Dettagli di crittografia di AWS KMS

AWS Key Management Service

AWS Key Management Service: Dettagli di crittografia di AWS KMS

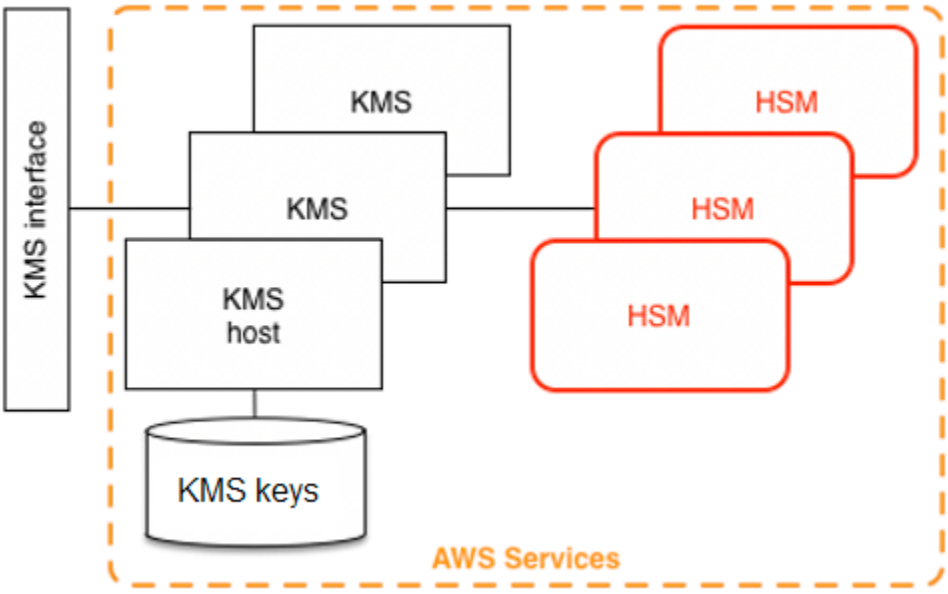
Table of Contents

Introduzione ai dettagli di crittografia di AWS KMS

AWS Key Management Service(AWS KMS) fornisce un'interfaccia Web per generare e gestire le chiavi di crittografia e funziona come provider di servizi crittografici per la protezione dei dati. AWS KMS offre servizi tradizionali di gestione delle chiavi integrati con AWS per fornire una visione coerente delle chiavi dei clienti in tutto AWS, con gestione centralizzata e verifica. Questo whitepaper fornisce una descrizione dettagliata delle operazioni di crittografia di AWS KMS per assistere l'utente nella valutazione delle funzionalità offerte dal servizio.

AWS KMS include un'interfaccia Web attraverso la AWS Management Console, l'interfaccia a riga di comando e le operazioni API RESTful per richiedere operazioni di crittografia di un parco istanze distribuito di moduli di sicurezza hardware (HSM) convalidati con FIPS 140-2 [1]. Il modulo di protezione hardware (HSM) AWS KMS è un'appliance hardware di crittografia autonoma progettata per fornire funzioni di crittografia dedicate per soddisfare i requisiti di sicurezza e scalabilità di AWS KMS. È possibile stabilire la propria gerarchia crittografica basata su HSM nelle chiavi gestite come AWS KMS keys. Queste chiavi sono rese disponibili sui moduli di protezione hardware e in memoria solo per il tempo necessario per elaborare la richiesta di crittografia. È possibile creare più chiavi KMS, ognuna rappresentata dal proprio ID chiave. Le chiavi KMS possono essere create, eliminate o utilizzate per crittografare, decrittografare, firmare o verificare i dati solo con i ruoli AWS IAM e gli account amministrati da ciascun cliente. È possibile definire controlli di accesso per gli utenti che possono gestire e/o utilizzare le chiavi KMS creando una policy collegata alla chiave. Tali policy consentono di definire usi specifici dell'applicazione per le chiavi per ogni operazione API.

Inoltre, la maggior parte dei servizi AWS supporta la crittografia dei dati a riposo utilizzando le chiavi KMS. Questa funzionalità consente ai clienti di controllare come e quando i servizi AWS possono accedere ai dati crittografati controllando come e quando è possibile accedere alle chiavi KMS.



AWS KMS è un servizio su più livelli costituito da host AWS KMS rivolti al Web e un livello di moduli di protezione hardware. Il raggruppamento di questi host a più livelli forma lo stack AWS KMS. Tutte le richieste a AWS KMS devono essere effettuate tramite il protocollo Transport Layer Security (TLS) e terminare su un host AWS KMS. Gli host AWS KMS consentono solo TLS con una suite di cifratura che fornisce forward secrecy. AWS KMS autentica e autorizza le richieste utilizzando gli stessi meccanismi di credenziali e policy di AWS Identity and Access Management (IAM) che sono disponibili per tutte le altre operazioni API AWS.

Concetti di base

Imparare alcuni termini e concetti di base aiuterà a sfruttare al meglio AWS Key Management Service.

AWS KMS key

> **Note**
>
> AWS KMS sta sostituendo il termine chiave master del cliente (CMK) con AWS KMS key e chiave KMS. Il concetto non è cambiato. Per evitare cambiamenti sostanziali, AWS KMS sta mantenendo alcune varianti di questo termine.

Una chiave logica che rappresenta la parte alta della gerarchia delle chiavi. A una chiave KMS viene assegnato un Amazon Resource Name (ARN) che include un identificatore della chiave univoco, o ID chiave. AWS KMS keys ha tre tipi di chiave:

- Chiave gestita dal cliente: i clienti creano e controllano il ciclo di vita e le policy di chiavi delle chiavi gestite dai clienti. Tutte le richieste effettuate con queste chiavi vengono registrate come CloudTrail eventi.
- Chiavi gestite da AWS: AWS crea e controlla il ciclo di vita e le policy di chiavi di Chiavi gestite da AWS, che sono le risorse in un Account AWS di un cliente. I clienti possono visualizzare le politiche di accesso e CloudTrail gli eventi perChiavi gestite da AWS, ma non possono gestire alcun aspetto di queste chiavi. Tutte le richieste effettuate con queste chiavi vengono registrate come CloudTrail eventi.
- Chiavi di proprietà di AWS: queste chiavi sono create e utilizzate esclusivamente da AWS per le operazioni di crittografia interne su diversi servizi AWS. I clienti non hanno visibilità sulle politiche chiave o Chiave di proprietà di AWS sull'utilizzo di CloudTrail.

Alias

Un nome intuitivo associato a una chiave KMS. L'alias può essere utilizzato in modo intercambiabile con l'ID chiave in molte delle operazioni API AWS KMS.

Autorizzazioni

Una policy associata a una chiave KMS che definisce le autorizzazioni per la chiave. La policy predefinita consente qualsiasi principale definito, oltre a consentire a Account AWS di aggiungere policy IAM che fanno riferimento alla chiave.

Concessioni

L'autorizzazione delegata per l'utilizzo di una chiave KMS quando i principal IAM previsti o la durata di utilizzo non sono noti all'inizio e pertanto non possono essere aggiunti a una chiave o a una policy IAM. Un uso delle concessioni è quello di definire le autorizzazioni di ambito per il modo in cui un servizio AWS può utilizzare una chiave KMS. Il servizio potrebbe essere necessario per utilizzare la chiave per eseguire lavori asincroni per conto dell'utente su dati crittografati in assenza di una chiamata API firmata diretta da parte dell'utente.

Chiavi di dati

Le chiavi di crittografia generate su moduli di protezione hardware (HSM), protette da una chiave KMS. AWS KMS consente alle entità autorizzate di ottenere chiavi dati protette da una chiave KMS. Possono essere restituite sia come chiavi dati in chiaro (non crittografate) che come

chiavi dati crittografate. Le chiavi dati possono essere simmetriche o asimmetriche (con le parti pubbliche e private restituite).

Testo cifrato

L'output crittografato di AWS KMS, a volte indicato come testo cifrato del cliente per eliminare la confusione. Il testo cifrato contiene dati crittografati con informazioni aggiuntive che identificano la chiave KMS da utilizzare nel processo di decrittografia. Le chiavi di dati crittografate sono un esempio comune di testo cifrato prodotto quando si utilizza una chiave KMS, ma tutti i dati di dimensioni inferiori a 4 KB possono essere crittografati con una chiave KMS per produrre un testo cifrato.

Contesto di crittografia

Una mappa di coppia chiave-valore di informazioni aggiuntive associate a informazioni protette da AWS KMS. AWS KMSutilizza la crittografia autenticata per proteggere le chiavi di dati. Il contesto di crittografia è incorporato nell'AAD della crittografia autenticata nei testi cifrati crittografati da AWS KMS. Queste informazioni di contesto sono facoltative e non vengono restituite quando si richiede una chiave (o un'operazione di crittografia). Ma se utilizzato, questo valore di contesto è necessario per completare correttamente un'operazione di decrittografia. Il contesto di crittografia offre informazioni autenticate supplementari. Queste informazioni possono aiutarti a far rispettare le politiche e possono essere incluse nei AWS CloudTrail registri. Ad esempio, è possibile utilizzare una coppia chiave-valore di {"key name":"satellite uplink key"} per assegnare un nome alla chiave di dati. L'uso successivo della chiave crea una voce AWS CloudTrail include “key name”: “satellite uplink key”. Queste informazioni aggiuntive possono fornire un contesto utile per comprendere il motivo per cui è stata utilizzata una determinata chiave KMS.

Chiavi pubbliche

Quando si utilizzano cifrature asimmetriche (RSA o curva ellittica), la chiave pubblica è il "componente pubblico" di una coppia di chiavi pubblica-privata. La chiave pubblica può essere condivisa e distribuita alle entità che devono crittografare i dati per il proprietario della coppia di chiavi pubblica-privata. Per le operazioni di firma digitale, la chiave pubblica viene utilizzata per verificare la firma.

Chiave privata

Quando si utilizzano cifrature asimmetriche (RSA o curva ellittica), la chiave privata è il "componente privato" di una coppia di chiavi pubblica-privata. La chiave privata viene utilizzata per decrittografare i dati o creare firme digitali. Analogamente alle chiavi KMS simmetriche, le chiavi private vengono crittografate in HSM. Vengono decifrate solo nella memoria a breve termine dell'HSM e solo per il tempo necessario per elaborare la richiesta di crittografia.

Obiettivi di progettazione di AWS KMS

AWS KMS è progettato per soddisfare i seguenti requisiti.

Durabilità

La durabilità delle chiavi di crittografia è progettata per eguagliare quella dei servizi di durabilità più elevati inAWS. Una singola chiave di crittografia può crittografare grandi volumi di dati accumulati per un lungo periodo di tempo.

Affidabile

L'utilizzo delle chiavi è protetto alle policy di controllo accessi definite e gestite dall'utente. Non esiste alcun meccanismo per esportare le chiavi KMS in chiaro. La riservatezza delle chiavi di crittografia è fondamentale. Per eseguire azioni amministrative sui moduli di protezione hardware sono necessari più dipendenti Amazon con accesso specifico ai controlli di accesso basati su quorum.

Bassa latenza e velocità effettiva elevata

AWS KMS fornisce operazioni crittografiche a livelli di latenza e velocità effettiva adatti per l'utilizzo da parte di altri servizi in AWS.

