AWS KMS Detalles criptográficos

AWS Key Management Service

AWS Key Management Service: AWS KMS Detalles criptográficos

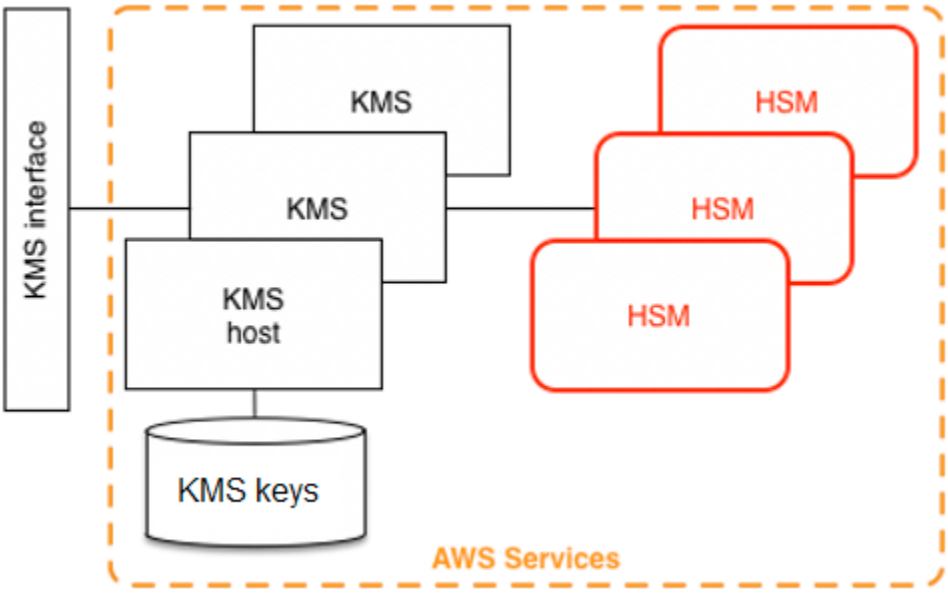
Table of Contents

Introducción a los detalles criptográficos de AWS KMS

AWS Key Management Service (AWS KMS) proporciona una interfaz web para generar y administrar claves criptográficas y funciona como proveedor de servicios criptográficos para proteger los datos. AWS KMS ofrece servicios de administración de claves tradicionales integrados con otros AWS servicios para proporcionar una visión uniforme de las claves de los clientes en todas sus áreas AWS, con administración y auditoría centralizadas. Este documento técnico proporciona una descripción detallada de las operaciones criptográficas AWS KMS para ayudarlo a evaluar las funciones que ofrece el servicio.

AWS KMS incluye una interfaz web a través de la Consola de administración de AWS interfaz de línea de comandos y las operaciones de RESTful API para solicitar las operaciones criptográficas de una flota distribuida de módulos de seguridad de hardware validados por el FIPS 140-3 () [1]. HSMs El AWS KMS HSM es un dispositivo criptográfico de hardware independiente y multichip diseñado para proporcionar funciones criptográficas dedicadas a cumplir con los requisitos de seguridad y escalabilidad de. AWS KMS Puede establecer su propia jerarquía criptográfica basada en el HSM con claves que administra como AWS KMS keys. Estas claves están disponibles únicamente en la memoria HSMs y solo en ella durante el tiempo necesario para procesar su solicitud criptográfica. Puede crear varias claves de KMS, cada una representada por su ID de clave. Solo en las funciones de AWS IAM y las cuentas administradas por cada cliente se pueden crear, eliminar o utilizar las claves KMS del cliente para cifrar, descifrar, firmar o verificar datos. Puede definir los controles de acceso sobre quién puede administrar el and/or uso de las claves de KMS mediante la creación de una política adjunta a la clave. Estas políticas permiten definir usos específicos de la aplicación para las claves en cada operación de la API.

Además, la mayoría de AWS los servicios admiten el cifrado de datos en reposo mediante claves KMS. Esta capacidad permite a los clientes controlar cómo y cuándo AWS los servicios pueden acceder a los datos cifrados al controlar cómo y cuándo se puede acceder a las claves KMS.



AWS KMS es un servicio por niveles que consta de AWS KMS hosts orientados a la web y un nivel de. HSMs La agrupación de estos hosts en niveles forma la pila. AWS KMS Todas las solicitudes AWS KMS deben realizarse a través del protocolo de seguridad de la capa de transporte (TLS) y terminar en un host. AWS KMS AWS KMS los hosts solo permiten el TLS con un conjunto de cifrado que proporciona un secreto directo perfecto. AWS KMS autentica y autoriza sus solicitudes utilizando los mismos mecanismos de credenciales y políticas AWS Identity and Access Management (IAM) que están disponibles para todas las demás operaciones de la API. AWS

Conceptos básicos

Aprender algunos términos y conceptos básicos le ayudará a sacarles el máximo provecho AWS Key Management Service.

AWS KMS key

> **Note**
>
> AWS KMS está sustituyendo el término clave maestra del cliente (CMK) por clave KMS. AWS KMS key El concepto no ha cambiado. Para evitar cambios importantes, AWS KMS mantiene algunas variaciones de este término.

Una clave lógica que representa la parte superior de la jerarquía de claves. Una clave de KMS se le asigna un nombre de recurso de Amazon (ARN) que incluye un identificador de clave único o un ID de clave. AWS KMS keys tienen tres tipos:

- Clave administrada por clientes: los clientes crean y controlan el ciclo de vida y las políticas clave de las claves administradas por el cliente. Todas las solicitudes realizadas con estas claves se registran como CloudTrail eventos.
- Claves administradas por AWS— AWS crea y controla el ciclo de vida y las Claves administradas por AWS políticas clave de los recursos de un cliente Cuenta de AWS. Los clientes pueden ver las políticas de acceso y CloudTrail los eventos de estas claves Claves administradas por AWS, pero no pueden administrarlas en ningún aspecto. Todas las solicitudes realizadas con estas claves se registran como CloudTrail eventos.
- Claves propiedad de AWS— Estas claves se crean y utilizan exclusivamente AWS para operaciones de cifrado internas en diferentes AWS servicios. Los clientes no tienen visibilidad de las políticas clave ni Clave propiedad de AWS de su uso CloudTrail.

Alias

Un nombre fácil de utilizar que se encuentra asociado a una clave de KMS. El alias se puede usar indistintamente con el identificador clave en muchas de las operaciones de la AWS KMS API.

Permisos

Una política adjunta a una clave de KMS que define permisos en la clave. La política predeterminada permite utilizar cualquier entidad principal que usted defina, además de añadir políticas de IAM que hagan referencia Cuenta de AWS a la clave.

Concesiones

El permiso delegado para utilizar una clave de KMS cuando las entidades principales de IAM o la duración de uso previstas no se conocen desde el principio y, por lo tanto, no se pueden agregar a una clave o política de IAM. Uno de los usos de las concesiones es definir permisos restringidos sobre la forma en que un servicio puede usar una AWS clave de KMS. Es posible que el servicio necesite utilizar su clave para realizar un trabajo asincrónico en su nombre en datos cifrados en ausencia de una llamada a la API firmada de forma directa por usted.

Claves de datos

Claves criptográficas generadas en HSMs, protegidas por una clave KMS. AWS KMS permite a las entidades autorizadas obtener claves de datos protegidas por una clave KMS. Se pueden devolver como claves de datos de texto sin formato (sin cifrar) y como claves de datos cifradas.

Las claves de datos pueden ser simétricas o asimétricas (con las partes públicas y privadas devueltas).

Textos cifrados

La salida cifrada de AWS KMS, a veces denominada texto cifrado del cliente, para evitar confusiones. El texto cifrado contiene datos cifrados con información adicional que identifica la clave de KMS que se utilizará en el proceso de descifrado. Las claves de datos cifradas son un ejemplo común de texto cifrado producido cuando se utiliza una clave de KMS, pero cualquier dato de menos de 4 KB de tamaño se puede cifrar bajo una clave de KMS para producir un texto cifrado.

Contexto de cifrado

Un mapa de pares clave-valor de información adicional asociada a la información protegida. AWS KMS AWS KMS utiliza un cifrado autenticado para proteger las claves de datos. El contexto de cifrado se incorpora al AAD del cifrado autenticado en AWS KMS textos cifrados. Esta información de contexto es opcional y no se devuelve cuando se solicita una clave (o una operación de cifrado). Pero si se utiliza, este valor de contexto es necesario para completar una operación de descifrado con éxito. Un uso previsto del contexto de cifrado es proporcionar información autenticada adicional. Esta información puede ayudarle a hacer cumplir las políticas y a incluirse en los registros. AWS CloudTrail Por ejemplo, podría utilizar un par de valor de clave de {"key name":"satellite uplink key"} para nombrar la clave de datos. El uso posterior de la clave crea una AWS CloudTrail entrada que incluye el «nombre de la clave»: «clave de enlace ascendente del satélite». Esta información adicional puede proporcionar un contexto útil para comprender por qué se utilizó una clave de KMS determinada.

Clave pública

Cuando se utilizan cifrados asimétricos (RSA o curva elíptica), la clave pública es el “componente público” de un par de claves público-privado. La clave pública se puede compartir y distribuir a entidades que necesitan cifrar datos para el propietario del par de claves público-privado. Para las operaciones de firma digital, la clave pública se utiliza a fin de verificar la firma.

Clave privada

Cuando se utilizan cifrados asimétricos (RSA o curva elíptica), la clave privada es el “componente privado” de un par de claves público-privado. La clave privada se utiliza para descifrar los datos o crear firmas digitales. Al igual que las claves KMS simétricas, las claves privadas se cifran. HSMs Solo se descifran en la memoria a corto plazo del HSM y únicamente durante el tiempo necesario para procesar su solicitud criptográfica.

AWS KMS objetivos de diseño

AWS KMS está diseñado para cumplir los siguientes requisitos.

Durabilidad

La durabilidad de las claves criptográficas está diseñada para ser igual a la de los servicios de mayor durabilidad. AWS Una única clave criptográfica puede cifrar grandes volúmenes de datos acumulados durante mucho tiempo.

Confiabilidad

El uso de las claves está protegido por las políticas de control de acceso que usted define y administra. No existe ningún mecanismo para exportar claves de KMS de texto no cifrado. La confidencialidad de las claves criptográficas es crucial. Se requieren varios empleados de Amazon con acceso específico a los controles de acceso basados en quórums para realizar acciones administrativas en el. HSMs

Baja latencia y alto rendimiento

AWS KMS proporciona operaciones criptográficas con niveles de latencia y rendimiento adecuados para su uso en otros servicios en. AWS

Regiones independientes

AWS proporciona regiones independientes para los clientes que necesitan restringir el acceso a los datos en diferentes regiones. El uso de claves se puede aislar dentro de una Región de AWS.

Fuente segura de números aleatorios

Debido a que la criptografía rigurosa depende de la generación de números aleatorios verdaderamente impredecibles, AWS KMS proporciona una fuente de alta calidad y con validación de números aleatorios.

Auditoría

AWS KMS registra el uso y la administración de las claves criptográficas en AWS CloudTrail los registros. Puede utilizar AWS CloudTrail los registros para inspeccionar el uso de sus claves criptográficas, incluido el uso de las claves por parte de los AWS servicios que actúan en su nombre.

