Detalhes criptográficos do AWS KMS

AWS Key Management Service

AWS Key Management Service: Detalhes criptográficos do AWS KMS

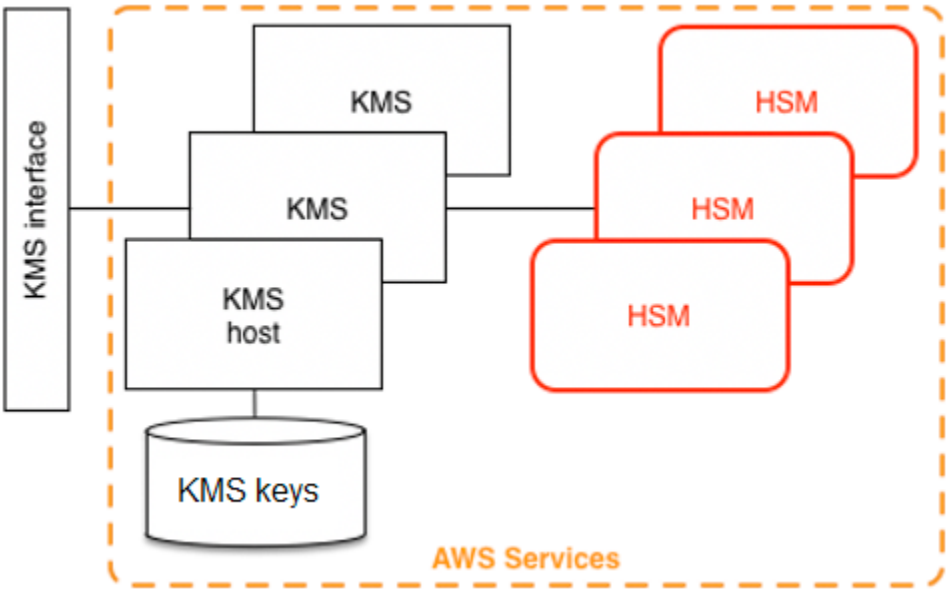
Table of Contents

Introdução aos detalhes criptográficos do AWS KMS

O AWS Key Management Service (AWS KMS) fornece uma interface web para gerar e gerenciar chaves criptográficas e opera como um provedor de serviços criptográficos para proteger dados. O AWS KMS oferece serviços tradicionais de gerenciamento de chaves integrados ao AWS para fornecer uma visão consistente das chaves dos clientes no AWS, com gerenciamento e auditoria centralizados. Este whitepaper fornece uma descrição detalhada das operações criptográficas do AWS KMS para ajudar você a avaliar os recursos oferecidos pelo serviço.

O AWS KMS inclui uma interface web através do AWS Management Console, da interface de linha de comando e de operações de API RESTful para solicitar operações criptográficas de uma frota distribuída de módulos de segurança de hardware (HSMs) validados para FIPS 140-2 [1]. O HSM AWS KMS é um dispositivo de hardware multichip independente criptográfico projetado para fornecer funções criptográficas dedicadas a fim de atender aos requisitos de segurança e escalabilidade do AWS KMS. Você pode estabelecer sua própria hierarquia criptográfica baseada em HSM sob chaves gerenciadas como AWS KMS keys. Essas chaves são disponibilizadas apenas nos HSMs e apenas na memória durante o tempo necessário para processar a sua solicitação criptográfica. Você pode criar várias chaves KMS, cada uma representada por seu ID de chave. As chaves KMS podem ser criadas, excluídas ou usadas para criptografar, descriptografar, assinar ou verificar dados somente nas funções do IAM doAWS e nas contas administradas por cada cliente. Você pode definir controles de acesso sobre quem pode gerenciar e/ou usar chaves KMS criando uma política anexada à chave. Essas políticas permitem que você defina usos específicos de aplicação para suas chaves para cada operação de API.

Além disso, a maioria dos serviços AWS oferecem suporte à criptografia de dados em repouso usando chaves KMS. Esse recurso permite que os clientes controlem como e quando o AWS pode acessar dados criptografados controlando como e quando as chaves KMS podem ser acessadas.



O AWS KMS é um serviço hierárquico que consiste em hosts AWS KMS voltados para a web e uma camada de HSMs. O agrupamento desses hosts hierárquicos forma a pilha AWS KMS. Todas as solicitações para o AWS KMS devem ser feitas por meio do protocolo TLS (Transport Layer Security) e terminar em um host AWS KMS. Os hosts AWS KMS só permitem TLS com uma ciphersuite que forneça confidencialidade de encaminhamento perfeita. O AWS KMS autentica e autoriza suas solicitações usando os mesmos mecanismos de credencial e política do AWS Identity and Access Management (IAM) que estão disponíveis para todas as outras Operações de API do AWS.

Conceitos básicos

Aprender alguns termos e conceitos básicos ajudará você a obter proveito máximo do AWS Key Management Service.

AWS KMS key

> **Note**
>
> O AWS KMS está substituindo o termo chave mestre do cliente (CMK) por AWS KMS key e Chave KMS. O conceito não mudou. Para evitar alterações interrompidas, o AWS KMS está mantendo algumas variações deste termo.

Uma chave lógica que representa o topo da hierarquia de chaves. Uma chave do KMS recebe um nome do recurso da Amazon (ARN) que inclui um identificador de chave exclusivo ou ID de chave. AWS KMS keys têm três tipos:

- Chave do cliente: os clientes criam e controlam o ciclo de vida e as principais políticas de chaves gerenciadas pelo cliente. Todas as solicitações feitas com base nessas chaves são registradas como CloudTrail eventos.
- Chaves gerenciadas pela AWS: AWS cria e controla o ciclo de vida e as principais políticas do Chaves gerenciadas pela AWS, que são recursos no Conta da AWS de um cliente. Os clientes podem visualizar políticas e CloudTrail eventos de acessoChaves gerenciadas pela AWS, mas não podem gerenciar nenhum aspecto dessas chaves. Todas as solicitações feitas com base nessas chaves são registradas como CloudTrail eventos.
- Chaves pertencentes à AWS: Essas chaves são criadas e usadas exclusivamente pelo AWS para operações de criptografia interna em diferentes serviços do AWS. Os clientes não têm visibilidade das principais políticas ou do Chave pertencente à AWS uso em CloudTrail.

Alias

Um nome fácil de usar que está associado a uma chave do KMS. O nome pode ser usado de forma intercambiável com ID de chave em muitas das Operações de API AWS KMS.

Permissões

Uma política anexada a uma chave KMS que define permissões na chave. A política padrão permite qualquer entidade principal que você defina, além de permitir que a Conta da AWS adicione políticas do IAM que fazem referência à chave.

Concessões

A permissão delegada para usar uma chave KMS quando os principais do IAM pretendidos ou a duração do uso não é conhecida no início e, portanto, não pode ser adicionada a uma chave ou política do IAM. Um uso das concessões é definir permissões com escopo para baixo para como um serviço AWS pode usar uma chave do KMS. O serviço pode precisar usar sua chave para fazer trabalho assíncrono em seu nome em dados criptografados na ausência de uma chamada de API com assinatura direta sua.

Chaves de dados

Chaves criptográficas geradas em HSMs, protegidas por uma chave KMS. O AWS KMS permite que entidades autorizadas obtenham chaves de dados protegidas por uma chave KMS. Elas podem ser retornadas como chaves de dados de texto simples (não criptografadas) e como

chaves de dados criptografadas. As chaves de dados podem ser simétricas ou assimétricas (com o retorno das partes públicas e privadas).

Texto cifrado

A saída criptografada do AWS KMS, às vezes chamada de texto cifrado do cliente, para eliminar a confusão. O texto cifrado contém dados criptografados com informações adicionais que identificam a chave KMS a ser usada no processo de descriptografia. As chaves de dados criptografados são um exemplo comum de texto cifrado produzido ao usar uma chave KMS, mas quaisquer dados com tamanho inferior a 4 KB podem ser criptografados sob uma chave KMS para produzir um texto cifrado.

Contexto de criptografia

Um mapa de par chave-valor de informações adicionais que está associado ao AWS KMS – informações protegidas. O AWS KMS usa a criptografia autenticada para proteger chaves de dados. O contexto de criptografia é incorporado ao AAD da criptografia autenticada no AWS KMS – textos criptografados. Essas informações de contexto são opcionais e não são retornadas ao solicitar uma chave (ou uma operação de criptografia). Mas se for usado, esse valor de contexto é necessário para concluir com êxito uma operação de descriptografia. Um uso pretendido do contexto de criptografia é fornecer informações adicionais autenticadas. Essas informações podem ajudar você a aplicar políticas e a serem incluídas nos AWS CloudTrail registros. Por exemplo, você pode usar um par chave-valor de {"key name":"satellite uplink key"} para nomear a chave de dados. O uso subsequente da chave cria uma entrada no AWS CloudTrail que inclui “nome da chave”: “chave de uplink de satélite”. Essas informações adicionais podem fornecer um contexto útil para entender por que uma determinada chave KMS foi usada.

Chave pública

Ao usar cifras assimétricas (RSA ou curva elíptica), a chave pública é o “componente público” de um par de chaves público-privadas. A chave pública pode ser compartilhada e distribuída para entidades que precisam criptografar dados para o proprietário do par de chaves público-privadas. Para operações de assinatura digital, a chave pública é usada para verificar a assinatura.

Chave privada

Ao usar cifras assimétricas (RSA ou curva elíptica), a chave privada é o “componente privado” de um par de chaves público-privadas. A chave privada é usada para descriptografar dados ou criar assinaturas digitais. Semelhante às chaves KMS simétricas, as chaves privadas são criptografadas em HSMs. Elas são descriptografadas somente na memória de curto prazo do HSM e somente pelo tempo necessário para processar sua solicitação criptográfica.

Objetivos de projeto do AWS KMS

O AWS KMS foi projetado para atender aos seguintes requisitos.

Durabilidade

A durabilidade das chaves criptográficas é projetada para ser igual à dos serviços de maior durabilidade no AWS. Uma única chave criptográfica pode criptografar grandes volumes dos seus dados acumulados ao longo de um longo período de tempo.

Confiável

O uso de chaves é protegido por políticas de controle de acesso que você define e gerencia. Não há mecanismo para exportar chaves KMS de texto simples. A confidencialidade das suas chaves criptográficas é crucial. Vários funcionários da Amazon com acesso específico a controles de acesso baseados em quórum têm a exigência de executar ações administrativas nos HSMs.

Baixa latência e alta taxa de transferência

O AWS KMS fornece operações criptográficas em níveis de latência e taxa de transferência adequados para uso por outros serviços no AWS.

Regiões independentes

O AWS fornece regiões independentes a clientes que precisam restringir o acesso a dados em diferentes regiões. O uso da chave pode ser isolado dentro de um Região da AWS.

