[ENGLISH]

Hello,

Cloud Gurus and welcome to this lecture where we're going to take a look at

envelope encryption in a little bit more detail.

So what is envelope encryption? Well,

the main thing to remember is that it's a process for encrypting your data

and it's generally used for files over and above four kilobytes in size.

So let's take a look at the process in action at a higher level.

So I've got a customer master key here in KMS,

and we want to encrypt some data. So first of all,

we'll use the generate data key API,

and this will create our data key and it's also sometimes known as an envelope

key.

So then on data key or envelope key is going to be used to encrypt the data.

So the customer master key encrypts the data key,

and then the data key is used to encrypt the data and finally,

the encrypted data key is stored locally with the data so that it can be

used later on for decryption purposes and KMS does not store

the data keys anywhere. Instead,

the encrypted copy of the data key is stored with your

data. So what about the decryption process? Well,

it's pretty much the same process in reverse.

So here is our encrypted data and here's our encrypted data

key, but in order to use our data key, we need to decrypt it first.

So that's where KMS comes in and in KMS we'll use the CMK and

the KMS API to run a decrypt operation and

return the data key in plain text form and then the

plain text data key is used to decrypt the data.

So then at the end of the process,

the data has been decrypted and the plain text key is deleted from

memory,

but you might be wondering why do we even use envelope encryption?

It seems a pretty convoluted process and it's a reasonable question.

Why not encrypt the data directly using the CMK? Well,

the main reason is for network performance because when you encrypt that

data directly with KMS,

that data needs to be transferred over the network into the KMS service

and with envelopes encryption,

only the data key goes over the network and not your data and then the data key

is used locally in your application or AWS service,

avoiding the need to transfer lots of data over the network to

KMS. So if we're talking about gigabytes or terabytes of data,

we don't want to send that over the network to KMS.

Even if it's going over the Amazon network,

it's just not going to be efficient or performance.

So instead with envelope encryption,

it's only the data key that gets sent over the network to KMS and your data

doesn't move anywhere.

So onto my exam tips for envelope encryption,

just remember that envelope encryption is all about encrypting the key,

which encrypts our data and the CMK is used to encrypt the data

key and it's also called at the envelope key and then it's the data key,

which encrypts our data and envelope encryption is used for

encrypting anything over four kilobytes and it avoids sending all your

data into KMS over the network and finally remember the

generate data key API call,

which is used by KMS to create an encrypted data key

and if you remember, when we were playing around with the KMS API,

we ran a generate data key and it returned an encrypted and plain text

version of a data key.

So that is everything that you should need to know for the exam about envelope

encryption. If you have any questions, please let me know.

Otherwise feel free to move on to the next lecture. Thank you.

[SPANISH]

Hola,

Cloud Gurus y bienvenidos a esta conferencia en la que vamos a echar un vistazo a

de sobres con un poco más de detalle.

Entonces, ¿qué es el cifrado de sobres? Bien,

lo principal que debe recordar es que es un proceso para cifrar sus datos

y generalmente se usa para archivos de más de cuatro kilobytes de tamaño.

Así que echemos un vistazo al proceso en acción a un nivel superior.

Así que tengo una clave maestra de cliente aquí en KMS,

y queremos cifrar algunos datos. Entonces, en primer lugar,

usaremos la API de generación de clave de datos,

y esto creará nuestra clave de datos y a veces también se conoce como sobre

llave \_

Entonces, se utilizará la clave de datos o la clave de sobre para cifrar los datos.

Entonces, la clave maestra del cliente encripta la clave de datos,

y luego la clave de datos se usa para cifrar los datos y finalmente,

la clave de datos cifrados se almacena localmente con los datos para que pueda ser

se utiliza más adelante con fines de descifrado y KMS no almacena

las claves de datos en cualquier lugar. En cambio,

la copia cifrada de la clave de datos se almacena con su

datos \_ Entonces, ¿qué pasa con el proceso de descifrado? Bien,

es más o menos el mismo proceso a la inversa.

Así que aquí están nuestros datos encriptados y aquí están nuestros datos encriptados

key , pero para usar nuestra clave de datos, primero debemos descifrarla.

Ahí es donde entra KMS y en KMS usaremos la CMK y

la API de KMS para ejecutar una operación de descifrado y

devolver la clave de datos en forma de texto sin formato y luego el

sin formato se utiliza para descifrar los datos.

Entonces, al final del proceso,

los datos se han descifrado y la clave de texto sin formato se ha eliminado de

memoria ,

pero es posible que se pregunte por qué usamos el cifrado de sobres.

Parece un proceso bastante complicado y es una pregunta razonable.

¿Por qué no cifrar los datos directamente con la CMK? Bien,

la razón principal es el rendimiento de la red porque cuando cifra eso

datos directamente con KMS,

que los datos deben transferirse a través de la red al servicio KMS

y con cifrado de sobres,

solo la clave de datos pasa por la red y no sus datos y luego la clave de datos

se usa localmente en su aplicación o servicio de AWS,

evitando la necesidad de transferir muchos datos a través de la red para

KMS. Entonces, si estamos hablando de gigabytes o terabytes de datos,

queremos enviar eso a través de la red a KMS.

Incluso si va a través de la red de Amazon,

no va a ser eficiente o de rendimiento.

Entonces, en lugar de encriptar sobres,

es solo la clave de datos que se envía a través de la red a KMS y sus datos

no se mueve a ningún lado.

Entonces, en mis consejos de examen para el cifrado de sobres,

solo recuerde que el cifrado del sobre consiste en cifrar la clave,

que cifra nuestros datos y la CMK se utiliza para cifrar los datos

key y también se llama en la clave del sobre y luego es la clave de datos,

que cifra nuestros datos y el cifrado de sobres se utiliza para

cifrar cualquier cosa de más de cuatro kilobytes y evita enviar todos sus

datos en KMS a través de la red y finalmente recordar el

generar llamada de API de clave de datos,

que utiliza KMS para crear una clave de datos cifrada

y si recuerdas, cuando jugábamos con la API de KMS,

ejecutamos una clave de generación de datos y devolvió un texto encriptado y sin formato

versión de una clave de datos.

Eso es todo lo que debe saber para el examen sobre sobres.

cifrado \_ Si tiene alguna pregunta, por favor hágamelo saber.

De lo contrario, siéntase libre de pasar a la siguiente lección. Gracias.