Para lograr estos objetivos, el AWS KMS sistema incluye un conjunto de AWS KMS operadores y operadores de hospedaje de servicios (denominados colectivamente «operadores») que administran

los «dominios». Un dominio es un conjunto de AWS KMS servidores y operadores definido regionalmente. HSMs Cada AWS KMS operador tiene un token de hardware que contiene un key pair de claves pública y privada que se utiliza para autenticar sus acciones. HSMsTienen un par de claves públicas y privadas adicionales para establecer claves de cifrado que protegen la sincronización de estados del HSM.

Este paper ilustra cómo AWS KMS protege sus claves y otros datos que desee cifrar. A lo largo de este documento, las claves de cifrado o los datos que desea cifrar se denominan “secretos” o “material secreto”.

AWS Key Management Service fundaciones

Los temas de este capítulo describen las primitivas criptográficas AWS Key Management Service y dónde se utilizan. También presentan los elementos básicos de. AWS KMS

Temas

Primitivas criptográficas

AWS KMS utiliza algoritmos criptográficos configurables para que el sistema pueda migrar rápidamente de un algoritmo o modo aprobado a otro. El conjunto inicial predeterminado de algoritmos criptográficos se ha seleccionado de algoritmos de los Estándares Federales de Procesamiento de la Información (aprobado por FIPS) para sus propiedades de seguridad y rendimiento.

Entropía y generación de números aleatorios

AWS KMS la generación de claves se realiza en. AWS KMS HSMs HSMs Implemente un generador híbrido de números aleatorios que utilice el NIST SP800-90A Deterministic Random Bit Generator (DRBG) CTR_DRBG using AES-256. Se encuentra sincronizado con un generador de bits aleatorio no determinista con 384 bits de entropía y actualizado con entropía adicional para proporcionar resistencia a la predicción en cada llamada de material criptográfico.

Operaciones de clave simétrica (solo cifrado)

Todos los comandos de cifrado con clave simétrica que se utilizan utilizan estándares de cifrado avanzados (AES) y, en el modo contador de Galois (GCM), utilizan claves de 256 bits. HSMs Las llamadas análogas para descifrar utilizan la función inversa.

AES-GCM es un esquema de cifrado autenticado. Además de cifrar texto sin formato a fin de producir texto cifrado, calcula una etiqueta de autenticación sobre el texto cifrado y los datos adicionales para los que se requiere autenticación (datos autenticados adicionales o AAD). La etiqueta de autenticación ayuda a garantizar que los datos provengan de la supuesta fuente y que el texto cifrado y los AAD no se hayan modificado.

Con frecuencia, AWS omite la inclusión del AAD en nuestras descripciones, especialmente cuando se refiere al cifrado de claves de datos. En estos casos, el texto circundante implica que la estructura que se cifrará se divide entre el texto sin formato que se cifrará y los AAD de texto sin cifrar que se protegerán.

AWS KMS ofrece una opción para importar el material clave a un, en AWS KMS key lugar de confiar en él AWS KMS para generar el material clave. Este material clave importado se puede cifrar mediante RSAES-OAEP o RSAES - PKCS1 -v1_5 para proteger la clave durante su transporte al HSM. AWS KMS Los AWS KMS HSMs pares de claves RSA se generan el. El material clave importado se descifra en un AWS KMS HSM y se vuelve a cifrar con el AES-GCM antes de que el servicio lo almacene.

Operaciones de clave asimétrica (cifrado, firma digital y verificación de firmas)

AWS KMS admite el uso de operaciones de clave asimétricas tanto para las operaciones de cifrado como para las de firma digital. Las operaciones de clave asimétrica se basan en un par de claves privadas y públicas relacionadas de forma matemática que puede utilizar para el cifrado y descifrado o la firma y verificación de la firma, pero no ambos. La clave privada nunca sale AWS KMS sin cifrar. Puedes usar la clave pública interna AWS KMS llamando a las operaciones de la AWS KMS API, o bien descargar la clave pública y usarla fuera de AWS KMS ella.

AWS KMS admite tres tipos de cifrados asimétricos.

- RSA-OAEP (para el cifrado) y RSA-PSS y RSA-PKCS-#1-v1_5 (para la firma y verificación): es compatible con longitudes de clave de RSA (en bits): 2048, 3072 y 4096 para diferentes requisitos de seguridad.
- Curva elíptica (ECC): se utiliza de forma exclusiva para la firma y la verificación. Es compatible con curvas ECC: NIST P256, P384, P521, SECP 256k1.
- Criptografía poscuántica: nuevos algoritmos criptográficos de clave pública resistentes a la computación cuántica. Es compatible con el algoritmo de firma digital de celosía modular FIPS 204 (ML-DSA) del NIST con los tamaños de clave ML_DSA_44, ML_DSA_65 y ML_DSA_87.

Funciones de derivación de claves

Una función de derivación de claves se utiliza para derivar claves adicionales de una clave o secreto inicial. AWS KMS utiliza una función de derivación de claves (KDF) a fin de derivar claves por

llamada para cada cifrado bajo una AWS KMS key. Todas las operaciones del KDF utilizan el KDF en modo contador mediante SHA256 FIPS180HMAC [] FIPS197con []. La clave derivada de 256 bits se utiliza con AES-GCM para cifrar o descifrar datos y claves del cliente.

AWS KMS uso interno de firmas digitales

Las firmas digitales también se utilizan para autenticar comandos y comunicaciones entre entidades de AWS KMS . Todas las entidades de servicio tienen un par de claves de algoritmo de firma digital de curva elíptica (ECDSA). Emplean ECDSA como se define en el Uso de algoritmos de criptografía de curva elíptica (ECC) en la sintaxis de mensajes criptográficos (CMS) y X9.62-2005: Criptografía de clave pública para el sector de servicios financieros: el Algoritmo de firma digital de curva elíptica (ECDSA). Las entidades utilizan el algoritmo de hash seguro definido en las publicaciones sobre normas federales de procesamiento de la información, FIPS PUB 180-4, conocido como. SHA384 Las claves se generan en la curva secp384r1 (NIST-P384).

Cifrado doble

Una construcción básica utilizada en muchos sistemas criptográficos es el cifrado doble. El cifrado doble utiliza dos o más claves criptográficas para proteger un mensaje. Por lo general, una clave se deriva de una clave estática K de plazo más largo y otra clave es una clave por mensaje, msgKey, que se genera para cifrar el mensaje. El doble cifrado se forma al cifrar el mensaje: ciphertext = Encrypt(msgKey, message). A continuación, la clave del mensaje se cifra con la clave estática a largo plazo: encKey = Encrypt(k, msgKey). Por último, los dos valores (encKey, ciphertext) se empaquetan en una sola estructura, o mensaje con cifrado doble.

El destinatario, con acceso a la K, puede abrir el mensaje con doble cifrado al descifrar primero la clave cifrada y, a continuación, al descifrar el mensaje.

AWS KMS ofrece la posibilidad de gestionar estas claves estáticas a largo plazo y automatizar el proceso de cifrado de sobres de sus datos.

Además de las funciones de cifrado incluidas en el AWS KMS servicio, el SDK de cifrado proporciona bibliotecas de AWS cifrado de sobres para el lado del cliente. Puede utilizar estas bibliotecas para proteger sus datos y las claves de cifrado que se utilizan a fin de cifrar esos datos.

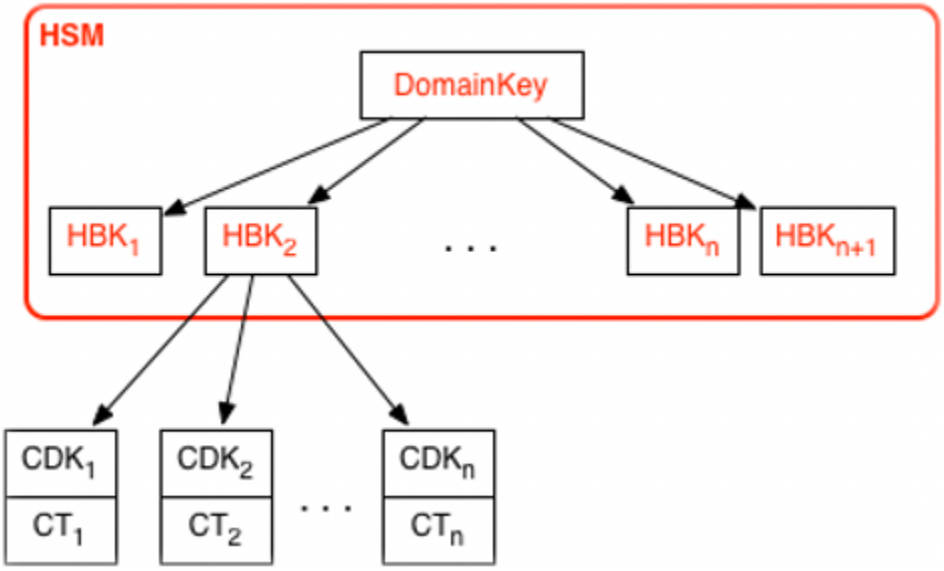
AWS KMS key jerarquía

La jerarquía de claves comienza con una clave lógica de nivel superior, una. AWS KMS key Una clave de KMS representa un contenedor para material clave de nivel superior y está definida de

forma única dentro del espacio de nombres del servicio de AWS con un nombre de recurso de Amazon (ARN). El ARN incluye un identificador de clave generado de forma única, un ID de clave. Se crea una clave KMS en función de una solicitud iniciada por el usuario mediante. AWS KMS Al recibirla, AWS KMS solicita la creación de una clave de respaldo HSM (HBK) inicial para colocarla en el contenedor de claves KMS. La HBK se genera en un HSM en el dominio y está diseñada para no exportarse nunca del HSM en texto sin formato. En su lugar, la HBK se exporta cifrada con claves de dominio administradas por HSM. Estos elementos exportados se HBKs denominan claves exportadas (EKTs).

El EKT se exporta a un almacenamiento de larga duración y de baja latencia. Por ejemplo, supongamos que recibe un ARN para la clave de KMS lógica. Esto representa la parte superior de una jerarquía de claves, o contexto criptográfico. Puede crear varias claves de KMS en su cuenta y establecer políticas en sus claves de KMS como cualquier otro recurso con AWS nombre.

Dentro de la jerarquía de una clave de KMS específica, la HBK puede considerarse como una versión de la clave de KMS. Cuando desee rotar la clave KMS AWS KMS, se creará un nuevo HBK que se asociará a la clave KMS como el HBK activo de la clave KMS. HBKs Las más antiguas se conservan y se pueden utilizar para descifrar y verificar datos previamente protegidos. Pero solo se puede usar la clave criptográfica activa para proteger nueva información.



Puede realizar solicitudes AWS KMS para usar sus claves de KMS para proteger directamente la información o solicitar claves adicionales generadas por HSM que estén protegidas por su clave de KMS. Estas claves se denominan claves de datos del cliente o. CDKs CDKs se pueden devolver cifradas como texto cifrado (CT), en texto plano o en ambos. Todos los objetos cifrados con una

clave KMS (ya sean datos proporcionados por el cliente o claves generadas por HSM) solo se pueden descifrar en un HSM mediante una llamada directa. AWS KMS

El texto cifrado devuelto, o la carga útil descifrada, nunca se almacena en él. AWS KMS La información se le devuelve a través de su conexión TLS a AWS KMS. Esto también se aplica a las llamadas realizadas por los AWS servicios en su nombre.