Fonte segura de números aleatórios

Como a criptografia forte depende da geração de números aleatórios verdadeiramente imprevisíveis, o AWS KMS fornece uma fonte de alta qualidade e validada de números aleatórios.

Auditoria

AWS KMSregistra o uso e o gerenciamento de chaves criptográficas em AWS CloudTrail registros. Você pode usar logs do AWS CloudTrail para inspecionar o uso de suas chaves criptográficas, incluindo o uso de chaves por serviços AWS em seu nome.

Para atingir esses objetivos, o sistema AWS KMS inclui um conjunto de operadores AWS KMS e operadores de host de serviço (coletivamente, “operadores”) que administram “domínios”. Um domínio é um conjunto regionalmente definido de servidores, HSMs e operadores AWS KMS. Cada operador AWS KMS tem um token de hardware que contém um par de chaves privadas e públicas

que é usado para autenticar suas ações. Os HSMs têm um par adicional de chaves privadas e públicas para estabelecer chaves de criptografia que protegem a sincronização do estado do HSM.

Este artigo ilustra como o AWS KMS protege suas chaves e outros dados que você deseja criptografar. Neste documento, as chaves de criptografia ou os dados que você deseja criptografar são chamados de “segredos” ou “material secreto”.

Fundamentos do AWS Key Management Service

Os tópicos deste capítulo descrevem os primitivos criptográficos doAWS Key Management Service e onde eles são usados. Eles também apresentam os elementos básicos do AWS KMS.

Tópicos

Primitivas criptográficas

O AWS KMS usa algoritmos criptográficos configuráveis para que o sistema possa migrar rapidamente de um algoritmo ou modo aprovado para outro. O conjunto padrão inicial de algoritmos criptográficos foi selecionado a partir de algoritmos do Padrão Federal de Processamento de Informações (aprovados pelo Federal Information Processing Standard – FIPS) para suas propriedades de segurança e performance.

Entropia e geração de números aleatórios

A geração de chaves do AWS KMS é realizada nos HSMs do AWS KMS. Os HSMs implementam um gerador de números aleatórios híbridos que usa o NIST SP800-90A Gerador de bits aleatórios determinísticos (DRBG) CTR_DRBG usando AES-256. Ele é preparado com um gerador de bits aleatórios não determinísticos com 384 bits de entropia e atualizado com entropia adicional para fornecer resistência de previsão em cada chamada de material criptográfico.

Operações de chave simétrica (somente criptografia)

Todos os comandos de criptografia de chave simétrica usados nos HSMs usam os Padrões avançados de criptografia (AES) no Modo Contador Galois (GCM), usando chaves de 256 bits. As chamadas análogas para descriptografar usam a função inversa.

AES-GCM é um esquema de criptografia autenticado. Além de criptografar texto sem formatação para produzir texto cifrado, ele calcula uma tag de autenticação sobre o texto cifrado e quaisquer dados adicionais para os quais a autenticação é necessária (dados autenticados adicionalmente – AAD). A tag de autenticação ajuda a garantir que os dados são da fonte suposta e que o texto cifrado e os AAD não foram modificados.

Frequentemente, o AWS omite a inclusão dos AAD em nossas descrições, especialmente quando se refere à criptografia de chaves de dados. Fica implícito pelo texto circundante nesses casos que a estrutura a ser criptografada é particionada entre o texto sem formatação a ser criptografado e o AAD de texto não criptografado a ser protegido.

A AWS KMS fornece uma opção para você importar material de chave para uma AWS KMS key em vez de depender do AWS KMS para gerar o material de chave. Este material de chave importado pode ser criptografado usando RSAES-OAEP ou RSAES-PKCS1-v1_5 para proteger a chave durante o transporte para o HSM do AWS KMS. Os pares de chaves RSA são gerados nos HSMs do AWS KMS. O material de chave importada é descriptografado em um HSM do AWS KMS e criptografado novamente no AES-GCM antes de ser armazenado pelo serviço.

Operações de chave assimétrica (criptografia, assinatura digital e verificação de assinatura)

O AWS KMS é compatível com o uso de operações de chave assimétrica para operações de criptografia e assinatura digital. Operações de chave assimétrica contam com uma chave pública e um par de chaves privadas relacionadas matematicamente que podem ser usadas para criptografia e descriptografia ou para assinatura e verificação de assinatura, mas não ambos. A chave privada nunca deixa o AWS KMS descriptografado. É possível usar a chave pública no AWS KMS chamando as operações de API do AWS KMS ou baixando a chave pública e usando-a fora do AWS KMS.

O AWS KMS é compatível com dois tipos de cifras assimétricas.

- RSA-OAEP (para criptografia) & RSA-PSS e RSA-PKCS- #1 -v1_5 (para assinatura e verificação): Suporta comprimentos de chave RSA (em bits): 2048, 3072 e 4096 para diferentes requisitos de segurança.
- Curva elíptica (ECC): usada somente para assinatura e verificação. Suporta curvas ECC: NIST P256, P384, P521, SECP 256k1.

Funções de derivação de chave

Uma função de derivação de chave é usada para derivar chaves adicionais a partir de um segredo ou chave inicial. O AWS KMS usa uma função de derivação de chave (KDF) para derivar chaves por chamada para cada criptografia sob um AWS KMS key. Todas as operações de KDF usam a KDF no modo contador usando o HMAC [FIPS197] com SHA256 [FIPS180]. A chave derivada de 256 bits é usada com AES-GCM para criptografar ou descriptografar dados e chaves do cliente.

Uso interno de assinaturas digitais no AWS KMS

Assinaturas digitais também são usadas para autenticar comandos e comunicações entre entidades do AWS KMS. Todas as entidades de serviço têm um par de chaves de algoritmo de assinatura digital de curva elíptica (ECDSA). Elas executam o ECDSA conforme definido na Uso de algoritmos de criptografia de curva elíptica (ECC) na sintaxe de mensagem criptográfica (CMS) e X9.62-2005: Criptografia de chave pública para o setor de serviços financeiros: o algoritmo de assinatura digital de curva elíptica (ECDSA). As entidades usam o algoritmo de hash seguro definido nas Publicações de padrões federais de processamento de informações, FIPS PUB 180-4, conhecido como SHA384. As chaves são geradas na curva secp384r1 (NIST-P384).

criptografia envelopada

Uma construção básica usada em muitos sistemas criptográficos é a criptografia de envelope. A criptografia de envelope usa duas ou mais chaves criptográficas para proteger uma mensagem. Normalmente, uma chave é derivada a partir de uma chave estática de longo prazo k, e outra chave é uma chave por mensagem msgKey, que é gerada para criptografar a mensagem. O envelope é formado criptografando a mensagem: texto cifrado = Criptografia(msgKey, mensagem). Em seguida, a chave de mensagem é criptografada com a chave estática de longo prazo:encKey = Criptografia(k, msgKey). Por fim, os dois valores (encKey, texto cifrado) são empacotados em uma única estrutura, ou mensagem criptografada de envelope.

O destinatário, com acesso a k, pode abrir a mensagem envolta primeiro descriptografando a chave criptografada e depois descriptografando a mensagem.

O AWS KMS fornece a capacidade de gerenciar essas chaves estáticas de longo prazo e automatizar o processo de criptografia de envelope dos seus dados.

Além dos recursos de criptografia fornecidos no serviço AWS KMS, o AWSSDK de criptografia fornece bibliotecas de criptografia de envelope do lado do cliente. Você pode usar essas bibliotecas para proteger os seus dados e as chaves de criptografia usadas para criptografar esses dados.

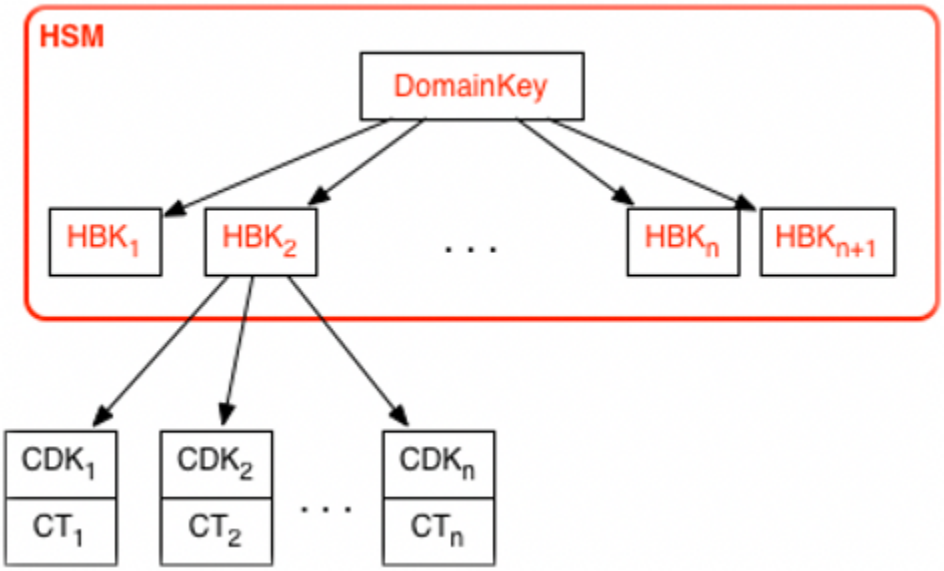
Hierarquia do AWS KMS key

A sua hierarquia de chaves começa com uma chave lógica de nível superior, um AWS KMS key. Uma chave KMS representa um contêiner para o material de chave de nível superior e é definida exclusivamente dentro do namespace de serviço AWS com um Nome do Recurso Amazon (ARN). O ARN inclui um identificador de chave gerado exclusivamente, um ID de chave. Uma chave KMS é

criada com base em uma solicitação iniciada pelo usuário por meio do AWS KMS. Após a recepção, o AWS KMS solicita a criação de uma chave de apoio HSM (HBK) inicial a ser colocada no contêiner de chaves KMS. O HBK é gerado em um HSM no domínio e foi projetado para nunca ser exportado do HSM em texto simples. Em vez disso, o HBK é exportado criptografado em chaves de domínio gerenciadas por HSM. Esses HBKs exportados são chamados de tokens de chave exportados (EKTs).

O EKT é exportado para um armazenamento altamente durável e de baixa latência. Por exemplo, suponha que você receba um ARN para a chave KMS lógica. Para você, isso representa o topo de uma hierarquia de chaves, ou contexto criptográfico. Você pode criar várias chaves KMS em sua conta e definir políticas em suas chaves KMS como qualquer outro recurso nomeado do AWS.

Dentro da hierarquia de uma chave KMS específica, o HBK pode ser considerado uma versão da chave KMS. Quando você deseja alternar a chave KMS através do AWS KMS, um novo HBK é criado e associado à chave KMS como o HBK ativo para a chave KMS. Os HBKs mais antigos são preservados e podem ser usados para descriptografar e verificar dados previamente protegidos. Mas somente a chave criptográfica ativa pode ser usada para proteger novas informações.



