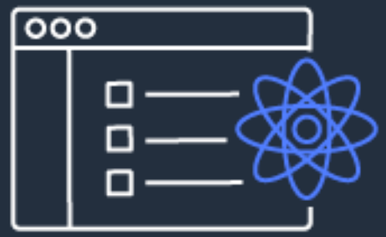
- 亚马逊组织服务
- 托管和自定义数据检测

自动化并采取行动

- 详细调查结果
- 管理API

Amazon Macie – 应用场景

评估您的数据隐私和安全性



保持适当级别的数据安全性的一个重要方面是能够连续识别您的敏感数据并评估安全性和访问控制。将数据（RDS快照，电子邮件，文件共享，协作工具等）临时移动到S3来灵活地识别驻留在其数据存储中的敏感数据。

Amazon Macie – 应用场景

保持合规性

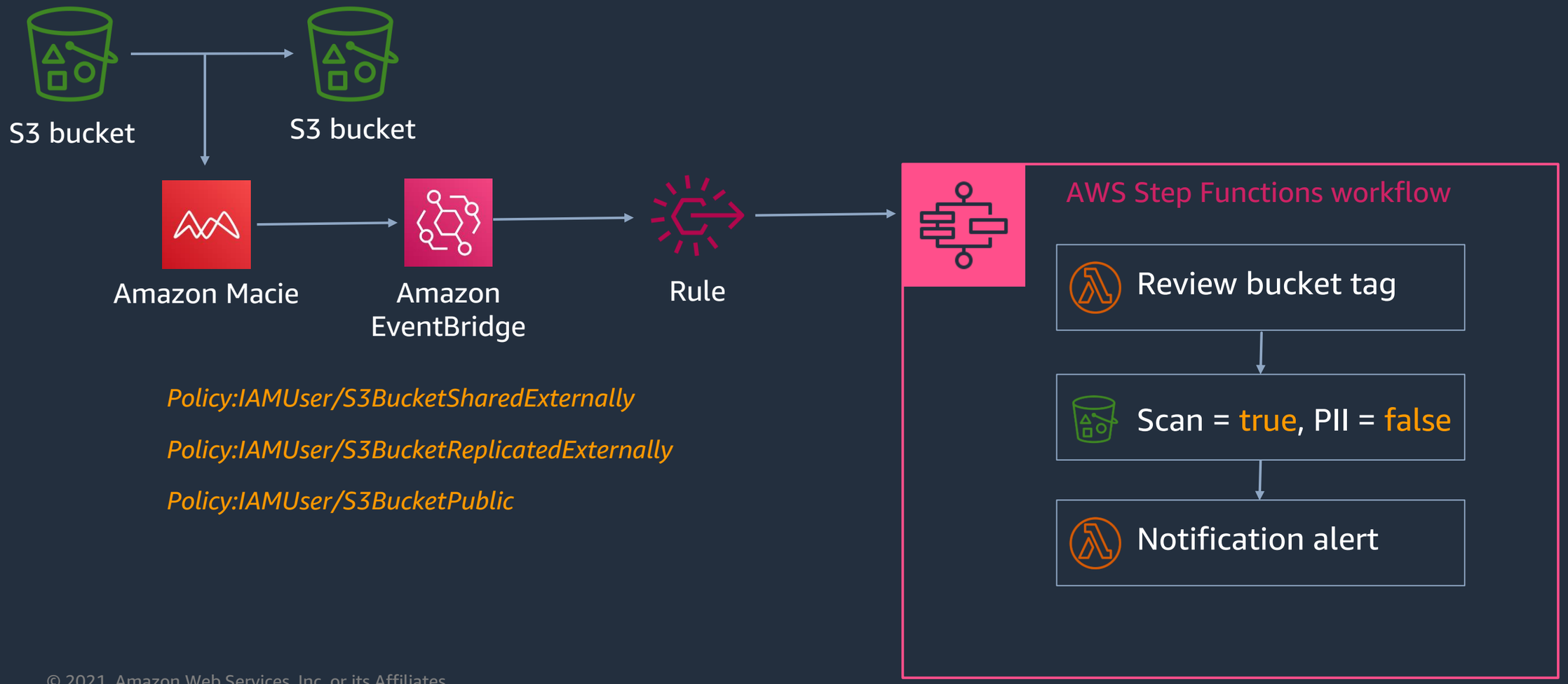
合规团队需要监视敏感数据所在的位置，对其进行适当的保护，并提供证据表明他们正在执行数据安全性和隐私以满足法规合规性要求。Amazon Macie提供了用于安排数据分析的不同选项，例如一次，每天，每周或每月一次的敏感数据发现作业，以帮助您满足并维护数据隐私和合规性要求。