La jerarquía de claves y las propiedades de clave específicas aparecen en la siguiente tabla.

Clave	Descripción	Ciclo de vida
Clave de dominio	Una clave AES-GCM de 256 bits solo en memoria de un HSM que se utiliza para ajustar versiones de las claves de KMS, las claves de backup de HSM.	Rotación diaria[1]
Clave de respaldo de HSM	Una clave simétrica de 256 bits, clave privada RSA o curva elíptica que se utiliza para proteger los datos y las claves del cliente y que se almacena de forma cifrada con claves de dominio. Una o más claves de backup de HSM comprenden la clave de KMS, representada por el keyId.	Rotación anual[2] (config. opcional)
Clave de cifrado derivada	Una clave AES-GCM de 256 bits solo en memoria de un HSM que se utiliza para cifrar datos y claves del cliente. Se deriva de una HBK para cada cifrado.	Se utiliza una vez por cifrado y se regenera al descifrarse.
Clave de datos del cliente	Clave simétrica o asimétrica delimitada por el usuario que se exporta desde un HSM en texto sin formato y texto cifrado.	Rotación y uso controlado por aplicación

Clave	Descripción	Ciclo de vida
	Se cifra con una clave de backup de HSM y se devuelve a los usuarios autorizados a través del canal TLS.	

De vez en cuando, AWS KMS podría reducir la rotación de claves de dominio a, como máximo, una vez por semana para tener en cuenta las tareas de administración y configuración del dominio.

[2] Por defecto, las que Claves administradas por AWS se crean y gestionan AWS KMS en tu nombre se rotan automáticamente una vez al año.

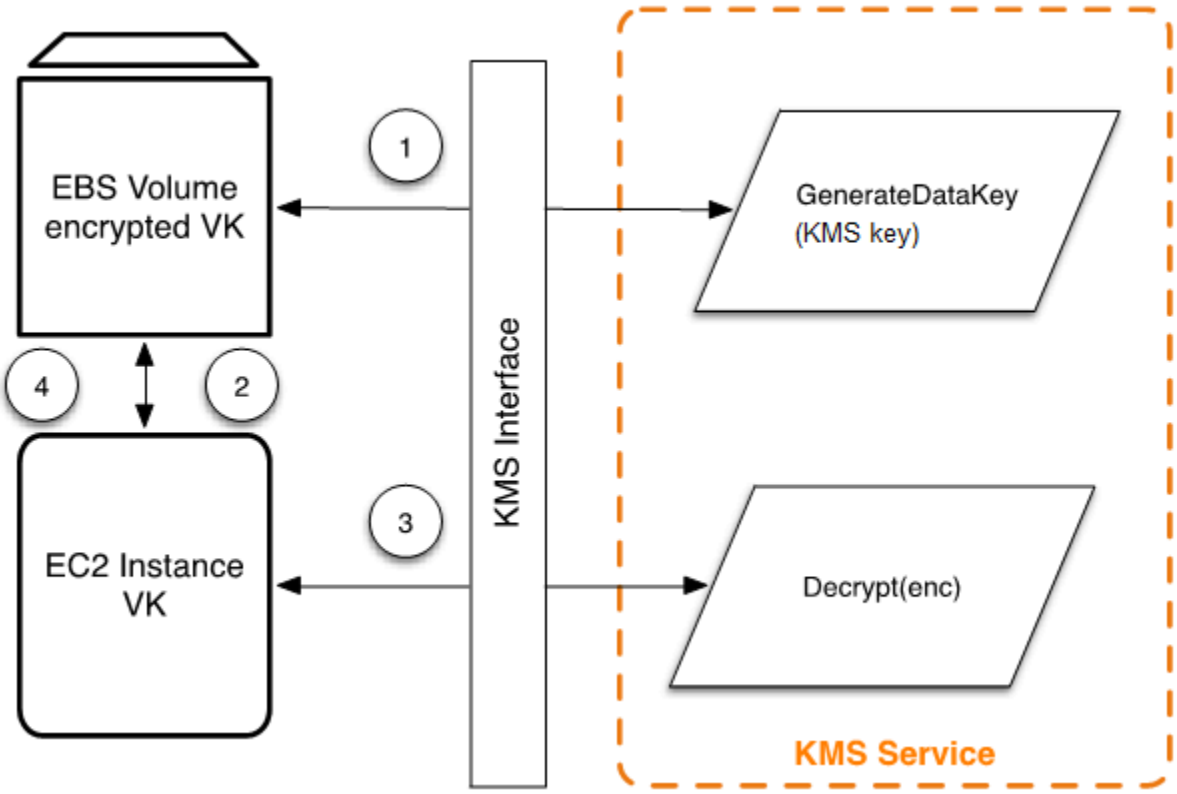
AWS KMS casos de uso

Los casos de uso pueden ayudarle a sacarle el máximo partido. AWS Key Management Service La primera muestra cómo se AWS KMS realiza el cifrado del lado del servidor AWS KMS keys en un volumen de Amazon Elastic Block Store (Amazon EBS). La segunda es una aplicación del lado del cliente que demuestra cómo se puede utilizar el cifrado de sobres para proteger el contenido. AWS KMS

Temas

Cifrado de volumen de Amazon EBS

Amazon EBS ofrece capacidad de cifrado de volumen. Cada volumen se cifra con claves AES-256-XTS. Esto requiere dos claves de volumen de 256 bits, lo que se puede considerar como una clave de volumen de 512 bits. La clave de volumen se cifra con una clave de KMS en su cuenta. Para que Amazon EBS pueda cifrar un volumen en su nombre, debe tener acceso a fin de generar una clave de volumen (VK) con una clave de KMS de la cuenta. Para ello, se debe proporcionar una concesión para Amazon EBS a la clave de KMS con el fin de crear claves de datos y cifrar y descifrar estas claves de volumen. Ahora Amazon EBS utiliza una clave AWS KMS de KMS para generar claves de volumen AWS KMS cifradas.



El siguiente flujo de trabajo cifra los datos que se están escribiendo en un volumen de Amazon EBS:

1. Amazon EBS obtiene una clave de volumen cifrada en una clave de KMS a AWS KMS través de una sesión de TLS y almacena la clave cifrada con los metadatos del volumen.
2. Cuando se monta el volumen de Amazon EBS, se recupera la clave de volumen cifrada.
3. Se realiza una llamada a AWS KMS través de TLS para descifrar la clave de volumen cifrada. AWS KMS identifica la clave KMS y realiza una solicitud interna a un HSM de la flota para descifrar la clave de volumen cifrada. AWS KMS a continuación, devuelve la clave de volumen al host de Amazon Elastic Compute Cloud (Amazon EC2) que contiene la instancia durante la sesión de TLS.
4. La clave de volumen se utiliza para cifrar y descifrar todos los datos que se envían a los volúmenes de Amazon EBS adjuntos y se reciben de ellos. Amazon EBS conserva la clave de volumen cifrada para su uso posterior en caso de que la clave de volumen en la memoria ya no esté disponible.

Para obtener más información sobre el cifrado de volúmenes de Amazon EBS con claves de KMS, consulte Cómo se usa Amazon Elastic Block Store AWS KMS en la Guía para AWS Key

Management Service desarrolladores y el cifrado de Amazon EBS en la Guía del usuario de Amazon y la Guía del EC2 usuario de Amazon EC2 .

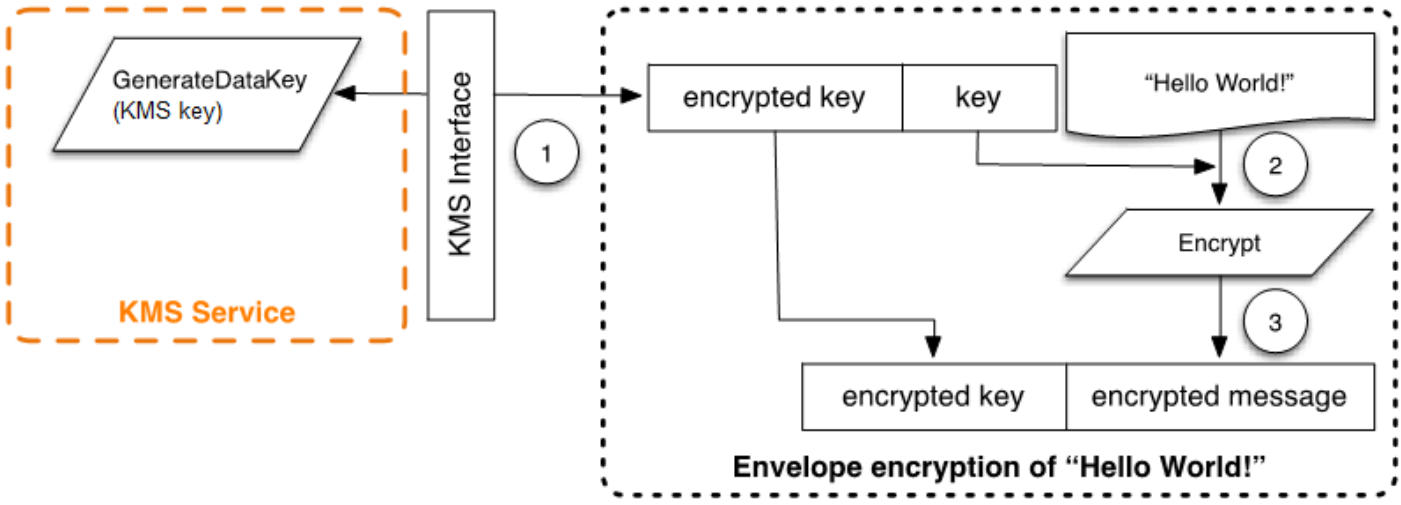
Cifrado del cliente

El AWS Encryption SDK incluye una operación de API para realizar el cifrado doble con una clave de KMS. Para obtener recomendaciones completas y detalles de uso, consulte la documentación relacionada. Las aplicaciones cliente pueden utilizarla para realizar el cifrado AWS Encryption SDK de sobres mediante. AWS KMS

```
// Instantiate the SDK
final AwsCrypto crypto = new AwsCrypto();
// Set up the KmsMasterKeyProvider backed by the default credentials
final KmsMasterKeyProvider prov = new KmsMasterKeyProvider(keyId);
// Do the encryption
final byte[] ciphertext = crypto.encryptData(prov, message);
```

La aplicación cliente puede ejecutar los siguientes pasos:

