UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

LONGBEAM TECHNOLOGIES LLC, Plaintiff v. **AMAZON.COM, INC., and AMAZON WEB SERVICES, INC.,** Defendants	**Case No. 1:21-cv-01559-CFC** **JURY TRIAL DEMANDED**

AMENDED COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Longbeam Technologies LLC ("Plaintiff" or "Longbeam"), by and through its undersigned counsel, files this Complaint against Amazon.com, Inc. ("Amazon") and Amazon Web Services, Inc. ("AWS Inc.") (collectively "Defendants") for patent infringement of United States Patent Nos. 7,512,989, 7,660,418, 8,472,627, and 10,715,316 (collectively, the "Patents-in-Suit") and alleges as follows:

NATURE OF THE ACTION

1. This is an action for patent infringement arising under the patent laws of the United States, 35 U.S.C. §§ 1 *et seq.*

THE PARTIES

2. Longbeam is a limited liability company organized and existing under the laws of the State of Texas with a principal place of business at 10900 Research Blvd., Suite 160C PMB 1113, Austin, TX 78759.

3. Amazon is a corporation organized and existing under the laws of the State of Delaware with a principal place of business at 410 Terry Ave N, Seattle, WA, 98109-5210.

4. AWS Inc. is a corporation organized and existing under the laws of the State of Delaware with a principal place of business at 410 Terry Ave N, Seattle, WA, 98109-5210.

JURISDICTION AND VENUE

5. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. §§ 1331 and 1338(a) because this action arises under the patent laws of the United States, 35 U.S.C. §§ 1 *et seq*.

6. Defendants are subject to the personal jurisdiction of this Court based upon them being Delaware corporations, such that each Defendant is essentially at home in the State of Delaware.

7. Venue is proper in this judicial district pursuant to 28 U.S.C. § 1400(b) because each Defendant is incorporated in Delaware and/or formed under the laws of Delaware, and therefore, resides in this District.

THE PATENTS-IN-SUIT

8. On March 30, 2009, the United States Patent and Trademark Office duly and legally issued United States Patent No. 7,512,989 ("the '989 Patent") entitled "DATA LOADER USING LOCATION IDENTITY TO PROVIDE SECURE COMMUNICATION OF DATA TO RECIPIENT DEVICES" to inventor Logan Scott. A true and correct copy of the '989 Patent is attached as Exhibit A.

9. The '989 Patent is presumed valid under 35 U.S.C. § 282.

10. Plaintiff owns all rights, title, and interest in the '989 Patent.

11. On February 9, 2010, the United States Patent and Trademark Office duly and legally issued United States Patent No. 7,660,418 ("the '418 Patent") entitled "CRYPTOGRAPHIC SYSTEM AND METHOD FOR GEOLOCKING AND SECURING DIGITAL INFORMATION" to inventors Barry J. Glick, Ronald S. Karpf, and Mark E. Seiler. A true and correct copy of the '418 Patent is attached as Exhibit B.

12. The '418 Patent is presumed valid under 35 U.S.C. § 282.

13. Plaintiff owns all rights, title, and interest in the '418 Patent.

14. On June 25, 2013, the United States Patent and Trademark Office duly and legally issued United States Patent No. 8,472,627 ("the '627 Patent") entitled "SYSTEM AND METHOD FOR DELIVERING ENCRYPTED INFORMATION IN A COMMUNICATION NETWORK USING LOCATION IDENTITY AND KEY TABLES" to inventors Dorothy E. Denning, Barry J. Glick, Ronald S. Karpf, and Mark E. Seiler. A true and correct copy of the '627 Patent is attached as Exhibit C.

15. The '627 Patent is presumed valid under 35 U.S.C. § 282.

16. Plaintiff owns all rights, title, and interest in the '627 Patent.

17. On July 14, 2020, the United States Patent and Trademark Office duly and legally issued United States Patent No. 10,715,316 ("the '316 Patent") entitled "SYSTEM AND METHOD FOR DELIVERING INFORMATION IN A COMMUNCATION NETWORK USING LOCATION IDENTITY" to inventors Dorothy E. Denning, Barry J. Glick, Ronald S. Karpf, and Mark E. Seiler. A true and correct copy of the '316 Patent is attached as Exhibit D.

18. The '316 Patent is presumed valid under 35 U.S.C. § 282.

19. Plaintiff owns all rights, title, and interest in the '316 Patent.

20. The claims of the Patents-in-Suit, including the asserted claims, when viewed as a whole, including as an ordered combination, are not merely the recitation

of well-understood, routine, or conventional technologies or components. *See* Decl. of Dr. Craig E. Wills at ¶¶ 2, 20-22, 25, 28, 31, 34.

21. The claimed inventions were not well-known, routine, or conventional at the time of the inventions—some almost twenty years ago—and represent specific improvements over the prior art and prior existing systems and methods, as well as technical solutions to technical problems in networks and computers. *See* Decl. of Dr. Craig E. Wills at ¶¶ 2, 20-22, 25, 28, 31, 34.

22. At the time of the inventions of the Patents-in-Suit, conventional cryptographic systems contained an inherent risk in distributing keys to recipients of encrypted information. ’989 Patent at 1:48-49. The security of a communication network depended on the physical control of devices used to transfer confidential information. ’989 at 1:48-67. If such a device were to be misplaced, then the security of the entire communication network would be compromised. *Id.*

23. Moreover, at the time of the inventions of the Patents-in-Suit, conventional cryptographic systems could not keep pace with the explosive growth of the Internet in providing proper information security. ’418 Patent at 1:21–2:7.

24. Including as of the year 2002, there were several, albeit vastly inferior, means outside of the claimed inventions for providing security to communication systems, such as private-key encryption systems and public-key encryption systems. *See* ’418 Patent at 2:8-55. Private-key systems faced a disadvantage in

controlling access to the volumes of information traffic on the Internet, due to the difficulty of distributing a secret key among many users without risking they key's compromise. '418 Patent at 2:14-18; *see also* Decl. of Dr. Craig E. Wills at ¶ 18. Public-key systems were disadvantageous because they were computationally intensive and therefore slow to use. '418 Patent at 2:31-32; *see also* Decl. of Dr. Craig E. Wills at ¶ 18. Further, as recited in the specification of the '418 Patent:

> The distribution of public keys present[ed] another problem, thereby spawning the growth of companies (e.g., Verisign, Inc.) that act[ed] as centralized registrars or signing authorities to access and validate public keys. In view of these disadvantages, public key encryption [were] used only for [a] small portion of total Internet communications. For most such communications, the security problem [was] not deemed serious enough to warrant the inconvenience and cost of public key management.

'418 Patent at 2:37-45.

25. Additionally, because key management is vested in a single entity in conventional encryption systems—particularly private-key systems—data providers that do not have key management authority were limited in their ability to control access to their digital data through the networks. '627 Patent at 2:62–3:2; *see also* Decl. of Dr. Craig E. Wills at ¶ 18.

26. At the time of the inventions of the Patents-in-Suit, the unauthorized copying of copyright-protected digital content was rampant. Using conventional computing and communication systems, individuals could easily make and distribute an unlimited number of identical copies of copyrighted works in digital

form (e.g., music, literary works, photography, video, software, etc.). ’418 Patent at 2:58-62. Commercially available file indexing services such as Napster and Gnutella allowed computer users to easily locate and access digital files on other user’s computer systems—increasing the potential for widespread copyright piracy and representing a serious threat to copyright owners. ’418 Patent at 2:56–3:17.

27. Available methods at the time of the inventions to combat copyright piracy presented incomplete and disadvantageous solutions. Actively policing the Internet, for example, was—and remains—logistically difficult given the widespread and anonymous nature of the Internet. ’418 Patent at 3:18-37. Further, digital rights management (DRM) systems were inferior for a number of reasons. As recited in the specification of the ’418 Patent:

> First, given the availability of pirated content on the Internet, it is far more convenient and inexpensive for a user to unlawfully download a digital file over the Internet than to purchase a legitimate copy of the material via conventional channels of trade. While the unlawfully obtained material may have reduced quality in comparison to the legitimate copy, the convenience and negligible cost often make up for this drawback. Second, most DRM technologies rely upon some form of encryption to protect the digital information. To be most effective, both parties to an encryption scheme must have a vested interest in maintaining the secrecy of the encrypted information. A legal purchaser of content has a right to view the content, but has no vested interest in ensuring that the secrecy afforded by encryption is maintained. For this reason, many DRM solutions utilize digital certificates or licenses that attempt to hide the decryption key from the user. In such systems, all copies of the content are encrypted in an identical manner, and the media player validates the user's right to display or play back the decrypted content. Since the encrypted content and decryption key are nevertheless accessible to the user albeit hidden, a sophisticated user

> may reverse engineer the DRM solution to strip away the encryption to thereby permit unimpeded copying and distribution of the decrypted content. Other less sophisticated ways of obtaining an unencrypted copy of the content are also available to unscrupulous users, such as videotaping each frame of a digital video data file as that content is legally displayed during playback.

’418 Patent at 3:39-67.

28. In light of these drawbacks in the prior art, the inventors of the Patents-in-Suit wanted, among other things, to provide a system for providing secure communication of information or access to data such that the information or data could only be communicated or accessed at a specified location. ’989 Patent at 2:19-22 (“[I]t would be desirable to provide a system for providing secure communication of information to recipient devices in a manner such that the information can be communicated or accessed at specified locations.”); *see also* ’627 Patent at 2:34-35; ’316 Patent at 2:37-38; ’418 Patent at 4:1-16.

29. The claims of the Patents-in-Suit are directed to a specific improvement over conventional encryption techniques that increases the security of communications and digital-information-sharing systems and networks. Decl. of Dr. Craig E. Wills at ¶¶ 19-22, 25, 28, 31, 34. The inventions provide a technical improvement over conventional encryption techniques, in that the claimed geo-encryption approach provides an additional layer of security beyond that provided by conventional cryptography in an unconventional manner. *Id.*; *see also* ’627 Patent at 2:59-61. As recited in the specification of the ’627 Patent:

> By enabling location-based encryption and path-dependent encryption, the present invention has numerous advantages over the prior art. One such advantage is that it adds an additional layer of security to any encryption system. Not only does the recipient need access to a secret key, but the recipient also must be at a particular location in order to decrypt data.

’627 Patent at 27:64–28:4.

30. Claim 31 of the ’989 Patent, for example, recites:

> 31. A method for communicating data to a recipient device, comprising:
>
> using a data encryption key to apply a first layer of encryption to said data;
>
> using at least a customer location value to apply a first layer of encryption to said data encryption key, said customer location value being generated using at least an authorized location of said recipient device;
>
> transmitting, at least indirectly, said encrypted data and said encrypted data encryption key to said recipient device;
>
> determining a current location of said recipient device;
>
> using at least said current location of said recipient device to generate a current location value;
>
> using at least said current location value to remove said first layer of encryption from said data encryption key if said current location value is consistent with said customer location value; and
>
> using said data encryption key to remove said first layer of encryption from said data.

’989 Patent at 17:38-57.

31. Using a unique customer location value and a current location value in the method recited by claim 31 was not well-understood, routine, or conventional at

the time of the ’989 Patent—particularly in applying a layer of encryption to a data encryption key. Decl. of Dr. Craig E. Wills at ¶ 25. Unlike other encryption systems at the time of the ’989 Patent, the inventive techniques claimed in the ’989 Patent added a layer of encryption that would be removable only if the current location a recipient device is consistent with the generated customer location value. *Id.* Claim 31’s recited “geo-encryption” technique is an inventive improvement over prior encryption techniques because, among other things, it increases the security of a communication system or network by allowing data to be encrypted for a specific place or broad geographic area. *Id.* Moreover, claim 31 requires a specific set of ordered steps which achieve this improvement.

32. Claim 12 of the ’418 Patent, for example, recites:

> 12. A file management system for use in an information processing device, the file management system comprising executable instructions fixed in a suitable medium and operable to perform the functions of:
>
> selecting location data corresponding to a specific geographic location at which access rights for a selected file by the information processing device is permitted;
>
> generating a location attribute value based in part on the location data;
>
> associating the location attribute value with the selected file; and
>
> inhibiting file management operations pertaining to the selected file, including any copying, saving and deleting of the selected file, unless a current location of the information processing device corresponds to the location attribute value;

> wherein the location attribute value is based in part on an area parameter defining a shape of a region that encompasses the specific geographic location;
>
> wherein the functions further include generating an encrypting key based on the area parameter; and
>
> wherein the associating function further comprises encrypting the selected file using the encrypting key.

’418 Patent at 22:35-57.

33. Claim 12 recites more than well-understood, routine, and conventional activities previously known in the encryption field at the time of the ’418 Patent. Decl. of Dr. Craig E. Wills at ¶ 28. By utilizing location data and a location attribute value, and further associating the location attribute value with a selected file, the invention of claim 12 recites an improvement over understood and practiced encryption techniques that increases the security of a communication system or network. *Id.* The invention of claim 12 ensures that the selected data cannot be conventionally managed unless, and *only* unless, an information processing device is in a particular, authorized location. Decl. of Dr. Craig E. Wills at ¶ 28. Claim 12 requires a specific set of ordered steps which achieve these improvements over prior techniques.

34. Use of this location attribute and shape of a region to generate a geo-locked key for the selected file was unconventional at the time of the ’418 Patent. *Id.*

35. Claim 22 of the ’627 Patent, for example, recites:

> 22. A method for controlling access to content data, comprising:

> a distributor device (i) using a data encrypting/decrypting key to encrypt the content data, (ii) using a key encrypting/decrypting key to encrypt both the data encrypting/decrypting key and at least one content-owner constraint, and (iii) sending the encrypted content data, the encrypted data encrypting/decrypting key and the at least one encrypted content-owner constraint to a receiver device via a communication network; and
>
> a receiver device (i) receiving via the communications network the encrypted content data, the encrypted data encrypting/decrypting key and the at least one encrypted content-owner constraint, (ii) decrypting both the encrypted data encrypting/decrypting key and the at least one encrypted content-owner constraint, (iii) decrypt the encrypted content data if the at least one content-owner constraint is satisfied, (iv) using a second key encrypting/decrypting key to re-encrypt the data encrypting/decrypting key, and (v) sending the encrypted content data and the re-encrypted data encrypting/decrypting key to at least one other receiver device via the communications network.

’627 Patent at 31:1-29.

36. As recited, the method of claim 22 involves more than well-understood, routine, and conventional activities in the encryption field at the time of the ’627 Patent. Decl. of Dr. Craig E. Wills at ¶ 31. By using a content-owner constraint—which can be a particular geographic location—in the manner recited, the invention improves upon prior encryption methods and provides increased security to a communication network by only allowing content data to be decrypted when the content-owner constraint is satisfied. *Id.* This, for example, could be if the recited receiver device is in an unauthorized geographic location to allow decryption. *Id.* Further, the method of claim 22 recites that a location-dependent distribution path for the content can be created among multiple devices. *Id.* Claim 22 requires a

specific set of ordered steps which achieve these improvements over prior techniques.