Você pode fazer solicitações por meio do AWS KMS para usar as suas chaves KMS para proteger diretamente as informações ou solicitar chaves adicionais geradas por HSM protegidas sob a sua chave KMS. Essas chaves são chamadas de chaves de dados do cliente, ou CDKs. As CDKs podem ser retornadas criptografadas como texto cifrado (CT), em texto simples ou ambos. Todos os objetos criptografados sob uma chave KMS (dados fornecidos pelo cliente ou chaves geradas pelo HSM) podem ser descriptografados somente em um HSM por meio de uma chamada através do AWS KMS.

O texto cifrado retornado, ou a carga descriptografada, nunca é armazenado no AWS KMS. As informações são retornadas a você através da sua conexão TLS com o AWS KMS. Isso também se aplica a chamadas feitas em seu nome pelos serviços do AWS.

A hierarquia de chaves e as propriedades específicas de chave aparecem na tabela a seguir.

Chave	Descrição	Ciclo de vida
Chave de domínio	Uma chave AES-GCM de 256 bits somente na memória de um HSM usado para quebrar versões das chaves KMS, as chaves de reserva HSM.	Alternado diariamente[1]
Chave de reserva HSM	Uma chave simétrica de 256 bits ou chave privada RSA ou curva elíptica, usada para proteger dados e chaves do cliente e armazenada criptogra fada sob chaves de domínio. Uma ou mais chaves de apoio HSM formam a chave KMS, representada pelo keyID.	Alternadas anualmente[2] (configuração opcional)
Chave de criptografia derivada	Uma chave AES-GCM de 256 bits somente na memória de um HSM usado para criptografar dados e chaves do cliente. Derivado de um HBK para cada criptografia.	Usado uma vez por criptografia e regenerado ao descriptografar
Chave de dados do cliente	Chave simétrica ou assimétrica definida pelo usuário exportada do HSM em texto simples e texto cifrado. Criptografado com uma chave de reserva HSM e retornado aos usuários autorizados pelo canal TLS.	Alternância e uso controlados por aplicação

[1] O AWS KMS pode, de tempos em tempos, relaxar a alternância da chave de domínio para, no máximo, semanalmente, para lidar com tarefas de administração e configuração do domínio.

[2] O Padrão Chaves gerenciadas pela AWS criado e gerenciado pelo AWS KMS em seu nome é alternado automaticamente cada ano.

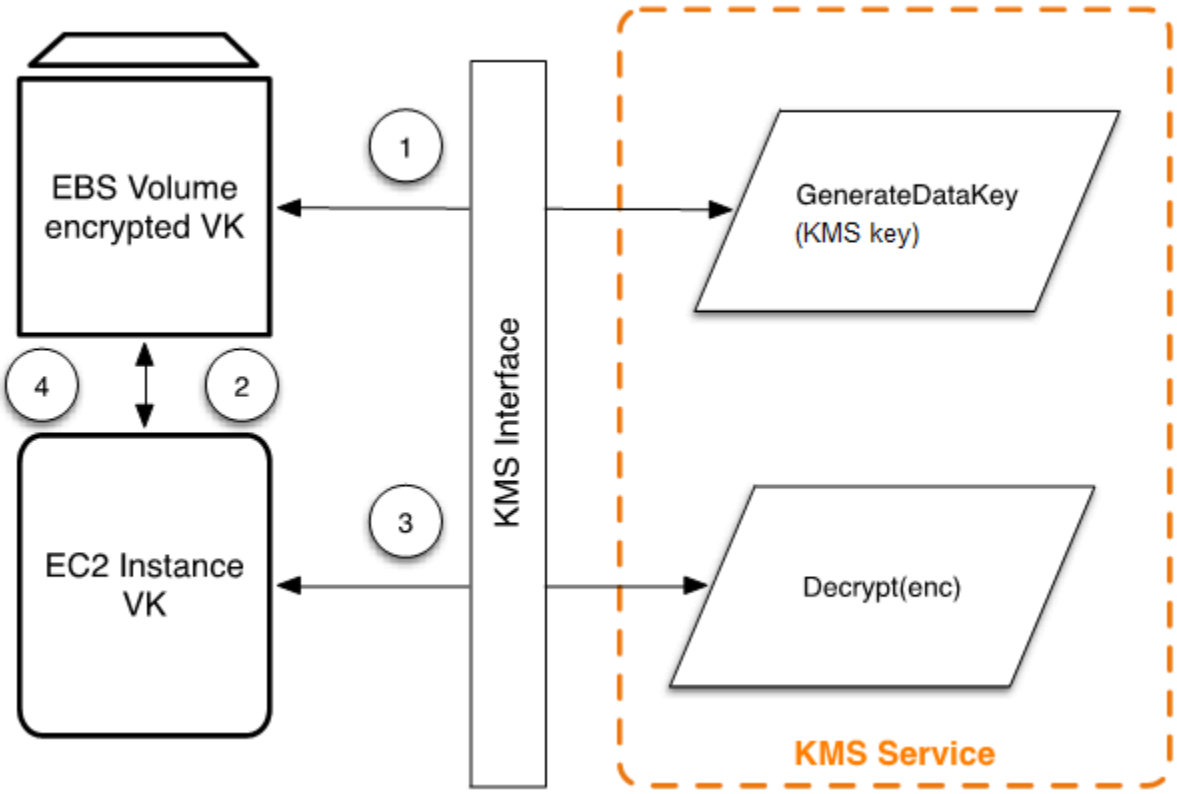
Casos de uso do AWS KMS

Os casos de uso podem ajudar a obter o máximo do AWS Key Management Service. O primeiro demonstra a performance do AWS KMS para criptografia no lado do servidor com AWS KMS keys em um volume do Amazon Elastic Block Store (Amazon EBS). O segundo é uma aplicação do lado do cliente que demonstra como você pode usar a criptografia de envelope para proteger o conteúdo com o AWS KMS.

Tópicos

Criptografia de volume do Amazon EBS

O Amazon EBS oferece capacidade de criptografia de volume. Cada volume é criptografado usando o AES-256-XTS. Isso requer duas chaves de volume de 256 bits, que você pode considerar como uma chave de volume de 512 bits. A chave de volume é criptografada sob uma chave KMS em sua conta. Para que o Amazon EBS criptografe um volume para você, ele deve ter acesso para gerar uma chave de volume (VK) sob uma chave KMS na conta. Você pode fazer isso fornecendo uma concessão para o Amazon EBS para a chave KMS para criar chaves de dados e criptografar e descriptografar essas chaves de volume. Agora, o Amazon EBS usa o AWS KMS com uma chave do KMS para gerar chaves de volume AWS KMS criptografadas.



O fluxo de trabalho a seguir criptografa os dados que estão sendo gravados em um volume do Amazon EBS:

1. O Amazon EBS obtém uma chave de volume criptografada em uma chave KMS por meio do AWS KMS em uma sessão TLS e armazena a chave criptografada com os metadados do volume.
2. Quando o volume do Amazon EBS é montado, a chave de volume criptografada é recuperada.
3. Uma chamada para o AWS KMS através de TLS é feita para descriptografar a chave de volume criptografada. O AWS KMS identifica a chave KMS e faz uma solicitação interna a um HSM na frota para descriptografar a chave de volume criptografada. Em seguida, o AWS KMS retorna a chave de volume para o host do Amazon Elastic Compute Cloud (Amazon EC2) que contém a sua instância na sessão do TLS.
4. A chave de volume é usada para criptografar e descriptografar todos os dados enviados e recebidos do volume do Amazon EBS anexado. O Amazon EBS retém a chave de volume criptografada para uso posterior caso a chave de volume na memória não esteja mais disponível.

Para obter mais informações sobre como criptografar volumes do Amazon EBS com chaves do KMS, consulte Como o Amazon Elastic Block Store usa AWS KMS no Guia do desenvolvedor do AWS

Key Management Service e Criptografia do Amazon EBS no Guia do usuário do Amazon EC2 para instâncias do Linux e no Guia do usuário do Amazon EC2 para instâncias do Windows.