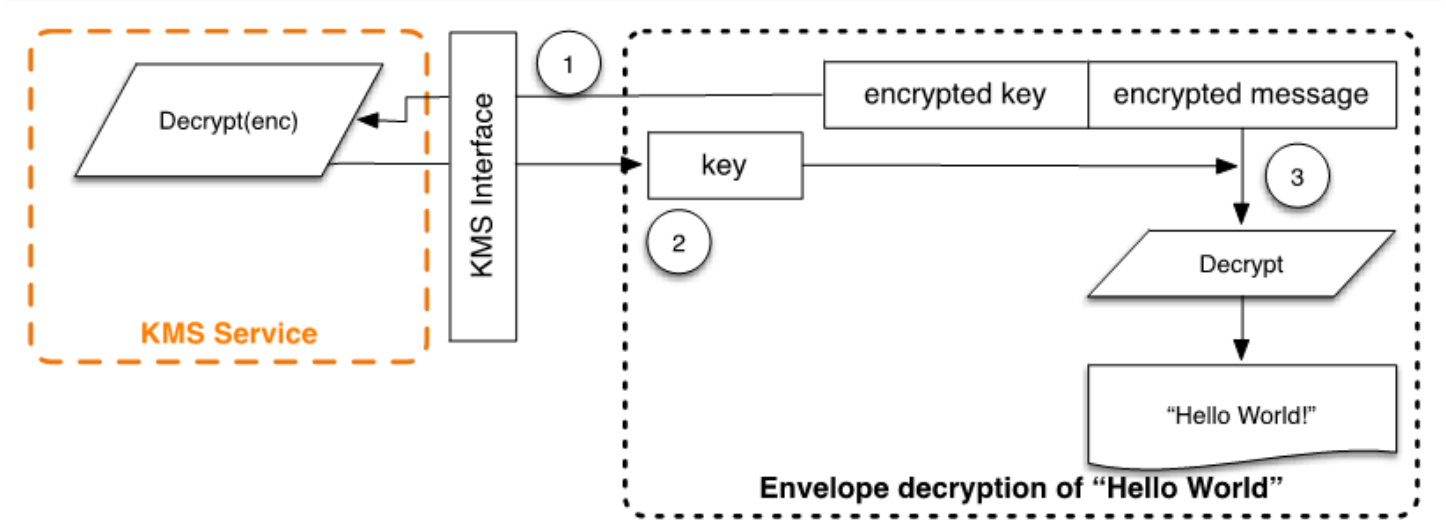
1. Se realiza una solicitud con una clave de KMS para obtener una nueva clave de datos. Se devuelve una clave de datos cifrada y una versión de texto sin formato de esta.
2. Dentro de AWS Encryption SDK, la clave de datos de texto plano se utiliza para cifrar el mensaje. A continuación, la clave de datos en texto sin formato se elimina de la memoria.
3. La clave de datos cifrada y el mensaje cifrado se combinan en una única matriz de bytes de texto cifrado.



El mensaje con cifrado doble se puede descifrar mediante la funcionalidad de descifrado para obtener el mensaje que se cifró originalmente.

```
final AwsCrypto crypto = new AwsCrypto();
final KmsMasterKeyProvider prov = new KmsMasterKeyProvider(keyId);
// Decrypt the data
final CryptoResult<byte[], KmsMasterKey> res = crypto.decryptData(prov, ciphertext);
// We need to check the KMS key to ensure that the
// assumed key was used
if (!res.getMasterKeyIds().get(0).equals(keyId)) {
     throw new IllegalStateException("Wrong key id!");
}
byte[] plaintext = res.getResult();
```

1. AWS Encryption SDK Analiza el mensaje cifrado en el sobre para obtener la clave de datos cifrada y realizar una solicitud para AWS KMS descifrarla.
2. AWS Encryption SDK Recibe la clave de datos en texto plano de. AWS KMS
3. La clave de datos se utiliza para descifrar el mensaje, lo que devuelve el texto sin formato inicial.

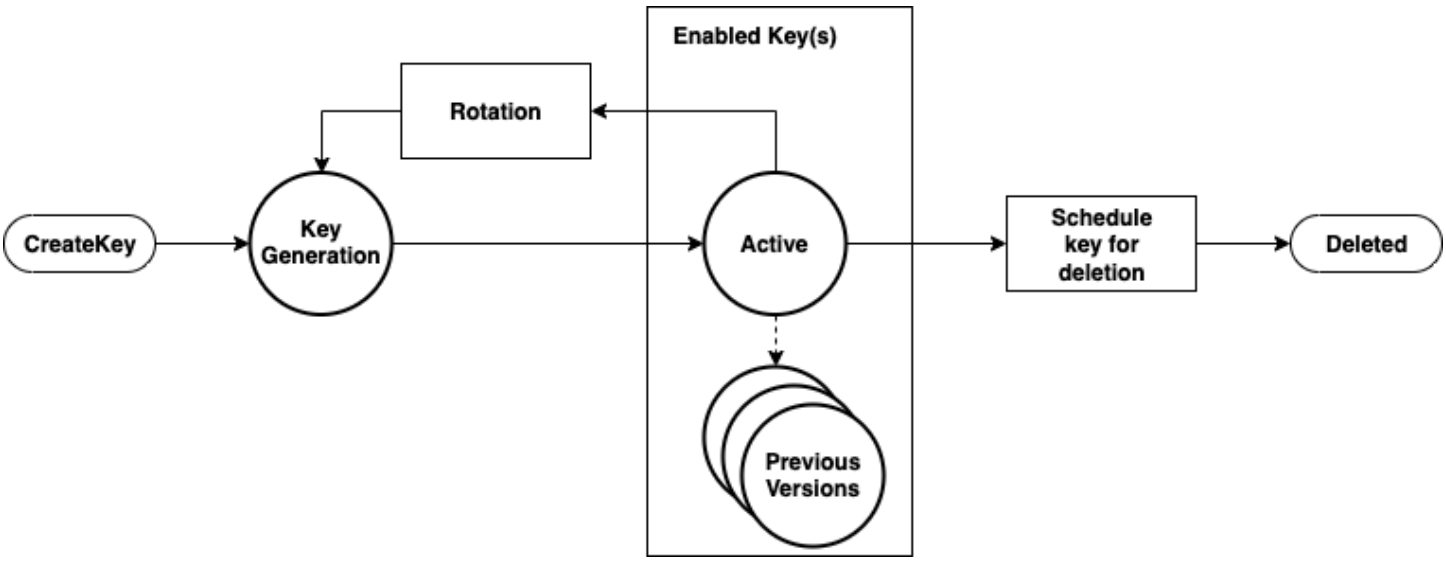


Trabajando con AWS KMS keys

Una AWS KMS key hace referencia a una clave lógica que puede hacer referencia a una o más claves de respaldo del módulo de seguridad de hardware (HSM) (HBKs). En este tema se explica cómo crear una clave de KMS, importar material de claves, y cómo habilitar, deshabilitar, rotar y eliminar claves de KMS.

> **Note**
>
> AWS KMS está sustituyendo el término clave maestra del cliente (CMK) por clave KMS. AWS KMS key El concepto no ha cambiado. Para evitar cambios importantes, AWS KMS mantiene algunas variaciones de este término.

En este capítulo se trata el ciclo de vida de una clave KMS desde su creación hasta su eliminación, como se muestra en la siguiente imagen.



Temas

- ¿Llamando CreateKey
- Importar material de claves
- Habilitación y desactivación de claves de
- Eliminación de claves de
- Rotar el material de claves

¿Llamando CreateKey

AWS KMS key Se genera una como resultado de una llamada a la `CreateKey`API.

A continuación se presenta un subconjunto de la sintaxis de la solicitud de `CreateKey`.

```
{
  "Description": "string",
  "KeySpec": "string",
  "KeyUsage": "string",
  "Origin": "string";
  "Policy": "string"
}
```

La solicitud acepta los siguientes datos en formato JSON.

Description (Descripción)

(Opcional) Descripción de la clave. Recomendamos elegir una descripción que permita decidir si la clave es adecuada para una tarea.

KeySpec

Especifica el tipo de KMS que se va a crear. El valor predeterminado, SYMMETRIC_DEFAULT, crea claves KMS de cifrado simétricas. Este parámetro es opcional para las claves de cifrado simétricas y obligatorio para todas las demás especificaciones de claves.

KeyUsage

Especifica el uso de las claves. Los valores válidos son `ENCRYPT_DECRYPT`, `SIGN_VERIFY` o `GENERATE_VERIFY_MAC`. El valor predeterminado es `ENCRYPT_DECRYPT`. Este parámetro es opcional para las claves de cifrado simétricas y obligatorio para todas las demás especificaciones de claves.

Origen

(Opcional) Especifica el origen del material de claves para la clave de KMS. El valor predeterminado es`AWS_KMS`, lo que indica que AWS KMS genera y administra el material clave de la clave KMS. Otros valores válidos son: `EXTERNAL` el que representa una clave de KMS creada sin material de claves para el material de claves importado y el `AWS_CLOUDHSM` que crea una clave de KMS en un almacén de claves personalizado respaldado por un AWS CloudHSM clúster que usted controla.

Política

(Opcional) Política para adjuntar a la clave. Si se omite la política, la clave se crea con la política predeterminada (siguiente) que permite a la cuenta raíz y a las entidades principales de IAM con permisos de AWS KMS administrarla.

Para obtener información detallada sobre la política, consulte Políticas de claves en AWS KMS y Política de claves predeterminada en la Guía para desarrolladores de AWS Key Management Service .

La solicitud de `CreateKey` devuelve una respuesta que incluye un ARN de claves.

```
arn:<partition>:kms:<region>:<account-id>:key/<key-id>
```

Si el `Origin` es `AWS_KMS`, después de crear el ARN, se realiza una solicitud a un HSM de AWS KMS a través de una sesión autenticada para aprovisionar una clave de respaldo (HBK) del módulo de seguridad de hardware (HSM). La HBK es una clave de 256 bits que se encuentra asociada a este ID de clave de la clave de KMS. Solo se puede generar en un HSM y se ha diseñado para no exportarse nunca fuera del límite de HSM en texto sin cifrar. La HBK se cifra en la clave de dominio actual, DK_0. Estos cifrados se HBKs denominan identificadores de clave cifrados (EKTs). Si bien se HSMs pueden configurar para utilizar diversos métodos de empaquetado de claves, la implementación actual utiliza el AES-256 en el modo contador de Galois (GCM), un esquema de cifrado autenticado. Este modo de cifrado autenticado permite proteger metadatos de token de clave exportados de texto sin cifrar.

Estilísticamente, esto se representa como:

```
EKT = Encrypt(DK₀, HBK)
```

Se proporcionan dos formas fundamentales de protección a las claves de KMS y a las siguientes HBKs: las políticas de autorización establecidas en las claves de KMS y las protecciones criptográficas de las claves asociadas. HBKs En las secciones restantes se describen las protecciones criptográficas y la seguridad de las funciones de administración incluidas. AWS KMS

Además del ARN, puede crear un nombre fácil de utilizar y asociarlo con la clave de KMS mediante la creación de un alias para la clave. Una vez asociado un alias a una clave de KMS, se puede utilizar el alias para identificar la clave de KMS en las operaciones de cifrado. Para más información detallada, consulte Uso de alias en la Guía para desarrolladores de AWS Key Management Service .