Regioni indipendenti

AWS offre regioni indipendenti per i clienti che devono limitare l'accesso ai dati in regioni diverse. L'utilizzo delle chiavi può essere isolato all'interno di una Regione AWS.

Fonte sicura di numeri casuali

Poiché la crittografia forte dipende dalla generazione di numeri casuali davvero imprevedibili, AWS KMS fornisce una fonte convalidata e a qualità elevata di numeri casuali.

Verifica

AWS KMSregistra l'uso e la gestione delle chiavi crittografiche nei AWS CloudTrail log. È possibile utilizzare i log AWS CloudTrail per ispezionare l'utilizzo delle chiavi di crittografia, nonché l'uso delle chiavi da parte dei servizi AWS per tuo conto.

Per raggiungere questi obiettivi, il sistema AWS KMS include un set di operatori AWS KMS e operatori host del servizio (noti collettivamente come "operatori") che amministrano "domini". Un dominio è un insieme di server AWS KMS, moduli di protezione hardware e operatori definito a livello regionale. Ciascun operatore AWS KMS dispone di un token hardware che contiene una coppia

di chiavi privata e pubblica che viene utilizzata per autenticare le sue azioni. I moduli di protezione hardware dispongono di una coppia di chiavi pubblica e privata aggiuntiva per stabilire le chiavi di crittografia che proteggono la sincronizzazione dello stato degli HSM.

In questo documento viene descritto come AWS KMS protegge le chiavi e gli altri dati che si desidera crittografare. In tutto il documento, le chiavi di crittografia o i dati da crittografare vengono definiti "segreti" o "materiale segreto".

Fondamenti di AWS Key Management Service

Gli argomenti di questo capitolo descrivono le primitive di crittografia di AWS Key Management Service e dove vengono utilizzate. Sono introdotti anche gli elementi di base di AWS KMS.

Argomenti

Primitive di crittografia

AWS KMS utilizza algoritmi di crittografia configurabili in modo che il sistema possa migrare rapidamente da un algoritmo approvato, o modalità, a un altro. Il set predefinito iniziale di algoritmi di crittografia è stato selezionato dagli algoritmi Federal Information Processing Standard (FIPS) approvati per le loro proprietà e prestazioni di sicurezza.

Entropia e generazione di numeri casuali

La generazione di chiavi AWS KMS viene eseguita sui moduli di protezione hardware (HSM) AWS KMS. Tali moduli implementano un generatore di numeri casuali ibridi che utilizza il Generatore di bit casuali deterministico (DRBG) NIST SP800-90A CTR_DRBG tramite AES-256. Inizia con un generatore di bit casuale non deterministico con 384 bit di entropia ed è aggiornato con entropia aggiuntiva per fornire resistenza di previsione su ogni chiamata per il materiale crittografico.

Operazioni con chiavi simmetriche (solo crittografia)

Tutti i comandi di cifratura a chiave simmetrica utilizzati all'interno dei moduli di protezione hardware utilizzanostandard di crittografia avanzati (Advanced Encryption Standards, AES), in Modalità contatore Galois (GCM) con chiavi a 256 bit. Le chiamate analoghe per decrittografare utilizzano la funzione inversa.

AES-GCM è uno schema di crittografia autenticato. Oltre a crittografare testo in chiaro per produrre testo cifrato, calcola un tag di autenticazione sul testo cifrato e tutti i dati aggiuntivi per i quali è richiesta l'autenticazione (dati autenticati in aggiunta, o AAD). Il tag di autenticazione consente di garantire che i dati provengano dall'origine presunta e che il testo cifrato e l'AAD non siano stati modificati.

Spesso AWS omette l'inclusione dell'AAD nelle nostre descrizioni, soprattutto quando si fa riferimento alla crittografia delle chiavi di dati. In questi casi, il testo circostante implica che la struttura da crittografare sia partizionata tra il testo in chiaro da crittografare e l'AAD in chiaro da proteggere.

AWS KMS fornisce un'opzione per importare il materiale chiave in una AWS KMS key invece di fare affidamento su AWS KMS per generare il materiale chiave. Questo materiale chiave importato può essere crittografato utilizzando RSAES-OAEP o RSAES-PKCS1-v1_5 per proteggere la chiave durante il trasporto all'HSM AWS KMS. Le coppie di chiavi RSA vengono generate sugli HSM AWS KMS. Il materiale chiave importato viene decrittato in un HSM AWS KMS ed è criptato nuovamente in AES-GCM prima di essere archiviato dal servizio.

Operazioni con chiave asimmetrica (crittografia, firma digitale e verifica della firma)

AWS KMS supporta l'utilizzo di operazioni con chiave asimmetrica sia per le operazioni di crittografia che per le operazioni di firma digitale. Le operazioni con chiave asimmetrica si basano su una coppia di chiavi, una pubblica e una privata, correlate matematicamente utilizzabili per la crittografia e la decrittazione o per la firma e la verifica, ma non per entrambe le azioni. Grazie alla chiave privata il servizio AWS KMS non è mai in chiaro. Puoi utilizzare la chiave pubblica all'interno di AWS KMS, chiamando le azioni API AWS KMS, o scaricare la chiave pubblica e usarla all'esterno di AWS KMS.

AWS KMS supporta due tipi di crittografie asimmetriche.

- RSA-OAEP (per la crittografia) e RSA-PSS e RSA-PKCS-#1-v1_5 (per la firma e la verifica): supporta le lunghezze delle chiavi RSA (in bit): 2048, 3072 e 4096 per diversi requisiti di sicurezza.
- Curva ellittica (ECC): utilizzata esclusivamente per la firma e la verifica. Supporta curve ECC: NIST P256, P384, P521, SECP 256k1.

Funzioni di derivazione chiave

Una funzione di derivazione chiave viene utilizzata per ricavare chiavi aggiuntive da una chiave o un segreto iniziale. AWS KMS utilizza una funzione di derivazione chiave (KDF) per derivare le chiavi per chiamata per ogni crittografia in una AWS KMS key. Tutte le operazioni KDF utilizzano il KDF in modalità contatore tramite di HMAC [FIPS197] con SHA256 [FIPS180]. La chiave derivata a 256 bit viene utilizzata con AES-GCM per crittografare o decrittare i dati e le chiavi dei clienti.

Uso interno di AWS KMS delle firme digitali

Le firme digitali vengono utilizzate anche per autenticare comandi e comunicazioni tra entità AWS KMS. Tutte le entità del servizio dispongono di una coppia di chiavi ECDSA (Elliptic Curve Digital Signature Algorithm). Eseguono ECDSA come definito in Utilizzo degli algoritmi ECC (Elliptic Curve Cryptography) nella sintassi del messaggio di crittografia (CMS) e X9.62-2005: Crittografia a chiave pubblica per il settore dei servizi finanziari: ECDSA (Elliptic Curve Digital Signature Algorithm). Le entità utilizzano l'algoritmo hash sicuro definito in Pubblicazioni degli standard di elaborazione delle informazioni federali, FIPS PUB 180-4, noto come SHA384. Le chiavi vengono generate sulla curva secp384r1 (NIST-P384).

Crittografia envelope

Una costruzione di base utilizzata all'interno di molti sistemi di crittografia è la crittografia envelope. La crittografia envelope utilizza due o più chiavi di crittografia per proteggere un messaggio. In genere, una chiave è derivata da una chiave statica a lungo termine k e un'altra chiave è una chiave per messaggio, msgKey, che viene generata per crittografare il messaggio. L'envelope è formata crittografando il messaggio: ciphertext = Encrypt(msgKey, message). Quindi la chiave del messaggio viene crittografata con la chiave statica a lungo termine: encKey = Encrypt(k, msgKey). Infine, i due valori (encKey, ciphertext) sono assemblati in un'unica struttura, o messaggio crittografato con envelope.

Il destinatario, con accesso a k, può aprire il messaggio con envelope decrittando prima la chiave crittografata e quindi il messaggio.

AWS KMS offre la possibilità di gestire queste chiavi statiche a lungo termine e automatizzare il processo di crittografia envelope dei dati.

Oltre alle funzionalità di crittografia fornite all'interno del servizio AWS KMS, l'SDK di crittografia AWS fornisce librerie di crittografia envelope lato client. È possibile utilizzare queste librerie per proteggere i dati e le chiavi di crittografia utilizzate per crittografare i dati.

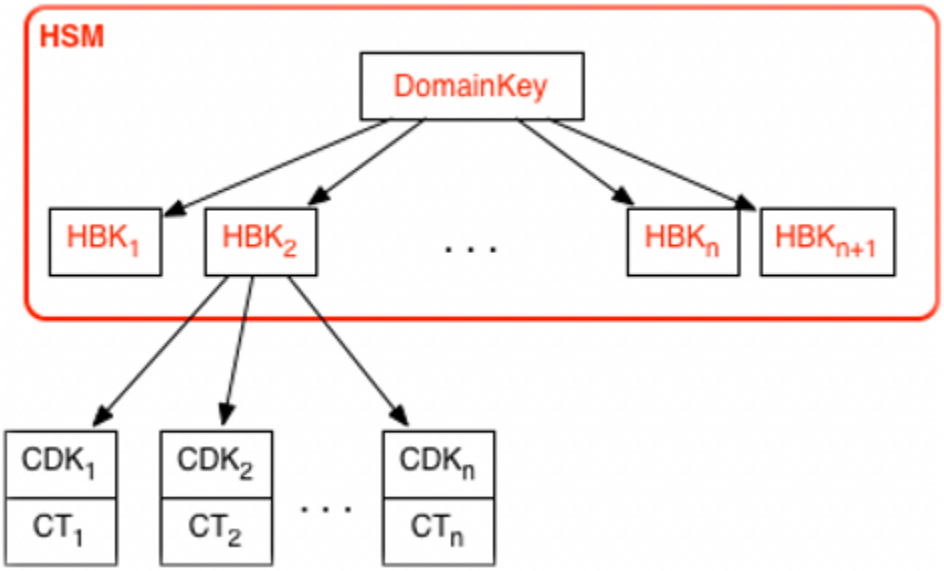
Gerarchia di AWS KMS key

La gerarchia delle chiavi inizia con una chiave logica di primo livello, una AWS KMS key. Una chiave KMS rappresenta un container per il materiale della chiave di primo livello ed è definita in modo univoco all'interno dello spazio dei nomi del servizio AWS con un Amazon Resource Name (ARN). L'ARN include un identificatore di chiave generato in modo univoco, un ID chiave. Una chiave KMS

viene creata in base a una richiesta avviata dall'utente tramite AWS KMS. Alla ricezione, AWS KMS richiede la creazione di una chiave di supporto HSM (HBK) iniziale da inserire nel container della chiave KMS. L'HBK viene generata su una HSM nel dominio ed è progettata per non essere mai esportata da HSM in testo normale. Invece, l'HBK viene esportata crittografata in chiavi di dominio gestite da HSM. Queste HBK esportate vengono definite come token di chiave esportati (EKT).

L'EKT viene esportato in uno spazio di archiviazione altamente durevole e a bassa latenza. Si supponga, ad esempio, di ricevere un ARN per la chiave logica KMS. Questo rappresenta la parte superiore di una gerarchia di chiavi, o contesto crittografico. È possibile creare più chiavi KMS all'interno dell'account e impostare policy sulle chiavi KMS come qualsiasi altra risorsa AWS specificata.