37. Claim 12 of the ’316 Patent, for example, recites:

> 12. An apparatus for controlling access to digital information, said digital information comprising a plurality of digital files, comprising:
>
> at least one memory device for storing a location identity for each one of said plurality of digital files, said location identity being received from a corresponding producer device via a network and comprising a location value and a proximity value, said location value comprising a geographical location and said proximity value identifying a geographical region in relation to said geographical location;
>
> at least one application processor in communication with said at least one memory device and configured to (i) prompt a receiver to provide its location to a distributor device, (ii) receive a current location from said receiver device, (iii) receive a request for data from said receiver, and (iv) select one of said plurality of files based on said current location of said receiver and said requested data, said selected one of said plurality of digital files including said data and having a location identity that matches said current location of said receiver device, wherein at least a first other one of said plurality of digital files includes said data but does not match said current location and at least a second other one of said plurality of digital files matches said current location but does not include said data;
>
> wherein said selected one of said plurality of digital files is provided to a user of said receiver device;
>
> wherein said one of said plurality of digital files is selected in response to receiving said request for said data.

’316 Patent at 30:53–31:16.

38. As recited, the elements of claim 12, individually and as a combination, involve more than well-understood, routine, and conventional activities in the

encryption field at the time of the ’316 Patent. Decl. of Dr. Craig E. Wills at ¶ 34. In particular, claim 12’s recited manner of using a location identity, requiring a receiver device to provide its current location to a distributor device, and only providing a digital file to a user of a receiver device if the current location of the receiver device matches the location identity of the requested data, is a specific improvement over prior encryption techniques. *Id.* The invention of claim 12 provides an additional layer of security to a system or network beyond that provided by conventional cryptography because the invention controls access to digital information based on the location of the recited receiver device. *Id.* Further, the invention of claim 12 also allows multiple data providers to make use of a network of distributor devices to deliver content and secret keys to receiver devices in a secure manner. *Id.* Claim 12 requires a specific set of ordered steps which achieve these improvements over prior techniques.

39. These noted improvements over the prior art represent meaningful limitations and/or inventive concepts based upon the state of the art almost twenty years ago. Further, including in view of these specific improvement, the inventions of the claims of the Patents-in-Suit, when such claims are viewed as a whole and in ordered combinations, are not routine, well-understood, conventional, generic, existing, commonly used, or well-known almost twenty years ago.

40. The elements of the claims of the Patents-in-Suit, including as a whole and as an ordered combination, comprise a non-conventional, technical improvement to communications and digital-information-sharing networks and systems, including those improvements listed above such as increased security of the systems and networks. Further, as described above, the Patents-in-Suit disclose a technical solution to a security problem in communication and digital-information-sharing systems and networks.

CLAIMS FOR RELIEF

Count I – Infringement of United States Patent No. 7,512,989

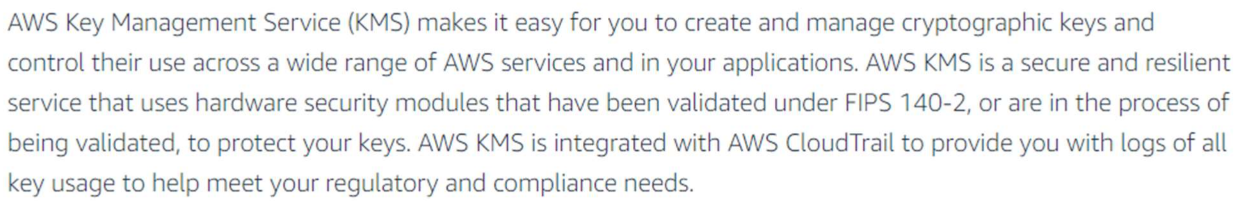
41. Plaintiff repeats, re-alleges, and incorporates by reference, as if fully set forth herein, the preceding paragraphs of this Complaint.

42. Defendants directly infringe (literally and/or under the doctrine of equivalents) the ’989 Patent by using the method covered by at least claim 31 of the ’989 Patent.

43. Defendants’ instrumentality that infringes one or more claims of the ’989 patent includes, but is not limited to, Amazon Web Services (“AWS”), and any other of Defendants’ networks, systems, devices, and/or services that practice a method for communicating data to a recipient device as claimed by the ’989 Patent.

44. AWS practices a method for communicating data to a recipient device.

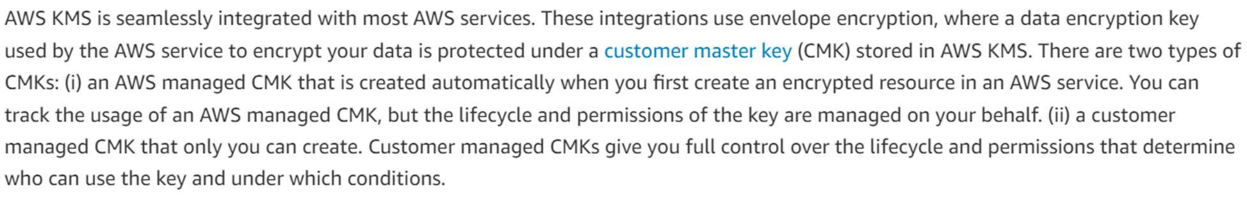
45. On information and belief, AWS provides on-demand cloud computing platforms and APIs to individuals, companies, and governments on a metered pay-as-you-go basis. AWS provides Amazon Key Management Service (KMS) to communicate data in a protected way through encryption/decryption mechanism. Amazon KMS gives a user a centralized control over cryptographic keys used to protect the data.



AWS Key Management Service (KMS) makes it easy for you to create and manage cryptographic keys and control their use across a wide range of AWS services and in your applications. AWS KMS is a secure and resilient service that uses hardware security modules that have been validated under FIPS 140-2, or are in the process of being validated, to protect your keys. AWS KMS is integrated with AWS CloudTrail to provide you with logs of all key usage to help meet your regulatory and compliance needs.

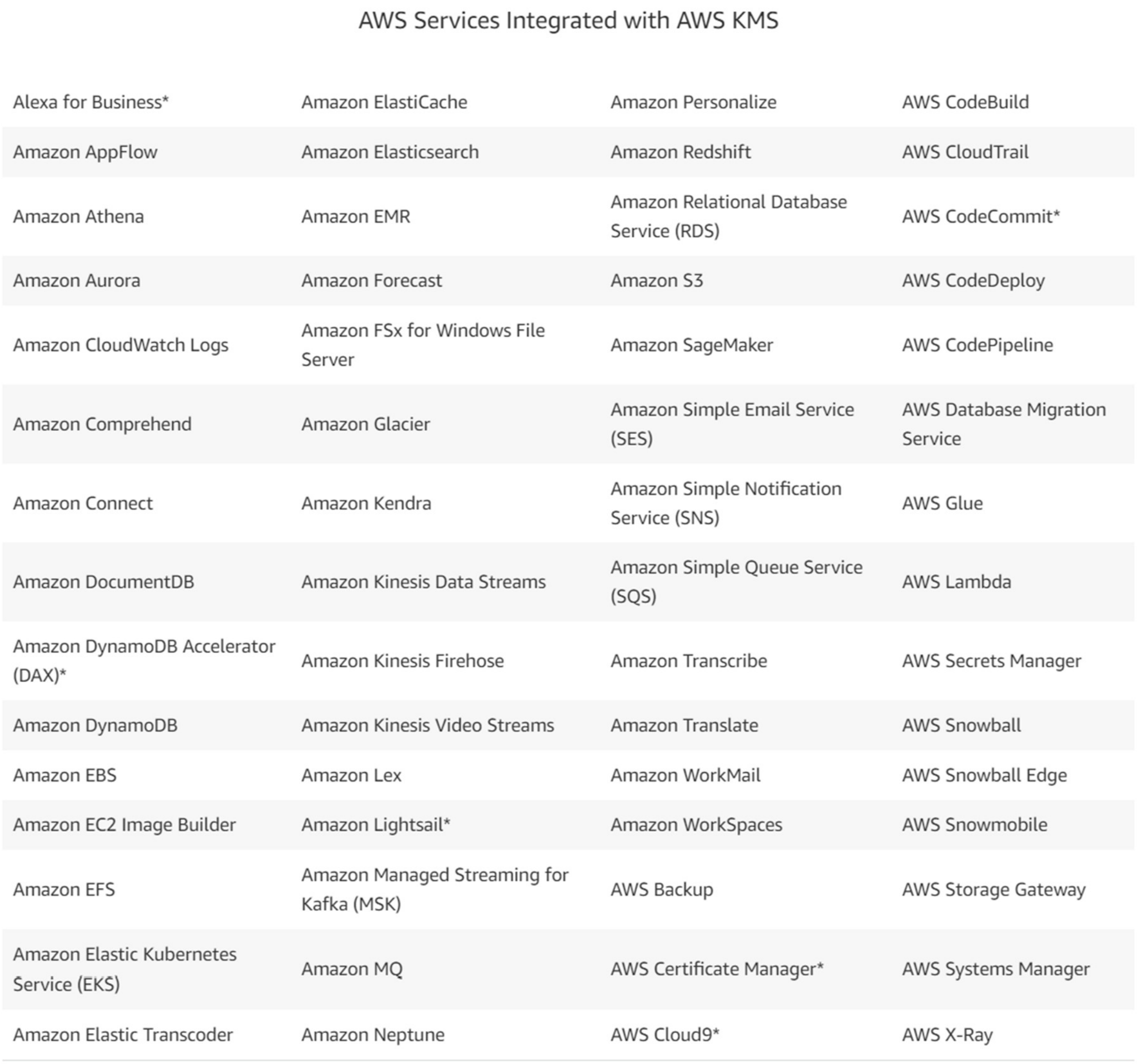
https://aws.amazon.com/kms/

46. On information and belief, the KMS is seamlessly integrated with other AWS services. This integration makes it easy to encrypt data that an AWS service receives, stores, or manages, and control access to the keys used for cryptographic operations.



AWS KMS is seamlessly integrated with most AWS services. These integrations use envelope encryption, where a data encryption key used by the AWS service to encrypt your data is protected under a customer master key (CMK) stored in AWS KMS. There are two types of CMKs: (i) an AWS managed CMK that is created automatically when you first create an encrypted resource in an AWS service. You can track the usage of an AWS managed CMK, but the lifecycle and permissions of the key are managed on your behalf. (ii) a customer managed CMK that only you can create. Customer managed CMKs give you full control over the lifecycle and permissions that determine who can use the key and under which conditions.

https://aws.amazon.com/kms/features/



AWS Services Integrated with AWS KMS

Alexa for Business*	Amazon ElastiCache	Amazon Personalize	AWS CodeBuild
Amazon AppFlow	Amazon Elasticsearch	Amazon Redshift	AWS CloudTrail
Amazon Athena	Amazon EMR	Amazon Relational Database Service (RDS)	AWS CodeCommit*
Amazon Aurora	Amazon Forecast	Amazon S3	AWS CodeDeploy
Amazon CloudWatch Logs	Amazon FSx for Windows File Server	Amazon SageMaker	AWS CodePipeline
Amazon Comprehend	Amazon Glacier	Amazon Simple Email Service (SES)	AWS Database Migration Service
Amazon Connect	Amazon Kendra	Amazon Simple Notification Service (SNS)	AWS Glue
Amazon DocumentDB	Amazon Kinesis Data Streams	Amazon Simple Queue Service (SQS)	AWS Lambda
Amazon DynamoDB Accelerator (DAX)*	Amazon Kinesis Firehose	Amazon Transcribe	AWS Secrets Manager
Amazon DynamoDB	Amazon Kinesis Video Streams	Amazon Translate	AWS Snowball
Amazon EBS	Amazon Lex	Amazon WorkMail	AWS Snowball Edge
Amazon EC2 Image Builder	Amazon Lightsail*	Amazon WorkSpaces	AWS Snowmobile
Amazon EFS	Amazon Managed Streaming for Kafka (MSK)	AWS Backup	AWS Storage Gateway
Amazon Elastic Kubernetes Service (EKS)	Amazon MQ	AWS Certificate Manager*	AWS Systems Manager
Amazon Elastic Transcoder	Amazon Neptune	AWS Cloud9*	AWS X-Ray

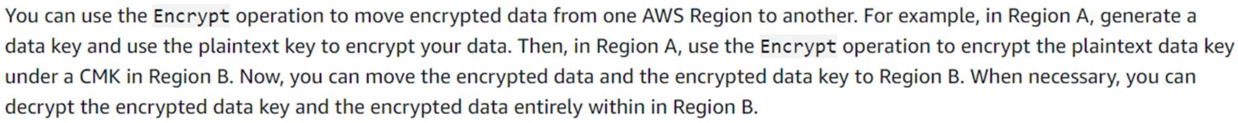
https://aws.amazon.com/kms/features/

47. AWS services are hosted though the AWS cloud infrastructure, which consists of data centers in various regions.

48. On information and belief, each data center is equipped with multiple servers.

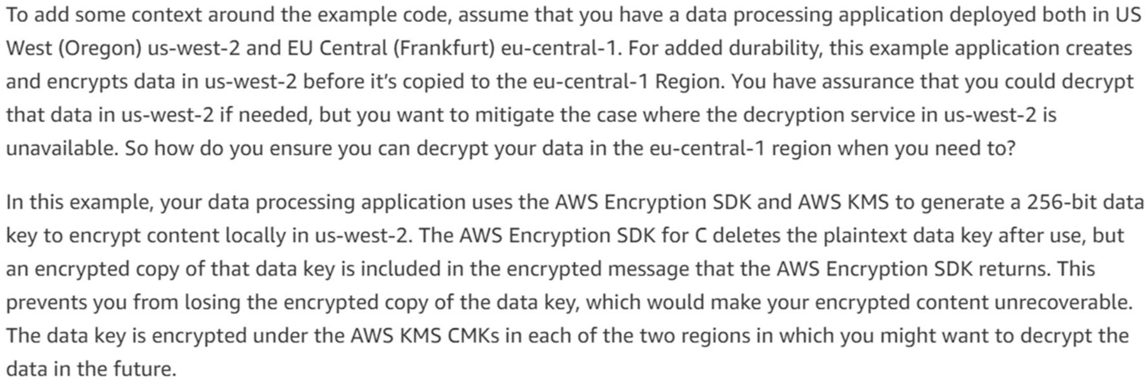
49. On information and belief, using KMS integration with AWS services, data can be transmitted from a server at one AWS region to another server at a

different AWS region securely (i.e. communicating data to a recipient device). For example, a data processing application deployed in two different AWS regions can copy data between regions and manage cryptographic operations through KMS. These integrations use envelope encryption. In envelope encryption, the data that is to be transmitted is encrypted using a data key and the data key is encrypted using a customer master key (CMK) of the intended destination Region.