El uso de claves KMS está relacionado con varios niveles de autorización. AWS KMS permite políticas de autorización independientes entre el contenido cifrado y la clave KMS. Por ejemplo, un objeto de Amazon Simple Storage Service (Amazon S3) con cifrado doble de AWS KMS hereda la política del bucket de Amazon S3. Sin embargo, la política de acceso de la clave de KMS determina el acceso a la clave de cifrado necesaria. Para obtener más información acerca de la autorización de claves de KMS, consulte Autenticación y control de acceso de AWS KMS en la Guía para desarrolladores de AWS Key Management Service .

Importar material de claves

AWS KMS proporciona un mecanismo para importar el material criptográfico utilizado en un HBK. Como se describe en¿Llamando CreateKey, cuando el CreateKey comando se utiliza con el valor `Origin` establecido en`EXTERNAL`, se crea una clave KMS lógica que no contiene ningún HBK subyacente. El material criptográfico debe importarse mediante la llamada a la API `ImportKeyMaterial`. Puede utilizar esta característica para controlar la creación de claves y la durabilidad del material criptográfico. Si utiliza esta característica, recomendamos que tenga cuidado con la manipulación y durabilidad de estas claves en su entorno. Para obtener detalles completos y recomendaciones sobre la importación de material de claves, consulte Importar material de claves en la Guía para desarrolladores de AWS Key Management Service .

¿Llamando ImportKeyMaterial

La solicitud `ImportKeyMaterial` importa el material criptográfico necesario para la HBK. El material criptográfico debe ser una clave simétrica de 256 bits. Debe cifrarse con el algoritmo especificado en `WrappingAlgorithm` bajo la clave pública devuelta de una solicitud `GetParametersForImport` reciente.

Una solicitud de `ImportKeyMaterial` adopta los siguientes argumentos.

```
{
  "EncryptedKeyMaterial": blob,
  "ExpirationModel": "string",
  "ImportToken": blob,
  "KeyId": "string",
  "ValidTo": number
}
```

EncryptedKeyMaterial

El material de claves cifradas importado con la clave pública devuelta en una solicitud de `GetParametersForImport` mediante el algoritmo de encapsulamiento especificado en esa solicitud.

ExpirationModel

Especifica si vence el material de claves. Cuando este valor es `KEY_MATERIAL_EXPIRES`, el parámetro `ValidTo` debe contener una fecha de vencimiento. Cuando este valor es `KEY_MATERIAL_DOES_NOT_EXPIRE`, no incluya el parámetro `ValidTo`. Los valores válidos son `"KEY_MATERIAL_EXPIRES"` y `"KEY_MATERIAL_DOES_NOT_EXPIRE"`.

ImportToken

El token de importación devuelto por la misma solicitud de `GetParametersForImport`que proporcionó la clave pública.

KeyId

La clave de KMS que se asociará al material de claves importado. El `Origin` de la clave de KMS debe ser `EXTERNAL`.

Puede eliminar y volver a importar el mismo material de claves importado en la clave de KMS especificada, pero no puede importar ni asociar la clave de KMS a ningún otro material de claves.

ValidTo

(Opcional) La hora a la que vence el material de claves importado. Cuando vence el material de claves, AWS KMS lo elimina y la clave de KMS ya no se puede utilizar. Este parámetro es obligatorio cuando el valor de `ExpirationModel` es `KEY_MATERIAL_EXPIRES`. Caso contrario, es inválido.

Cuando la solicitud se realiza correctamente, la clave KMS está disponible para su uso AWS KMS hasta la fecha de caducidad especificada, si se proporciona alguna. Cuando el material clave importado caduca, el EKT se elimina de la capa de AWS KMS almacenamiento.

Habilitación y desactivación de claves de

Desactivar una clave de KMS impide que se la utilice en operaciones criptográficas. Suspende la capacidad de usar todo lo HBKs que esté asociado a la clave KMS. Al habilitar, se restaura el uso de

la clave KMS HBKs y de la clave KMS. Habilitar y deshabilitar son solicitudes simples que solo toman el ID de clave o el ARN de clave de la clave de KMS.

Eliminación de claves de

Los usuarios autorizados pueden usar la `ScheduleKeyDeletion`API para programar la eliminación de una clave de KMS y de todas las claves asociadas HBKs. Se trata de una operación intrínsecamente destructiva, por lo que debe tener cuidado al eliminar claves de AWS KMS ella. AWS KMS impone un tiempo de espera mínimo de siete días al eliminar las claves de KMS. Durante el periodo de espera, la clave se coloca en el estado deshabilitado con un estado de clave de Eliminación pendiente. Se producirán errores en todas las llamadas para utilizar la clave en operaciones criptográficas. ScheduleKeyDeletion toma los siguientes argumentos.

```
{
  "KeyId": "string",
  "PendingWindowInDays": number
}
```

KeyId

El identificador único de la clave de KMS a eliminar. Para especificar este valor, utilice el ID de clave único o el ARN de clave de la clave de KMS.

PendingWindowInDays

(Opcional) El periodo de espera, en número de días. Este valor es opcional. El intervalo es de 7 a 30 días y el valor predeterminado es de 30 días. Una vez finalizado el período de espera, AWS KMS elimina la clave KMS y todas las claves asociadas HBKs.

Rotar el material de claves

Los usuarios autorizados pueden habilitar la rotación anual automática de las claves de KMS administradas por el cliente. Las Claves administradas por AWS siempre rotan anualmente.

Cuando se rota una clave de KMS, se crea una HBK nueva y se marca como la versión actual del material de claves para todas las solicitudes nuevas de cifrado. Todas las versiones anteriores de HBK permanecen disponibles para su uso a perpetuidad para descifrar cualquier texto cifrado que se haya cifrado con esta versión de HBK. Como AWS KMS no almacena ningún texto cifrado con una clave KMS, los textos cifrados con un HBK antiguo y rotado requieren que HBK lo descifre. Puede

utilizar la API de `ReEncrypt` para volver a cifrar cualquier texto cifrado con la nueva HBK para la clave de KMS o con una clave de KMS diferente sin exponer el texto sin formato.

Para obtener información acerca de habilitar y deshabilitar la rotación de claves, consulte Rotación de claves de AWS KMS en la Guía para desarrolladores de AWS Key Management Service .

Operaciones de datos de clientes

Después de establecer una clave de KMS, se puede utilizar para llevar a cabo operaciones criptográficas. Siempre que los datos se cifran bajo una clave de KMS, el objeto resultante es un texto cifrado del cliente. El texto cifrado contiene dos secciones: una parte de encabezado no cifrado (o texto sin cifrar), protegida por el esquema de cifrado autenticado como datos autenticados adicionales, y una parte cifrada. La parte de texto sin cifrar incluye el identificador de HBK (HBKID). Estos dos campos inmutables del valor del texto cifrado ayudan a garantizar que se AWS KMS pueda descifrar el objeto en el futuro.

Temas

Generar claves de datos

Los usuarios autorizados pueden usar la GenerateDataKey API (y otras relacionadas APIs) para solicitar un tipo específico de clave de datos o una clave aleatoria de longitud arbitraria. En este tema se proporciona una vista simplificada de esta operación de API. Para obtener más información, consulta GenerateDataKey APIs la referencia de la AWS Key Management Service API.

- GenerateDataKey
- GenerateDataKeyWithoutPlaintext
- GenerateDataKeyPair
- GenerateDataKeyPairWithoutPlaintext

A continuación se presenta la sintaxis de la solicitud `GenerateDataKey`.

```
{
 “EncryptionContext”: {“string” : “string”},
 “GrantTokens”: [“string”],
 “KeyId”: “string”,
 “NumberOfBytes”: “number”
```

```
}
```

La solicitud acepta los siguientes datos en formato JSON.

KeyId

Identificador de clave de la clave utilizada para cifrar la clave de datos. Este valor debe identificar una clave KMS de cifrado simétrica.

Este parámetro es obligatorio.

NumberOfBytes

Un número entero que contiene el número de bytes que se generará. Este parámetro es obligatorio.

La persona que llama debe proporcionar `KeySpec` o `NumberOfBytes`, pero no ambos.

EncryptionContext

(Opcional) Par de nombre-valor que contiene datos adicionales para autenticarse durante los procesos de cifrado y descifrado que utilizan la clave.

GrantTokens

(Opcional) Una lista de tokens de concesión que representan concesiones que proporcionan permisos para generar o utilizar una clave. Para obtener más información sobre las concesiones y los tokens de concesión, consulte Autenticación y control de acceso de AWS KMS en la Guía para desarrolladores de AWS Key Management Service .

Tras autenticar el comando AWS KMS, adquiere el EKT activo actual asociado a la clave KMS. Transfiere el EKT junto con la solicitud proporcionada y cualquier contexto de cifrado a un HSM a través de una sesión protegida entre el AWS KMS host y un HSM del dominio.

El HSM realiza lo siguiente:

1. Genera el material secreto solicitado y lo mantiene en la memoria volátil.
2. Descifra el EKT que coincide con el ID de clave de la clave de KMS que se define en la solicitud para obtener el HBK = Decrypt(DK_i, EKT) activo.
3. Genera un nonce N aleatorio.
4. Genera una clave de cifrado K derivada de AES-GCM de 256 bits desde HBK y N.
5. Cifra el material secreto ciphertext = Encrypt(K, context, secret).

`GenerateDataKeyle` devuelve el texto simple del material secreto y el texto cifrado a través del canal seguro entre el anfitrión y el HSM. AWS KMS AWS KMS a continuación, se lo envía a través de la sesión TLS. AWS KMS no conserva el texto sin formato ni el texto cifrado. Sin tener el texto cifrado, el contexto de cifrado y la autorización para utilizar la clave de KMS, no se puede devolver el secreto subyacente.

A continuación, se muestra la sintaxis de respuesta.

```
{
 "CiphertextBlob": "blob",
 "KeyId": "string",
 "Plaintext": "blob"
}
```

La gestión de claves de datos queda a su cargo como desarrollador de aplicaciones. Para obtener las mejores prácticas de cifrado del lado del cliente con claves de AWS KMS datos (pero no pares de claves de datos), puede utilizar el. AWS Encryption SDK

Las claves de datos se pueden rotar a cualquier frecuencia. Además, la clave de datos se puede volver a cifrar en una clave de KMS diferente o en una clave de KMS rotada mediante la operación de API `ReEncrypt`. Para obtener más información, consulte la ReEncryptreferencia de la AWS Key Management Service API.

Encrypt

Una función básica de AWS KMS es cifrar un objeto con una clave KMS. Por diseño, AWS KMS proporciona operaciones criptográficas de baja latencia en. HSMs Por lo tanto, hay un límite de 4 KB en la cantidad de texto sin formato que se puede cifrar en una llamada directa a la función de cifrado. Se AWS Encryption SDK puede usar para cifrar mensajes más grandes. AWS KMS, tras autenticar el comando, adquiere el EKT activo actual correspondiente a la clave KMS. Pasa el EKT junto con el texto sin formato y el contexto de cifrado a cualquier HSM disponible en la región. Se envían a través de una sesión autenticada entre el AWS KMS host y un HSM del dominio.

El HSM ejecuta lo siguiente:

1. Descifra el EKT para obtener la HBK = Decrypt(DK_i, EKT) .
2. Genera un nonce N aleatorio.
3. Obtiene una clave de cifrado derivada K de AES-GCM de 256 bits desde HBK y N.