All'interno della gerarchia di una chiave KMS specifica, l'HBK può essere considerata come una versione della chiave KMS. Quando si desidera ruotare la chiave KMS tramite AWS KMS, viene creata una nuova HBK che viene associata alla chiave KMS come HBK attiva per la chiave KMS. Le HBK meno recenti vengono conservate e possono essere utilizzatei per decrittografare e verificare i dati precedentemente protetti. Ma solo la chiave di crittografia attiva può essere utilizzata per proteggere nuove informazioni.



È possibile effettuare richieste tramite AWS KMS per utilizzare le chiavi KMS per proteggere direttamente le informazioni o richiedere ulteriori chiavi generate da HSM protette con la chiave KMS. Queste chiavi sono chiamate chiavi dati del cliente, o CDK. Le CDK possono essere restituite crittografate come testo cifrato (CT), in testo normale o con entrambe le opzioni. Tutti gli oggetti crittografati con una chiave KMS (dati forniti dal cliente o chiavi generate da HSM) possono essere decrittografati solo su una HSM tramite una chiamata con AWS KMS.

Il testo cifrato restituito, o il payload decrittografato, non viene mai memorizzato all'interno di AWS KMS. Le informazioni vengono restituite tramite la connessione TLS a AWS KMS. Questo vale anche per le chiamate effettuate dai servizi AWS per tuo conto.

La gerarchia delle chiavi e le proprietà della chiave specifiche vengono visualizzate nella tabella seguente.

Chiave	Descrizione	Ciclo di vita
Chiave di dominio	Una chiave AES-GCM a 256 bit solo in memoria di un HSM utilizzato per avvolgere le versioni delle chiavi KMS, le chiavi di supporto HSM.	Rotazione giornaliera[1]
Materiale della chiave HSM	Una chiave simmetrica a 256 bit o RSA o chiave privata della curva ellittica, utilizzata per proteggere i dati e le chiavi dei clienti e archiviata crittografata con le chiavi di dominio. Una o più chiavi di supporto HSM comprendono la chiave KMS, rappresentata da keyId.	Rotazione annuale[2] (config. facoltativa)
Chiave di crittografia derivata	Una chiave AES-GCM a 256 bit solo in memoria di un HSM utilizzato per crittografare i dati e le chiavi dei clienti. Derivato da una HBK per ogni crittografia.	Usato una volta per crittografare e rigenerato sulla decrittografia
Chiave dei dati del cliente	Chiave simmetrica o asimmetrica definita dall'utente esportata da HSM in testo normale e cifrato. Crittografata con una chiave di supporto HSM e restituita agli utenti autorizzati sul canale TLS.	Rotazione e utilizzo controllati dall'applicazione

[1] AWS KMS di tanto in tanto potrebbe ridurre la rotazione delle chiavi di dominio al massimo a una settimana per tenere conto delle attività di amministrazione e configurazione del dominio.

[2] Le Chiavi gestite da AWS di default create e gestite da AWS KMS per tuo conto vengono ruotate ogni anno.

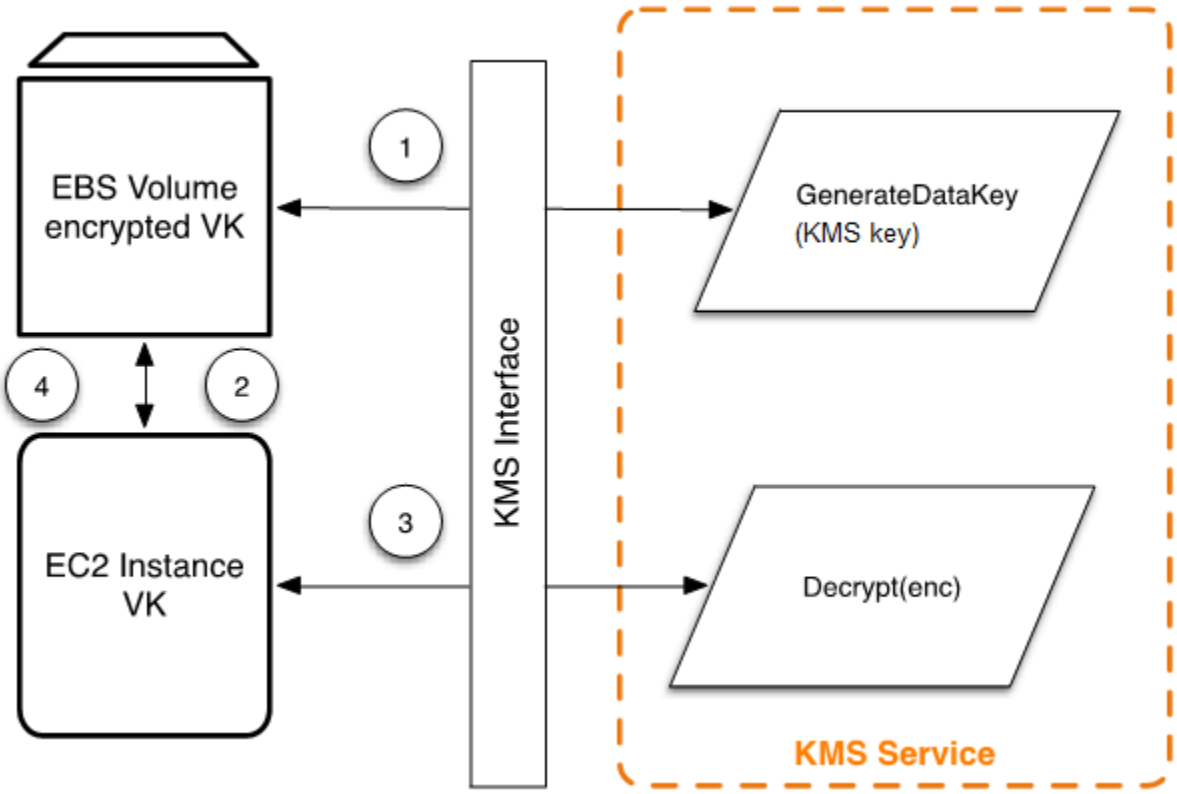
Casi d'uso AWS KMS

I casi d'uso possono aiutarti a ottenere il massimo daAWS Key Management Service. Il primo dimostra come AWS KMS esegue la crittografia lato server con AWS KMS keys su un volume Amazon Elastic Block Store (Amazon EBS). La seconda è un'applicazione lato client che dimostra come è possibile utilizzare la crittografia envelope per proteggere il contenuto con AWS KMS.

Argomenti

Crittografia dei volumi Amazon EBS

Amazon EBS offre funzionalità di crittografia dei volumi. Ogni volume viene crittografato tramite AES-256-XTS. Ciò richiede due chiavi di volume a 256 bit, che possono essere considerate come una chiave di volume a 512 bit. La chiave di volume è crittografata con una chiave KMS nell'account. Affinché Amazon EBS possa crittografare un volume per tuo conto, deve avere accesso per generare una chiave del volume (VK) con una chiave KMS nell'account. Ciò è possibile fornendo una concessione per Amazon EBS alla chiave KMS per creare chiavi di dati e per crittografare e decrittografare queste chiavi di volume. Ora Amazon EBS utilizza AWS KMS con una chiave KMS per generare chiavi di volume crittografate con AWS KMS.



Il seguente flusso di lavoro crittografa i dati che vengono scritti in un volume Amazon EBS:

1. Amazon EBS ottiene una chiave di volume crittografata con una chiave KMS tramite AWS KMS su una sessione TLS e memorizza la chiave crittografata con i metadati del volume.
2. Quando viene montato il volume Amazon EBS, viene recuperata la chiave di volume crittografata.
3. Una chiamata a AWS KMS su TLS viene eseguita per decrittografare la chiave del volume crittografata. AWS KMSidentifica la chiave KMS ed effettua una richiesta interna a un HSM del parco istanze per decrittografare la chiave di volume crittografata. AWS KMS quindi restituisce la chiave di volume all'host Amazon Elastic Compute Cloud (Amazon EC2) che contiene l'istanza durante la sessione TLS.
4. La chiave di volume viene utilizzata per crittografare e decrittografare tutti i dati provenienti dal volume Amazon EBS allegato. Amazon EBS conserva la chiave di volume crittografata per un utilizzo successivo nel caso in cui la chiave di volume in memoria non sia più disponibile.

Per ulteriori informazioni sulla crittografia dei volumi Amazon EBS con le chiavi KMS, consulta Come Amazon Elastic Block Store utilizza AWS KMS nella Guida per gli sviluppatori di AWS Key

Management Service eCrittografia Amazon EBS nella Guida per l'utente di Amazon EC2 per le istanze Linux e Guida per l'utente di Amazon EC2 per le istanze Windows.