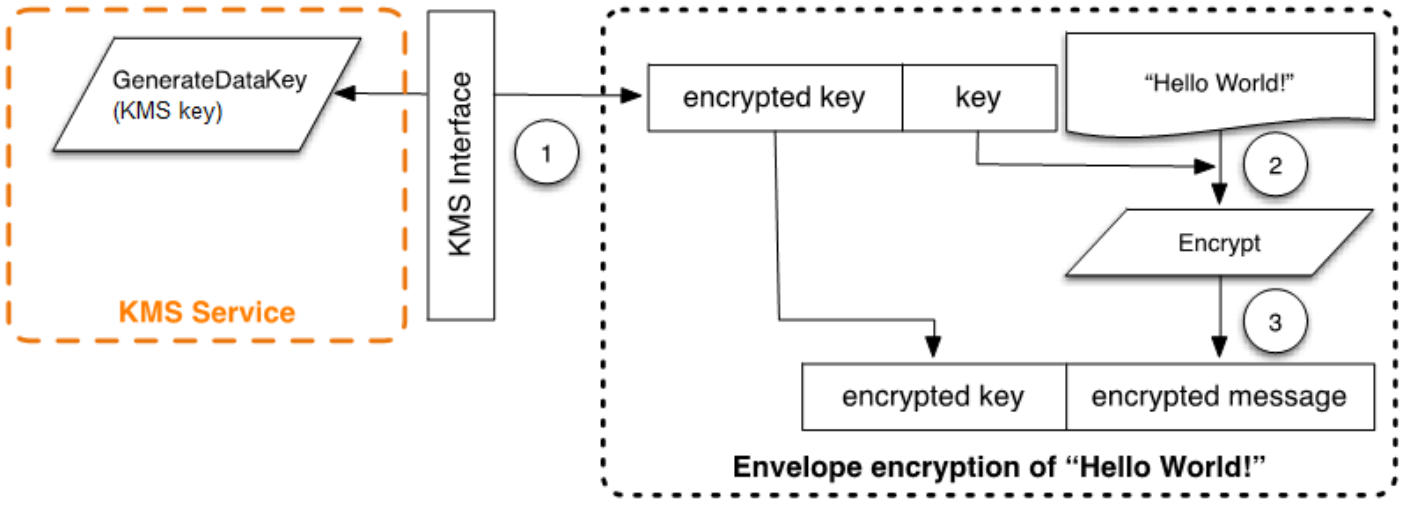
Criptografia do lado do cliente

O AWS Encryption SDK inclui uma operação de API para executar criptografia de envelope usando uma chave KMS. Para obter recomendações completas e detalhes de uso, consulte a documentação relacionada. Os aplicativos do cliente podem usar o AWS Encryption SDK para executar criptografia de envelope usando o 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);
```

A aplicação do cliente pode executar as etapas a seguir:

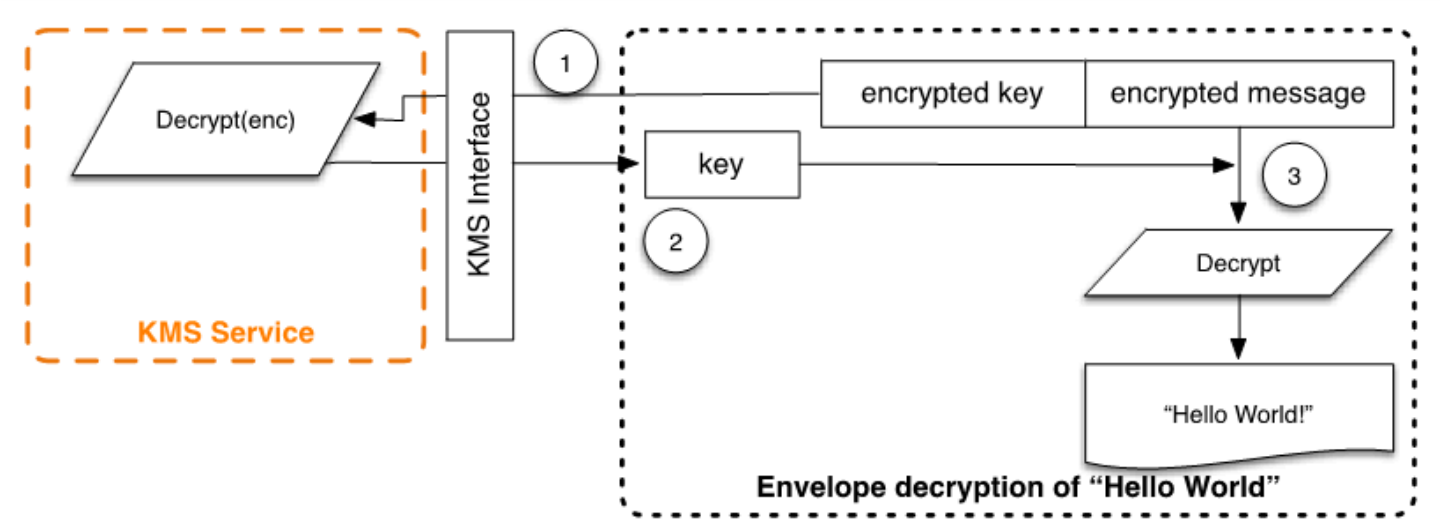
1. Uma solicitação é feita sob uma chave KMS para uma nova chave de dados. Uma chave de dados criptografada e uma versão em texto simples da chave de dados são retornados.
2. No AWS Encryption SDK, a chave de dados de texto simples é usada para criptografar a mensagem. Então, a chave de dados de texto simples é excluída da memória.
3. A chave de dados e mensagem criptografadas são combinadas em uma única matriz de bytes de texto cifrado.



A mensagem criptografada com envelope pode ser descriptografada usando a funcionalidade de descriptografia para obter a mensagem criptografada 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. O AWS Encryption SDK analisa a mensagem criptografada com envelope para obter a chave de dados criptografada e fazer uma solicitação para o AWS KMS descriptografar a chave de dados.
2. O AWS Encryption SDK recebe a chave de dados de texto simples do AWS KMS.
3. A chave de dados é, então, usada para descriptografar a mensagem, com retorno do texto simples inicial.

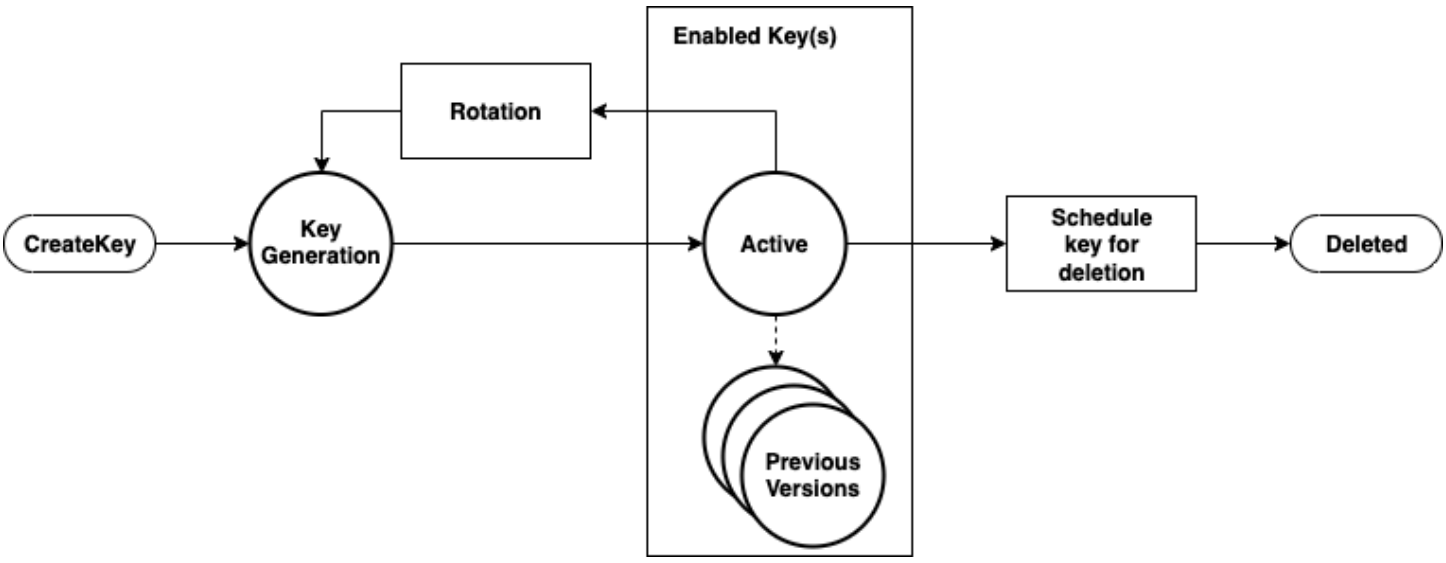


Trabalhar com o AWS KMS keys

Uma AWS KMS key refere-se a uma chave lógica que pode se referenciar a uma ou mais chaves de reserva (HBKs) do módulo de segurança de hardware (HSM). Este tópico explica como criar uma chave do KMS, importar materiais de chave, bem como habilitar, desabilitar, alternar e excluir chaves do KMS.

> **Note**
>
> AWS KMS está substituindo o termo chave mestre do cliente (CMK) por AWS KMS key e Chave KMS. O conceito não mudou. Para evitar alterações interrompidas, o AWS KMS está mantendo algumas variações deste termo.

Este capítulo discute o ciclo de vida de uma chave do KMS, desde a criação até exclusão, como mostra a imagem a seguir.



Tópicos

Chamando CreateKey

Um AWS KMS key é gerado como resultado de uma chamada para o método de Chamada de API `CreateKey`.

Veja a seguir um subconjunto da sintaxe da solicitação `CreateKey`.

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

A solicitação aceita os dados a seguir no formato JSON.

Descrição

(Opcional) Descrição da chave. Recomendamos que você escolha uma descrição que ajude a decidir se a chave é apropriada para uma tarefa.

KeySpec

Especifica o tipo de chave do KMS a ser criado. O valor padrão, SYMMETRIC_DEFAULT, cria uma chave do KMS com criptografia simétrica. Esse parâmetro é opcional para chaves de criptografia simétrica e é obrigatório para todas as outras especificações de chaves.

KeyUsage

Especifica o uso da chave. Os valores válidos são `ENCRYPT_DECRYPT`, `SIGN_VERIFY` ou `GENERATE_VERIFY_MAC`. O valor padrão é `ENCRYPT_DECRYPT`. Esse parâmetro é opcional para chaves de criptografia simétrica e é obrigatório para todas as outras especificações de chaves.

Origem

(Opcional) Especifica a origem do material de chave da chave do KMS. O valor padrão é `AWS_KMS`, indicando que o AWS KMS gera e gerencia o material de chave para a chave do KMS. Outros valores válidos são `EXTERNAL`, que representa uma chave do KMS criada sem materiais de chave para materiais de chave importados, e `AWS_CLOUDHSM`, que cria uma chave do KMS em um armazenamento de chaves personalizado com o suporte de um cluster do AWS CloudHSM controlado por você.

Política

(Opcional) Política a anexar à chave. Se a política for omitida, a chave será criada com a política padrão (a seguir) que permite que a conta raiz e as entidades principais do IAM com permissões do AWS KMS a gerenciem.

Para obter mais detalhes sobre a política, consulte Políticas de chaves no AWS KMS e Política de chave padrão, no Guia do desenvolvedor do AWS Key Management Service.

A solicitação `CreateKey` retorna uma resposta que inclui um ARN de chave.

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

Se `Origin` for `AWS_KMS`, depois que o ARN for criado, será feita uma solicitação para um HSM do AWS KMS em uma sessão autenticada para provisionar uma chave de reserva (HBK) do módulo de segurança de hardware (HSM). O HBK é uma chave de 256 bits que está associada a essa ID de chave da chave do KMS. Ele pode ser gerado apenas em um HSM e foi projetado para nunca ser exportado fora do limite do HSM em texto simples. O HBK é criptografado com a chave de domínio atual, DK_0. Esses HBKs criptografados são referenciados como tokens de chave criptografados (EKTs). Embora os HSMs possam ser configurados para usar vários métodos de encapsulamento de chaves, a implementação atual usa o AES-256 no Galois Counter Mode (GCM), um esquema de criptografia autenticada. O modo de criptografia autenticada permite proteger alguns metadados de tokens de chaves exportados em texto simples.

Isso é representado estilisticamente como:

$$EKT = Encrypt(DK_0, HBK)$$

Duas formas fundamentais de proteção são fornecidas para suas chaves KMS e HBKs subsequentes: políticas de autorização definidas em suas chaves KMS e as proteções criptográficas em seus HBKs associados. As demais seções descrevem as proteções criptográficas e a segurança das funções de gerenciamento no AWS KMS.

Além do ARN, você pode criar um nome fácil de usar e associá-lo à chave do KMS criando um alias para a chave. Depois que um alias tiver sido associado a uma chave do KMS, ele poderá ser usado para identificar essa chave em operações criptográficas. Para obter informações detalhadas, consulte Usar aliases, no Guia do desenvolvedor do AWS Key Management Service.

Vários níveis de autorizações envolvem o uso de chaves KMS. O AWS KMS permite políticas de autorização separadas entre o conteúdo criptografado e a chave KMS. Por exemplo, um objeto criptografado em envelope AWS KMS do Amazon Simple Storage Service (Amazon S3) herda a política no bucket do Amazon S3. No entanto, o acesso à chave de criptografia necessária é determinado pela política de acesso na chave KMS. Para obter mais informações sobre como autorizar chaves do KMS, consulte Autenticação e controle de acesso para o AWS KMS, no Guia do desenvolvedor do AWS Key Management Service.

Importar o material de chave

O AWS KMS fornece um mecanismo para importar o material criptográfico usado para um HBK. Conforme descrito emChamando CreateKey, quando o CreateKey comando é usado com `Origin` set to`EXTERNAL`, é criada uma chave KMS lógica que não contém nenhum HBK subjacente. O material criptográfico deve ser importado usando a chamada de API do `ImportKeyMaterial`. Você pode usar esse recurso para controlar a criação de chaves e a durabilidade do material criptográfico. Se você usar esse recurso, recomendamos que tome bastante cuidado no manuseio e durabilidade dessas chaves em seu ambiente. Para obter detalhes completos e recomendações sobre a importação de material chave, consulte Importar o material de chave no Guia do desenvolvedor AWS Key Management Service.

Chamando ImportKeyMaterial

A solicitação do `ImportKeyMaterial` importa o material criptográfico necessário para o HBK. O material criptográfico deve ser uma chave simétrica de 256 bits. Ela deve ser criptografada usando o algoritmo especificado em `WrappingAlgorithm` sob a chave pública retornada de uma solicitação recente do `GetParametersForImport`.

Uma solicitação `ImportKeyMaterial` usa os seguintes argumentos:

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

EncryptedKeyMaterial

O material de chave importada, criptografado com a chave pública retornada em uma solicitação `GetParametersForImport` usando o algoritmo de encapsulamento especificado nessa solicitação.

ExpirationModel

Especifica se o material de chave expira. Quando este valor é `KEY_MATERIAL_EXPIRES`, o parâmetro `ValidTo` deve conter uma data de validade. Quando este valor é `KEY_MATERIAL_DOES_NOT_EXPIRE`, não inclua o parâmetro `ValidTo`. Os valores válidos são `"KEY_MATERIAL_EXPIRES"` e `"KEY_MATERIAL_DOES_NOT_EXPIRE"`.

ImportToken

O token de importação retornado pela mesma solicitação `GetParametersForImport` que forneceu a chave pública.

KeyId

A chave do KMS que será associada ao material de chave importado. O `Origin` da chave KMS deve ser `EXTERNAL`.

É possível excluir e reimportar o mesmo material de chave importado para a chave do KMS especificada, mas não é possível importar ou associar a chave do KMS a nenhum outro material de chave.

ValidTo

(Opcional) O horário em que o material de chave importada perde a validade. Quando o material de chave perde a validade, o AWS KMS exclui o material de chave e a chave KMS se torna inutilizável. Esse parâmetro é necessário quando o valor de `ExpirationModel` é `KEY_MATERIAL_EXPIRES`. Caso contrário, ele será inválido.

Quando a solicitação for bem-sucedida, a chave do KMS ficará disponível para uso no AWS KMS até a data de expiração especificada, se fornecida. Depois que o material de chave importado expirar, o EKT é excluído da camada de armazenamento do AWS KMS.

Habilitar e desabilitar chaves

O ato de desabilitar uma chave do KMS impede que ela seja usada em operações de criptografia. Isso suspende a capacidade de utilizar todas as HBKs associadas à chave do KMS. O ato de

habilitá-las restaura o uso das HBKs e da chave do KMS. Enable e Disable são solicitações simples que usam apenas o ID de chave ou o ARN de chave da chave do KMS.

Excluir chaves

Usuários autorizados podem usar a API `ScheduleKeyDeletion` para agendar a exclusão de uma chave do KMS e de todas as HBKs associadas. Esta é uma operação inerentemente destrutiva, e você deve ter cuidado ao excluir chaves do AWS KMS. O AWS KMS impõe um tempo de espera mínimo de sete dias ao excluir chaves KMS. Durante o período de espera, a chave é colocada em um estado desativado com um estado de chave Exclusão pendente. Todas as chamadas para usar a chave para operações criptográficas falharão. ScheduleKeyDeletion usa os seguintes argumentos.

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

KeyId

O identificador exclusivo da chave KMS que será excluída. Para especificar esse valor, use o ID de chave exclusivo ou o ARN de chave da chave KMS.

PendingWindowInDays

(Opcional) O período de espera, em número de dias. Este valor é opcional. O intervalo é de 7 a 30 dias, e o valor padrão é de 30 dias. Após o término do período de espera, o AWS KMS exclui a chave KMS e todos os HBKs associados.

Alternar material de chave

Os usuários autorizados podem ativar a rotação anual automática de suas chaves do KMS gerenciadas pelo cliente. Chaves gerenciadas pela AWS sempre são alternadas todos os anos.

Quando uma chave do KMS é alternada, uma nova HBK é criada e marcada como a versão atual do material de chave para todas as novas solicitações de criptografia. Todas as versões anteriores da HBK permanecem disponíveis para uso permanente com o objetivo de descriptografar qualquer texto cifrado que tenha sido criptografado usando uma versão da HBK. Como o AWS KMS não armazena texto cifrado criptografado em uma chave do KMS, os textos cifrados criptografados com uma HBK mais antiga e alternada exigem que essa HBK os descriptografem. Você pode usar a API

`ReEncrypt` para criptografar novamente qualquer texto cifrado com a nova HBK para a chave do KMS ou com uma chave do KMS diferente sem expor o texto simples.

Para obter mais informações sobre como habilitar e desabilitar a alternância de chaves, consulte Alternar chaves do AWS KMS, no Guia do desenvolvedor do AWS Key Management Service.

Operações de dados do cliente

Depois de estabelecer uma chave KMS, você pode usá-la para executar operações criptográficas. Sempre que os dados são criptografados sob uma chave KMS, o objeto resultante é um texto cifrado do cliente. O texto cifrado contém duas seções: uma parte de cabeçalho não criptografado (ou texto simples), protegida pelo esquema de criptografia autenticado como os dados autenticados adicionais e uma parte criptografada. A parte de texto não criptografado inclui o identificador HBK (HBKID). Esses dois campos imutáveis do valor de texto cifrado ajudam a garantir que o AWS KMS poderá descriptografar o objeto no futuro.

Tópicos

Gerando chaves de dados

Usuários autorizados podem usar a GenerateDataKey API (e as APIs relacionadas) para solicitar um tipo específico de chave de dados ou uma chave aleatória de tamanho arbitrário. Este tópico oferece uma visão simplificada dessa operação de API. Para obter detalhes, consulte as GenerateDataKey APIs na Referência da AWS Key Management Service API.

- GenerateDataKey
- GenerateDataKeyWithoutPlaintext
- GenerateDataKeyPair
- GenerateDataKeyPairWithoutPlaintext

Veja, a seguir, a sintaxe de solicitação do `GenerateDataKey`.

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