You can use the `Encrypt` operation to move encrypted data from one AWS Region to another. For example, in Region A, generate a data key and use the plaintext key to encrypt your data. Then, in Region A, use the `Encrypt` operation to encrypt the plaintext data key under a CMK in Region B. Now, you can move the encrypted data and the encrypted data key to Region B. When necessary, you can decrypt the encrypted data key and the encrypted data entirely within in Region B.

https://docs.aws.amazon.com/kms/latest/APIReference/API_Encrypt.html



To add some context around the example code, assume that you have a data processing application deployed both in US West (Oregon) us-west-2 and EU Central (Frankfurt) eu-central-1. For added durability, this example application creates and encrypts data in us-west-2 before it's copied to the eu-central-1 Region. You have assurance that you could decrypt that data in us-west-2 if needed, but you want to mitigate the case where the decryption service in us-west-2 is unavailable. So how do you ensure you can decrypt your data in the eu-central-1 region when you need to?

In this example, your data processing application uses the AWS Encryption SDK and AWS KMS to generate a 256-bit data key to encrypt content locally in us-west-2. The AWS Encryption SDK for C deletes the plaintext data key after use, but an encrypted copy of that data key is included in the encrypted message that the AWS Encryption SDK returns. This prevents you from losing the encrypted copy of the data key, which would make your encrypted content unrecoverable. The data key is encrypted under the AWS KMS CMKs in each of the two regions in which you might want to decrypt the data in the future.

https://aws.amazon.com/blogs/security/how-to-decrypt-ciphertexts-multiple-regionsaws-encryption-sdk-in-c/

50. On information and belief, the encrypted data and the encrypted data key are then sent to a recipient region.

51. If the recipient region is the intended destination, the data key (and hence the data) can be successfully decrypted since the data key is encrypted using the destination CMK—and CMKs are bound to the regions where they are created.

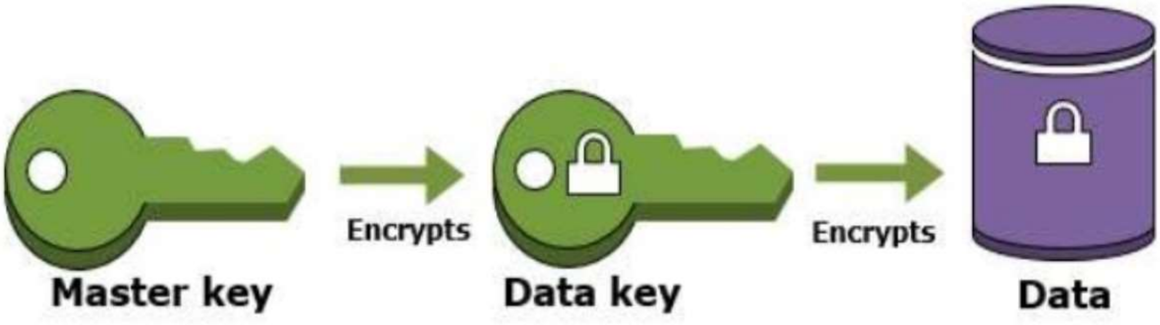
52. If the recipient region is not the intended destination, it does not have the CMK to decrypt the data key (and in turn the data), and therefore cannot decrypt the data. Thus, KMS provides a region-based access to data.

53. On information and belief, AWS allows using a data encryption key to apply a first layer of encryption to said data. AWS allows for integration of KMS with other services enabling secure data transfer using envelope encryption.

54. With envelope encryption, the data that is to be protected is encrypted (i.e. apply a first layer of encryption) using the data key (i.e., data encryption key) generated by AWS KMS.

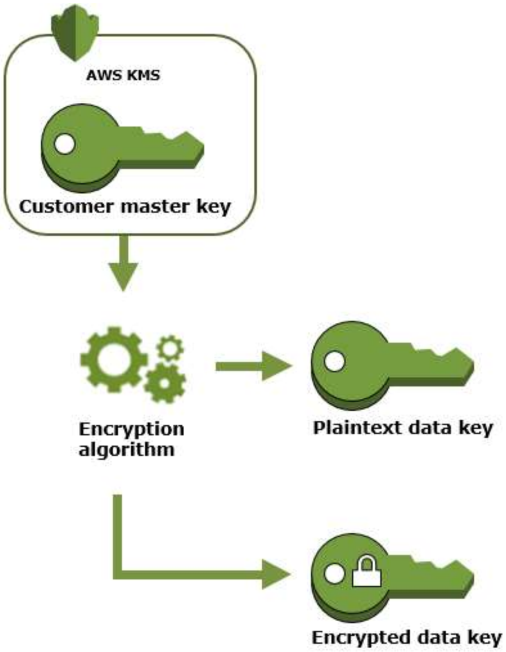
55. On information and belief, the method practiced by AWS comprises using at least a customer location value to apply a first layer of encryption (e.g., encryption of data key using CMK) to said data encryption key (e.g., data key), said customer location value being generated using at least an authorized location (e.g., intended region of data centre, etc.) of said recipient device (e.g., a server at AWS data centre). AWS employs envelope encryption for encrypting the data using the data key (i.e., data encryption key) and then encrypting (i.e. apply a first layer of

encryption) the data key using customer master key (CMK) (i.e., key encrypting key).

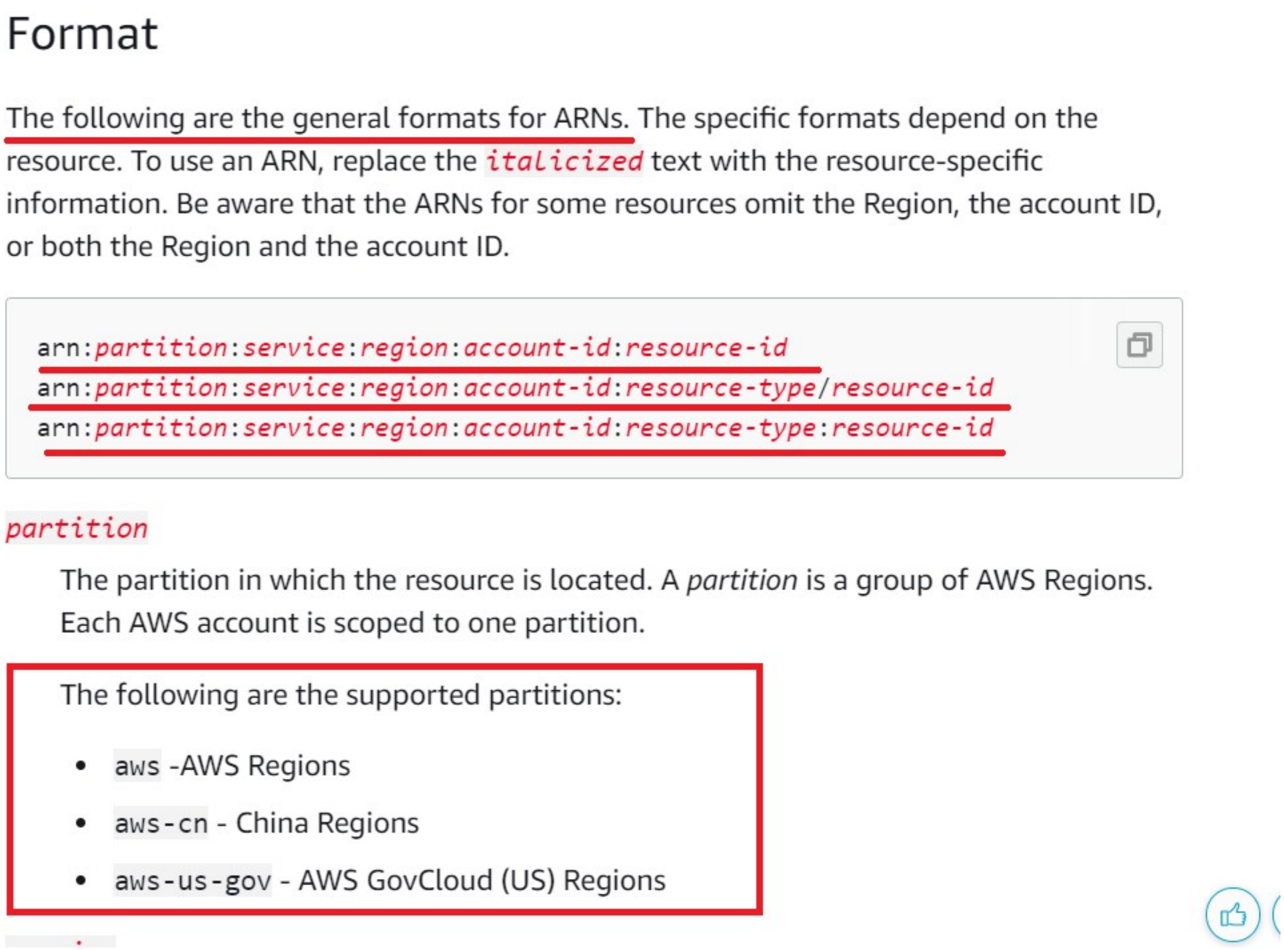


https://www.slideshare.net/AmazonWebServices/aws-security-webinar-the-key-to-effective-cloud-encryption

56. On information and belief, the Data Key is encrypted under the Customer master keys (CMKs). The Customer Master Key (CMK) is bound to an AWS region for which it is meant to work and cannot work outside that specific AWS region. Thus, each CMK indicates an AWS region (and a region code) for which it is meant to work in its ARN value.



https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html



Format

The following are the general formats for ARNs. The specific formats depend on the resource. To use an ARN, replace the *italicized* text with the resource-specific information. Be aware that the ARNs for some resources omit the Region, the account ID, or both the Region and the account ID.

```
arn:partition:service:region:account-id:resource-id
arn:partition:service:region:account-id:resource-type/resource-id
arn:partition:service:region:account-id:resource-type:resource-id
```

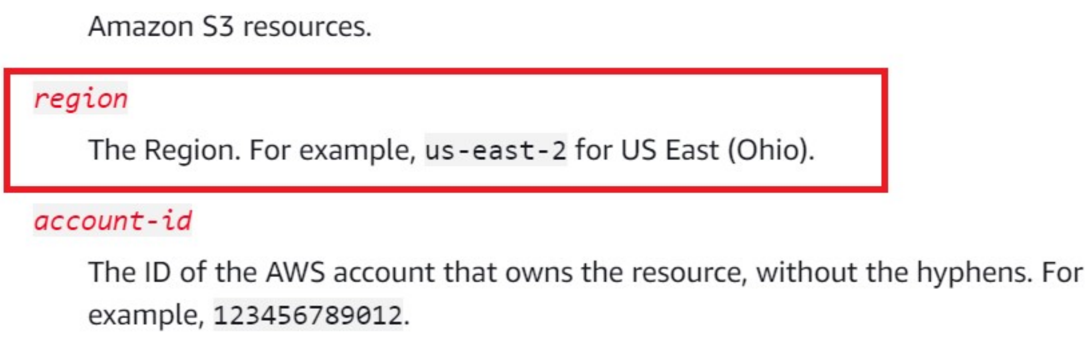
partition

The partition in which the resource is located. A *partition* is a group of AWS Regions. Each AWS account is scoped to one partition.

The following are the supported partitions:

- `aws` -AWS Regions
- `aws-cn` - China Regions
- `aws-us-gov` - AWS GovCloud (US) Regions

https://docs.aws.amazon.com/general/latest/gr/aws-arns-and-namespaces.html



Amazon S3 resources.

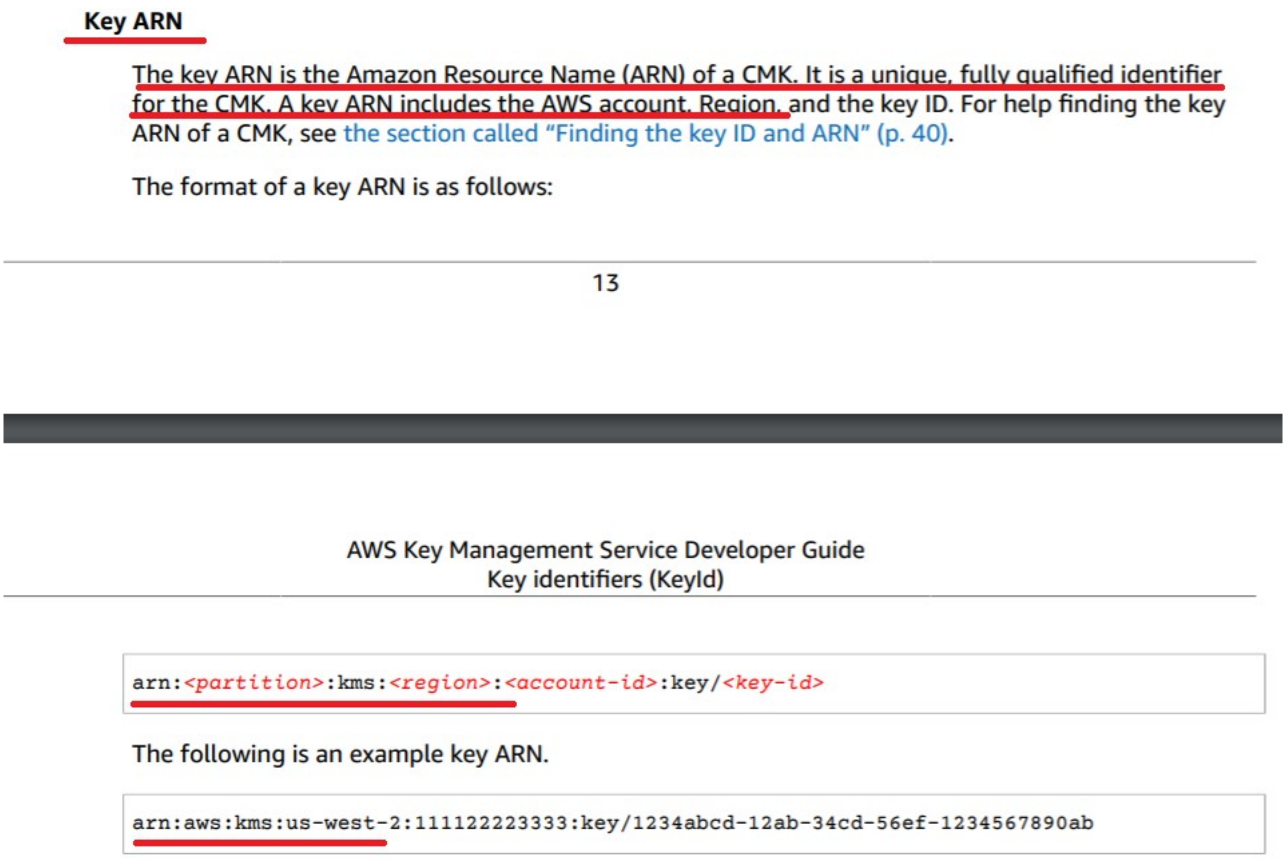
region

The Region. For example, `us-east-2` for US East (Ohio).

account-id

The ID of the AWS account that owns the resource, without the hyphens. For example, `123456789012`.

https://docs.aws.amazon.com/general/latest/gr/aws-arns-and-namespaces.html



Key ARN

The key ARN is the Amazon Resource Name (ARN) of a CMK. It is a unique, fully qualified identifier for the CMK. A key ARN includes the AWS account, Region, and the key ID. For help finding the key ARN of a CMK, see the section called "Finding the key ID and ARN" (p. 40).