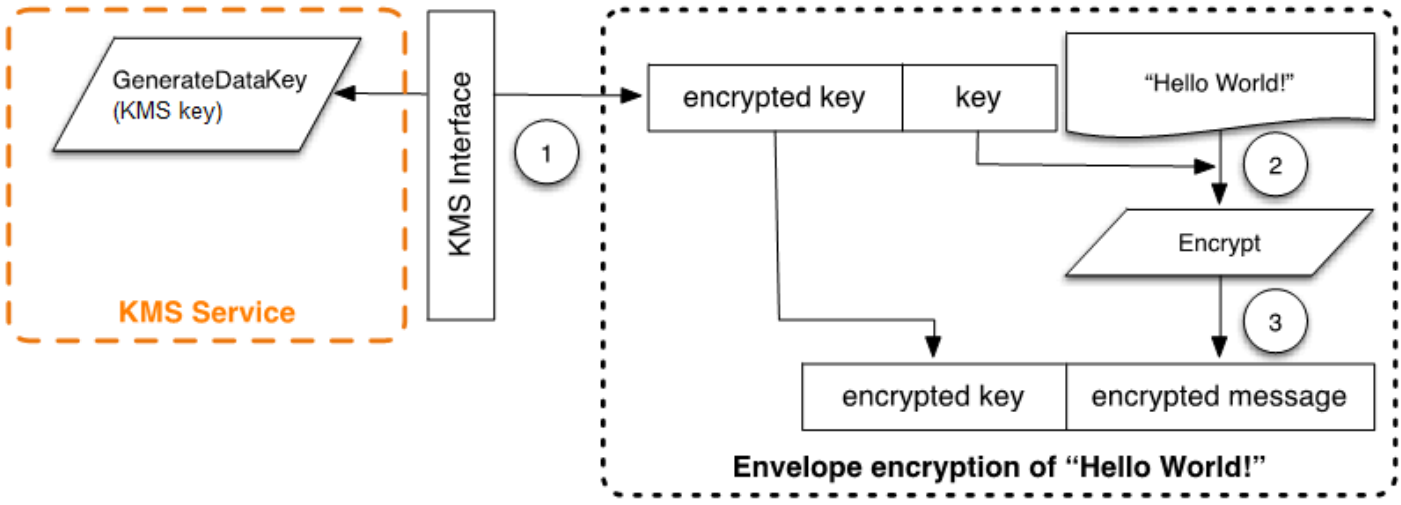
Crittografia lato client

AWS Encryption SDK include un'operazione API per eseguire la crittografia envelope utilizzando una chiave KMS. Per i suggerimenti completi e i dettagli sull'utilizzo, consultare la documentazione correlata. Le applicazioni client possono utilizzare AWS Encryption SDK per eseguire la crittografia envelope tramite 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);
```

L'applicazione client può completare la seguente procedura:

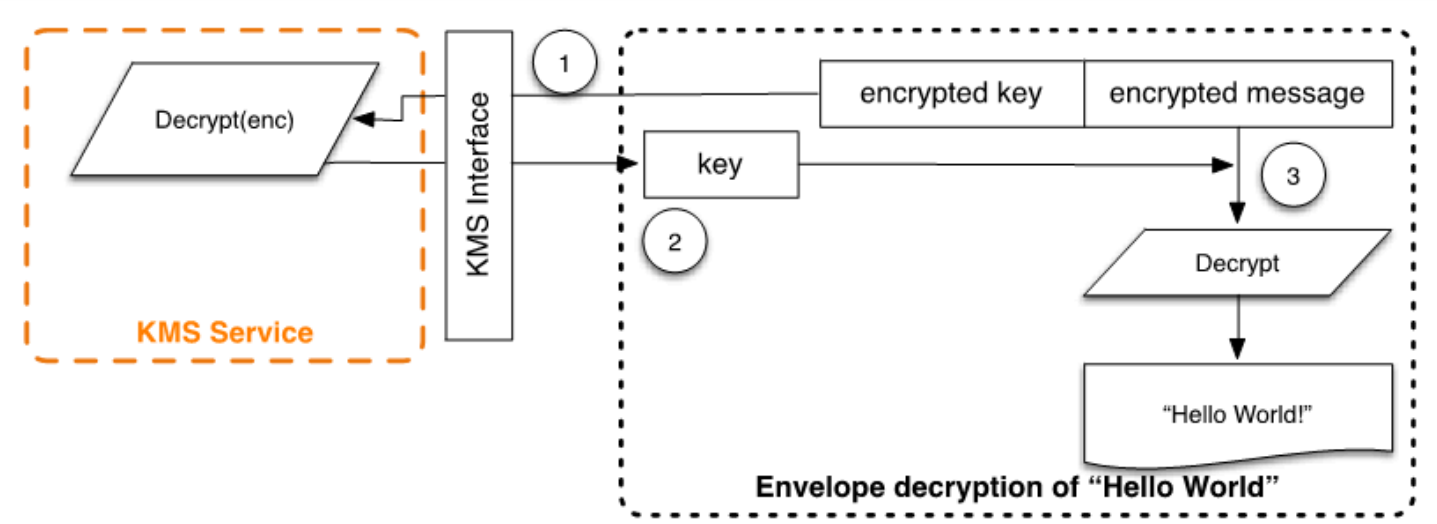
1. Una richiesta viene effettuata con la chiave KMS per una nuova chiave dati. Vengono restituite una chiave di dati crittografati e una versione di testo normale della chiave di dati.
2. All'interno di AWS Encryption SDK, la chiave di dati di testo normale viene utilizzata per crittografare il messaggio. La chiave di dati di testo normale viene quindi eliminata dalla memoria.
3. La chiave dati crittografata e il messaggio crittografato vengono combinati in un unico array di byte cifrato.



Il messaggio crittografato con envelope può essere decrittografato utilizzando la funzionalità di decrittografia in modo da ottenere il messaggio crittografato in origine.

```
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 analizza il messaggio crittografato con envelope per ottenere la chiave dati crittografata ed effettuare una richiesta a AWS KMS per decrittare la chiave di dati.
2. AWS Encryption SDK riceve la chiave di dati di testo normale da AWS KMS.
3. La chiave di dati viene quindi utilizzata per decrittare il messaggio, restituendo il testo normale iniziale.

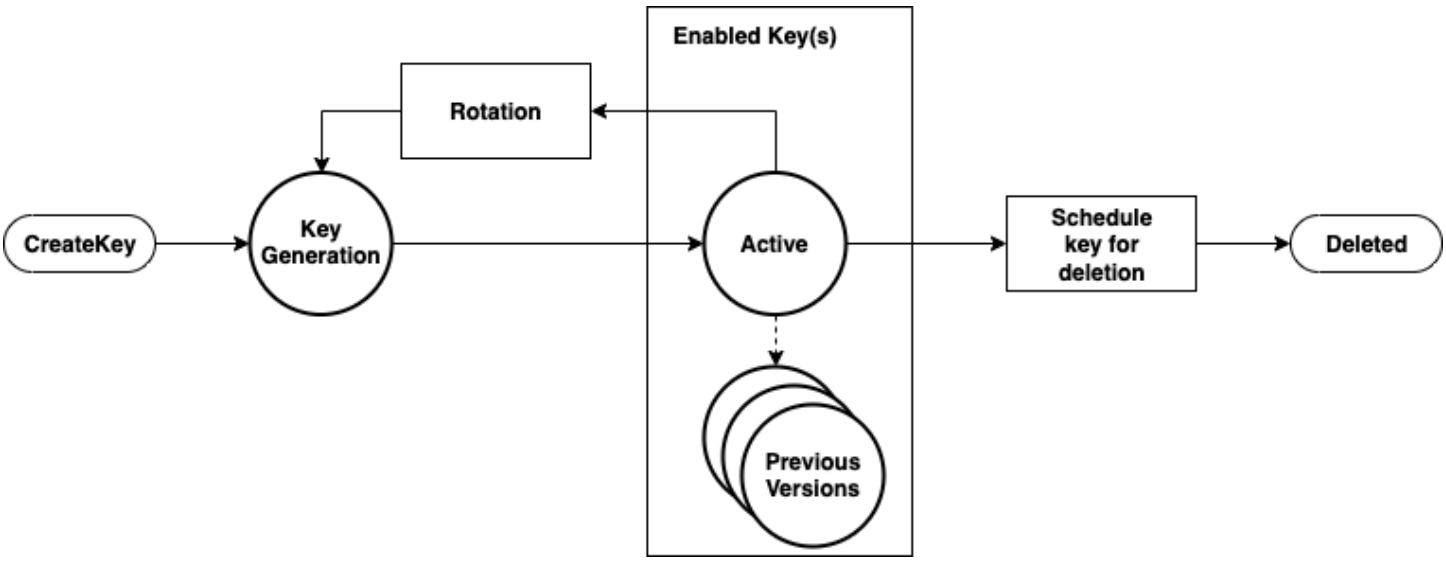


Utilizzo di AWS KMS keys

Un AWS KMS key si riferisce a una chiave logica che può fare riferimento a una o più chiavi di supporto del modulo di sicurezza hardware (HSM), dette HBK. Questo argomento illustra come creare una chiave KMS, importare materiale chiave e come abilitare, disabilitare, ruotare ed eliminare le chiavi KMS.

> **Note**
>
> AWS KMS sta sostituendo il termine chiave master del cliente (CMK) con AWS KMS key e chiave KMS. Il concetto non è cambiato. Per evitare cambiamenti sostanziali, AWS KMS sta mantenendo alcune varianti di questo termine.

Questo capitolo descrive il ciclo di vita di una chiave KMS dalla creazione alla cancellazione, come illustrato nell'immagine seguente.



Argomenti

Chiamata CreateKey

Una AWS KMS key viene generata come risultato di una chiamata alla chiamata API `CreateKey`.

Di seguito è riportato un sottoinsieme della sintassi della richiesta da `CreateKey`.

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

La richiesta accetta i seguenti dati in formato JSON.

Descrizione

(Facoltativo) Descrizione della chiave. Si consiglia di scegliere una descrizione che consenta di decidere se la chiave è appropriata per una determinata attività.

KeySpec

Specifica il tipo di chiave KMS da creare. Il valore predefinito, SYMMETRIC_DEFAULT, crea una chiave KMS di crittografia simmetrica. Questo parametro è facoltativo per le chiavi di crittografia simmetrica e richiesto per tutte le altre specifiche di chiave.

KeyUsage

Specifica l'utilizzo della chiave. I valori validi sono `ENCRYPT_DECRYPT`, `SIGN_VERIFY` o `GENERATE_VERIFY_MAC`. Il valore predefinito è `ENCRYPT_DECRYPT`. Questo parametro è facoltativo per le chiavi di crittografia simmetrica e richiesto per tutte le altre specifiche di chiave.

Origin

(Facoltativo) Specifica l'origine del materiale chiave della chiave KMS. Il valore predefinito è `AWS_KMS`, indica che AWS KMS genera e gestisce il materiale della chiave per la chiave KMS. Gli altri valori validi includono: `EXTERNAL`, che rappresenta una chiave KMS creata senza materiale chiave per il materiale della chiave importato e `AWS_CLOUDHSM` che crea una chiave KMS in un archivio delle chiavi personalizzato supportato da un cluster AWS CloudHSM controllato da te.

Policy

(Facoltativo) Policy da collegare alla chiave. Se la policy viene omessa, la chiave viene creata con la policy di predefinita (seguente) che consente all'account root e i principali IAM con autorizzazioni AWS KMS di gestirla.

Per i dettagli della policy, consulta Policy delle chiavi in AWS KMS e Policy della chiave predefinita nella Guida per gli sviluppatori di AWS Key Management Service.

La richiesta `CreateKey` restituisce una risposta che include una chiave ARN.

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

Se `Origin` è `AWS_KMS`, dopo aver creato l'ARN, viene effettuata una richiesta a un HSM AWS KMS su una sessione autenticata per eseguire il provisioning del materiale della chiave (HBK) del modulo di sicurezza hardware (HSM). L'HBK è una chiave a 256 bit associata a questo ID della chiave KMS. Può essere generata solo su un HSM ed è progettata per non essere mai esportata al di fuori del limite HSM in chiaro. L'HBK è crittografato con la chiave di dominio corrente, DK_0. Queste chiavi HBK crittografate sono note come token di chiavi crittografate (EKT). Sebbene i moduli di protezione hardware (HSM) possano essere configurati per utilizzare una varietà di metodi di wrapping delle chiavi, l'implementazione corrente utilizza uno schema di crittografia autenticato AES-256 in modalità contatore Galois (GCM). Questa modalità di crittografia autenticata consente di proteggere alcuni metadati dei token delle chiavi esportate in cleartext.

Questo è rappresentato stilisticamente come:

```
EKT = Encrypt(DK0, HBK)
```

Alle chiavi KMS e le HBK successive vengono fornite due forme fondamentali di protezione: le policy di autorizzazione impostate sulle chiavi KMS e le protezioni crittografiche sulle HBK associate. Le sezioni rimanenti descrivono le protezioni crittografiche e la sicurezza delle funzioni di gestione in AWS KMS.

Oltre all'ARN, è possibile creare un nome significativo e associarlo alla chiave KMS creando un alias per la chiave. Una volta che un alias è stato associato a una chiave KMS, l'alias può essere utilizzato per identificare la chiave KMS nelle operazioni di crittografia. Per ulteriori informazioni, consulta Using aliases (Utilizzo di alias) nella Guida per lo sviluppatore di AWS Key Management Service.

L'uso delle chiavi KMS è caratterizzato da più livelli di autorizzazioni. AWS KMS consente policy di autorizzazione separate tra il contenuto crittografato e la chiave KMS. Ad esempio, un oggetto Amazon Simple Storage Service (Amazon S3) crittografato con envelope AWS KMSeredita la policy sul bucket Amazon S3. Tuttavia, l'accesso alla chiave di crittografia necessaria è determinato dalla policy di accesso sulla chiave KMS. Per informazioni sull'autorizzazione delle chiavi KMS, consulta Autenticazione e controllo degli accessi per AWS KMS nella Guida per gli sviluppatori diAWS Key Management Service.