4. Cifra el texto sin formato ciphertext = Encrypt(K, context, plaintext).

Se le devuelve el valor del texto cifrado y ni los datos en texto simple ni el texto cifrado se conservan en ninguna parte de la infraestructura. AWS Sin tener el texto cifrado, el contexto de cifrado y la autorización para utilizar la clave de KMS, no se puede devolver el texto sin formato subyacente.

Decrypt

Una llamada AWS KMS a para descifrar un valor de texto cifrado acepta un texto cifrado con un valor cifrado y un contexto de cifrado. AWS KMS autentica la llamada mediante solicitudes firmadas con la versión 4 de la AWS firma y extrae del texto cifrado el HBKID de la clave de empaquetado. El HBKID se utiliza para obtener el EKT necesario a fin de descifrar el texto cifrado, el ID de clave y la política del ID de clave. La solicitud se autoriza en función de la política de clave, las concesiones que puedan encontrarse presentes y las políticas de IAM asociadas que hagan referencia al ID de clave. La función `Decrypt` es análoga a la función de cifrado.

A continuación se presenta la sintaxis de la solicitud `Decrypt`.

```
{
 "CiphertextBlob": "blob",
 "EncryptionContext": { "string" : "string" }
 "GrantTokens": ["string"]
}
```

A continuación se presentan los parámetros de solicitud.

CiphertextBlob

Texto cifrado, incluido metadatos.

EncryptionContext

(Opcional) El contexto de cifrado. Si esto se especificó en la función `Encrypt`, debe especificarse aquí o se produce un error en la operación de descifrado. Para obtener más información, consulte Contexto de cifrado en la Guía para desarrolladores de AWS Key Management Service .

GrantTokens

(Opcional) Una lista de tokens de concesión que representan concesiones que proporcionan permisos para realizar el descifrado.

El texto cifrado y EKT se envían, junto con el contexto de cifrado, a través de una sesión autenticada a un HSM para su descifrado.

El HSM ejecuta lo siguiente:

1. Descifra el EKT para obtener la HBK = Decrypt(DK_i, EKT) .
2. Extrae el nonce N desde la estructura del texto cifrado.
3. Vuelve a generar una clave de cifrado K derivada de AES-GCM de 256 bits desde HBK y N.
4. Descifra el texto cifrado para obtener plaintext = Decrypt(K, context, ciphertext).

El identificador de clave y el texto sin formato resultantes se devuelven al AWS KMS host a través de la sesión segura y, a continuación, a la aplicación del cliente que realiza la llamada a través de una conexión TLS.

A continuación, se muestra la sintaxis de respuesta.

```
{
    "KeyId": "string",
    "Plaintext": blob
}
```

Si la aplicación que llama desea asegurarse de la autenticidad del texto sin formato, debe verificar que el ID de clave devuelto es el esperado.

Volver a cifrar un objeto cifrado

Un texto cifrado de cliente existente cifrado en una clave de KMS se puede volver a cifrar en otra clave de KMS mediante un comando reencrypt. Reencrypt cifra datos del lado del servidor con una clave de KMS nueva sin exponer el texto sin formato de la clave en el lado del cliente. Los datos se descifran en primer lugar y luego se cifran.

A continuación se presenta la sintaxis de la solicitud.

```
{
 "CiphertextBlob": "blob",
 "DestinationEncryptionContext": { "string" : "string" },
 "DestinationKeyId": "string",
 "GrantTokens": ["string"],
       "SourceKeyId": "string",
```

```
 "SourceEncryptionContext": { "string" : "string"}
}
```

La solicitud acepta los siguientes datos en formato JSON.

CiphertextBlob

Texto cifrado de los datos que se volverán a cifrar.

DestinationEncryptionContext

(Opcional) Contexto de cifrado que se utilizará cuando se vuelvan a cifrar los datos.

DestinationKeyId

Identificador de clave de la clave utilizada para volver a cifrar los datos.

GrantTokens

(Opcional) Una lista de tokens de concesión que representan concesiones que proporcionan permisos para realizar el descifrado.

SourceKeyId

(Opcional) Identificador de clave de la clave utilizada para descifrar los datos.

SourceEncryptionContext

(Opcional) Contexto de cifrado utilizado para cifrar y descifrar los datos especificados en el parámetro `CiphertextBlob`.

El proceso combina las operaciones de descifrado y cifrado de las descripciones anteriores: el texto cifrado del cliente se descifra en la HBK inicial a la que hace referencia el texto cifrado del cliente a la HBK actual en la clave de KMS prevista. Cuando las claves de KMS utilizadas en este comando son iguales, este comando mueve el texto cifrado del cliente de una versión anterior de una HBK a la última versión de una HBK.

A continuación, se muestra la sintaxis de respuesta.

```
{
    "CiphertextBlob": blob,
    "DestinationEncryptionAlgorithm": "string",
    "KeyId": "string",
    "SourceEncryptionAlgorithm": "string",
```

```
    "SourceKeyId": "string"
}
```

Si la aplicación que realiza la llamada quiere garantizar la autenticidad del texto sin formato subyacente, debe comprobar que el texto devuelto es el esperado. SourceKeyId

AWS KMS operaciones internas

AWS KMS los componentes internos son necesarios para escalar y proteger HSMs un servicio de administración de claves distribuido a nivel mundial.

Temas

Dominios y estado de dominio

Un conjunto cooperativo de AWS KMS entidades internas de confianza dentro de un dominio Región de AWS se denomina dominio. Un dominio incluye un conjunto de entidades de confianza, un conjunto de reglas y un conjunto de claves secretas, denominadas claves de dominio. Las claves de dominio se comparten entre HSMs los miembros del dominio. Un estado de dominio consta de los siguientes campos.

Nombre

: Un nombre de dominio para identificar este dominio.

Miembros

: Una lista de los HSMs que son miembros del dominio, incluida su clave de firma pública y sus claves de acuerdo públicas.

Operadores

: Una lista de entidades, claves de firma públicas y un rol (AWS KMS operador o anfitrión del servicio) que representa a los operadores de este servicio.

Reglas

: Una lista de reglas de quórum para cada comando que se deben cumplir para ejecutar un comando en el HSM.

Claves de dominio

: Una lista de claves de dominio (claves simétricas) actualmente en uso dentro del dominio.

El estado de dominio completo solo está disponible en el HSM. El estado de dominio se sincroniza entre los miembros del dominio de HSM como un token de dominio exportado.

Claves de dominio

Todos los HSMs elementos de un dominio comparten un conjunto de claves de dominio, $\{DK_r\}$. Estas claves se comparten a través de una rutina de exportación de estado de dominio. El estado de dominio exportado se puede importar a cualquier HSM que sea miembro del dominio.

El conjunto de claves de dominio, $\{DK_r\}$, siempre incluye una clave de dominio activa y varias claves de dominio desactivadas. Las claves de dominio se rotan a diario para garantizar que AWS cumplen con la recomendación para la gestión de claves (parte 1). Durante la rotación de claves de dominio, todas las claves de KMS existentes cifradas con la clave de dominio saliente se vuelven a cifrar con la nueva clave de dominio activa. La clave de dominio activa se utiliza para cifrar cualquier clave nueva. EKTs Las claves de dominio caducadas solo se pueden usar para descifrar previamente cifradas EKTs durante un número de días equivalente al número de claves de dominio rotadas recientemente.

Tokens de dominio exportados

Existe una necesidad periódica de sincronizar el estado entre los participantes del dominio. Esto se logra al exportar el estado de dominio cada vez que se realiza un cambio en el dominio. El estado de dominio se exporta como un token de dominio exportado.

Nombre

Un nombre de dominio para identificar este dominio.

Miembros

Una lista de las HSMs que son miembros del dominio, incluidas sus claves públicas de firma y acuerdo.

Operadores

Una lista de entidades, claves de firma públicas y un rol que representa a los operadores de este servicio.

Reglas

Una lista de reglas de quórum para cada comando que se deben cumplir para ejecutar un comando en un miembro de dominio de HSM.

Claves de dominio cifradas

Claves de dominio con cifrado doble. El miembro firmante cifra las claves de dominio para cada uno de los miembros enumerados anteriormente y las vuelve a cifrar con su clave de acuerdo pública.

Signature

Una firma en el estado de dominio producida por un HSM, necesariamente el miembro del dominio que exportó el estado de dominio.

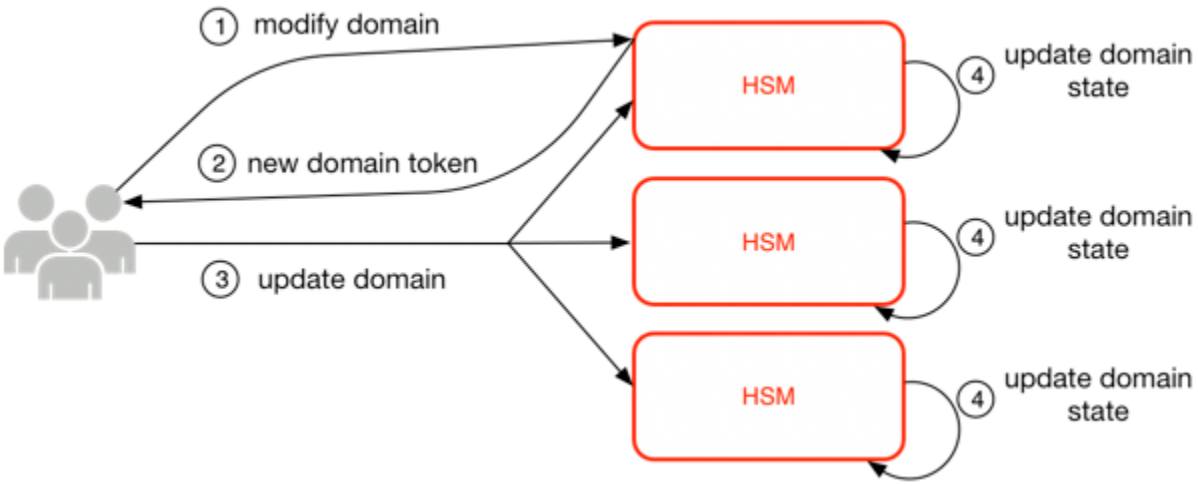
El token de dominio exportado forma la fuente fundamental de confianza para las entidades que operan dentro del dominio.

Administración de estados de dominio

El estado de dominio se administra a través de comandos autenticados con quórum. Estos cambios incluyen la actualización de la lista de participantes de confianza en el dominio, la modificación de las reglas de quórum para ejecutar comandos de HSM y la rotación periódica de las claves de dominio. Estos comandos se autentican por cada comando en lugar de operaciones de sesión autenticadas, como se muestra en la imagen siguiente.

Un HSM, en su estado inicializado y operativo, contiene un conjunto de claves de identidad asimétricas generadas de forma automática, un par de claves de firma y un par de claves de establecimiento de claves. Mediante un proceso manual, un AWS KMS operador puede establecer un dominio inicial que se creará en el primer HSM de una región. Este dominio inicial consta de un estado de dominio completo como se definió anteriormente en este tema. Se instala mediante un comando de unión para cada uno de los miembros del HSM definidos en el dominio.