The format of a key ARN is as follows:

13

AWS Key Management Service Developer Guide
Key identifiers (KeyId)

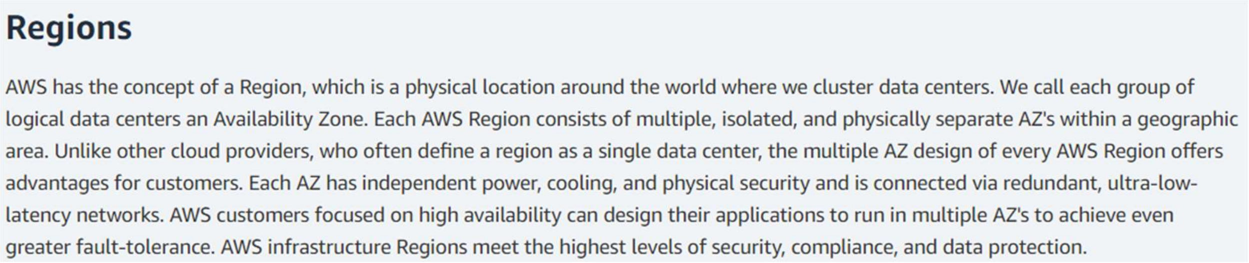
```
arn:<partition>:kms:<region>:<account-id>:key/<key-id>
```

The following is an example key ARN.

```
arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab
```

https://docs.aws.amazon.com/kms/latest/developerguide/kms-dg.pdf#workflow

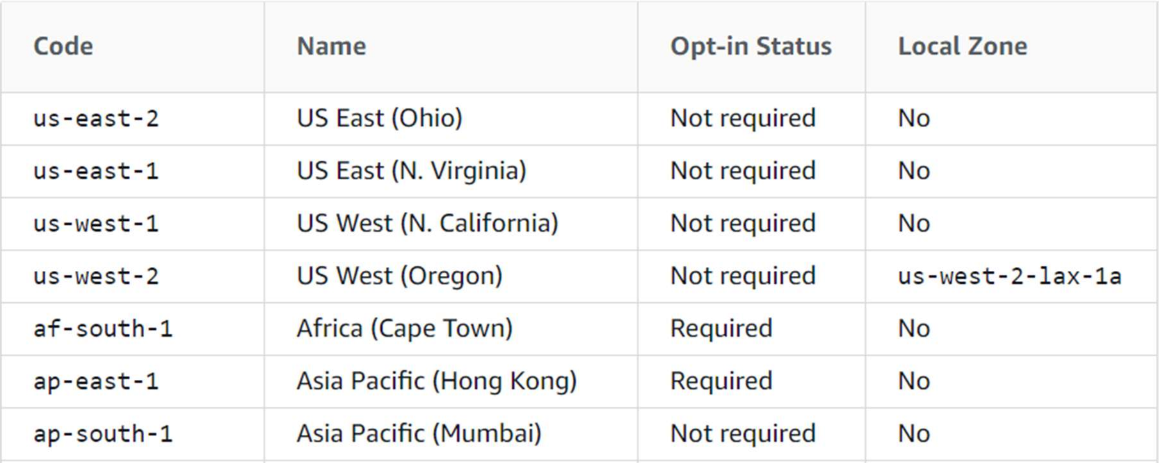
57. On information and belief, the name of the AWS region serves as an authorized location where the decryption process will work. The region code for the region can be generated using this name. As an example, AWS Region in Ohio is named "US East (Ohio)" and represented as "us-east-2" (i.e. customer location value). Further, each AWS region has a cluster of data centers that contain servers where all the services are hosted. AWS services receive data at these servers (i.e., recipient device). The code of the AWS region to which the encrypted data is intended to be sent can be construed as customer location value.



Regions

AWS has the concept of a Region, which is a physical location around the world where we cluster data centers. We call each group of logical data centers an Availability Zone. Each AWS Region consists of multiple, isolated, and physically separate AZ's within a geographic area. Unlike other cloud providers, who often define a region as a single data center, the multiple AZ design of every AWS Region offers advantages for customers. Each AZ has independent power, cooling, and physical security and is connected via redundant, ultra-low-latency networks. AWS customers focused on high availability can design their applications to run in multiple AZ's to achieve even greater fault-tolerance. AWS infrastructure Regions meet the highest levels of security, compliance, and data protection.

https://aws.amazon.com/about-aws/global-infrastructure/regions_az/

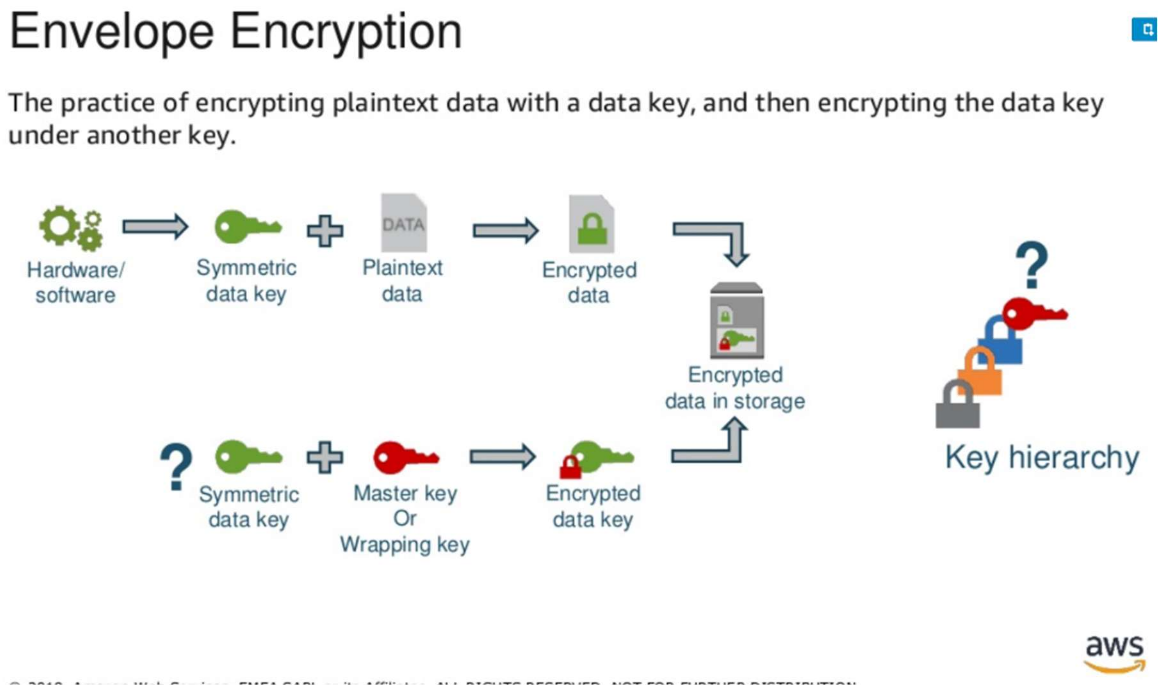


Code	Name	Opt-in Status	Local Zone
`us-east-2`	US East (Ohio)	Not required	No
`us-east-1`	US East (N. Virginia)	Not required	No
`us-west-1`	US West (N. California)	Not required	No
`us-west-2`	US West (Oregon)	Not required	`us-west-2-lax-1a`
`af-south-1`	Africa (Cape Town)	Required	No
`ap-east-1`	Asia Pacific (Hong Kong)	Required	No
`ap-south-1`	Asia Pacific (Mumbai)	Not required	No

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html

58. To securely move encrypted data, data keys (i.e., data encryption key) can be encrypted (i.e., apply a first layer of encryption) using CMK that is associated with a destination AWS region such as us-west-2 (i.e., customer location value). In this manner, the protected data can be accessed (or decrypted) only by services in the destined AWS region that CMK is used initially to encrypt data. Thus, the data key is encrypted using the customer master key (CMK), which already has an inherited location identity.

59. On information and belief, the method practiced by AWS comprises communicating the encrypted location-modified data encrypting Key and the encrypted digital information (e.g., envelope encrypted data) to a recipient device such that the encrypted digital information can be decrypted by the recipient only at specific geographic location. AWS encrypts data keys using region-based CMKs. After the envelope encryption, both encrypted data and encrypted data key (i.e., said encrypted data and encrypted data encrypting key) are stored together to enable other applications to decrypt the data. Using KMS integration, the stored data can be transmitted from the AWS server in the source region to the AWS server in the destination region (i.e. recipient device).



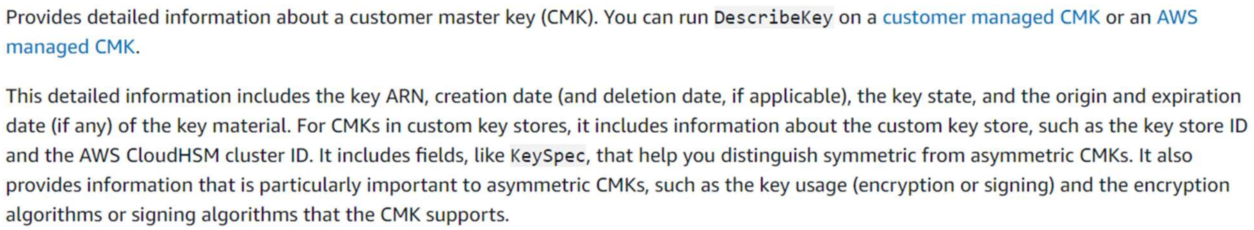
Envelope Encryption

The practice of encrypting plaintext data with a data key, and then encrypting the data key under another key.

https://www.slideshare.net/AmazonWebServices/aws-security-webinar-the-key-to-effective-cloud-encryption

60. On information and belief, AWS determines a current location of the recipient device and using at least said current location of said recipient device to generate a current location value. AWS practices location-based access to data.

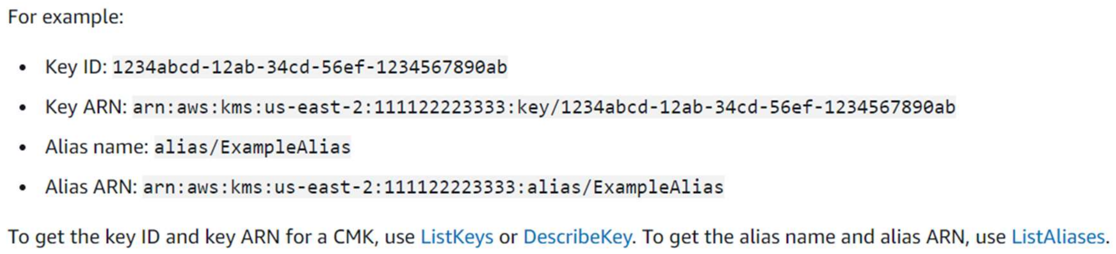
61. The Data Key is generated under the Customer Master Key (CMK). As shown below, details of Master Key can be viewed using the command – Describe key, which entails information of the origin (i.e. location), creation date, etc. Master keys are stored by AWS KMS in the data center of the AWS region in which the master key is meant to work and cannot be shared across AWS regions. Thus, the CMK of the region where encrypted data is received indicates the current location (e.g., "US East (Ohio)") and current location value (e.g., "us-east-2") of the AWS server (i.e. recipient device).



Provides detailed information about a customer master key (CMK). You can run `DescribeKey` on a customer managed CMK or an AWS managed CMK.

This detailed information includes the key ARN, creation date (and deletion date, if applicable), the key state, and the origin and expiration date (if any) of the key material. For CMKs in custom key stores, it includes information about the custom key store, such as the key store ID and the AWS CloudHSM cluster ID. It includes fields, like `KeySpec`, that help you distinguish symmetric from asymmetric CMKs. It also provides information that is particularly important to asymmetric CMKs, such as the key usage (encryption or signing) and the encryption algorithms or signing algorithms that the CMK supports.

https://docs.aws.amazon.com/kms/latest/APIReference/API_DescribeKey.html

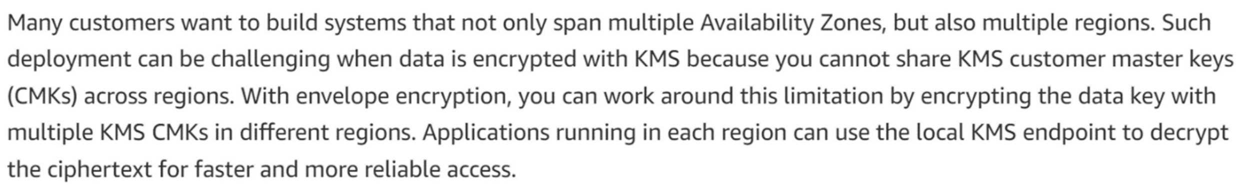


For example:

- Key ID: `1234abcd-12ab-34cd-56ef-1234567890ab`
- Key ARN: `arn:aws:kms:us-east-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`
- Alias name: `alias/ExampleAlias`
- Alias ARN: `arn:aws:kms:us-east-2:111122223333:alias/ExampleAlias`

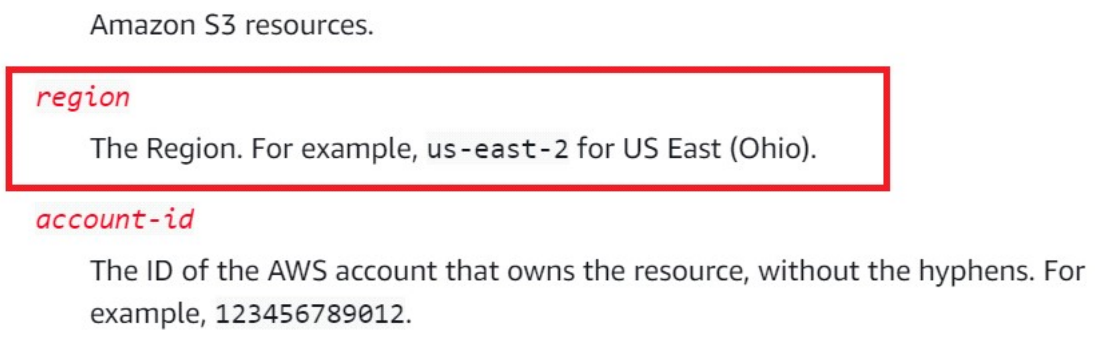
To get the key ID and key ARN for a CMK, use ListKeys or DescribeKey. To get the alias name and alias ARN, use ListAliases.

https://docs.aws.amazon.com/kms/latest/APIReference/API_DescribeKey.html



Many customers want to build systems that not only span multiple Availability Zones, but also multiple regions. Such deployment can be challenging when data is encrypted with KMS because you cannot share KMS customer master keys (CMKs) across regions. With envelope encryption, you can work around this limitation by encrypting the data key with multiple KMS CMKs in different regions. Applications running in each region can use the local KMS endpoint to decrypt the ciphertext for faster and more reliable access.

https://aws.amazon.com/blogs/security/how-to-use-the-new-aws-encryption-sdk-to-simplify-data-encryption-and-improve-application-availability/



Amazon S3 resources.