Importazione del materiale delle chiavi

AWS KMS fornisce un meccanismo per importare il materiale crittografico utilizzato per una HBK. Come descritto inChiamata CreateKey, quando il CreateKey comando viene utilizzato con `Origin` set to`EXTERNAL`, viene creata una chiave KMS logica che non contiene HBK sottostante. Il materiale crittografico deve essere importato utilizzando la chiamata API `ImportKeyMaterial`. È possibile utilizzare questa funzione per controllare la creazione della chiave e la durabilità del materiale crittografico. Se si utilizza questa funzione, si consiglia di prestare molta attenzione alla gestione e alla durabilità di queste chiavi nell'ambiente in uso. Per dettagli completi e suggerimenti per l'importazione di materiale chiave, consultare Importazione del materiale delle chiavi nella Guida per gli sviluppatori di AWS Key Management Service.

Chiamata ImportKeyMaterial

La richiesta `ImportKeyMaterial` importa il materiale crittografico necessario per l'HBK. Il materiale crittografico deve essere una chiave simmetrica a 256 bit. Deve essere crittografato utilizzando l'algoritmo specificato in `WrappingAlgorithm` con la chiave pubblica restituita da una richiesta `GetParametersForImport` recente.

Una richiesta `ImportKeyMaterial` accetta gli argomenti seguenti.

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

EncryptedKeyMaterial

Il materiale chiave importato crittografato con la chiave pubblica restituito in una richiesta `GetParametersForImport` utilizzando l'algoritmo di wrapping specificato in quella richiesta.

ExpirationModel

Specifica se il materiale chiave scade. Quando questo valore è `KEY_MATERIAL_EXPIRES`, il parametro `ValidTo` deve contenere una data di scadenza. Se il valore è `KEY_MATERIAL_DOES_NOT_EXPIRE`, non includere il parametro `ValidTo`. I valori validi sono `"KEY_MATERIAL_EXPIRES"` e `"KEY_MATERIAL_DOES_NOT_EXPIRE"`.

ImportToken

Il token di importazione restituito dalla stessa richiesta `GetParametersForImport` che ha fornito la chiave pubblica.

KeyId

La chiave KMS che verrà associata al materiale chiave importato. L'`Origin` della chiave KMS deve essere `EXTERNAL`.

È possibile eliminare e reimportare il stesso materiale chiave importato nella chiave KMS specificata, ma non è possibile importare o associare la chiave KMS a nessun altro materiale chiave.

ValidTo

(Facoltativo) L'ora in cui scade il materiale chiave importato. Quando il materiale chiave scade, AWS KMS elimina tale materiale e la chiave KMS diventa inutilizzabile. Questo parametro è obbligatorio quando il valore di `ExpirationModel` è `KEY_MATERIAL_EXPIRES`. In caso contrario non è valido.

Dopo aver completato la richiesta, la chiave KMS è disponibile per l'utilizzo in AWS KMS fino alla data di scadenza specificata, se ne viene fornita una. Una volta che il materiale della chiave importato scade, l'EKT viene eliminato dal livello di archiviazione AWS KMS.

Abilitazione e disabilitazione delle chiavi

La disabilitazione di una chiave KMS impedisce che venga utilizzata nelle operazioni di crittografia. Il comando sospende la possibilità di utilizzare tutti gli HBK associate alla chiave KMS. L’abilitazione

ripristina l'uso degli HBK e della chiave KMS. Enable (Abilita) e Disable (Disabilita) sono richieste semplici che accettano solo l'ID o l'ARN della chiave KMS.

Eliminazione delle chiavi

Gli utenti autorizzati possono utilizzare l'API `ScheduleKeyDeletion` per pianificare la cancellazione di una chiave KMS e di tutti gli HBK associati. Questa è un'operazione intrinsecamente distruttiva e si dovrebbe prestare attenzione quando si eliminano le chiavi da AWS KMS. AWS KMS applica un tempo minimo di sette giorni da attendere per l'eliminazione delle chiavi KMS. Durante il periodo di attesa la chiave viene posizionata in uno stato disabilitato con uno stato chiave di In attesa di eliminazione. Tutte le chiamate per utilizzare la chiave per le operazioni crittografiche falliranno. ScheduleKeyDeletion accetta i seguenti argomenti.

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

KeyId

L'identificatore univoco della chiave KMS da eliminare. Per specificare questo valore, utilizzare l'ID chiave univoco o l'ARN della chiave KMS.

PendingWindowInDays

(Facoltativo) Il periodo di attesa, specificato in numero di giorni. Questo valore è facoltativo. L'intervallo è 7-30 giorni e il valore predefinito è 30 giorni. Al termine del periodo di attesa, AWS KMS eliminerà la chiave KMS e tutte le HBK associate.

Rotazione del materiale chiave

Gli utenti autorizzati possono abilitare la rotazione annuale automatica delle chiavi KMS gestite dal cliente. Le Chiavi gestite da AWS vengono sempre ruotate ogni anno.

Quando una chiave KMS viene ruotata, viene creata un nuovo HBK che viene contrassegnato come versione attiva del materiale della chiave per tutte le nuove richieste di crittografia. Tutte le versioni precedenti di HBK rimangono disponibili per l'uso perpetuo per decrittografare qualsiasi testo criptato crittografato utilizzando questa versione dell'HBK. Poiché AWS KMS non memorizza alcun testo criptato crittografato sotto una chiave KMS, i testi criptati con un HBK più vecchio e ruotato richiedono

che HBK per la decrittografia. Puoi utilizzare l'API `ReEncrypt` per crittografare nuovamente qualsiasi testo criptato sotto il nuovo HBK per la chiave KMS o sotto una chiave KMS diversa senza esporre il testo plaintext.

Per ulteriori informazioni sull'abilitazione e disabilitazione della rotazione automatica della chiave, consulta Rotating AWS KMS keys (Rotazione delle chiavi KMS) nella Guida per svilppatori di AWS Key Management Service.

Operazioni con i dati dei clienti

Dopo aver stabilito una chiave KMS, è possibile utilizzarla per eseguire operazioni di crittografia. Ogni volta che i dati vengono crittografati con una chiave KMS, l'oggetto risultante è un testo cifrato del cliente. Il testo cifrato contiene due sezioni: una porzione di intestazione (o testo non crittografato), protetta dallo schema di crittografia autenticata come dati autenticati aggiuntivi e una parte crittografata. La parte di testo in chiaro include l'identificatore HBK (HBKID). Questi due campi immutabili del valore del testo cifrato aiutano a garantire che AWS KMS possa decrittare l'oggetto in futuro.

Argomenti

- Generazione delle chiavi di dati
- Crittografa
- Decrypt
- Nuova crittografia di un oggetto crittografato

Generazione delle chiavi di dati

Gli utenti autorizzati possono utilizzare l' GenerateDataKey API (e le relative API) per richiedere un tipo specifico di chiave dati o una chiave casuale di lunghezza arbitraria. In questo argomento viene fornita una vista semplificata di questa operazione API. Per i dettagli, consulta le GenerateDataKey API nell'API Reference. AWS Key Management Service

- GenerateDataKey
- GenerateDataKeyWithoutPlaintext
- GenerateDataKeyPair
- GenerateDataKeyPairWithoutPlaintext

Di seguito è riportata la sintassi di una richiesta `GenerateDataKey`.

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

```
}
```

La richiesta accetta i seguenti dati in formato JSON.

KeyId

Identificatore della chiave utilizzato per crittografare la chiave dati. Questo valore deve identificare una chiave KMS di crittografia simmetrica.

Questo parametro è obbligatorio.

NumberOfBytes

Un numero intero che contiene il numero di byte da generare. Questo parametro è obbligatorio.

Il chiamante deve fornire `KeySpec` o `NumberOfBytes`, ma non entrambi.

EncryptionContext

(Facoltativo) Coppia nome-valore che contiene dati aggiuntivi per l'autenticazione durante i processi di crittografia e decrittografia che utilizzano la chiave.

GrantTokens

(Facoltativo) Un elenco dei token di concessione che rappresentano le concessioni che forniscono autorizzazioni per generare o utilizzare una chiave. Per ulteriori informazioni sulle concessioni e i token di concessione, consultare Autenticazione e controllo degli accessi per AWS KMS nella Guida per gli sviluppatori di AWS Key Management Service.

Dopo aver autenticato il comando, AWS KMS,acquisisce l'EKT attivo corrente associato alla chiave KMS. Quindi passa l'EKT insieme alla richiesta fornita e a qualsiasi contesto di crittografia a un HSM su una sessione protetta tra l'host AWS KMS e un HSM nel dominio.

L'HSM completa le seguenti operazioni:

1. Genera il materiale segreto richiesto e lo conserva nella memoria volatile.
2. Decritta l'EKT corrispondente all'ID chiave della chiave KMS definito nella richiesta per ottenere HBK = Decrypt(DK_i, EKT).
3. Genera un nonce casuale N.
4. Genera una chiave di crittografia derivata AES-GCM a 256 bit K da HBK e N.
5. Crittografa il materiale segreto ciphertext = Encrypt(K, context, secret).

`GenerateDataKey` restituisce il materiale segreto in chiaro e il testo criptato all'utente attraverso il canale sicuro tra l'host AWS KMS e l'HSM. AWS KMS quindi lo invia durante la sessione TLS. AWS KMS non mantiene il testo in chiaro o il testo criptato. Senza il testo cifrato, il contesto di crittografia e l'autorizzazione a utilizzare la chiave KMS, il segreto non può essere restituito.

Di seguito è riportata la sintassi della risposta.

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

La gestione delle chiavi di dati è lasciata allo sviluppatore dell'applicazione. Per una migliore pratica di crittografia lato client con chiavi dati AWS KMS (ma non coppie di chiavi dati), è possibile utilizzare il AWS Encryption SDK.

Le chiavi dati possono essere ruotate a qualsiasi frequenza. Inoltre, la chiave dati può essere crittografata nuovamente su una chiave KMS diversa o in una chiave KMS ruotata utilizzando l'operazione API `ReEncrypt`. Per i dettagli, consulta ReEncryptl'AWS Key Management ServiceAPI Reference.

Crittografa

Una funzione di base di AWS KMS è quella di crittografare un oggetto con una chiave KMS. In base alla progettazione, AWS KMS fornisce operazioni crittografiche a bassa latenza sui moduli di protezione hardware. Quindi c'è un limite di 4 KB sulla quantità di testo in chiaro che può essere crittografato in una chiamata diretta alla funzione di crittografia. Per crittografare i messaggi più grandi è possibile utilizzare AWS Encryption SDK. AWS KMS, dopo aver autenticato il comando, acquisisce l'EKT attivo corrente relativo alla chiave KMS. Trasmette l'EKT insieme al testo in chiaro e al contesto di crittografia a qualsiasi HSM disponibile nella regione. Questi vengono inviati tramite una sessione autenticata tra l'host AWS KMS e un HSM nel dominio.

L'HSM completa le seguenti operazioni:

1. Decritta l'EKT per ottenere HBK = Decrypt(DK_i, EKT).
2. Genera un nonce casuale N.
3. Deriva una chiave di crittografia derivata AES-GCM a 256 bit K da HBK e N.