```
}
```

A solicitação aceita os dados a seguir no formato JSON.

KeyId

Identificador de chave da chave usada para criptografar a chave de dados. O valor deve identificar uma chave do KMS de criptografia simétrica.

Este parâmetro é obrigatório.

NumberOfBytes

Um inteiro que contém o número de bytes a serem gerados. Este parâmetro é obrigatório.

O autor da chamada deve fornecer `KeySpec` ou `NumberOfBytes`, mas não ambos.

EncryptionContext

(Opcional) Nome: par de valores que contém dados adicionais para autenticar durante os processos de criptografia e descriptografia que usam a chave.

GrantTokens

(Opcional) Uma lista de tokens de concessão que representam concessões que fornecem permissões para geração ou uso de uma chave. Para obter mais informações sobre concessões e tokens de concessão, consulte Autenticação e controle de acesso para o AWS KMS no Guia do desenvolvedor do AWS Key Management Service.

Depois de autenticar o comando, AWS KMS, adquire o EKT ativo atual associado à chave KMS. Ele envia o EKT junto com sua solicitação fornecida e qualquer contexto de criptografia para um HSM em uma sessão protegida entre o host AWS KMS e um HSM no domínio.

O HSM faz o seguinte:

1. Gera o material secreto solicitado e mantém esse material na memória volátil.
2. Descriptografa o EKT fazendo a correspondência do ID de chave da chave KMS definida na solicitação para obter o HBK = Descriptografia(DK_i, EKT) ativo.
3. Gera um nonce N aleatório.
4. Gera uma chave de criptografia derivada do AES-GCM de 256 bits K de HBK e N.
5. Criptografa o material secreto texto cifrado = Criptografia(K, contexto, segredo).

O `GenerateDataKey` retorna o material secreto de texto simples e o texto cifrado a você através do canal seguro entre o host AWS KMS e o HSM. Em seguida, o AWS KMS envia esse material para você através da sessão TLS. O AWS KMS não retém o texto sem formatação ou texto cifrado. Sem a posse do texto cifrado, do contexto de criptografia e da autorização para usar a chave KMS, o segredo subjacente não pode ser retornado.

Veja, a seguir, a sintaxe de resposta.

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

O gerenciamento de chaves de dados é deixado para você como o desenvolvedor do aplicativo. Para a melhor prática de criptografia no lado do cliente com chaves de dados do AWS KMS (mas não pares de chaves de dados), é possível utilizar o AWS Encryption SDK.

Chaves de dados podem ser alternadas em qualquer frequência. Além disso, a chave de dados em si pode ser recriptografada para uma chave KMS diferente ou uma chave KMS alternada usando a operação da API do `ReEncrypt`. Para obter detalhes, consulte ReEncrypta Referência AWS Key Management Service da API.

Encrypt

Uma função básica do AWS KMS é criptografar um objeto sob uma chave KMS. Por projeto, o AWS KMS fornece operações criptográficas de baixa latência HSMs. Portanto, há um limite de 4 KB na quantidade de texto simples que pode ser criptografado em uma chamada direta para a função de criptografia. O AWS Encryption SDK pode ser usado para criptografar mensagens maiores. O AWS KMS, depois de autenticar o comando, adquire o atual EKT ativo pertencente à chave KMS. Ele passa o EKT, junto com o texto simples e o contexto de criptografia, para qualquer HSM disponível na região. Estes são enviados através de uma sessão autenticada entre o host AWS KMS e um HSM no domínio.

O HSM executa o seguinte:

1. Descriptografa o EKT para obter o HBK = Descriptografia(DK_i, EKT).
2. Gera um nonce N aleatório.
3. Deriva uma chave de criptografia derivada do AES-GCM de 256 bits K de HBK e N.

4. Criptografa o texto simples texto cifrado = Criptografia(K, contexto, texto simples).

O valor de texto cifrado é retornado para você, e nem os dados de texto simples ou cifrado são retidos em qualquer lugar na infraestrutura AWS. Sem a posse do texto cifrado e do contexto de criptografia e a autorização para usar a chave KMS, o texto simples subjacente não pode ser retornado.

Decrypt

Uma chamada para o AWS KMS descriptografar um valor de texto cifrado aceita um valor de texto cifrado e um contexto de criptografia. O AWS KMS autentica a chamada usando as solicitações de assinatura AWS versão 4 assinadas e extrai o HBKID da chave de quebra de texto cifrado. O HBKID é usado para obter o EKT necessário para descriptografar o texto cifrado, o ID da chave e a política para o ID da chave. A solicitação é autorizada com base na política de chaves, concessões que podem estar presentes e quaisquer políticas do IAM associadas que façam referência ao ID da chave. A função `Decrypt` é análoga à função de criptografia.

Veja a seguir a sintaxe de solicitação do `Decrypt`.

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

Os parâmetros de solicitação são os seguintes.

CiphertextBlob

Texto cifrado incluindo metadados.

EncryptionContext

(Opcional) O contexto de criptografia. Se isso foi especificado na função `Encrypt`, deve ser especificado aqui ou a operação de descriptografia falhará. Para obter mais informações, consulte Contexto de criptografia no Guia do desenvolvedor AWS Key Management Service.

GrantTokens

(Opcional) Uma lista de tokens de concessão que representam concessões que fornecem permissões para executar a descriptografia.

O texto cifrado e o EKT são enviados, juntamente com o contexto de criptografia, por uma sessão autenticada para um HSM para descriptografia.

O HSM executa o seguinte:

1. Descriptografa o EKT para obter o HBK = Descriptografia(DK_i, EKT) .
2. Extrai o nonce N da estrutura do texto cifrado.
3. Regenera uma chave de criptografia derivada do AES-GCM de 256 bits K de HBK e N.
4. Descriptografa o texto cifrado para obter o texto simples = Descriptografia(K, contexto, texto cifrado) .

O ID de chave resultante e o texto simples são retornados para o host AWS KMS durante a sessão segura e, em seguida, de volta para a aplicação do cliente autor da chamada através de uma conexão TLS.

Veja, a seguir, a sintaxe de resposta.

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

Se a aplicação de chamada quiser garantir a autenticidade do texto simples, ela deve verificar se o ID de chave retornado é o esperado.

Criptografando novamente um objeto criptografado

Um texto cifrado de cliente existente criptografado em uma chave KMS pode ser criptografado novamente para outra chave KMS por meio de um comando reencrypt. O comando Reencrypt criptografa dados no servidor com uma nova chave KMS sem expor o texto simples dos dados no lado do cliente. Primeiro os dados são descriptografados e, depois, criptografados.

Veja, a seguir, a sintaxe de solicitação.