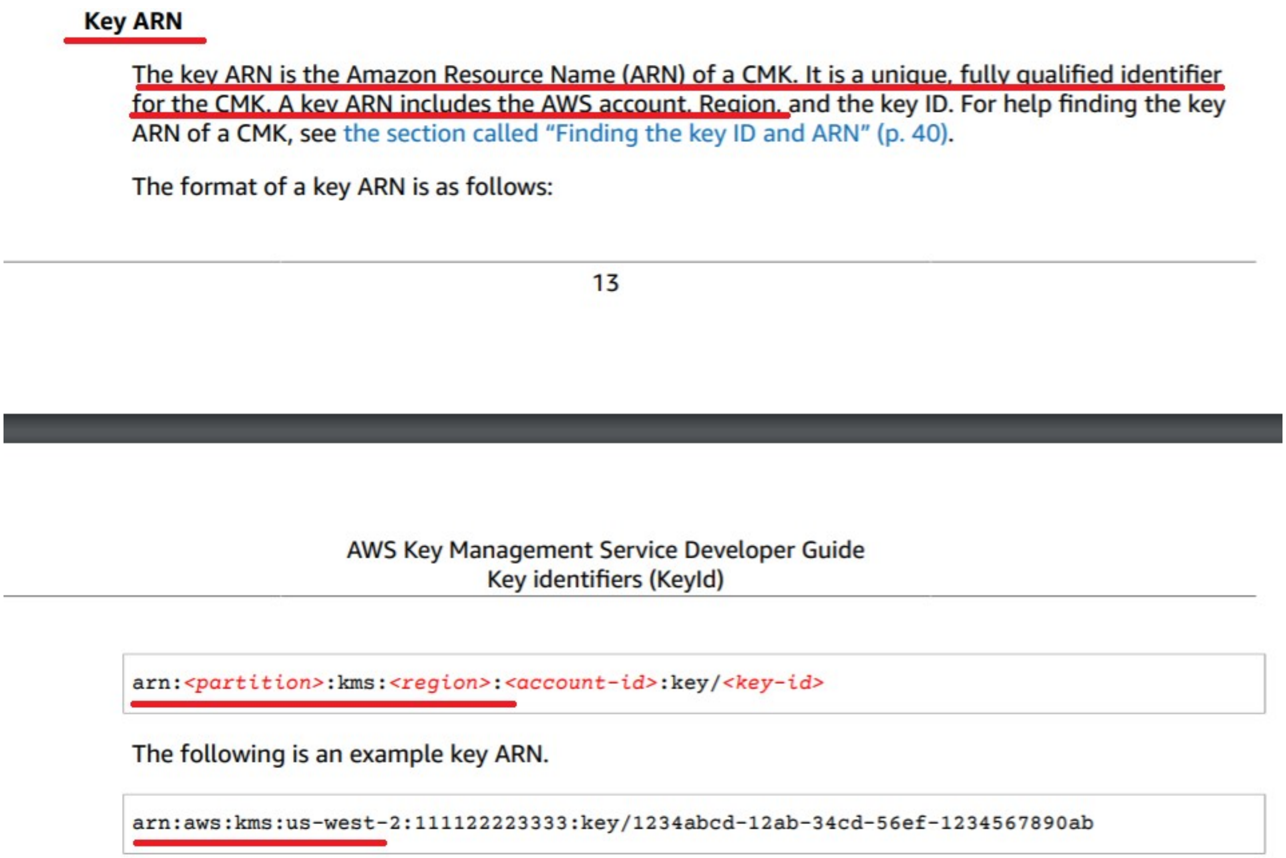
region

The Region. For example, `us-east-2` for US East (Ohio).

account-id

The ID of the AWS account that owns the resource, without the hyphens. For example, `123456789012`.

https://docs.aws.amazon.com/kms/latest/developerguide/kms-dg.pdf#workflow



Key ARN

The key ARN is the Amazon Resource Name (ARN) of a CMK. It is a unique, fully qualified identifier for the CMK. A key ARN includes the AWS account, Region, and the key ID. For help finding the key ARN of a CMK, see the section called "Finding the key ID and ARN" (p. 40).

The format of a key ARN is as follows:

13

AWS Key Management Service Developer Guide
Key identifiers (KeyId)

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

The following is an example key ARN.

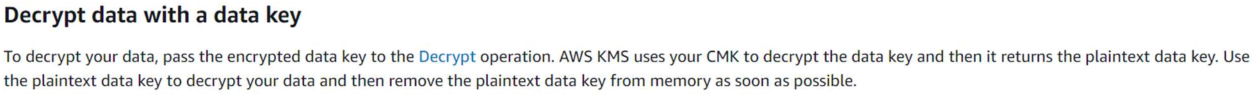
```
arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab
```

https://docs.aws.amazon.com/kms/latest/developerguide/kms-dg.pdf#workflow

62. On information and belief, the method practiced by AWS comprises using at least said current location value to remove said first layer of encryption from said data encryption key (e.g., encrypted data key) if said current location value is consistent with said customer location value. AWS practices transmitting encrypted data to a destination AWS region, and the data key is encrypted under the CMK of the destination AWS region (which inherits a customer location value). The CMK of the region in which the protected information is being decrypted indicates the current location value. The data key (i.e. data encryption key) can be decrypted (i.e., remove first layer of encryption) only if it is being decrypted in the region it was

initially encrypted for (i.e. if current location value is consistent with customer location value).

63. On information and belief, the method practiced by AWS comprises using said data encryption key (e.g., data key) to remove said first layer of encryption from said data. As shown, AWS practices decrypting the encrypted data key by passing the encrypted key to the Decrypt operation and using the CMK of the destination region. The decrypt operation returns a plaintext data key. Once, the data key is decrypted, the encrypted data can be decrypted (i.e. remove first layer of encryption from data) using the data key (i.e. data encryption key).

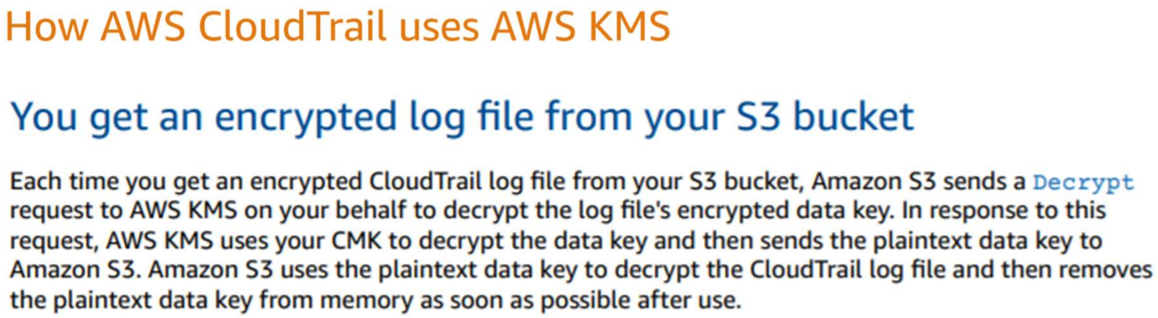


Decrypt data with a data key

To decrypt your data, pass the encrypted data key to the Decrypt operation. AWS KMS uses your CMK to decrypt the data key and then it returns the plaintext data key. Use the plaintext data key to decrypt your data and then remove the plaintext data key from memory as soon as possible.

https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html

64. As an example, the plaintext data key is used by S3 to decrypt the log files and then the plaintext key is removed from the memory.



How AWS CloudTrail uses AWS KMS

You get an encrypted log file from your S3 bucket

Each time you get an encrypted CloudTrail log file from your S3 bucket, Amazon S3 sends a `Decrypt` request to AWS KMS on your behalf to decrypt the log file's encrypted data key. In response to this request, AWS KMS uses your CMK to decrypt the data key and then sends the plaintext data key to Amazon S3. Amazon S3 uses the plaintext data key to decrypt the CloudTrail log file and then removes the plaintext data key from memory as soon as possible after use.

https://docs.aws.amazon.com/kms/latest/developerguide/kms-dg.pdf

65. Plaintiff has been damaged by the direct infringement of Defendants and is suffering and will continue to suffer irreparable harm and damages as a result of this infringement.

Count II – Infringement of United States Patent No. 7,660,418

66. Plaintiff repeats, re-alleges, and incorporates by reference, as if fully set forth herein, the preceding paragraphs of this Complaint.

67. Defendants directly infringe (literally and/or under the doctrine of equivalents) the ’418 Patent by using the method covered by at least claim 12 of the ’418 Patent.

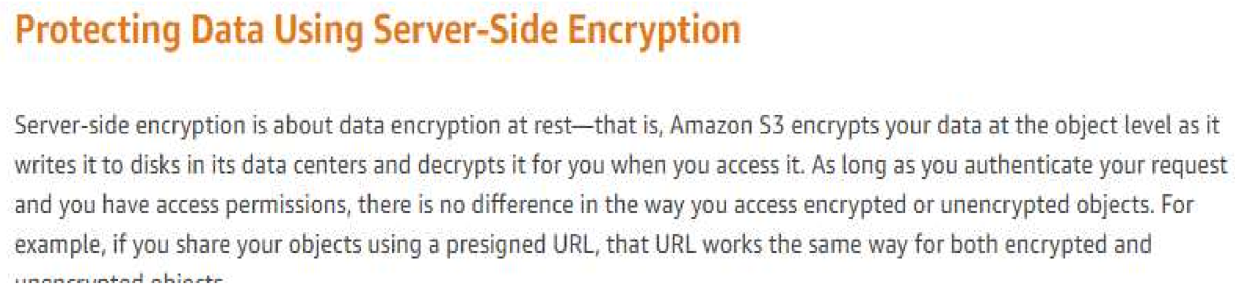
68. Defendants’ instrumentality that infringes one or more claims of the ’418 Patent includes, but is not limited to, AWS and any other of Defendants’ network, systems, devices, and/or services that practice a file management system as claimed in the ’418 Patent.

69. AWS has a file management system for use in an information processing device, the file management system comprising executable instructions fixed in a suitable medium. AWS provides on-demand cloud computing platforms and APIs to individuals, companies, and governments, on a metered pay-as-you-go basis. AWS provides services like S3, EBS etc which are data storage infrastructures. AWS also includes KMS as one of its services to protect data through

encryption/decryption mechanism. KMS seamlessly integrates with AWS storage services like S3, to provide a File Management System.

70. AWS services are hosted through the AWS cloud infrastructure, which consists of data centers in various regions. These data centers are equipped with servers (i.e. information processing device) that have processors and memory to store coded instructions. These processors perform the operations requested by various AWS services.

71. AWS selects a location data (e.g. region field in CMK) corresponding to a specific geographic location (e.g. US west, US east, etc.) at which access rights for a selected file by the information processing device is permitted. Amazon S3, by AWS, encrypts user data using server-side encryption and decrypts it upon access. The decryption is done based on authentication and access permissions.



Protecting Data Using Server-Side Encryption

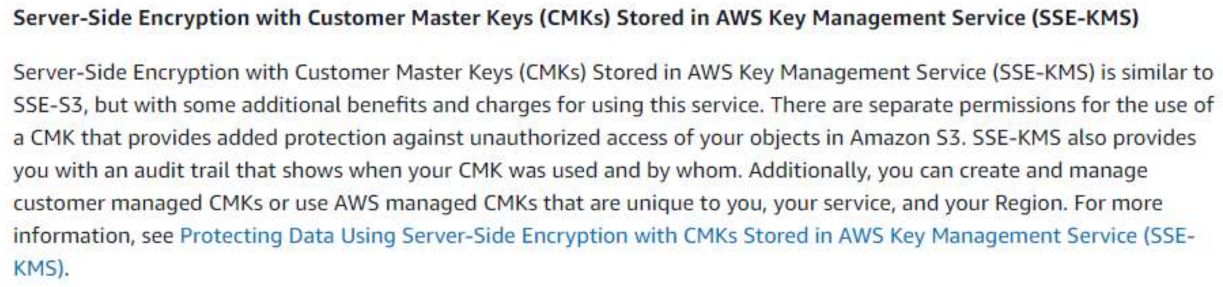
Server-side encryption is about data encryption at rest—that is, Amazon S3 encrypts your data at the object level as it writes it to disks in its data centers and decrypts it for you when you access it. As long as you authenticate your request and you have access permissions, there is no difference in the way you access encrypted or unencrypted objects. For example, if you share your objects using a presigned URL, that URL works the same way for both encrypted and unencrypted objects.

https://docs.aws.amazon.com/AmazonS3/latest/dev/serv-side-encryption.html

72. The server-side encryption by S3 can be performed by using either S3 only, or by using S3 in integration with AWS KMS.

73. AWS KMS provides customer master keys for better security and additional benefits. With KMS based encryption of S3 content, a CMK can be

specified for encryption process. The CMK can contain the location (geographical region – e.g. US-west-2) as a parameter.



Server-Side Encryption with Customer Master Keys (CMKs) Stored in AWS Key Management Service (SSE-KMS)

Server-Side Encryption with Customer Master Keys (CMKs) Stored in AWS Key Management Service (SSE-KMS) is similar to SSE-S3, but with some additional benefits and charges for using this service. There are separate permissions for the use of a CMK that provides added protection against unauthorized access of your objects in Amazon S3. SSE-KMS also provides you with an audit trail that shows when your CMK was used and by whom. Additionally, you can create and manage customer managed CMKs or use AWS managed CMKs that are unique to you, your service, and your Region. For more information, see Protecting Data Using Server-Side Encryption with CMKs Stored in AWS Key Management Service (SSE-KMS).

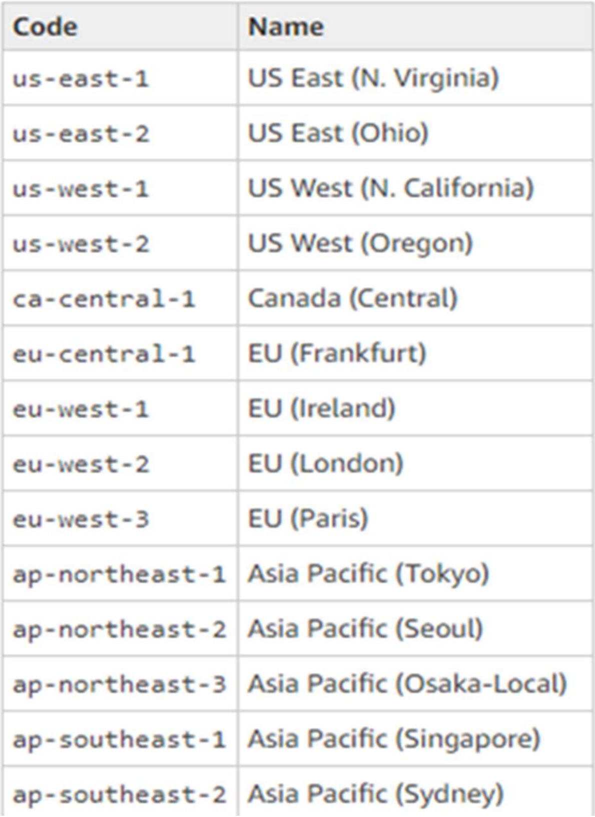
https://docs.aws.amazon.com/AmazonS3/latest/dev/serv-side-encryption.html

74. When S3 content is encrypted using KMS, the content cannot be decrypted across multiple AWS regions as the CMK used for encryption process are region specific. Before encryption, the CMK used for encryption can be created while specifying the specific geographic location/ region in which that CMK will work.