4. Crittografa il testo in chiaro ciphertext = Encrypt(K, context, plaintext).

Il valore del testo cifrato viene restituito all'utente e né il testo in chiaro né quello cifrato viene mantenuto in alcun punto dell'infrastruttura AWS. Senza il testo cifrato, il contesto di crittografia e l'autorizzazione a utilizzare la chiave KMS, il testo in chiaro non può essere restituito.

Decrypt

Una chiamata a AWS KMS per decrittare un valore di testo cifrato accetta un testo cifrato del valore crittografato e un contesto di crittografia. AWS KMS autentica la chiamata usando richieste firmate versione 4 della firma AWS ed estrae l'HBKID per la chiave di wrapping dal testo cifrato. L'HBKID viene utilizzato per ottenere l'EKTnecessario per decrittare il testo cifrato, l'ID chiave e la policy per l'ID chiave. La richiesta è autorizzata in base alla policy di chiave, alle concessioni che possono essere presenti e a eventuali policy IAM associate che fanno riferimento all'ID chiave. La funzione `Decrypt` è analoga alla funzione di crittografia.

Di seguito è riportata la sintassi di una richiesta `Decrypt`.

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

Di seguito sono riportati i parametri della richiesta.

CiphertextBlob

Testo cifrato che include i metadati.

EncryptionContext

(Facoltativo) Il contesto di crittografia. Se è stato specificato nella funzione `Encrypt`, deve essere specificato anche qui o l'operazione di decrittografia non avrà esito positivo. Per ulteriori informazioni, consultare Contesto della crittografia nella Guida per gli sviluppatori di AWS Key Management Service.

GrantTokens

(Facoltativo) Un elenco dei token di concessione che rappresentano le concessioni che forniscono autorizzazioni per eseguire la decrittografia.

Il testo cifrato e l'EKT vengono inviati, insieme al contesto di crittografia, su una sessione autenticata a un HSM per la decrittografia.

L'HSM completa le seguenti operazioni:

1. Decritta l'EKT per ottenere HBK = Decrypt(DK_i, EKT).
2. Estrae il nonce N dalla struttura del testo cifrato.
3. Rigenera una chiave di crittografia derivata AES-GCM a 256 bit K da HBK e N.
4. Decritta il testo cifrato per ottenere plaintext = Decrypt(K, context, ciphertext).

L'ID chiave risultante e il testo in chiaro vengono restituiti all'host AWS KMS sulla sessione sicura e quindi di nuovo all'applicazione cliente chiamante tramite una connessione TLS.

Di seguito è riportata la sintassi della risposta.

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

Se l'applicazione chiamante vuole garantire che l'autenticità del testo in chiaro, deve verificare che l'ID chiave restituito sia quello previsto.

Nuova crittografia di un oggetto crittografato

Un testo cifrato del cliente esistente crittografato con una chiave KMS può essere ricrittografato con un'altra chiave KMS tramite un comando di ricrittografia. La nuova crittografia crittografa i dati sul lato server con una nuova chiave KMS senza esporre il testo in chiaro della chiave sul lato client. I dati vengono prima decrittati e quindi crittografati.

Di seguito è riportata la sintassi della richiesta.

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

```
}
```

La richiesta accetta i seguenti dati in formato JSON.

CiphertextBlob

Testo cifrato dei dati da ricrittografare.

DestinationEncryptionContext

(Facoltativo) Contesto di crittografia da utilizzare quando i dati vengono ricrittografati.

DestinationKeyId

Identificatore chiave della chiave utilizzata per ricrittografare i dati.

GrantTokens

(Facoltativo) Un elenco dei token di concessione che rappresentano le concessioni che forniscono autorizzazioni per eseguire la decrittografia.

SourceKeyId

(Facoltativo) Identificatore chiave della chiave utilizzata per decrittare i dati.

SourceEncryptionContext

(Facoltativo) Contesto di crittografia utilizzato per crittografare e decrittare i dati specificati nel parametro `CiphertextBlob`.

Il processo combina le operazioni di decrittografia e crittografia delle descrizioni precedenti: il testo cifrato del cliente viene decrittato nell'HBK iniziale a cui fa riferimento il testo cifrato del cliente nell'HBK corrente con la chiave KMS desiderata. Quando le chiavi KMS utilizzate in questo comando sono uguali, il comando sposta il testo cifrato del cliente da una versione precedente di una HBK alla sua versione più recente.

Di seguito è riportata la sintassi della risposta.

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

```
}
```

Se l'applicazione chiamante desidera garantire l'autenticità del testo in chiaro sottostante, deve verificare che il risultato SourceKeyId restituito sia quello previsto.

Operazioni interne di AWS KMS

Gli elementi interni di AWS KMS sono necessari per dimensionare e proteggere i moduli di protezione hardware (HSM) per un servizio di gestione delle chiavi distribuito a livello globale.

Argomenti

Domini e stato del dominio

Una raccolta cooperativa di entità AWS KMS interne attendibili in una Regione AWS viene definita dominio. Un dominio include un set di entità attendibili, un insieme di regole e un set di chiavi segrete, chiamate chiavi di dominio. Le chiavi di dominio sono condivise tra i moduli di protezione hardware (HSM) membri del dominio. Uno stato di dominio è costituito dai seguenti campi:

Nome

Un nome di dominio per identificare questo dominio.

Membri

Un elenco di moduli di protezione hardware (HSM) membri del dominio che includono la chiave di firma pubblica e le chiavi di accordo pubblico.

Operatori

Un elenco di entità, chiavi di firma pubbliche e un ruolo (operatore AWS KMS o host di servizio) che rappresenta gli operatori di questo servizio.

Regolamento

Un elenco di regole quorum per ogni comando che deve essere soddisfatto per eseguire un comando sull'HSM.

Chiavi di dominio

Un elenco di chiavi di dominio (chiavi simmetriche) attualmente in uso all'interno del dominio.

Lo stato completo del dominio è disponibile solo sull'HSM. Lo stato del dominio viene sincronizzato tra i membri del dominio dell'HSM come token di dominio esportato.

Chiavi di dominio

Tutti i moduli di protezione hardware in un dominio condividono un insieme di chiavi di dominio, $\{DK_r\}$. Queste chiavi vengono condivise tramite una routine di esportazione dello stato del dominio. Lo stato del dominio esportato può essere importato in qualsiasi HSM membro del dominio.

L'insieme di chiavi di dominio, $\{DK_r\}$, include sempre una chiave di dominio attiva e diverse chiavi di dominio disattivate. Le chiavi di dominio vengono ruotate ogni giorno per garantire che AWS sia conforme a quanto riportato in Suggerimento per la gestione delle chiavi - Parte 1. Durante la rotazione della chiave di dominio, tutte le chiavi KMS crittografate nella chiave di dominio in uscita vengono nuovamente crittografate con la nuova chiave di dominio attiva. La chiave di dominio attiva viene utilizzata per crittografare qualsiasi nuovo EKT. Le chiavi di dominio scadute possono essere utilizzate solo per decrittare EKT precedentemente crittografati per un numero di giorni equivalente al numero di chiavi di dominio ruotate di recente.

Token di dominio esportati

Esiste una normale necessità di sincronizzare lo stato tra i partecipanti al dominio. Ciò avviene esportando lo stato del dominio ogni volta che viene apportata una modifica al dominio. Lo stato del dominio viene esportato come token di dominio esportato.

Nome

Un nome di dominio per identificare questo dominio.

Membri

Un elenco di moduli di protezione hardware (HSM) membri del dominio che includono la chiave di firma pubblica e la chiavi di accordo pubblico.

Operatori

Un elenco di entità, chiavi di firma pubbliche e un ruolo che rappresenta gli operatori di questo servizio.

Regolamento

Un elenco di regole quorum per ogni comando che deve essere soddisfatto per eseguire un comando su un membro del dominio dell'HSM.

Chiavi di dominio crittografate

Chiavi di dominio crittografate con envelope. Le chiavi di dominio vengono crittografate dal membro firmatario per ciascuno dei membri elencati sopra, con envelope nella chiave di accordo pubblico.

Firma

Una firma sullo stato del dominio prodotto da un HSM, necessariamente un membro del dominio che ha esportato lo stato del dominio.

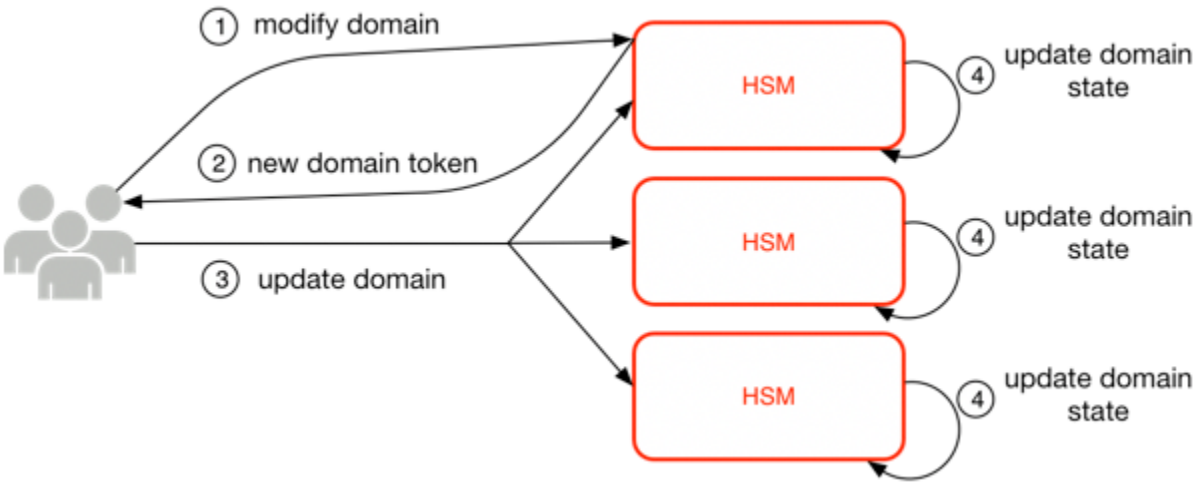
Il token di dominio esportato costituisce la base dell'attendibilità per le entità che operano all'interno del dominio.

Gestione degli stati del dominio

Lo stato del dominio viene gestito tramite comandi autenticati con quorum. Queste modifiche includono la modifica dell'elenco dei partecipanti attendibili nel dominio, la modifica delle regole del quorum per l'esecuzione dei comandi HSM e la rotazione periodica delle chiavi di dominio. Questi comandi vengono autenticati in base al comando anziché alle operazioni di sessione autenticate, come illustrato nell'immagine seguente.

Nel suo stato inizializzato e operativo, un HSM contiene un set di chiavi di identità asimmetriche auto-generate, una coppia di chiavi di firma e una coppia di chiavi per la creazione delle chiavi. Attraverso un processo manuale, un operatore AWS KMS può stabilire un dominio iniziale da creare su un primo HSM in una regione. Questo dominio iniziale è costituito da uno stato di dominio completo, come definito in precedenza in questo argomento. Viene installato tramite un comando join su ciascuno dei membri HSM definiti nel dominio.