Una vez que un HSM se haya unido a un dominio inicial, este estará vinculado a las reglas que se definen en ese dominio. Estas reglas rigen los comandos que utilizan claves criptográficas de cliente o realizan cambios en el estado del anfitrión o del dominio. Las operaciones de API de sesión autenticadas que utilizan las claves criptográficas se han definido anteriormente.



La imagen anterior muestra cómo se modifica un estado de dominio. El proceso consta de cuatro pasos:

1. Se envía un comando basado en quórum a un HSM para modificar el dominio.
2. El nuevo estado de dominio se crea y se exporta como un nuevo token de dominio exportado. El estado en el HSM no se modifica, lo que significa que el cambio no se implementa en el HSM.
3. Se envía un segundo comando a cada uno de los componentes del HSMs token de dominio recién exportado para actualizar el estado de su dominio con el nuevo token de dominio.
4. Lo que HSMs aparece en el nuevo token de dominio exportado puede autenticar el comando y el token de dominio. También pueden desempaquetar las claves de dominio para actualizar el estado del dominio HSMs en todo el dominio.

HSMs no se comunican directamente entre sí. En su lugar, un quórum de operadores solicita un cambio en el estado de dominio que da como resultado un nuevo token de dominio exportado. Un miembro del anfitrión de servicio del dominio se utiliza para distribuir el nuevo estado de dominio a cada HSM del dominio.

La salida y unión de un dominio se realizan a través de las funciones de gestión de HSM. La modificación del estado de dominio se realiza a través de las funciones de gestión del dominio.

Salir del dominio

> Hace que un HSM salga de un dominio, lo que elimina todos los restos y claves de ese dominio de la memoria.

Unirse al dominio

Hace que un HSM se una a un nuevo dominio o actualice su estado de dominio actual al nuevo estado del dominio. El dominio existente se utiliza como fuente del conjunto inicial de reglas para autenticar este mensaje.

Crear un dominio

Hace que se cree un nuevo dominio en un HSM. Devuelve un primer token de dominio que se puede distribuir a los miembros HSMs del dominio.

Modificar operadores

Agrega o elimina operadores de la lista de operadores autorizados y sus respectivos roles en el dominio.

Modificar miembros

Agrega o elimina un HSM de la lista de autorizados HSMs en el dominio.

Modificar reglas

Modifica el conjunto de reglas de quórum necesario para ejecutar comandos en un HSM.

Rotar claves de dominio

Hace que se cree una nueva clave de dominio y que esta se marque como la clave de dominio activa. De esta manera, se mueve la clave activa existente a una clave desactivada y elimina la clave desactivada más antigua del estado de dominio.

Seguridad de la comunicación interna

Los comandos entre los hosts u AWS KMS operadores del servicio HSMs se protegen mediante dos mecanismos descritos enSesiones autenticadas: un método de solicitud firmado por quórum y una sesión autenticada mediante un protocolo de host de servicio HSM.

Los comandos firmados por quórum están diseñados para que ningún operador pueda modificar por sí solo las protecciones de seguridad críticas que proporcionan. HSMs Los comandos que se ejecutan en las sesiones autenticadas ayudan a garantizar que solo los operadores de servicio autorizados puedan realizar operaciones con claves de KMS. Toda la información secreta vinculada al cliente está protegida en toda la infraestructura. AWS

Establecimiento de claves

Para proteger las comunicaciones internas, AWS KMS utiliza dos métodos diferentes de establecimiento de claves. El primero se define como C (1, 2, ECC DH) en la Recomendación para los esquemas de establecimiento de claves por pares que utilizan criptografía de logaritmos discretos (Revisión 2). Este esquema tiene un iniciador con una clave de firma estática. El iniciador genera y firma una clave de ephemeral elliptic curve Diffie-Hellman (ECDH, curva elíptica de Diffie-Hellman efímera), dirigida a un destinatario con una clave de acuerdo de ECDH estática. Este método utiliza dos claves estáticas y dos claves efímeras, cada una mediante el uso de ECDH. Esa es la derivación de la etiqueta C (1, 2, ECC DH). Este método a veces se denomina ECDH directa.

El segundo método de establecimiento de claves es C (2, 2, ECC, DH). En este esquema, ambas partes tienen una clave de firma estática y generan, firman e intercambian una clave de ECDH efímera. Este método utiliza dos claves estáticas y dos claves efímeras, cada una mediante el uso de ECDH. Esa es la derivación de la etiqueta C (2, 2, ECC, DH). Este método a veces se denomina ECDH efímero o ECDHE. Todas las claves ECDH se generan en la curva secp384r1 (NIST-P384).

Límite de seguridad del HSM

El límite de seguridad interior de AWS KMS es el HSM. El HSM tiene una interfaz propietaria y ninguna otra interfaz de activación física en su estado operativo. Un HSM operativo se aprovisionará durante la inicialización con las claves criptográficas necesarias para establecer su rol en el dominio. Los materiales criptográficos sensibles del HSM solo se almacenan en la memoria volátil y se borran cuando el HSM sale del estado operativo, incluidos los bloqueos o reinicios previstos o no intencionadas.

Las operaciones de la API del HSM se autentican mediante comandos individuales o mediante una sesión confidencial mutuamente autenticada establecida por un anfitrión de servicio.

Comandos firmados por quórum

Los operadores emiten comandos firmados por quórum para. HSMs En esta sección se describe cómo se crean, firman y autentican los comandos basados en quórum. Estas reglas son bastante simples. Por ejemplo, el comando Foo requiere dos miembros del rol Bar para que lo autentique. Hay tres pasos en la creación y verificación de un comando basado en quórum. El primer paso es la creación inicial del comando; el segundo es el envío a operadores adicionales para firmar y el tercero es la verificación y ejecución.

Con el fin de presentar los conceptos, suponga que existe un conjunto auténtico de claves públicas y roles del operador $\{QOS_s\}$ y un conjunto de reglas de quórum QR = $\{Command_i, Rule_{\{i, t\}}\}$ donde cada regla es un conjunto de roles y un número mínimo N $\{Role_t, N_t\}$. A fin de que un comando satisfaga la regla de quórum, el conjunto de datos del comando debe estar firmado por un conjunto de operadores enumerados en $\{QOS_s\}$ de manera que cumplan con una de las reglas enumeradas para ese comando. Como se mencionó anteriormente, el conjunto de reglas de quórum y operadores se almacenan en el estado de dominio y el token de dominio exportado.

En la práctica, un firmante inicial firma el comando $Sig_1 = Sign(dO_{p1}, Command)$. Un segundo operador también firma el comando $Sig_2 = Sign(dO_{p2}, Command)$. El mensaje con doble firma se envía a un HSM para su ejecución. El HSM realiza las siguientes tareas:

1. Para cada firma, extrae la clave pública del firmante del estado del dominio y verifica la firma en el comando.
2. Comprueba que el conjunto de firmantes cumpla una regla para el comando.

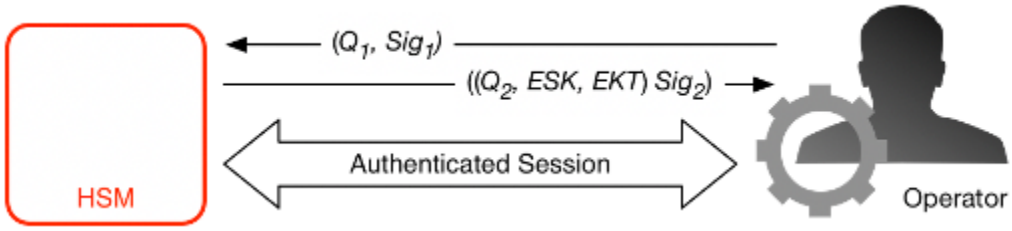
Sesiones autenticadas

Sus operaciones clave se ejecutan entre los AWS KMS hosts externos y el. HSMs Estos comandos se refieren a la creación y la utilización de claves criptográficas y a la generación segura de números aleatorios. Los comandos se ejecutan a través de un canal autenticado por sesión entre los hosts del servicio y el. HSMs Además de la necesidad de autenticidad, estas sesiones requieren confidencialidad. Los comandos que se ejecutan en estas sesiones incluyen la devolución de claves de datos de texto sin cifrar y mensajería descifrada destinados a usted. Para garantizar que estas sesiones no se puedan subvertir mediante man-in-the-middle ataques, las sesiones se autentican.

Este protocolo realiza un acuerdo de clave de ECDHE mutuamente autenticado entre el HSM y el anfitrión de servicio. El anfitrión de servicio inicia el intercambio y el HSM lo completa. El HSM

también devuelve una session key (SK, clave de sesión) cifrada por la clave negociada y un token de clave exportado que contiene la clave de sesión. El token de clave exportado contiene un periodo de validez, después del cual el anfitrión de servicio debe renegociar una clave de sesión.

Un host de servicio es miembro del dominio y tiene un par de claves de firma de identidad ($DHos_i$, $QHOS_i$) y una copia auténtica de las claves públicas de «identidad HSMs». Utiliza el conjunto de claves de firma de identidad para negociar de forma segura una clave de sesión que se puede utilizar entre el anfitrión de servicio y cualquier HSM del dominio. Los tokens de clave exportados tienen un periodo de validación asociado a ellos, después del cual se debe negociar una nueva clave.



El proceso comienza con el reconocimiento del anfitrión de servicio de que requiere una clave de sesión para enviar y recibir flujos de comunicación sensibles entre sí y un miembro del HSM del dominio.

1. Un anfitrión de servicio genera un par de claves efímeras de ECDH (d_1, Q_1) y lo firma con la clave de identidad Sig1 = Sign(dOS, Q_1).
2. El HSM verifica la firma en la clave pública recibida mediante el token de dominio actual y crea un par de claves efímeras de ECDH (d_2, Q_2). A continuación, completa la información de ECDH-key-exchange acuerdo con la recomendación para sistemas de establecimiento de claves por pares que utilicen criptografía de logaritmos discretos (revisada) para formar una clave AES-GCM negociada de 256 bits. El HSM genera una nueva clave de sesión AES-GCM de 256 bits. Cifra la clave de sesión con la clave negociada para formar la encrypted session key (ESK, clave de sesión cifrada). También cifra la clave de sesión bajo la clave de dominio como un token de clave exportado (EKT). Finalmente, firma un valor de retorno con el par de claves de identidad Sig_2 = Sign(dHSK, [Q_2, ESK, EKT]).
3. El anfitrión de servicio verifica la firma en las claves recibidas mediante el token de dominio actual. Luego, el anfitrión de servicio completa el intercambio de claves de ECDH según la Recomendación para esquemas de establecimiento de claves por pares que utilizan criptografía de logaritmo discreta (revisada). A continuación, descifra la ESK a fin de obtener la clave de sesión (SK).

Durante el periodo de validación del EKT, el anfitrión de servicio puede utilizar la clave de sesión negociada SK para enviar comandos cifrados sobre el HSM. Todos los service-host-initiated comandos de esta sesión autenticada incluyen el EKT. El HSM responde con la utilización de la misma clave de sesión negociada SK.