```
{
 "CiphertextBlob": "blob",
 "DestinationEncryptionContext": { "string" : "string" },
 "DestinationKeyId": "string",
```

```
 "GrantTokens": ["string"],
       "SourceKeyId": "string",
 "SourceEncryptionContext": { "string" : "string"}
}
```

A solicitação aceita os dados a seguir no formato JSON.

CiphertextBlob

Texto cifrado dos dados a serem criptografados novamente.

DestinationEncryptionContext

(Opcional) Contexto de criptografia a ser usado quando os dados são recriptografados.

DestinationKeyId

Identificador de chave da chave usada para criptografar novamente os dados.

GrantTokens

(Opcional) Uma lista de tokens de concessão que representam concessões que fornecem permissões para executar a descriptografia.

SourceKeyId

(Opcional) Identificador de chave da chave usada para descriptografar os dados.

SourceEncryptionContext

(Opcional) Contexto de criptografia usado para criptografar e descriptografar os dados especificados no parâmetro `CiphertextBlob`.

O processo combina as operações de descriptografia e criptografia das descrições anteriores: o texto cifrado do cliente é descriptografado sob o HBK inicial referenciado pelo texto cifrado do cliente para o HBK atual sob a chave KMS pretendida. Quando as chaves KMS usadas neste comando são as mesmas, esse comando move o texto cifrado do cliente de uma versão antiga de um HBK para a versão mais recente de um HBK.

Veja, a seguir, a sintaxe de resposta.

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