Dopo che un HSM ha aderito a un dominio iniziale, è legato alle regole definite in quel dominio. Queste regole definiscono i comandi che utilizzano le chiavi crittografiche del cliente o apportano modifiche allo stato dell'host o del dominio. Le operazioni dell'API di sessione autenticate che utilizzano le chiavi crittografiche sono state definite in precedenza.



L'immagine precedente mostra come viene modificato uno stato di dominio. Il processo è costituito da quattro fasi:

1. Un comando basato su quorum viene inviato a un HSM per modificare il dominio.
2. Un nuovo stato di dominio viene generato ed esportato come nuovo token di dominio esportato. Lo stato sull'HSM non viene modificato, il che significa che la modifica non viene promulgata sull'HSM.
3. Un secondo comando viene inviato a ciascuno degli HSM nel token di dominio appena esportato per aggiornare lo stato del dominio con il nuovo token di dominio.
4. Gli HSM elencati nel nuovo token di dominio esportato possono autenticare il comando e il token di dominio. Possono anche decomprimere le chiavi di dominio per aggiornare lo stato del dominio su tutti gli HSM del dominio.

Gli HSM non comunicano direttamente tra loro. Invece, un quorum di operatori richiede una modifica allo stato del dominio che si traduce in un nuovo token di dominio esportato. Un membro host del servizio del dominio viene utilizzato per distribuire il nuovo stato del dominio a tutti gli HSM del dominio.

L'abbandono e l'unione di un dominio vengono eseguiti tramite le funzioni di gestione HSM. La modifica dello stato del dominio avviene tramite le funzioni di gestione del dominio.

Abbandona dominio

> Fa sì che un HSM lasci un dominio, eliminando dalla memoria tutti i residui e le chiavi di quel dominio.

Unisci dominio

Fa sì che un HSM si unisca a un nuovo dominio o aggiorni lo stato corrente del dominio al nuovo stato del dominio. Il dominio esistente viene utilizzato come origine del set iniziale di regole per autenticare questo messaggio.

Crea dominio

Provoca la creazione di un nuovo dominio su un HSM. Restituisce un primo token di dominio che può essere distribuito agli HSM membri del dominio.

Modifica operatori

Aggiunge o rimuove gli operatori dall'elenco degli operatori autorizzati e i relativi ruoli nel dominio.

Modifica membri

Aggiunge o rimuove un HSM dall'elenco degli HSM autorizzati nel dominio.

Modifica regole

Modifica il set di regole quorum necessarie per eseguire i comandi su un HSM.

Ruota chiavi di dominio

Fa sì che una nuova chiave di dominio venga creata e contrassegnata come chiave di dominio attiva. Questo sposta la chiave attiva esistente su una chiave disattivata e rimuove la chiave disattivata più vecchia dallo stato del dominio.

Sicurezza delle comunicazioni interne

I comandi tra gli host del servizio o gli operatori AWS KMS e i moduli di protezione hardware (HSM) sono protetti tramite due meccanismi descritti in Sessioni autenticate: un metodo di richiesta firmato con quorum e una sessione autenticata tramite un protocollo host del servizio HSM.

I comandi firmati con quorum sono progettati in modo che nessun singolo operatore possa modificare le protezioni di sicurezza critiche fornite dai moduli di protezione hardware. I comandi eseguiti sulle sessioni autenticate garantiscono che solo gli operatori del servizio autorizzati possano eseguire operazioni relative alle chiavi KMS. Tutte le informazioni segrete legate al cliente sono protette nell'infrastruttura AWS.

Creazione delle chiavi

Per proteggere le comunicazioni interne ,AWS KMS utilizza due diversi metodi di creazione delle chiavi. Il primo è definito come C(1, 2, ECC DH) in Suggerimento per schemi di creazione di chiavi a coppia che utilizzano la crittografia a logaritmo discreto (Revisione 2). Questo schema ha un iniziatore con una chiave di firma statica. L'iniziatore genera e firma una chiave sulla curva ellittica Diffie-Hellman (ECDH) effimera, per un destinatario con una chiave di accordo ECDH statica. Questo metodo utilizza una chiave effimera e due chiavi statiche con ECDH. Questa è la derivazione dell'etichetta C(1, 2, ECC DH). Il metodo è talvolta chiamato ECDH a un passaggio.

Il secondo metodo per la creazione di una chiave è C(2, 2, ECC, DH). In questo schema, entrambe le parti hanno una chiave di firma statica e generano, firmano e scambiano una chiave ECDH effimera. Questo metodo utilizza due chiavi statiche e due chiavi effimere, ognuna con ECDH. Questa è la derivazione dell'etichetta C(2, 2, ECC DH). Questo metodo è talvolta chiamato ECDH effimero o ECDHE. Tutte le chiavi ECDH vengono generate sulla curva secp384r1 (NIST-P384).

Limite di sicurezza HSM

Il limite di sicurezza interno di AWS KMS è l'HSM. L'HSM ha un'interfaccia proprietaria e nessun'altra interfaccia fisica attiva nel suo stato operativo. Durante l'inizializzazione viene eseguito il provisioning di un HSM operativo con le chiavi di crittografia necessarie per stabilire il proprio ruolo nel dominio. I materiali crittografici sensibili dell'HSM vengono archiviati nella memoria volatile e sono cancellati solo quando il modulo HSM non è in stato operativo, inclusi arresti o ripristini previsti o non intenzionali.

Le operazioni API HSM vengono autenticate da singoli comandi o tramite una sessione riservata autenticata reciprocamente stabilita da un host di servizio.

Comandi firmati con quorum

I comandi firmati con quorum vengono emessi dagli operatori ai moduli di protezione hardware. In questa sezione viene descritto come i comandi basati su quorum vengono creati, firmati e autenticati.

Queste regole sono abbastanza semplici. Ad esempio, per essere autenticato il comando Foo richiede due membri dal ruolo Bar. Per la creazione e la verifica di un comando basato su quorum sono necessari tre passaggi. Il primo passo è la creazione iniziale del comando, il secondo è l'invio ad operatori aggiuntivi per la firma e il terzo è la verifica e l'esecuzione.

Ai fini dell'introduzione dei concetti, si supponga che esista un insieme autentico di chiavi pubbliche e ruoli dell'operatore $\{QOS_s\}$ e una serie di regole con quorum QR = $\{Command_i, Rule_{\{i, t\}}\}$ dove ogni Rule è un insieme di ruoli e numero minimo N $\{Ruolo_t, N_t\}$. Affinché un comando soddisfi la regola del quorum, il set di dati dei comandi deve essere firmato da un set di operatori elencati in $\{QOS_s\}$ in modo che soddisfino una delle regole elencate per quel comando. Come accennato in precedenza, l'insieme di regole del quorum e degli operatori viene memorizzato nello stato del dominio e nel token di dominio esportato.

In pratica, un firmatario iniziale firma il comando $Sig_1 = Sign(dO_{p1}, Command)$. Anche un secondo operatore firma il comando $Sig_2 = Sign(dO_{p2}, Command)$. Il messaggio doppiamente firmato viene inviato a un HSM per l'esecuzione. L'HSM completa le seguenti attività:

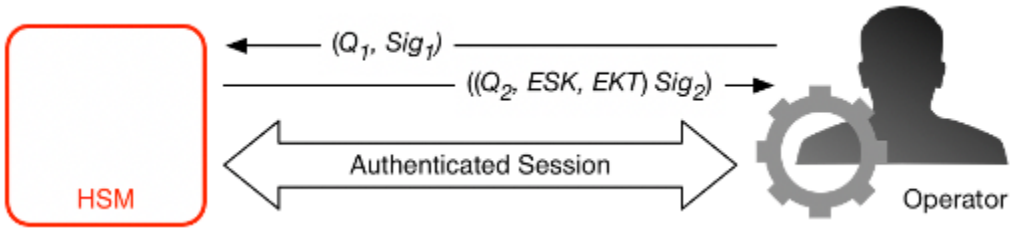
1. Per ogni firma, viene estratta la chiave pubblica del firmatario dallo stato del dominio e viene verificata la firma sul comando.
2. Verifica che il set di firmatari soddisfi una regola per il comando.

Sessioni autenticate

Le operazioni principali vengono eseguite tra gli host AWS KMS che puntano all'esterno e i moduli di protezione hardware. Questi comandi riguardano la creazione e l'uso di chiavi di crittografia e la generazione di numeri casuali sicuri. I comandi vengono eseguiti su un canale autenticato dalla sessione tra gli host del servizio e i moduli di protezione hardware. Oltre alla necessità di autenticità, queste sessioni richiedono la riservatezza. I comandi in esecuzione su queste sessioni includono la restituzione di chiavi di dati in chiaro e messaggi decrittografati destinati all'utente. Per garantire che queste sessioni non possano essere sovvertite da man-in-the-middle attacchi, le sessioni vengono autenticate.

Questo protocollo esegue un accordo chiave ECDHE reciprocamente autenticato tra HSM e l'host del servizio. Lo scambio viene avviato dall'host del servizio e completato dall'HSM. L'HSM restituisce anche una chiave di sessione (SK) crittografata dalla chiave negoziata e un token chiave esportato che contiene la chiave di sessione. Il token chiave esportato contiene un periodo di validità, dopo il quale l'host del servizio deve rinegoziare una chiave di sessione.

Un host di servizio è un membro del dominio e dispone di una coppia di chiavi con firma dell'identità($dHOS_i$, $QHOS_i$) e una copia autentica delle chiavi pubbliche di identità degli HSM. Utilizza il set di chiavi di firma dell'identità per negoziare in modo sicuro una chiave di sessione che può essere utilizzata tra l'host del servizio e qualsiasi HSM nel dominio. Ai token chiave esportati è associato un periodo di validità, dopodiché è necessario negoziare una nuova chiave.



Il processo inizia con il riconoscimento host del servizio che richiede una chiave di sessione per inviare e ricevere flussi di comunicazione sensibili tra sé stesso e un membro HSM del dominio.

1. Un host di servizio genera una coppia di chiavi ECDH effimere d_1, Q_1) e la firma con la sua chiave di identità Sig1 = Sign(dOS, Q_1).
2. HSM verifica la firma sulla chiave pubblica ricevuta utilizzando il token dominio corrente e crea una coppia di chiavi ECDH effimere d_2, Q_2). Completa quindi lo scambio di chiavi ECDH-in base a quanto riportato in Suggerimento per schemi di creazione di chiavi a coppia che utilizzano la crittografia a logaritmo discreto (revisionata) per formare una chiave AES-GCM a 256 bit negoziata. L'HSM genera una nuova chiave di sessione AES-GCM a 256 bit. Crittografa la chiave di sessione con la chiave negoziata per formare la chiave di sessione crittografata (ESK). Crittografa anche la chiave di sessione con la chiave di dominio come token chiave esportato EKT. Infine, firma un valore di ritorno con la sua coppia di chiavi di identità Sig_2 =Sign(dHSK, (Q_2, ESK, EKT)).
3. L'host del servizio verifica la firma sulle chiavi ricevute utilizzando il token di dominio corrente. Completa quindi lo scambio di chiavi ECDH-in base a quanto riportato in Suggerimento per schemi di creazione di chiavi a coppia che utilizzano la crittografia a logaritmo discreto (revisionata). Successivamente decrittografa l'ESK per ottenere la chiave di sessione SK.