Amazon Macie – 应用场景

在数据迁移中识别敏感数据

将大量数据迁移到AWS时，您可以设置一个安全的Amazon S3环境，当作使用Macie来发现敏感数据的初始暂存区。结果可用于告知应将迁移后的数据存储在何处以及需要使用哪些安全控制（例如加密和资源标记）。

触发有关桶标签和策略发现的警报

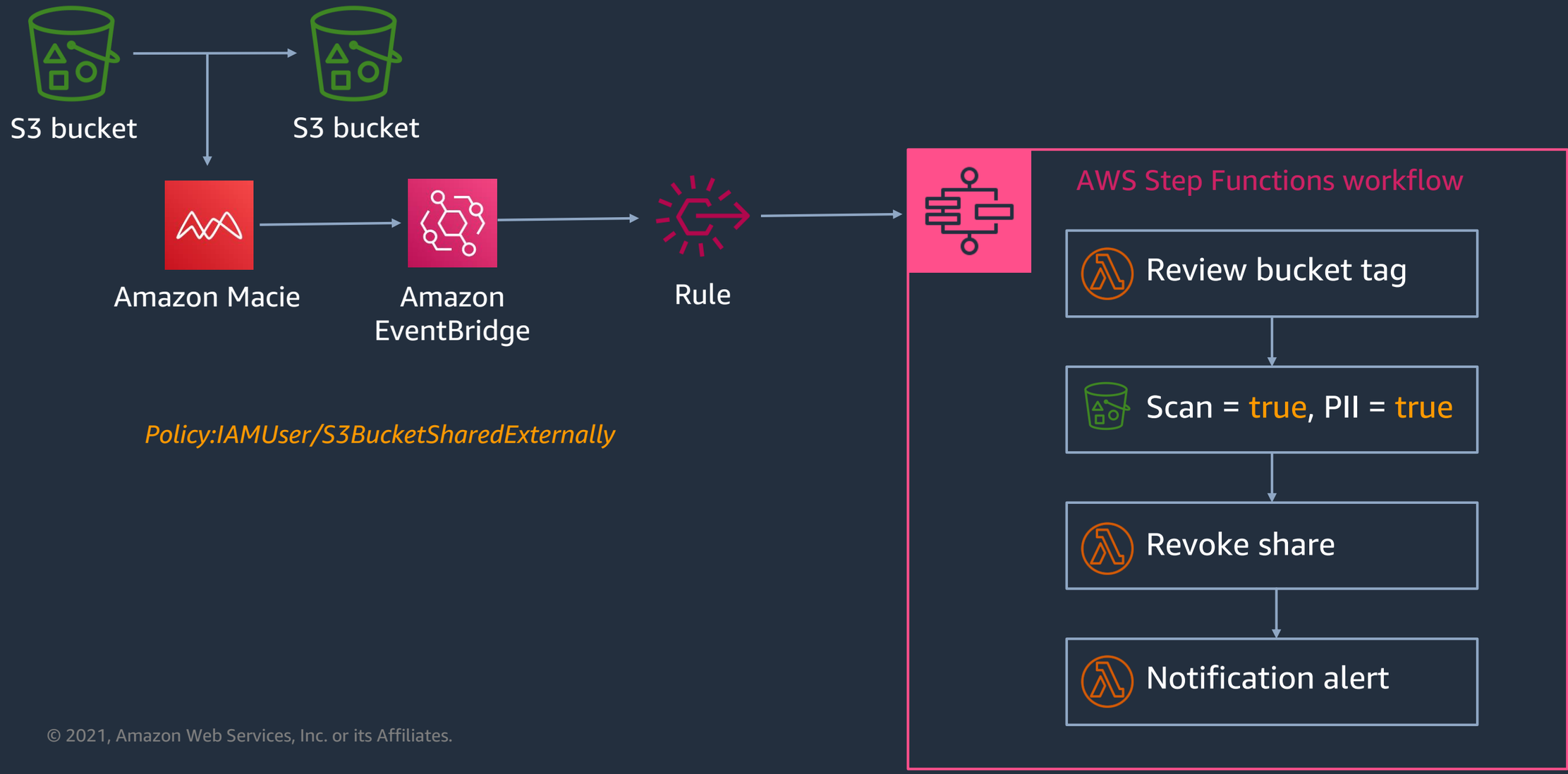


Policy:IAMUser/S3BucketSharedExternally

Policy:IAMUser/S3BucketReplicatedExternally

Policy:IAMUser/S3BucketPublic

查看具有敏感数据的存储桶的策略发现并自动采取措施

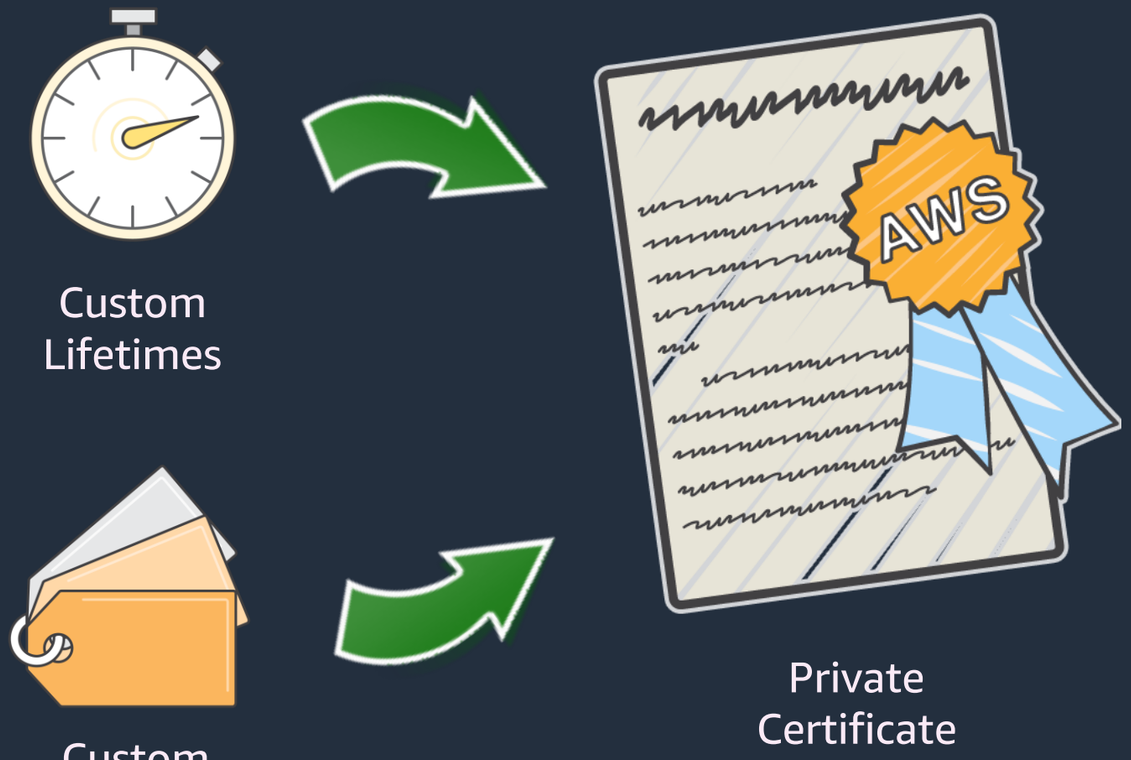


Policy:IAMUser/S3BucketSharedExternally

Thank You

亚马逊云科技

Customization for Standalone Certificates



Key Algorithms	Signing Algorithms
RSA 2048	SHA256 with RSA
RSA 4096	SHA384 with RSA
	SHA512 with RSA
ECDSA P256	SHA256 with ECDSA
ECDSA P384	SHA384 with ECDSA
	SHA512 with ECDSA

ACM Managed versus Unmanaged Certificates

	ACM-Managed Certificates	Unmanaged
Certificate private keys	ACM generates and manages the private key	Customer generates and manages the private key
Certificate subject/SANs	Valid DNS names only	Any valid X.509 subject/SANs
Validity period	13 months	Any validity period
Key and signature algorithm	RSA 2048 with SHA-256 hashing	ECDSA or RSA keys SHA-256, SHA-384, SHA-512 hashing
Export	Available for private certificates	n/a – Customer manages the private keys and certs
Renewals	ACM-managed	Customer-managed
Deployment	ACM-managed for ACM-integrated services Customer-managed for on-premises, EC2, IoT	Customer-managed
Benefits	Central management	Flexibility

AWS KMS custom key store: Best of two worlds

	AWS KMS	KMS CustomKeyStore (CloudHSM)
Where keys are generated	HSMs controlled by AWS	HSMs controlled by you
Where keys are stored	HSMs controlled by AWS	HSMs controlled by you
Where keys are used	HSMs controlled by AWS	HSMs controlled by you
How to control key use	JSON key policies you define	JSON key policies you define
Responsibility for performance/scale	AWS	You
Integration with AWS services?	Yes	Yes
Pricing model	$1/key + usage	$1/key + usage; Hourly charge for each HSM