Proceso de replicación de claves multirregión

AWS KMS utiliza un mecanismo de replicación entre regiones para copiar el material clave de una clave KMS de un HSM en uno Región de AWS a un HSM en otro diferente. Región de AWS Para que este mecanismo funcione, la clave KMS que se replica debe ser una clave multirregión. Al replicar una clave KMS de una región a otra, las regiones no pueden comunicarse directamente porque están HSMs en redes aisladas. En su lugar, los mensajes intercambiados durante la replicación entre regiones los entrega un servicio proxy.

Durante la replicación entre regiones, todos los mensajes generados por un AWS KMS HSM se firman criptográficamente con una clave de firma de replicación. Las claves de firma de replicación (RSKs) son claves ECDSA en la curva P-384 del NIST. Cada región posee al menos un RSK y el componente público de cada RSK se comparte con todas las demás regiones de la misma partición. AWS

El proceso de replicación entre regiones para copiar material de clave de la región A a la región B funciona como se explica a continuación:

1. El HSM de la región B genera una clave ECDH efímera en la curva NIST P-384, Clave B del acuerdo de replicación (RAKB). El componente público de RAKB se envía a un HSM de la región A por el servicio proxy.
2. El HSM de la región A recibe el componente público de RAKB y, a continuación, genera otra clave ECDH efímera en la curva NIST P-384, Clave A del acuerdo de replicación (RAKA). El HSM ejecuta el esquema de establecimiento de claves ECDH en RAKA y el componente público de RAKB, y obtiene una clave simétrica de la salida, la Clave de encapsulamiento de replicación (RWK). La RWK se utiliza para cifrar el material de clave de la clave KMS multirregión que se está replicando.
3. El componente público de RAKA y el material de clave cifrado con la RWK se envían al HSM de la región B a través del servicio proxy.
4. El HSM de la región B recibe el componente público de RAKA y el material de clave cifrado mediante la RWK. El HSM se obtiene por la RWK ejecutando el esquema de establecimiento de claves ECDH en RAKB y el componente público de RAKA.

5. El HSM de la región B utiliza la RWK para descifrar el material de clave de la región A.

Protección de durabilidad

La durabilidad adicional del servicio para las claves generadas por el servicio se consigue mediante el uso del almacenamiento fuera de línea HSMs, el almacenamiento múltiple y no volátil de los tokens de dominio exportados y el almacenamiento redundante de claves KMS cifradas. Los que HSMs están fuera de línea son miembros de los dominios existentes. Con la excepción de no estar en línea y participar en las operaciones normales del dominio, las personas sin conexión HSMs aparecen en el estado del dominio del mismo modo que los miembros del HSM existentes.

El diseño de durabilidad tiene por objeto proteger todas las claves KMS de una región en caso de que se AWS produzca una pérdida masiva de las claves KMS en línea HSMs o del conjunto de claves KMS almacenadas en nuestro sistema de almacenamiento principal. AWS KMS keys con material de clave importado, no están incluidas en las protecciones de durabilidad que ofrecen otras claves KMS. En caso de que se produzca un error en toda la región AWS KMS, es posible que sea necesario volver a importar el material clave importado a una clave KMS.

Los objetos sin conexión HSMs y las credenciales para acceder a ellos se guardan en cajas fuertes dentro de salas seguras supervisadas en varias ubicaciones geográficas independientes. Cada caja fuerte requiere al menos un oficial de AWS seguridad y un AWS KMS operador, de dos equipos independientes AWS, para obtener estos materiales. El uso de estos materiales se rige por una política interna que exige la presencia de un quórum de AWS KMS operadores.

Referencia

Utilice el siguiente material de referencia para obtener información acerca las abreviaturas, las claves, los colaboradores y las fuentes citadas en este documento.

Temas

Abreviaturas

En la siguiente lista se aclaran las abreviaturas a las que se hace referencia en este documento.

AES

estándar de cifrado avanzado

CDK

clave de datos del cliente

DK

clave de dominio

ECDH

curva elíptica de Diffie-Hellman

ECDHE

curva elíptica efímera de Diffie-Hellman

ECDSA

algoritmo de firma digital de curva elíptica

EKT

token de clave exportado

ESK

clave de sesión cifrada

GCM

Galois/Counter Mode

HBK

clave de backup de HSM

HBKID

identificador de clave de backup de HSM

HSM

módulo de seguridad de hardware

RSA

Rivest Shamir y Adleman (criptológico)

secp384r1

estándares para la criptografía eficiente de la curva aleatoria de 384 bits 1

SHA256

algoritmo hash seguro de longitud de resumen de 256 bits

Claves

En la siguiente lista se definen las claves a las que se hace referencia en este documento.

HBK

Clave de backup de HSM: las claves de backup de HSM son claves raíz de 256 bits, de las cuales se derivan las claves de uso específico.

DK

Clave de dominio: una clave de dominio es una clave AES-GCM de 256 bits. Se comparte entre todos los miembros de un dominio y se utiliza para proteger el material de las claves de backup de HSM y las claves de sesión de anfitrión del servicio de HSM.

DKEK

Clave de cifrado de clave de dominio: una clave de cifrado de clave de dominio es una clave AES-256-GCM generada en un anfitrión que se utiliza para cifrar el conjunto actual de claves de dominio que sincronizan el estado de dominio en los anfitriones de HSM.

(dHAK,QHAK)

Par de claves de acuerdo de HSM: cada HSM iniciado tiene un par de claves de acuerdo de curva elíptica de Diffie-Hellman generado de forma local en la curva secp384r1 (NIST-P384).

(dE, QE)

Par de claves de acuerdo efímeras: el HSM y los anfitriones de servicio generan claves de acuerdo efímeras. Estas son las claves de la curva elíptica de Diffie-Hellman en la curva secp384r1 (NIST-P384). Se generan en dos casos de uso: para establecer una clave de host-to-host cifrado para transportar las claves de cifrado de claves de dominio en fichas de dominio y para establecer claves de sesión del host del servicio HSM para proteger las comunicaciones confidenciales.

(dHSK, QHSK)

Par de claves de firma de HSM: cada HSM iniciado tiene un par de claves de firma digital de curva elíptica generado de forma local en la curva secp384r1 (NIST-P384).

(dOS, QOS)

Par de claves de firma del operador: tanto los operadores del host del servicio como AWS KMS los operadores tienen una clave de firma de identidad que se utiliza para autenticarse ante otros participantes del dominio.

K

Clave de cifrado de datos: clave AES-GCM de 256 bits derivada de un HBK que utilizaba el NIST SP800 -108 KDF en modo contador y utilizaba HMAC con. SHA256

SK

Clave de sesión: se crea una clave de sesión como resultado de una clave de curva elíptica de Diffie-Hellman autenticada que se intercambia entre un operador de anfitrión de servicio y un HSM. El propósito del intercambio es asegurar la comunicación entre el anfitrión de servicio y los miembros del dominio.

Colaboradores

Las siguientes personas y organizaciones han colaborado en este documento:

- Ken Beer, AWS director general de criptografía de KMS
- Matthew Campagna, ingeniero principal de seguridad, criptografía AWS

Bibliografía

Para obtener información sobre el AWS Key Management Service HSMs, vaya a la página de búsqueda del programa de validación de módulos criptográficos del Centro de Recursos de Seguridad Informática del NIST y busque HSM.AWS Key Management Service

Amazon Web Services, Referencia general (versión 1.0), «Solicitud de AWS API de firma», http://docs.aws.amazon. com/general/latest/gr/signing_aws_api_requests.html.

Amazon Web Services, «What is the» AWS Encryption SDK, http://docs.aws.amazon. com/encryption-sdk/latest/developer-guide/introduction.html.

Federal Information Processing Standards Publications (FIPS, Publicaciones de los Estándares de procesamiento de la información federal), PUB 180-4. Estándar de hash seguro, agosto de 2012. Disponible en https://nvlpubs.nist. gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf.

Publicación de los Estándares de procesamiento de la información federal 197, Announcing the Advanced Encryption Standard (AES), noviembre de 2001. Disponible en http://csrc.nist. gov/publications/fips/fips197/fips-197.pdf.

Publicación de los Estándares de procesamiento de la información federal 198-1, The Keyed-Hash Message Authentication Code (HMAC), julio de 2008. Disponible en http://csrc.nist. gov/publications/fips/fips198-1/FIPS-198-1_final.pdf.

Publicación especial 800-52 del NIST, revisión 2, Directrices para la selección, configuración y uso de las implementaciones de seguridad de la capa de transporte (TLS), agosto de 2019. https://nvlpubs.nist. gov/nistpubs/SpecialPublications/NIST.sp.800-52R2.pdf.

PKCS #1 v2.2: Estándar de criptografía RSA (RFC 8017), Grupo de trabajo sobre ingeniería de Internet (IETF), noviembre de 2016. https://tools.ietf.org/html/rfc8017.

Recomendación sobre los modos de funcionamiento del cifrado por bloques: Galois/Counter modo (GCM) y GMAC, publicación especial 800-38D del NIST, noviembre de 2007. Disponible en http://csrc.nist. gov/publications/nistpubs/800-38D/SP-800-38D.pdf.

Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices, publicación especial del NIST 800-38E, enero de 2010. Disponible en https://nvlpubs.nist. gov/nistpubs/Legacy/SP/nistspecialpublication800-38e.pdf.

Recomendación para la derivación de claves mediante funciones pseudoaleatorias, publicación especial 800-108 del NIST, octubre de 2009, disponible en https://nvlpubs.nist. gov/nistpubs/legacy/sp/nistspecialpublication800-108.pdf.

Recommendation for Key Management - Part 1: General (Revision 5), publicación especial del NIST 800-57A, mayo de 2020, disponible en https://doi.org/10.6028/NIST.SP.800-57pt1r5.

Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revised), publicación especial del NIST 800-56A, Revisión 3, abril de 2018. Disponible en https://nvlpubs.nist. gov/nistpubs/SpecialPublications/NIST.sp.800-56AR3.pdf.

Recomendación para la generación de números aleatorios mediante generadores de bits aleatorios deterministas, publicación especial 800-90A del NIST, revisión 1, de junio de 2015, disponible en https://nvlpubs.nist. gov/nistpubs/SpecialPublications/NIST.sp.800-90AR1.pdf.

SEC 2: Recommended Elliptic Curve Domain Parameters, Standards for Efficient Cryptography Group, versión 2.0, 27 de enero de 2010.

Uso de algoritmos de criptografía de curva elíptica (ECC) en la sintaxis de mensajes criptográficos (CMS), Brown, D., Turner, S., Internet Engineering Task Force, julio de 2010, http://tools.ietf. org/html/rfc5753/.

X9.62-2005: Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA, algoritmo de firma digital de curva elíptica), American National Standards Institute, 2005.

Historial de documentos para AWS KMS detalles criptográficos

En la siguiente tabla se describen cambios importantes en la documentación de Detalles Criptográficos de AWS Key Management Service . Actualizamos la documentación con frecuencia para responder a los comentarios que nos envían.

Cambio	Descripción	Fecha
Contenido actualizado	Se agregaron detalles sobre la implementación de la AWS KMS `ReplicateKey` operación.	28 de octubre de 2021
Cambio de documentación	Sustituir el término clave maestra del cliente (CMK) por AWS KMS key y clave KMS.	30 de agosto de 2021
Versión inicial	Se creó esta guía a partir del documento técnico Detalles criptográficos de KMS	30 de diciembre de 2020

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.