```
    "KeyId": "string",
    "SourceEncryptionAlgorithm": "string",
    "SourceKeyId": "string"
}
```

Se o aplicativo de chamada quiser garantir a autenticidade do texto simples subjacente, ele deverá verificar se o SourceKeyId retornado é o esperado.

Operações internas do AWS KMS

As operações internas do AWS KMS são necessárias para escalar e proteger HSMs para um serviço de gerenciamento de chaves distribuído globalmente.

Tópicos

Domínios e estado do domínio

Uma coleção cooperativa de entidades internas confiáveis do AWS KMS dentro de um Região da AWS é chamada de um domínio. Um domínio inclui um conjunto de entidades confiáveis, um conjunto de regras e um conjunto de chaves secretas, chamadas chaves de domínio. As chaves de domínio são compartilhadas entre HSMs que são membros do domínio. Um estado de domínio consiste nos campos a seguir.

Nome

Um nome de domínio para identificar este domínio.

Membros

Uma lista de HSMs que são membros do domínio, incluindo sua chave de assinatura pública e chaves de acordo público.

Operadores

Uma lista de entidades, chaves de assinatura pública e uma função (operador do AWS KMS ou host de serviço) que representa os operadores deste serviço.

Regras

Uma lista de regras de quórum para cada comando que deve ser satisfeita para executar um comando no HSM.

Chaves de domínio

Uma lista de chaves de domínio (chaves simétricas) atualmente em uso no domínio.

O estado completo do domínio está disponível apenas no HSM. O estado do domínio é sincronizado entre os membros do domínio HSM como um token de domínio exportado.

Chaves de domínio

Todos os HSMs em um domínio compartilham um conjunto de chaves de domínio, $\{DK_r\}$. Essas chaves são compartilhadas por meio de uma rotina de exportação de estado de domínio. O estado do domínio exportado pode ser importado para qualquer HSM membro do domínio.

O conjunto de chaves de domínio, $\{DK_r\}$, sempre inclui uma chave de domínio ativa e várias chaves de domínio desativadas. As chaves de domínio são alternadas diariamente para garantir que o AWS está em conformidade com a Recomendação para o gerenciamento de chaves - Parte 1. Durante a alternância das chaves de domínio, todas as chaves KMS existentes criptografadas sob a chave de domínio de saída são criptografadas novamente sob a nova chave de domínio ativa. A chave de domínio ativa é usada para criptografar quaisquer novos EKTs. As chaves de domínio expiradas podem ser usadas apenas para descriptografar EKTs previamente criptografados por um número de dias equivalente ao número de chaves de domínio recentemente alternadas.

Tokens de domínio exportados

Há uma necessidade regular de sincronizar o estado entre os participantes do domínio. Isso é feito através da exportação do estado do domínio sempre que uma alteração é feita no domínio. O estado do domínio é exportado como um token de domínio exportado.

Nome

Um nome de domínio para identificar este domínio.

Membros

Uma lista de HSMs que são membros do domínio, incluindo suas chaves públicas de assinatura e acordo.

Operadores

Uma lista de entidades, chaves de assinatura pública e uma função que representa os operadores deste serviço.

Regras

Uma lista de regras de quórum para cada comando que deve ser satisfeita para executar um comando em um membro do domínio HSM.

Chaves de domínio criptografadas

Chaves de domínio criptografadas por envelope. As chaves de domínio são criptografadas pelo membro de assinatura para cada um dos membros listados acima, envoltas em sua chave de contrato público.

Assinatura

Uma assinatura no estado do domínio produzida por um HSM, necessariamente um membro do domínio que exportou o estado do domínio.

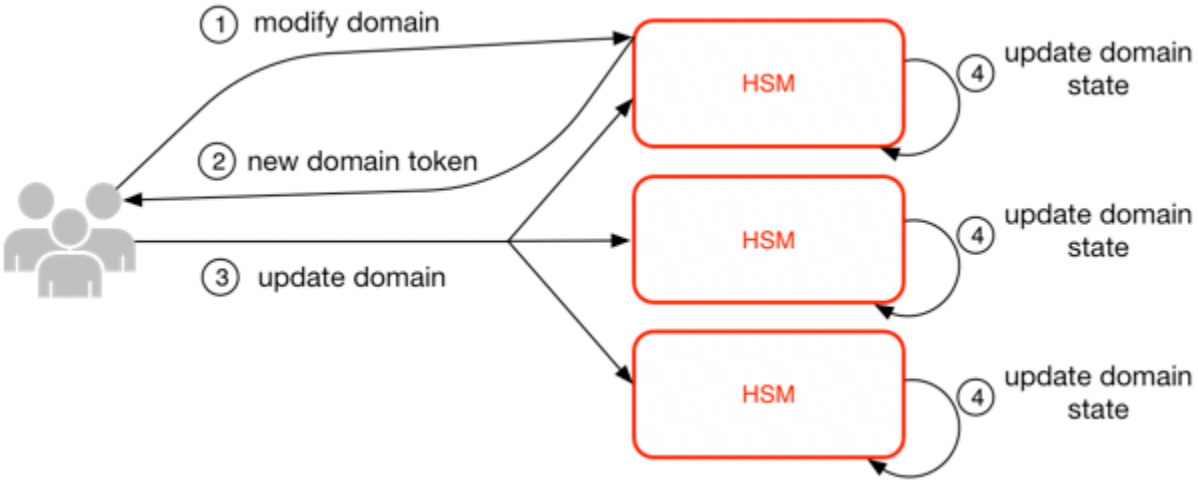
O token de domínio exportado forma a fonte fundamental de confiança para entidades que operam no domínio.

Gerenciar estados de domínio

O estado do domínio é gerenciado por meio de comandos autenticados por quórum. Essas alterações incluem modificar a lista de participantes confiáveis no domínio, modificar as regras de quórum para executar comandos HSM e alternar periodicamente as chaves de domínio. Esses comandos são autenticados um a um, e não por meio de operações de sessão autenticada, como mostrado na imagem a seguir.

Em seu estado inicializado e operacional, um HSM contém um conjunto de chaves de identidade assimétricas autogeradas, um par de chaves de assinatura e um par de chaves de estabelecimento de chave. Por um processo manual, um operador do AWS KMS pode estabelecer um domínio inicial a ser criado em um primeiro HSM de uma região. Este domínio inicial consiste em um estado de domínio completo, conforme definido anteriormente neste tópico. Ele é instalado por meio de um comando “join” para cada um dos membros do HSM definidos no domínio.

Depois que um HSM ingressou em um domínio inicial, ele fica vinculado às regras definidas nesse domínio. Essas regras regem os comandos que usam chaves criptográficas do cliente ou fazem alterações no estado do host ou do domínio. As operações de API de sessão autenticada que usam suas chaves criptográficas foram definidas anteriormente.



A imagem anterior mostra como um estado de domínio é modificado. O processo consiste em quatro etapas:

1. Um comando baseado em quórum é enviado para um HSM para modificar o domínio.
2. Um novo estado de domínio é gerado e exportado como um novo token de domínio exportado. O estado no HSM não é modificado, ou seja, a alteração não é promulgada no HSM.
3. Um segundo comando é enviado para cada um dos HSMs no token de domínio recém-exportado para atualizar seu estado de domínio com o novo token de domínio.
4. Os HSMs listados no novo token de domínio exportado podem autenticar o comando e o token de domínio. Eles também podem descompactar as chaves de domínio para atualizar o estado do domínio em todos os HSMs no domínio.

Os HSMs não se comunicam diretamente entre si. Em vez disso, um quórum de operadores solicita uma alteração no estado do domínio que resulta em um novo token de domínio exportado. Um membro de host de serviço do domínio é usado para distribuir o novo estado de domínio para cada HSM no domínio.

A saída e a adesão a um domínio são feitas por meio das funções de gerenciamento do HSM. A modificação do estado do domínio é feita através das funções de gerenciamento de domínio.

Sair do domínio

> Faz com que um HSM saia de um domínio, excluindo da memória todos os resquícios e chaves daquele domínio.

Ingressar no domínio

Faz com que um HSM ingresse em um novo domínio ou atualize seu estado de domínio atual para o novo estado de domínio. O domínio existente é usado como fonte do conjunto inicial de regras para autenticar esta mensagem.

Criar um domínio

Faz com que um novo domínio seja criado em um HSM. Retorna um primeiro token de domínio que pode ser distribuído aos HSMs membros do domínio.

Modificar operadores

Adiciona ou remove operadores da lista de operadores autorizados e suas funções no domínio.

Modificar membros

Adiciona ou remove um HSM da lista de HSMs autorizados no domínio.

Modificar regras

Modifica o conjunto de regras de quórum necessárias para executar comandos em um HSM.

Alternar chaves de domínio

Faz com que uma nova chave de domínio seja criada e marcada como a chave de domínio ativa. Isso move a chave ativa existente para uma chave desativada e remove a chave desativada mais antiga do estado do domínio.

Segurança de comunicação interna

Comandos entre os hosts de serviço ou operadores AWS KMS e HSMs são protegidos por meio de dois mecanismos exibidos em Sessões autenticadas: um método de solicitação assinado por quórum e uma sessão autenticada usando um protocolo de host de serviço HSM.

Os comandos assinados por quórum são projetados para que nenhum operador único possa modificar as proteções de segurança críticas fornecidas pelos HSMs. Os comandos executados nas sessões autenticadas ajudam a garantir que apenas operadores de serviço autorizados possam executar operações envolvendo chaves KMS. Todas as informações secretas vinculadas ao cliente são protegidas na infraestrutura AWS.

Estabelecimento de chaves

Para proteger as comunicações internas, o AWS KMS usa dois métodos de estabelecimento de chave diferentes. O primeiro é definido como C(1, 2, ECC DH) na Recomendação para Esquemas de Estabelecimento de Chave em Par usando Criptografia de Logaritmo Discreto (Revisão 2). Este esquema tem um iniciador com uma chave de assinatura estática. O iniciador gera e assina uma chave efêmera curva elíptica Diffie-Hellman (ECDH) destinada a um destinatário com uma chave de acordo ECDH estática. Este método usa uma chave efêmera e duas chaves estáticas usando ECDH. Essa é a derivação do rótulo C(1, 2, ECC DH). Este método, às vezes, é chamado de ECDH de uma passagem.

O segundo método de estabelecimento de chave é C(2, 2, ECC, DH). Neste esquema, ambas as partes têm uma chave de assinatura estática e geram, assinam e trocam uma chave ECDH efêmera. Este método usa duas chaves estáticas e duas chaves efêmeras, cada uma usando ECDH. Essa é a derivação do rótulo C(2, 2, ECC, DH). Este método é, por vezes, chamado ECDH efêmero ou ECDHE. Todas as chaves ECDH são geradas na curva secp384r1 (NIST-P384).

Limite de segurança do HSM

O limite interno de segurança do AWS KMS é o HSM. O HSM tem uma interface proprietária e nenhuma outra interface física ativa em seu estado operacional. Um HSM operacional é implantado durante a inicialização com as chaves criptográficas necessárias para estabelecer sua função no domínio. Materiais criptográficos sensíveis do HSM são armazenados somente na memória volátil e apagados quando o HSM sai do estado operacional, incluindo desligamentos ou reinicializações intencionais ou não.

As operações da API do HSM são autenticadas por comandos individuais ou por uma sessão confidencial mutuamente autenticada estabelecida por um host de serviço.

Comandos assinados por quórum

Comandos assinados por quórum são emitidos por operadores para os HSMs. Esta seção descreve como os comandos baseados em quórum são criados, assinados e autenticados. Estas regras são bastante simples. Por exemplo, o comando Foo requer dois membros da função Bar para ser autenticado. Há três etapas na criação e verificação de um comando baseado em quórum. A primeira etapa é a criação inicial do comando; a segunda é o envio a operadores adicionais para assinar e a terceira é a verificação e execução.

Com a finalidade de introduzir os conceitos, suponha que existe um conjunto autêntico de chaves públicas e funções do operador $\{QOS_s\}$ e um conjunto de regras de quórum QR = $\{Comando_i, Regra_{\{i, t\}}\}$ onde cada Regra é um conjunto de funções e número mínimo N $\{Função_t, N_t\}$. Para que um comando satisfaça a regra de quórum, o conjunto de dados de comando deve ser assinado por um conjunto de operadores listados em $\{QOS_s\}$ de forma que atendam a uma das regras listadas para esse comando. Como mencionado anteriormente, o conjunto de regras de quórum e operadores são armazenados no estado de domínio e no token de domínio exportado.

Na prática, um signatário inicial assina o comando $Sig_1 = Sign(dO_{p1}, Comando)$. Um segundo operador também assina o comando $Sig_2 = Sign(dO_{p2}, Comando)$. A mensagem duplamente assinada é enviada para um HSM para execução. O HSM executa o seguinte:

1. Para cada assinatura, ele extrai a chave pública do signatário do estado do domínio e verifica a assinatura no comando.
2. Ele verifica se o conjunto de signatários satisfaz a uma regra para o comando.

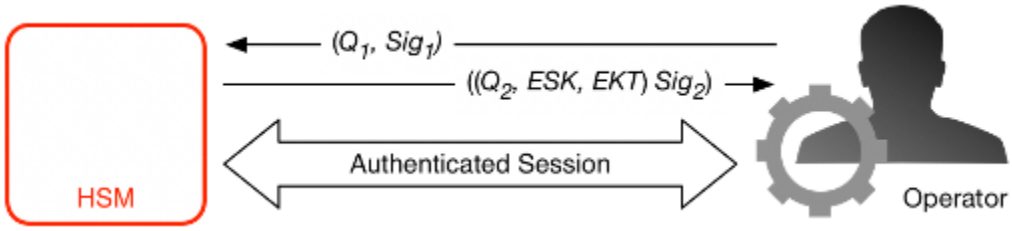
Sessões autenticadas

Suas principais operações-chave são executadas entre os hosts AWS KMS e os HSMs. Esses comandos dizem respeito à criação e uso de chaves criptográficas e geração de números aleatórios seguros. Os comandos são executados em um canal autenticado por sessão entre os hosts de serviço e os HSMs. Além da necessidade de autenticação, essas sessões exigem confidencialidade. Os comandos executados nessas sessões incluem o retorno de chaves de dados de texto não criptografado e mensagens descriptografadas destinadas a você. Para garantir que essas sessões não possam ser subvertidas por meio de man-in-the-middle ataques, as sessões são autenticadas.

Este protocolo executa um contrato de chave ECDHE mutuamente autenticado entre o HSM e o host do serviço. A troca é iniciada pelo host do serviço e concluída pelo HSM. O HSM também retorna uma chave de sessão (SK) criptografada pela chave negociada e um token de chave exportado que

contém a chave de sessão. O token de chave exportado contém um período de validade, após o qual o host de serviço deve renegociar uma chave de sessão.

Um host de serviço é um membro do domínio e tem um par de chaves de assinatura de identidade ($DHOS_i$, $QHOS_i$) e uma cópia autêntica das chaves públicas de identidade dos HSMs. Ele usa seu conjunto de chaves de assinatura de identidade para negociar com segurança uma chave de sessão que pode ser usada entre o host de serviço e qualquer HSM no domínio. Os tokens de chave exportados têm um período de validade associado após o qual uma nova chave deve ser negociada.