75. The encryption of data using CMK of a specified region is construed as selecting location of the specific geographic location where access rights are permitted, as the CMK is bound to a unique geographic region and does not work outside a region. The ability to decrypt the encrypted content and to access it is, therefore, restricted to the region where the CMK belongs i.e. the data center server (such as EC2) of specified AWS region will be able to carry out the decryption process.

76. As mentioned above, AWS KMS allows to select the region for CMK while its generation and the selected AWS region signifies the location data i.e. the exact geographic location of the AWS data center where the CMK is designed to work. E.g. US East (N. Virginia) where "N. Virginia" identifies the exact location of the associated AWS data center.

77. Upon information and belief, Amazon codes the geographic region using numeric values such as "1" for N. Virginia and "2" for "Ohio". The location data, therefore, can be construed either as the alphabetic name of the location (such as N. Virginia) or the numeric value (such as 1) of the location as they are interlinked.



Code	Name
us-east-1	US East (N. Virginia)
us-east-2	US East (Ohio)
us-west-1	US West (N. California)
us-west-2	US West (Oregon)
ca-central-1	Canada (Central)
eu-central-1	EU (Frankfurt)
eu-west-1	EU (Ireland)
eu-west-2	EU (London)
eu-west-3	EU (Paris)
ap-northeast-1	Asia Pacific (Tokyo)
ap-northeast-2	Asia Pacific (Seoul)
ap-northeast-3	Asia Pacific (Osaka-Local)
ap-southeast-1	Asia Pacific (Singapore)
ap-southeast-2	Asia Pacific (Sydney)

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html

78. On information and belief, AWS generates a location attribute value based in part on the location data (e.g. region field in CMK).

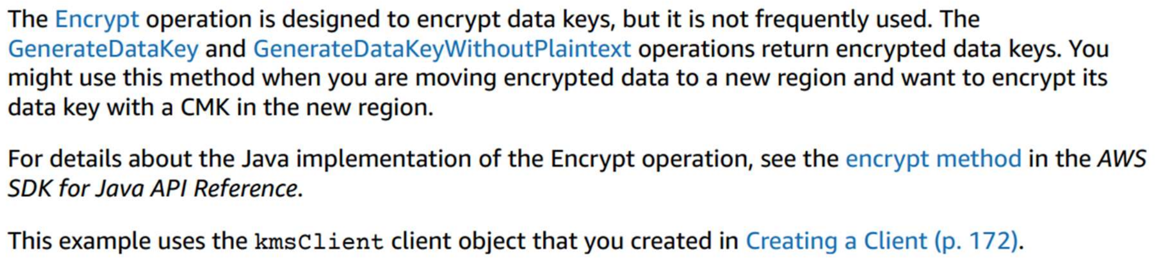
79. On information and belief, AWS associates the location attribute value (e.g. CMK) with the selected file and uses the CMK for encryption. CMK is used to generate data key which is further used to encrypt data in the S3 bucket. The encrypted data key is stored with encrypted data. Since the encrypted data key is derived from region specific CMK, the CMK is associated with the encrypted data.

80. On information and belief, AWS inhibits file management operations (e.g. copying, saving, etc.) pertaining to the selected file, including any copying, saving and deleting of the selected file, unless a current location of the information processing device corresponds to the location attribute value.

81. On information and belief, AWS uses a location attribute value which is based in part on an area parameter defining a region (e.g. region like US-west) that encompasses a specific geographic location. AWS uses CMK for encryption. The Key ARN of a CMK defines the region as a geographical area defining the region such as a US-west-2, to generate key for that region.

82. AWS uses functions which further include generating an encrypting key (e.g. data key) based on the area parameter (e.g. generating data key from CMK).

AWS KMS disclosed by AWS includes a GenerateDataKey operation to generate a data encryption key. The data key is generated from CMK which is region-specific and contains the area parameter in its ARN. Thus, the data encrypting key is inherently based on the area parameter.

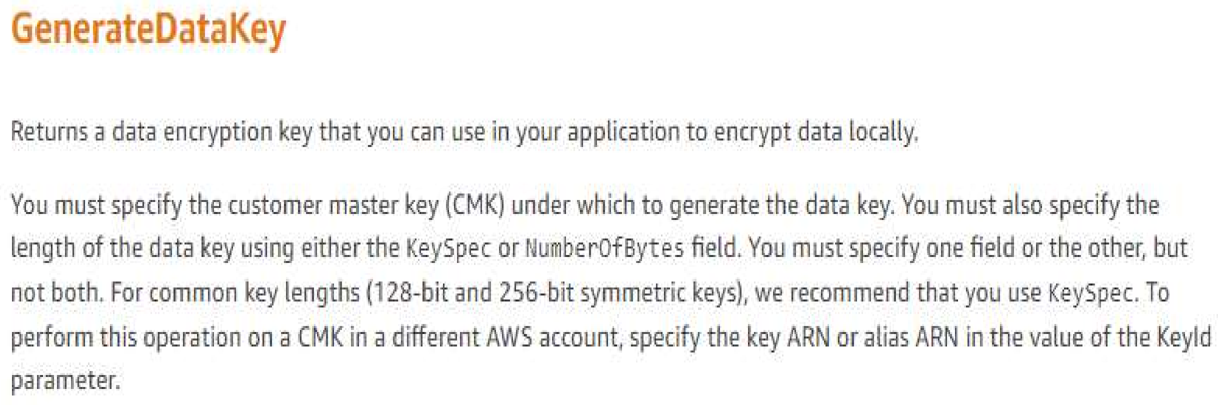


The Encrypt operation is designed to encrypt data keys, but it is not frequently used. The GenerateDataKey and GenerateDataKeyWithoutPlaintext operations return encrypted data keys. You might use this method when you are moving encrypted data to a new region and want to encrypt its data key with a CMK in the new region.

For details about the Java implementation of the Encrypt operation, see the encrypt method in the *AWS SDK for Java API Reference*.

This example uses the `kmsClient` client object that you created in Creating a Client (p. 172).

https://docs.aws.amazon.com/kms/latest/developerguide/kms-dg.pdf#programming-encryption



GenerateDataKey

Returns a data encryption key that you can use in your application to encrypt data locally.

You must specify the customer master key (CMK) under which to generate the data key. You must also specify the length of the data key using either the `KeySpec` or `NumberOfBytes` field. You must specify one field or the other, but not both. For common key lengths (128-bit and 256-bit symmetric keys), we recommend that you use `KeySpec`. To perform this operation on a CMK in a different AWS account, specify the key ARN or alias ARN in the value of the KeyId parameter.

https://docs.aws.amazon.com/kms/latest/APIReference/API_GenerateDataKey.html

83. AWS uses an associating function which further comprises encrypting the selected file using the encrypting key (e.g. encrypting data file using data key).

AWS generates a data key based on CMK. Amazon S3 integrates with KMS and uses this CMK to encrypt the objects in the S3 bucket with the data key.

84. Plaintiff has been damaged by the direct infringement of Defendants and is suffering and will continue to suffer irreparable harm and damages as a result of this infringement.

Count III – Infringement of United States Patent No. 8,472,627

85. Plaintiff repeats, re-alleges, and incorporates by reference, as if fully set forth herein, the preceding paragraphs of this Complaint.

86. Defendants directly infringe (literally and/or the under the doctrine of equivalents) the ’627 Patent by using the method covered by at least claim 22 of the ’627 Patent.

87. Defendants’ instrumentality that infringes one or more claims of the ’627 Patent includes, but is not limited to, AWS and any other of Defendants’ networks, systems, devices, and/or services that practice a method for controlling access to content data as claimed by the ’627 Patent.

88. AWS provides a method for controlling access to content data. AWS provides on-demand cloud computing platforms and APIs to individuals, companies, and governments, on a metered pay-as-you-go basis. AWS includes Amazon KMS as one of its services to protect data through encryption/decryption mechanism. KMS gives the user a centralized control over the cryptographic keys that are used

to protect the data and control its access. KMS seamlessly integrates with other AWS services such as storage services (S3, EBS, and EFS) to protect the data that the service receives, stores, and manages.

89. Using KMS integration with other services, data can be transmitted from one region to another securely—e.g., a data processing application deployed in two different AWS regions can copy data between regions and manage cryptographic operations through KMS. These integrations use envelope encryption in which the data that is to be transmitted is encrypted using a data key, and the data key is encrypted using the CMK of the intended destination region.

90. Upon information and belief, the encrypted data and the encrypted data key is sent to a service in the recipient region. If the recipient region is the intended destination, the data key (and hence the data) can be decrypted by the AWS services, since the data key is encrypted using the destination CMK, and CMKs are bound to the region where they are created.

91. If the recipient region is not the intended destination, the AWS services in that region does not have access to the necessary CMK to decrypt the data key (and in turn the data), and therefore cannot decrypt the data. Thus, AWS services along with KMS provide region-based access to data (i.e. controlling access to content data).

92. The method practiced by AWS comprises a distributor device (e.g. Source AWS region's server) which uses a data encrypting/decrypting key (e.g. data key) to encrypt the content data.

93. Using KMS integration in AWS with various services, data stored in a source region can be easily moved to a destination region. Each AWS region consists of data centers that employ servers. Thus, the data can be sent from a source server (i.e., a distributor device) to a destination server (i.e., a receiver device).

94. KMS integration with various services enables secure data transfer through envelope encryption. In this system, first, the data that is to be protected (i.e., content data) is encrypted using the data key (i.e., data encrypting/decrypting key) generated by AWS KMS.

95. The method practiced by AWS comprises of a distributor device using a key encrypting/decrypting key (e.g. CMK) to encrypt both the data encrypting/decrypting key(e.g. data key) and at least one content-owner constraint (e.g. geographical location). AWS practices envelope encryption, in which data is encrypted using the data key (i.e. data encrypting/decrypting key), and the data key is encrypted using CMK (i.e. key encrypting/decrypting key) of the destination region. The CMK contains content owner constraint details like geographical region.

96. To securely move encrypted data, data keys (i.e., data encryption key) can be encrypted (i.e., apply a first layer of encryption) using CMK that is associated

with a destination AWS region such as us-west-2 (i.e., content owner location constraint). In this manner, the protected data can be accessed (or decrypted) only by services in the destined AWS region whose CMK is used initially to encrypt data. Thus, the data key is encrypted using the CMK that already has an inherited location identity. The content owner can impose a constraint using CMK, the geographical regions from where the respective contents can be accessed.

97. The encryption of data using CMK of a specified region constitutes selecting location of the specific geographic location where access rights are permitted, as the CMK is bound to a unique geographic region and can't work outside a region. Thus, the ability to decrypt the encrypted content and to access it is restricted to the region where the CMK belongs i.e. only the data center server (such as EC2) of specified AWS region will be able to carry out the decryption process. If the recipient region is not the intended destination, it does not have the CMK to decrypt the data key (and in turn the data), and therefore cannot decrypt the data. Thus, KMS provides a region-based access to data.

98. The method practiced by AWS comprises of a distributor device (e.g. Source AWS region server) sending the encrypted content data, the encrypted data encrypting/decrypting key and the at least one encrypted content-owner constraint to a receiver device (e.g. destination AWS region server) via a communication network.

99. KMS allows sending encrypted data between various AWS regions. The data can be sent from a source AWS region's server (i.e. a distributor device) to a destination AWS region's server (i.e. a receiver device). After the envelope encryption, both encrypted data and encrypted data key (i.e., said encrypted data and encrypted data encrypting key) are stored together to enable other applications to decrypt the data. Using KMS integration, the stored data can be transmitted from the AWS server in the source region to the AWS server in the destination region (i.e. recipient device). The encrypted data is stored together with the encrypted data key. Thus, while transferring the encrypted data to new regions, the encrypted data and encrypted data key are transferred together.

100. To securely move encrypted data, data keys (i.e., data encryption key) can be encrypted (i.e., apply a first layer of encryption) using CMK that is associated with a destination AWS region such as us-west-2 (i.e., content owner location constraint). In this manner, the protected data can be accessed (or decrypted) only by services in the destined AWS region whose CMK is used initially to encrypt data. Thus, the data key is encrypted using the customer master key (CMK), which already has an inherited location identity. The content owner can impose a constraint using CMK, the geographical regions from where the respective contents can be accessed. If the recipient region is not the intended destination, it does not have the CMK to

decrypt the data key (and in turn the data), and therefore cannot decrypt the data. Thus, KMS provides a region-based access to data.

101. The method practiced by AWS comprises of a receiver device (e.g. destination AWS region server) receiving via the communications network the encrypted content data, the encrypted data encrypting/decrypting key and the at least one encrypted content-owner constraint (e.g. the geographical location). In AWS, the plain text data key to decrypt the data is generated using the customer master key, which includes the content owner constraint – the geographical region. After the envelope encryption, both encrypted data and encrypted data key (i.e., said encrypted data and encrypted data encrypting key) are stored together to enable other applications to decrypt the data. Using KMS integration, the stored data can be transmitted from the AWS server in the source region to the AWS server in the destination region (i.e. recipient device).

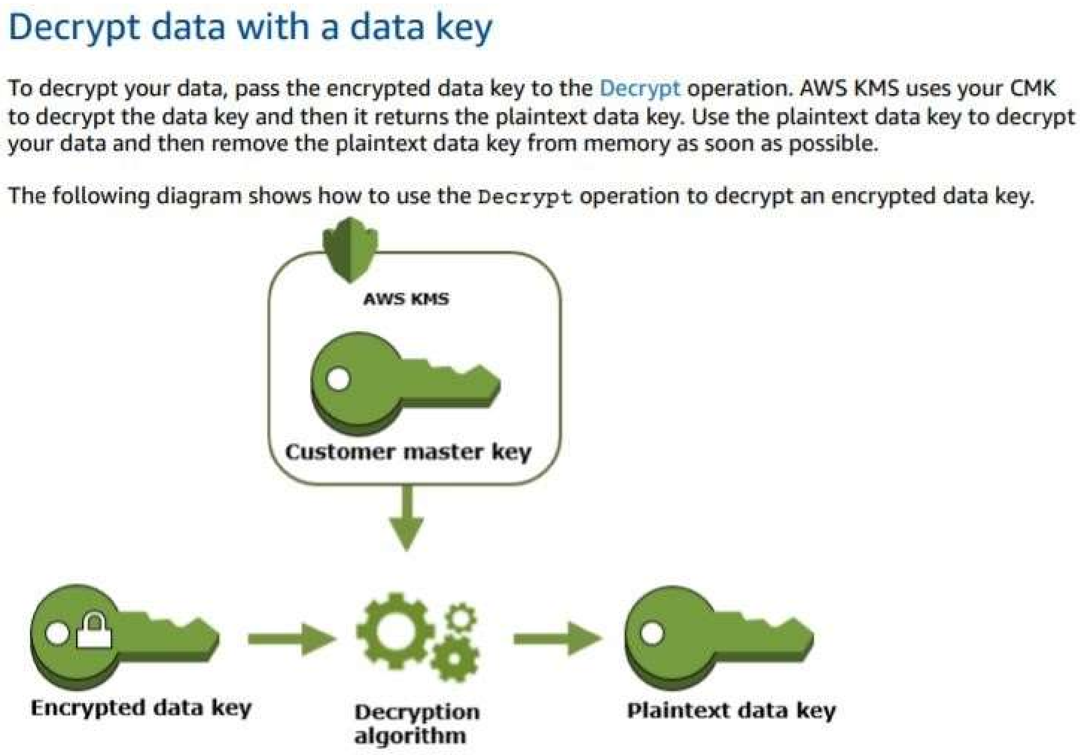
102. To securely move encrypted data, data keys (i.e., data encryption key) can be encrypted (i.e., apply a first layer of encryption) using CMK that is associated with a destination AWS region such as us-west-2 (i.e., content owner location constraint). In this manner, the protected data can be accessed (or decrypted) only by services in the destined AWS region that CMK is used initially to encrypt data. Thus, the data key is encrypted using the customer master key (CMK), which already has an inherited location identity. The content owner can impose a constraint using

CMK, the geographical regions from where the respective contents can be accessed. If the recipient region is not the intended destination, it does not have the CMK to decrypt the data key and the data. Thus, KMS provides a region-based access to data.