Durante il periodo di validità nell'EKT, l'host del servizio può utilizzare la chiave di sessione negoziataSK per inviare comandi crittografati con envelope all'HSM. Ogni service-host-initiated comando di questa sessione autenticata include l'EKT. L'HSM risponde utilizzando la stessa chiave di sessione negoziata SK.

Processo di replica per chiavi multi-regione

AWS KMS utilizza un meccanismo di replica tra regioni per copiare il materiale chiave in una chiave KMS da un HSM in una Regione AWS in un HSM in un'altra Regione AWS. Perché questo meccanismo funzioni, la chiave KMS replicata deve essere una chiave multi-regione. Quando si replica una chiave KMS da una regione all'altra, gli HSM nelle regioni non possono comunicare direttamente perché si trovano in reti isolate. I messaggi scambiati durante la replica tra regioni vengono invece recapitati da un servizio proxy.

Durante la replica tra regioni, ogni messaggio generato da un HSM AWS KMS è firmato crittograficamente tramite unachiave di firma della replica. Le chiavi di firma della replica (RSK, Replication Signing Keys) sono chiavi ECDSA sulla curva NIST P-384. Ogni regione possiede almeno una chiave RSK e la componente pubblica di ogni RSK è condivisa con ogni altra regione nella stessa partizione AWS.

Il processo di replica tra regioni per copiare il materiale chiave dalla regione A alla regione B funziona come segue:

1. L'HSM nella regione B genera una chiave ECDH effimera sulla curva NIST P-384, la chiave B dell'accordo di replica (RAKB). La componente pubblica della chiave RAKB viene inviata a un HSM nella regione A dal servizio proxy.
2. L'HSM nella regione A riceve la componente pubblica di RAKB e genera quindi un'altra chiave ECDH effimera sulla curva NIST P-384, la chiave A dell'accordo di replica (RAKA). L'HSM gestisce lo schema di istituzione della chiave ECDH su RAKA e la componente pubblica di RAKB e deriva una chiave simmetrica dall'output, la chiave di replica di wrapping (RWK). La chiave RWK viene utilizzata per crittografare il materiale delle chiavi della chiave KMS multi-regione che viene replicata.
3. La componente pubblica di RAKA e il materiale chiave crittografato con la RWK vengono inviati all'HSM nella regione B tramite il servizio proxy.
4. L'HSM nella regione B riceve la componente pubblica di RAKA e il materiale chiave crittografato tramite la RWK. L'HSM deriva da RWK eseguendo lo schema di istituzione della chiave ECDH su RAKB e la componente pubblica di RAKA.
5. L'HSM nella regione B utilizza la RWK per decrittare il materiale chiave dalla regione A.

Protezione della durabilità

La durabilità aggiuntiva dei servizi per le chiavi generate dal servizio è fornita dall'uso di moduli di protezione hardware (HSM) offline, più archiviazione non volatile dei token di dominio esportati e archiviazione ridondante delle chiavi KMS crittografate. I moduli di protezione hardware offline sono membri dei domini esistenti. Ad eccezione del non essere online e partecipare alle normali operazioni di dominio, gli HSM offline vengono visualizzati in modo identico nello stato del dominio dei membri HSM esistenti.

Il design della durabilità è destinato a proteggere tutte le chiavi KMS in una regione nel caso in cui in AWS si verifichi una perdita su larga scala degli HSM online o del set di chiavi KMS archiviati nel sistema di archiviazione principale. Le AWS KMS keys con il materiale principale importato non sono incluse nelle protezioni di durabilità offerte dalle altre chiavi KMS. In caso di errore a livello di regione in AWS KMS, il materiale delle chiavi importate potrebbe dover essere reimportato in una chiave KMS.

Gli HSM offline e le credenziali per accedervi vengono archiviati in casseforti all'interno di sale protette monitorate in più località geografiche indipendenti. Per ottenere questi materiali, ogni cassaforte richiede almeno un addetto alla sicurezza AWS e un operatore AWS KMS, da due team indipendenti in AWS. L'uso di questi materiali è regolato da una policy interna che richiede la presenza un quorum di operatori AWS KMS.

Riferimento

Utilizzare il seguente materiale di riferimento per ottenere informazioni su abbreviazioni, chiavi, collaboratori e fonti citate in questo documento.

Argomenti

Abbreviazioni

Nell'elenco seguente vengono illustrate le abbreviazioni a cui si fa riferimento in questo documento.

AES

: Standard di crittografia avanzata

CDK

: chiave di dati dei clienti

DK

: chiave di dominio

ECDH

: Curva ellittica Diffie-Hellman

ECDHE

: Curva ellittica Diffie-Hellman effimera

ECDSA

: Elliptic-Curve Digital Signature Algorithm (ECDSA)

EKT

: token di chiave esportato

ESK

chiave di sessione crittografata

GCM

Galois Counter Mode

HBK

Chiave di supporto HSM

HBKID

Identificatore chiave di supporto HSM

HSM

Modulo di sicurezza hardware

RSA

Rivest Shamir and Adleman (criptologico)

secp384r1

Standard per la crittografia efficiente Curva casuale 1 a 384 bit primi

SHA256

Lunghezza algoritmo hash sicuro del digest 256 bit

Chiavi

L'elenco seguente riporta le chiavi a cui si fa riferimento in questo documento.

HBK

Chiave di supporto HSM: le chiavi di supporto HSM sono chiavi root a 256 bit, da cui derivano chiavi di utilizzo specifiche.

DK

Chiave di dominio: una chiave di dominio è una chiave AES-GCM a 256 bit. È condivisa tra tutti i membri di un dominio e viene utilizzata per proteggere il materiale delle chiavi di supporto HSM e le chiavi di sessione host del servizio HSM.

DKEK

Chiave di crittografia della chiave di dominio: una chiave di crittografia della chiave di dominio è una chiave AES-256-GCM generata su un host e utilizzata per crittografare il set corrente di chiavi di dominio per sincronizzare lo stato del dominio tra gli host HSM.

(dHAK,QHAK)

Coppia di chiavi di accordo HSM: ogni HSM avviato dispone di una coppia di chiavi di accordo sulla curva ellittica Diffie-Hellman generata in locale sulla curva secp384r1 (NIST-P384).

(dE, QE)

Coppia di chiavi di accordo effimero: HSM e host di servizio generano le chiavi di accordo effimero. Queste sono chiavi a curva ellittica Diffie-Hellman sulla curva secp384r1 (NIST-P384). Questi vengono generati in due casi d'uso: per stabilire una chiave di host-to-host crittografia per trasportare le chiavi di crittografia delle chiavi di dominio nei token di dominio e per stabilire le chiavi di sessione dell'host del servizio HSM per proteggere le comunicazioni sensibili.

(dHSK,QHSK)

Coppia di chiavi di firma HSM: ogni HSM avviato dispone di una chiave di firma digitale su curva ellittica generata in locale sulla curva secp384r1 (NIST-P384).

(dOS,QOS)

Coppia di chiavi di firma dell'operatore: sia gli operatori host del servizio che gli operatori AWS KMS dispongono di una chiave di firma dell'identità utilizzata per autenticarsi con altri partecipanti al dominio.

K

Chiave di crittografia dei dati: una chiave AES-GCM a 256 bit derivata da un HBK che utilizza il KDF SP800-108 NIST in modalità contatore utilizzando HMAC con SHA256.

SK

Chiave di sessione: una chiave di sessione viene creata come risultato di una chiave su curva ellittica Diffie-Hellman autenticata scambiata tra un operatore host di servizio e un HSM. Lo scopo dello scambio è quello di proteggere la comunicazione tra l'host del servizio e i membri del dominio.

Collaboratori

Le seguenti persone e organizzazioni hanno contribuito a questo documento:

- Ken Beer, General Manager - KMS, crittografia AWS
- Matthew Campagna, Principal Security Engineer, crittografia AWS

Bibliografia

Per informazioni sugli HSM AWS Key Management Service, passare alla pagina di ricerca del Cryptographic Module Validation Program del Centro risorse per la sicurezza informatica NIST e cercare AWS Key Management Service HSM.

Amazon Web Services, Riferimento generale (versione 1.0), "Firma della richiesta API AWS" http://docs.aws.amazon.com/general/latest/gr/signing_aws_api_requests.html.

Amazon Web Services, "Qual è AWS Encryption SDK", http://docs.aws.amazon.com/encryption-sdk/latest/developer-guide/introduction.html.

Pubblicazioni di Federal Information Processing Standards, FIPS PUB 180-4. Secure Hash Standard, agosto 2012. Disponibile da https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf.

Federal Information Processing Standards Publication 197, Announcing the Advanced Encryption Standard (AES), novembre 2001. Disponibile da http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

Federal Information Processing Standards Publication 198-1, The Keyed-Hash Message Authentication Code (HMAC), luglio 2008. Disponibile da http://csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1_final.pdf.

Pubblicazione speciale NIST 800-52 Revisione 2, Linee guida per la selezione, la configurazione e l'uso delle implementazioni di Transport Layer Security (TLS), agosto 2019. SpecialPublicationshttps://nvlpubs.nist.gov/nistpubs/ /NIST.sp.800-52R2.pdf.

PKCS#1 v2.2: RSA Cryptography Standard (RFC 8017), Internet Engineering Task Force (IETF), novembre 2016. https://tools.ietf.org/html/rfc8017.

Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, NIST Special Publication 800-38D, novembre 2007. Disponibile da 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, NIST Special Publication 800-38E, gennaio 2010. Disponibile da https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38e.pdf.

Recommendation for Key Derivation Using Pseudorandom Functions, NIST Special Publication 800-108, ottobre 2009, disponibile da https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-108.pdf.

Recommendation for Key Management - Part 1: General (Revision 5), NIST Special Publication 800-57A, maggio 2020, disponibile da https://doi.org/10.6028/NIST.SP.800-57pt1r5.

Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revised), NIST Special Publication 800-56A Revision 3 aprile 2018. Disponibile all'indirizzo https://nvlpubs.nist.gov/nistpubs/ /NIST.sp.800-56ar3.pdf. SpecialPublications

Raccomandazione per la generazione di numeri casuali utilizzando generatori di bit casuali deterministici, pubblicazione speciale NIST 800-90A revisione 1, giugno 2015, disponibile su https://nvlpubs.nist.gov/nistpubs/ /NIST.sp.800-90AR1.pdf. SpecialPublications

SEC 2: Recommended Elliptic Curve Domain Parameters, Standards for Efficient Cryptography Group, Version 2.0, 27 gennaio 2010.

Use of Elliptic Curve Cryptography (ECC) Algorithms in Cryptographic Message Syntax (CMS), Brown, D., Turner, S., Internet Engineering Task Force, luglio 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), American National Standards Institute, 2005.

Cronologia dei documenti per Dettagli della crittografia di AWS KMS

Nella tabella seguente vengono descritte importanti modifiche apportate a Dettagli della crittografia di AWS Key Management Service. Inoltre, aggiorniamo la documentazione frequentemente per dar spazio al feedback inviatoci.

Modifica	Descrizione	Data
Contenuti aggiornati	Aggiunti dettagli sull'implementazione dell'operazione AWS KMS `ReplicateKey` .	28 ottobre 2021
Modifica della documentazione	Sostituzione del termine chiave master cliente (CMK) con AWS KMS key e chiave KMS.	30 agosto 2021
Versione iniziale	Creata questa guida dal documento tecnico Dettagli della crittografia KMS	30 dicembre 2020

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.