O processo começa com o reconhecimento do host de serviço que requer uma chave de sessão para enviar e receber fluxos de comunicação confidenciais entre ele e um membro do HSM do domínio.

1. Um host de serviço gera um par de chaves efêmero ECDH (d_1, Q_1) e o assina com sua chave de identidade Sig1 = Sign(dOS,Q_1).
2. O HSM verifica a assinatura na chave pública recebida usando seu token de domínio atual e cria um par de chaves efêmero ECDH (d_2, Q_2). Em seguida, ele conclui a troca de chaves ECDH de acordo com a Recomendação para Esquemas de Estabelecimento de Chave em Par usando Criptografia de Logaritmo Discreto (Revisado) para formar uma chave AES-GCM de 256 bits negociada. O HSM gera uma nova chave de sessão AES-GCM de 256 bits. Ele criptografa a chave de sessão com a chave negociada para formar a chave de sessão criptografada (ESK). Ele também criptografa a chave de sessão sob a chave de domínio como um token de chave EKT exportado. Finalmente, ele assina um valor de retorno com seu par de chaves de identidade Sig_2 = Sign(dHsK, (Q_2, ESK, EKT)).
3. O host do serviço verifica a assinatura nas chaves recebidas usando seu token de domínio atual. O host de serviço conclui, então, a troca de chaves ECDH de acordo com a Recomendação para Esquemas de Estabelecimento de Chave em Par usando Criptografia de Logaritmo Discreto (Revisado). Em seguida, ele desencripta o ESK para obter a chave de sessão SK.

Durante o período de validade no EKT, o host de serviço pode usar a chave de sessão negociada SK para enviar comandos criptografados com envelope para o HSM. Cada service-host-initiated

comando sobre essa sessão autenticada inclui o EKT. O HSM responde usando a mesma chave de sessão negociada SK.

Processo de replicação para chaves em multirregiões

O AWS KMS usa um mecanismo de replicação entre regiões para copiar o material de chaves em uma chave do KMS de um HSM em uma Região da AWS para um HSM em uma Região da AWS diferente. Para que esse mecanismo funcione, a chave do KMS que está sendo replicada deve ser uma chave multirregião. Ao replicar uma chave do KMS de uma região para outra, os HSMs nas Regiões não podem se comunicar diretamente, porque estão em redes isoladas. Em vez disso, as mensagens trocadas durante a replicação entre regiões são entregues por um serviço proxy.

Durante a replicação entre regiões, todas as mensagens geradas por um HSM do AWS KMS é assinado criptograficamente usando uma chave de assinatura de replicação. As chaves de assinatura de replicação (RSKs) são chaves ECDSA na curva NIST P-384. Cada região possui pelo menos uma RSK, e o componente público de cada RSK é compartilhado com todas as outras regiões na mesma partição da AWS.

O processo de replicação entre regiões para copiar material de chaves da Região A para a Região B funciona da seguinte forma:

1. O HSM na Região B gera uma chave ECDH efêmera na curva NIST P-384, Contrato de replicação da chave B (RAKB). O componente público do RAKB é enviado para um HSM na Região A pelo serviço de proxy.
2. O HSM na Região A recebe o componente público do RAKB e, em seguida, gera outra chave ECDH efêmera na curva NIST P-384, Contrato de replicação da Chave A (RAKA). O HSM executa o esquema de estabelecimento de chave ECDH no RAKA e no componente público do RAKB, e deriva uma chave simétrica da saída, o Empacotamento de replicação de chave (RWK). O RWK é usado para criptografar o material de chaves da chave do KMS de várias regiões que está sendo replicada.
3. O componente público do RAKA e o material de chaves criptografado com o RWK são enviados para o HSM na Região B por meio do serviço de proxy.
4. O HSM na Região B recebe o componente público do RAKA e o material de chaves criptografado usando o RWK. O HSM deriva pela RWK executando o regime de estabelecimento de chave ECDH no RAKB e o componente público do RAKA.
5. O HSM na Região B usa o RWK para descriptografar o material de chaves da Região A.

Proteção de durabilidade

A durabilidade de serviço adicional para chaves geradas pelo serviço é fornecida por HSMs offline, armazenamento múltiplo não volátil de tokens de domínio exportados e armazenamento redundante de chaves KMS criptografadas. Os HSMs offline são membros dos domínios existentes. Com exceção de não estar online e participar de operações regulares de domínio, os HSMs offline aparecem de forma idêntica no estado do domínio como os membros existentes do HSM.

O design de durabilidade destina-se a proteger todas as chaves KMS em uma Região caso o AWS experimente uma perda em larga escala dos HSMs online ou do conjunto de chaves KMS armazenadas em nosso sistema de armazenamento principal. O AWS KMS keys com material de chave importado não está incluído nas proteções de durabilidade oferecidas outras chaves KMS. Em caso de falha em toda a região no AWS KMS, o material de chave importado pode precisar ser reimportado para uma chave KMS.

Os HSMs offline (e as credenciais para acessá-los) são armazenados em cofres dentro de salas seguras monitoradas em várias localizações geográficas independentes. Cada cofre requer pelo menos um oficial de segurança AWS e um operador AWS KMS, de duas equipes independentes no AWS, para obter esses materiais. O uso desses materiais é regido pela política interna que exige um quórum de operadores AWS KMS presentes.

Referência

Use o material de referência a seguir para obter informações sobre abreviações, chaves, colaboradores e fontes citadas neste documento.

Tópicos

Abreviações

A lista a seguir esclarece as abreviaturas referenciadas neste documento.

AES

: Padrão de criptografia avançada

CDK

: chave de dados do cliente

DK

: chave de domínio

ECDH

: Curva elíptica Diffie-Hellman

ECDHE

: Efêmera de curva elíptica Diffie-Hellman

ECDSA

: Algoritmo de assinatura digital de curva elíptica

EKT

: token de chave exportado

ESK

chave de sessão criptografada

GCM

Modo Contador Galois

HBK

Chave de reserva HSM

HBKID

Identificador de chave de reserva HSM

HSM

módulo de segurança de hardware

RSA

Rivest Shamir e Adleman (criptológico)

secp384r1

Padrões para criptografia eficiente curva aleatória prima de 384 bits 1

SHA256

Algoritmo Hash Seguro de comprimento de resumo 256 bits

Chaves

A lista a seguir define as chaves mencionadas neste documento.

HBK

Chave de reserva HSM: as chaves de reserva HSM são chaves raiz de 256 bits, das quais as chaves de uso específicas são derivadas.

DK

Chave de domínio: uma chave de domínio é uma chave AES-GCM de 256 bits. Ela é compartilhada entre todos os membros de um domínio e é usada para proteger o material de chaves de reserva HSM e as chaves de sessão do host do serviço HSM.

DKEK

Chave de criptografia de chave de domínio: uma chave de criptografia de chave de domínio é uma chave AES-256-GCM gerada em um host e usada para criptografar o conjunto atual de chaves de domínio sincronizando o estado do domínio entre os hosts HSM.

(dHAK,QHAK)

Par de chaves de acordo HSM: cada HSM iniciado tem um par de chaves de acordo de curva elíptica Diffie-Hellman gerado localmente na curva secp384r1 (NIST-P384).

(dE, QE)

Par de chaves de acordo efêmero: HSM e hosts de serviço geram chaves de acordo efêmeras. Estas são as chaves de curva elíptica Diffie-Hellman na curva secp384r1 (NIST-P384). Eles são gerados em dois casos de uso: estabelecer uma chave de host-to-host criptografia para transportar chaves de criptografia de chave de domínio em tokens de domínio e estabelecer chaves de sessão de host de serviços HSM para proteger comunicações confidenciais.

(dHSK,QHSK)

Par de chaves de assinatura HSM: cada HSM iniciado tem um par de chaves de assinatura digital de curva elíptica gerado localmente na curva secp384r1 (NIST-P384).

(dOS,QOS)

Par de chaves de assinatura do operador: tanto os operadores do host de serviço quanto operadores do AWS KMS têm uma chave de assinatura de identidade usada para se autenticar para outros participantes do domínio.

K

Chave de criptografia de dados: uma chave AES-GCM de 256 bits derivada de um HBK usando o NIST SP800-108 KDF no modo contador usando HMAC com SHA256.

SK

Chave de sessão: uma chave de sessão é criada como resultado de uma chave de curva elíptica de Diffie-Hellman autenticada trocada entre um operador do host de serviço e um HSM. O objetivo da troca é proteger a comunicação entre o host de serviço e os membros do domínio.

Colaboradores

Os seguintes indivíduos e organizações contribuíram para este documento:

- Ken Beer, General Manager - KMS, Criptografia do AWS
- Matthew Campagna, Engenheiro Principal de Segurança, Criptografia do AWS

Bibliografia

Para obter mais informações sobre os HSMs do AWS Key Management Service, visite o Centro de Recursos de Segurança do Computador NIST na página de pesquisa do Programa de Validação de Módulos Criptográficos e procure por HSM do AWS Key Management Service.

Amazon Web Services, Referência geral (versão 1.0), “Assinatura de Solicitações de API do AWS,” http://docs.aws.amazon.com/general/latest/gr/signing_aws_api_requests.html.

Amazon Web Services, “O que é o AWS Encryption SDK,” http://docs.aws.amazon.com/encryption-sdk/latest/developer-guide/introduction.html.

Publicações de Padrões Federais de Processamento de Informações, FIPS PUB 180-4. Padrão de Secure Hash, agosto de 2012. Disponível em https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf.

Publicação 197 dos Padrões Federais de Processamento de Informações, Anunciando o Padrão Avançado de Criptografia (AES), novembro de 2001. Disponível em http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

Publicação 198-1 dos Padrões Federais de Processamento de Informações, O Código de Autenticação de Mensagens com Chaves Hash (HMAC), julho de 2008. Disponível em http://csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1_final.pdf.

Publicação especial 800-52 do NIST, Revisão 2, Diretrizes para a seleção, configuração e uso de implementações de Transport Layer Security (TLS), agosto de 2019. https://nvlpubs.nist.gov/nistpubs/ SpecialPublications /NIST.SP.800-52R2.pdf.

PKCS#1 v2.2: Padrão de Criptografia RSA (RFC 8017), Força-tarefa de Engenharia de Internet (IETF), novembro de 2016. https://tools.ietf.org/html/rfc8017.

Recomendação para Modos de Operação de Cifra de Bloco: Galois/Modo Contador (GCM) e GMAC, Publicação Especial NIST 800-38D, novembro de 2007. Disponível em http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf.

Recomendação para Modos de Operação de Cifra de Bloco: o Modo XTS-AES para Confidencialidade em Dispositivos de Armazenamento, Publicação Especial NIST

800-38E, janeiro de 2010. Disponível em https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38e.pdf.

Recomendação para Derivação de Chave usando Funções Pseudoaleatórias, Publicação Especial NIST 800-108, outubro de 2009, disponível em https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-108.pdf.

Recomendação para Gerenciamento de Chaves - Parte 1: Geral (Revisão 5), Publicação Especial NIST 800-57A, maio de 2020, disponível em https://doi.org/10.6028/NIST.SP.800-57pt1r5.

Recomendação para Esquemas de Estabelecimento de Chave em Par usando Criptografia de Logaritmo Discreto (Revisado), Publicação Especial NIST 800-56A Revisão 3, abril de 2018. Disponível em https://nvlpubs.nist.gov/nistpubs/ SpecialPublications /NIST.SP.800-56AR3.pdf.

Recomendação para geração de números aleatórios usando geradores determinísticos de bits aleatórios, publicação especial 800-90A do NIST, revisão 1, junho de 2015, disponível em https://nvlpubs.nist.gov/nistpubs/ /NIST.SP.800-90AR1.pdf. SpecialPublications

SEC 2: Parâmetros de Domínio de Curva Elíptica Recomendados, Grupo de Padrões para Criptografia Eficiente, Versão 2.0, 27 de janeiro de 2010.

Uso de Algoritmos de Criptografia de Curva Elíptica (ECC) na Sintaxe de Mensagens Criptográficas (CMS), Brown, D., Turner, S., Força-tarefa de Engenharia de Internet, julho de 2010,http://tools.ietf.org/html/rfc5753/.

X9.62-2005: Criptografia de Chave Pública para o Setor de Serviços Financeiros: o Algoritmo de Assinatura Digital de Curva Elíptica (ECDSA), Instituto Nacional de Padrões Americanos, 2005.

Histórico de documentos dos Detalhes criptográficos do AWS KMS

A tabela a seguir descreve mudanças importantes na documentação dos Detalhes criptográficos do AWS Key Management Service. Também atualizamos a documentação com frequência para abordar os comentários enviados por você.

Alteração	Descrição	Data
Conteúdo atualizado	Detalhes adicionados sobre a implementação da operação `ReplicateKey` do AWS KMS.	28 de outubro de 2021
Alteração na documentação	Substituição da condição chave mestra do cliente (CMK) porAWS KMS key e chave do KMS.	30 de agosto de 2021
Lançamento inicial	Este guia foi criado a partir do documento técnico de Detalhes criptográficos do KMS	30 de dezembro de 2020

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.