103. The method practiced by AWS comprises a receiver device decrypting both the encrypted data encrypting/decrypting key (e.g. data key) and the at least one encrypted content-owner constraint (e.g. the geographical location). The decryption of the content data requires Geographical location (i.e., content-owner constraint) and data key to decrypt the encrypted data successfully. The CMK contains content owner constraint details like geographical region.

104. The method practiced by AWS comprises a receiver device that decrypts the encrypted content data (e.g., encrypted data) if the at least one content-owner constraint (e.g. the geographical location) is satisfied. Geographical location acts as an additional check and enforces the constraint as configured.

105. Upon information and belief, the decryption process in the destination region is processed only if the correct CMK is generated to decrypt. Encrypted data is decrypted only if geographical location constraint is satisfied. If the geographical location matches, the encrypted data key can be decrypted to plaintext data key which is the used to decrypt the encrypted data (i.e., encrypted content data) successfully.



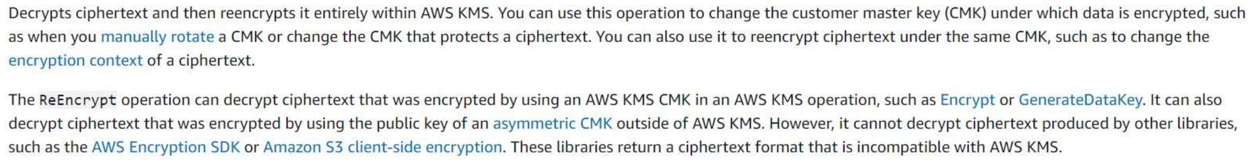
Decrypt data with a data key

To decrypt your data, pass the encrypted data key to the Decrypt operation. AWS KMS uses your CMK to decrypt the data key and then it returns the plaintext data key. Use the plaintext data key to decrypt your data and then remove the plaintext data key from memory as soon as possible.

The following diagram shows how to use the `Decrypt` operation to decrypt an encrypted data key.

https://docs.aws.amazon.com/kms/latest/developerguide/kms-dg.pdf#workflow

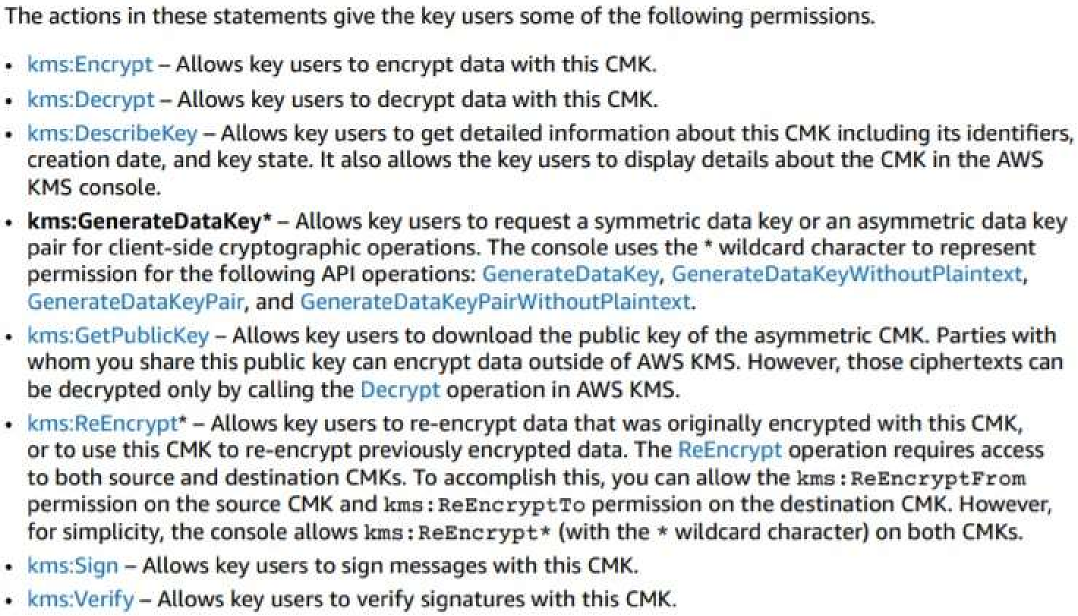
106. The method practiced by AWS comprises a receiver device using a second key encrypting/decrypting key to re-encrypt the data encrypting/decrypting key. The data that is decrypted can be re-encrypted for transfer to some other region. This process of decrypting, followed by encrypting, is termed as Re-encrypting and is carried out by ReEncrypt operation defined in KMS. In AWS key management services, a different customer master key is used to re-encrypt the data key.



Decrypts ciphertext and then reencrypts it entirely within AWS KMS. You can use this operation to change the customer master key (CMK) under which data is encrypted, such as when you manually rotate a CMK or change the CMK that protects a ciphertext. You can also use it to reencrypt ciphertext under the same CMK, such as to change the encryption context of a ciphertext.

The `ReEncrypt` operation can decrypt ciphertext that was encrypted by using an AWS KMS CMK in an AWS KMS operation, such as Encrypt or GenerateDataKey. It can also decrypt ciphertext that was encrypted by using the public key of an asymmetric CMK outside of AWS KMS. However, it cannot decrypt ciphertext produced by other libraries, such as the AWS Encryption SDK or Amazon S3 client-side encryption. These libraries return a ciphertext format that is incompatible with AWS KMS.

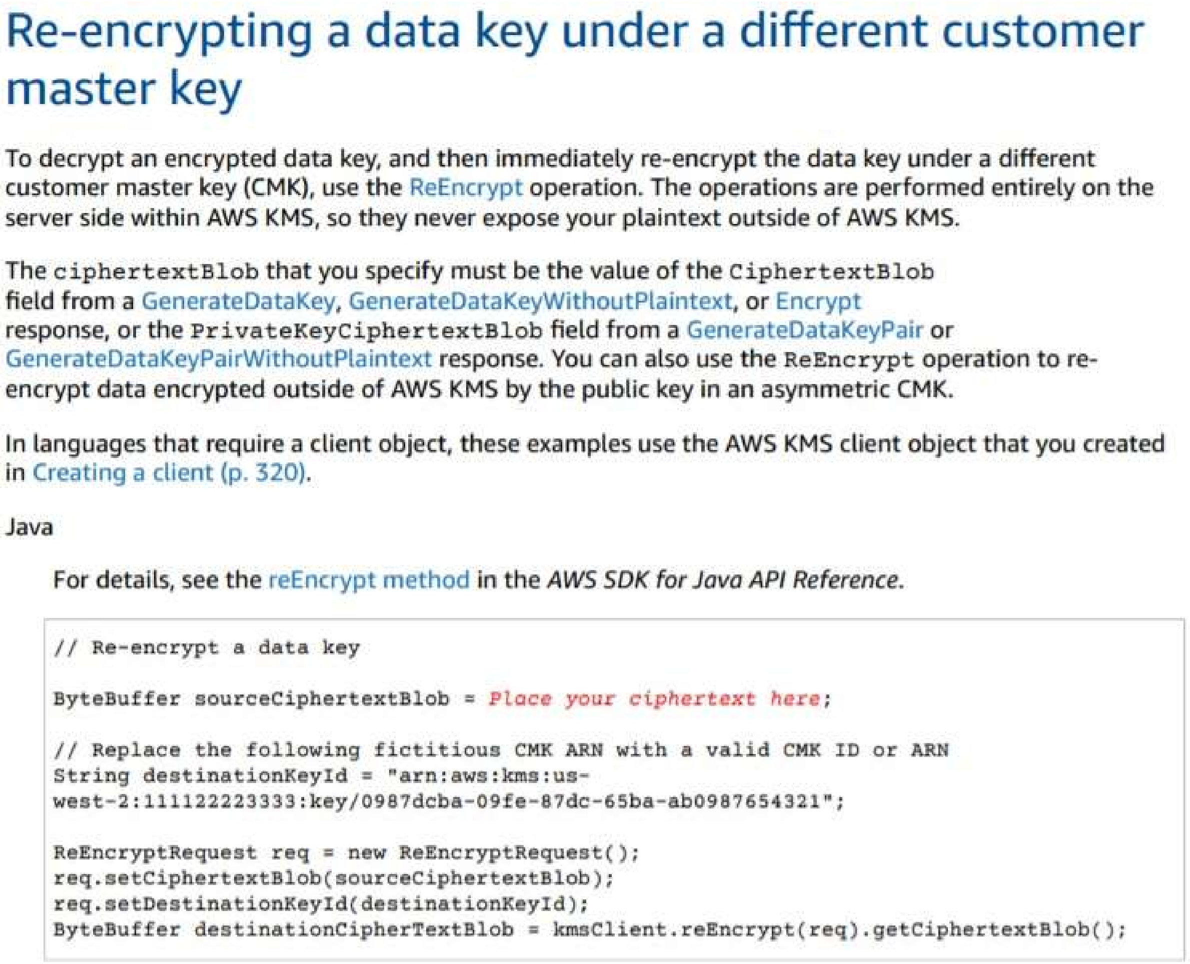
https://docs.aws.amazon.com/kms/latest/APIReference/API_ReEncrypt.html



The actions in these statements give the key users some of the following permissions.

- kms:Encrypt – Allows key users to encrypt data with this CMK.
- kms:Decrypt – Allows key users to decrypt data with this CMK.
- kms:DescribeKey – Allows key users to get detailed information about this CMK including its identifiers, creation date, and key state. It also allows the key users to display details about the CMK in the AWS KMS console.
- **kms:GenerateDataKey*** – Allows key users to request a symmetric data key or an asymmetric data key pair for client-side cryptographic operations. The console uses the * wildcard character to represent permission for the following API operations: GenerateDataKey, GenerateDataKeyWithoutPlaintext, GenerateDataKeyPair, and GenerateDataKeyPairWithoutPlaintext.
- kms:GetPublicKey – Allows key users to download the public key of the asymmetric CMK. Parties with whom you share this public key can encrypt data outside of AWS KMS. However, those ciphertexts can be decrypted only by calling the Decrypt operation in AWS KMS.
- kms:ReEncrypt* – Allows key users to re-encrypt data that was originally encrypted with this CMK, or to use this CMK to re-encrypt previously encrypted data. The ReEncrypt operation requires access to both source and destination CMKs. To accomplish this, you can allow the `kms:ReEncryptFrom` permission on the source CMK and `kms:ReEncryptTo` permission on the destination CMK. However, for simplicity, the console allows `kms:ReEncrypt*` (with the `*` wildcard character) on both CMKs.
- kms:Sign – Allows key users to sign messages with this CMK.
- kms:Verify – Allows key users to verify signatures with this CMK.

https://docs.aws.amazon.com/kms/latest/developerguide/kms-dg.pdf#workflow



Re-encrypting a data key under a different customer master key

To decrypt an encrypted data key, and then immediately re-encrypt the data key under a different customer master key (CMK), use the ReEncrypt operation. The operations are performed entirely on the server side within AWS KMS, so they never expose your plaintext outside of AWS KMS.

The `ciphertextBlob` that you specify must be the value of the `CiphertextBlob` field from a GenerateDataKey, GenerateDataKeyWithoutPlaintext, or Encrypt response, or the `PrivateKeyCiphertextBlob` field from a GenerateDataKeyPair or GenerateDataKeyPairWithoutPlaintext response. You can also use the `ReEncrypt` operation to re-encrypt data encrypted outside of AWS KMS by the public key in an asymmetric CMK.

In languages that require a client object, these examples use the AWS KMS client object that you created in Creating a client (p. 320).

Java

For details, see the reEncrypt method in the *AWS SDK for Java API Reference*.

```
// Re-encrypt a data key

ByteBuffer sourceCiphertextBlob = Place your ciphertext here;

// Replace the following fictitious CMK ARN with a valid CMK ID or ARN
String destinationKeyId = "arn:aws:kms:us-
west-2:111122223333:key/0987dcba-09fe-87dc-65ba-ab0987654321";

ReEncryptRequest req = new ReEncryptRequest();
req.setCiphertextBlob(sourceCiphertextBlob);
req.setDestinationKeyId(destinationKeyId);
ByteBuffer destinationCipherTextBlob = kmsClient.reEncrypt(req).getCiphertextBlob();
```

https://docs.aws.amazon.com/kms/latest/developerguide/kms-dg.pdf#workflow

107. The method practiced by AWS comprises a receiver device sending the encrypted content data and the re-encrypted data encrypting/decrypting key to at least one other receiver device (e.g., destination AWS server) via the communications network. The use of replicating data across regions multiple times is to satisfy compliance as well as to minimize latency. To do this, the process of replication could be repeated across multiple regions in a similar manner. On information and belief, for each replication, the encrypted data needs to be decrypted and re-encrypted using another destination region's CMK and then sent to that destination region (destination AWS server).

108. Plaintiff has been damaged by the direct infringement of Defendants and is suffering and will continue to suffer irreparable harm and damages as a result of this infringement.

Count IV – Infringement of United States Patent No. 10,715,316

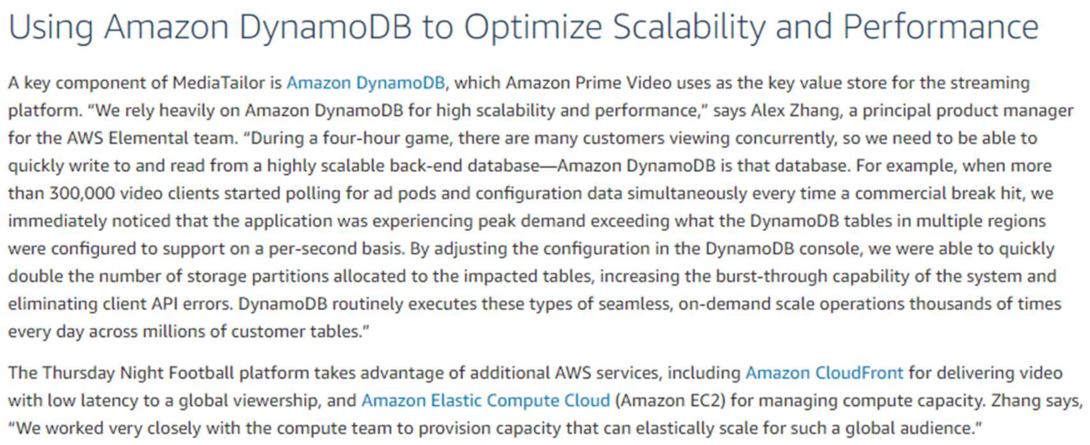
109. Plaintiff repeats, re-alleges, and incorporates by reference, as if fully set forth herein, the preceding paragraphs of this Complaint.

110. Defendants directly infringe (literally and/or under the doctrine of equivalents) the '316 Patent by using the apparatus covered by at least claim 12 of the '316 Patent.

111. Defendants' instrumentality that infringes one or more claims of the '316 Patent includes, but is not limited to, Amazon Prime Video, and any other of Defendants' networks, systems, devices, and/or services that comprise an apparatus for controlling access to digital information, said digital information comprising a plurality of digital files as claimed by the '316 Patent.

112. Amazon Prime Video comprises an apparatus for controlling access to digital information, said digital information comprising a plurality of digital files. Amazon Prime Video is an American Internet video-on-demand/ streaming service that is developed, owned, and operated by Amazon. Amazon Prime Video provides a selection of original content, licensed movies, and TV shows that can be streamed as part of the Amazon Prime subscription. It offers a wide variety of TV shows, movies, Amazon Originals, and more on thousands of internet-connected devices. Amazon Prime Video allows users to stream movies and TV shows (i.e. digital files) over the internet using various compatible devices such as TVs, computers, smartphones, and other devices.

113. Amazon Prime Video uses the Amazon Web Service (AWS) Cloud as the underlying technology for its streaming service. Amazon Prime Video uses various AWS technologies for its computational and storage requirements including such as DynamoDB, Elastic Compute, CloudFront, etc.



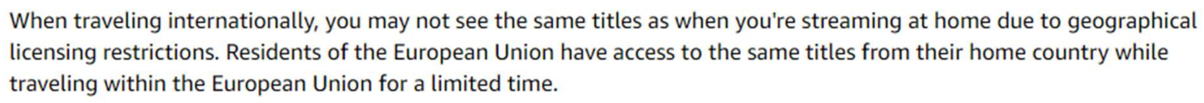
Using Amazon DynamoDB to Optimize Scalability and Performance

A key component of MediaTailor is Amazon DynamoDB, which Amazon Prime Video uses as the key value store for the streaming platform. "We rely heavily on Amazon DynamoDB for high scalability and performance," says Alex Zhang, a principal product manager for the AWS Elemental team. "During a four-hour game, there are many customers viewing concurrently, so we need to be able to quickly write to and read from a highly scalable back-end database—Amazon DynamoDB is that database. For example, when more than 300,000 video clients started polling for ad pods and configuration data simultaneously every time a commercial break hit, we immediately noticed that the application was experiencing peak demand exceeding what the DynamoDB tables in multiple regions were configured to support on a per-second basis. By adjusting the configuration in the DynamoDB console, we were able to quickly double the number of storage partitions allocated to the impacted tables, increasing the burst-through capability of the system and eliminating client API errors. DynamoDB routinely executes these types of seamless, on-demand scale operations thousands of times every day across millions of customer tables."

The Thursday Night Football platform takes advantage of additional AWS services, including Amazon CloudFront for delivering video with low latency to a global viewership, and Amazon Elastic Compute Cloud (Amazon EC2) for managing compute capacity. Zhang says, "We worked very closely with the compute team to provision capacity that can elastically scale for such a global audience."

https://aws.amazon.com/solutions/case-studies/amazon-prime-video/

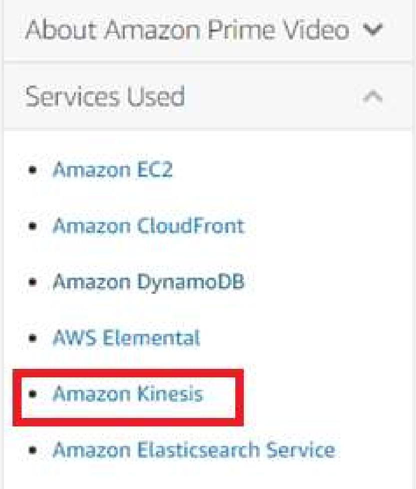
114. Amazon Prime Video offers content owned by other producers and hence the content is usually licensed and copyrighted. Most of these ownership rights may be exclusive or territorial depending on certain factors. The licenses and copyrights make the contents to be legible for a particular region and restrict Amazon Prime Video from offering the same content to other locations. For this, on information and belief, Amazon Prime Video uses geo-blocking or geo-restriction to control access to digital content or offer selective content to its users based on their location and avoid violation of the content owner's copyright and/ or license agreements.



When traveling internationally, you may not see the same titles as when you're streaming at home due to geographical licensing restrictions. Residents of the European Union have access to the same titles from their home country while traveling within the European Union for a limited time.

https://www.primevideo.com/region/na/help/ref=atv_hp_nd_srchr?nodeId=GJ2P83PMNC54XKV9

115. As shown, Amazon Prime Video uses Amazon kinesis and other services which uses Amazon KMS. Amazon KMS uses region-based keys for transmission and thus can control access of media across a geographical location.

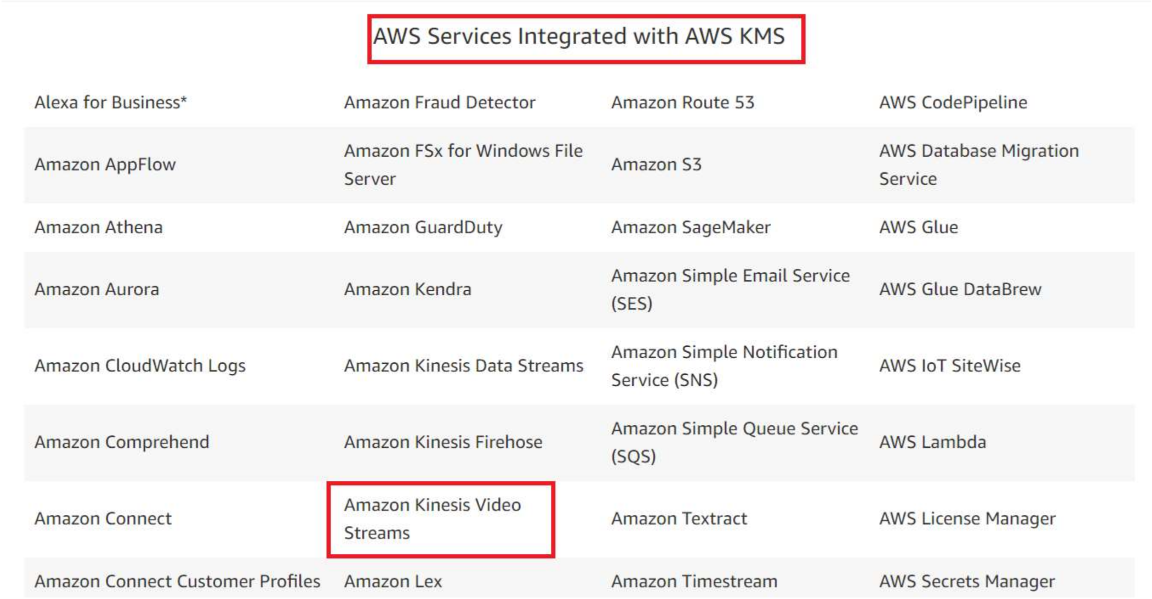


About Amazon Prime Video

Services Used

- Amazon EC2
- Amazon CloudFront
- Amazon DynamoDB
- AWS Elemental
- Amazon Kinesis
- Amazon Elasticsearch Service

https://aws.amazon.com/solutions/case-studies/amazon-prime-video/



AWS Services Integrated with AWS KMS

Alexa for Business*	Amazon Fraud Detector	Amazon Route 53	AWS CodePipeline
Amazon AppFlow	Amazon FSx for Windows File Server	Amazon S3	AWS Database Migration Service
Amazon Athena	Amazon GuardDuty	Amazon SageMaker	AWS Glue
Amazon Aurora	Amazon Kendra	Amazon Simple Email Service (SES)	AWS Glue DataBrew
Amazon CloudWatch Logs	Amazon Kinesis Data Streams	Amazon Simple Notification Service (SNS)	AWS IoT SiteWise
Amazon Comprehend	Amazon Kinesis Firehose	Amazon Simple Queue Service (SQS)	AWS Lambda
Amazon Connect	Amazon Kinesis Video Streams	Amazon Textract	AWS License Manager
Amazon Connect Customer Profiles	Amazon Lex	Amazon Timestream	AWS Secrets Manager

https://aws.amazon.com/kms/features/

116. Amazon Prime Video comprises at least one memory device (e.g. AWS EC2, Amazon DynamoDB, CloudFront, etc.) for storing a location identity for each of said plurality of digital files. Amazon Prime Video uses AWS EC2, Amazon DynamoDB, CloudFront, etc. for computing and storage requirements. Each media file has associated territory information (such as US, UK, DE, JP) in the form of the metadata. Amazon Prime Video has a separate metadata file for each territory to deliver a movie or a TV show (i.e. digital files). Amazon Prime Video stores the territory information which defines the location or region (location identity) from where the digital file, present on Amazon Prime Video, can be accessed the users. Amazon Prime Video uses Amazon kinesis and other services which uses Amazon KMS. Amazon KMS uses region-based keys for transmission and thus can control access of media across a geographical location. Amazon Prime Video stores the territory information or the location information for each digital file to allow the streaming of any specific content at only allowed locations.

117. Amazon Prime Video includes the said location identity being received from a corresponding producer device (e.g. content provider) via a network and comprising a location value (e.g. region - us-west-2, etc) and a proximity value (e.g. partition - aws, aws-cn, etc). As stated, Amazon Prime Video uses Amazon kinesis and other services which utilize Amazon KMS. Amazon KMS uses region-based keys for transmission and thus can control access of media across a geographical

location. Producer can add the location identity based on CMK key used. The ARN of CMK key specifies the proximity value using the partition field present in ARN (e.g. aws, aws-cn, etc.) and the location value using the region field (e.g. us-east-2, us-west-1, etc.)

118. Amazon Prime Video includes a location value comprising a geographical location (e.g. region - us-west-2, etc.) and a proximity value (e.g. partitions – aws, aws-cn, etc.) identifying a geographical region in relation to said geographical location. As previously alleged, Amazon Prime Video uses Amazon kinesis and other services which uses Amazon KMS. Amazon KMS uses region-based keys for transmission and thus can control access of media across a geographical location. As shown the location value include a geographical location (region - e.g. us-west-2, etc.) and a proximity value (e.g. partitions – aws, aws-cn, etc.) identifying a geographical region in relation to said geographical location.

119. Amazon Prime Video comprises of, at least one application processor (e.g. AWS server) in communication with said at least one memory device (e.g. AWS EC2, Amazon DynamoDB, CloudFront, etc.) and configured to (i) prompt a receiver to provide its location to a distributor device, (ii) receive a current location from said receiver device, (iii) receive a request for data from said receiver, and (iv) select one of said plurality of files based on said current location of said receiver and said requested data. Amazon Prime Video stores all the data such as user

information, content information on multiple AWS server instances from where users across nations are served based on their geographic location. Amazon server instances (e.g. EC2 instance) comprise varying combinations of processor, memory, storage, and networking capacity which gives Amazon Prime Video the flexibility to choose the appropriate resource for serving its userbase. On information and belief, Amazon Prime Video uses geo-restriction or geo-blocking to restrict content to different geographic locations. Amazon Prime Video determines the location of the user based on the retrieved IP of the user device. Accordingly, Amazon Prime Video determines the location address from the user device and accordingly controls the access to its content. Amazon Prime Video uses AWS EC2, Amazon DynamoDB, CloudFront, etc. for computing and storage requirements. Amazon Prime Video uses Amazon kinesis and other services which uses Amazon KMS. Amazon KMS uses region-based keys for transmission and thus can control access of media across a geographical location.

120. Amazon Prime Video comprises, said selected one of said plurality of digital files including said data and having a location identity that matches said current location of said receiver device. Amazon Prime Video retrieves one of the plurality of digital files from the Amazon Prime Video library based on the current location of the user and the requested data by the user. In other words, a movie is selected by Amazon Prime Video from its library and offered to the user for

streaming because of two reasons: (1) the licensed location associated with this content matches the user’s location i.e. USA, and (2) the content includes the requested data. As alleged, Amazon Prime Video uses Amazon kinesis and other services which uses Amazon KMS. Amazon KMS uses region-based keys for transmission and thus can control access of media across a geographical location.

121. Amazon Prime Video comprises wherein at least a first other one of said plurality of digital files includes said data but does not match said current location and at least a second other one of said plurality of digital files matches said current location but does not include said data. The accused instrumentality in Amazon Prime Video library (or the plurality of digital files) comprises at least one other digital file that includes the requested data but does not match the current location of the user. Amazon Prime Video uses Amazon kinesis and other services which uses Amazon KMS. Amazon KMS uses region-based keys for transmission and thus can control access of media across a geographical location. As shown the location value include a geographical location (e.g. partitions – aws, aws-cn, etc.) and a proximity value (e.g. us-west-2) identifying a geographical region in relation to said geographical location.

122. Amazon Prime Video comprises, said plurality of digital files being selected in response to receiving said request for said data. Amazon Prime Video

processes the user's request (search query) and accordingly selects the digital file(s) from its digital library (i.e. plurality of digital files) in response to the user's request.

123. Plaintiff has been damaged by the direct infringement of Defendants, and is suffering, and will continue to suffer irreparable harm and damages as a result of this infringement.

JURY DEMAND

124. Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiff requests a trial by jury on all issues so triable.

PRAYER FOR RELIEF

Plaintiff respectfully requests this Court to enter judgment in Plaintiff's favor and against Defendants as follows:

a. finding that Defendants directly infringe one or more claims of the Patents-in-Suit;

b. awarding Plaintiff damages under 35 U.S.C. § 284, or otherwise permitted by law, including supplemental damages for any continued post-verdict infringement;

c. awarding Plaintiff pre-judgment and post-judgment interest on the damages award and costs;

d. awarding cost of this action (including all disbursements) and attorney fees pursuant to 35 U.S.C § 285, or as otherwise permitted by the law;

and

e. awarding such other costs and further relief that the Court determines to be just and reasonable.

Dated: February 14, 2022

Respectfully submitted,
/s/ Richard C. Weinblatt
Stamatios Stamoulis (#4606)
Richard C. Weinblatt (#5080)
STAMOULIS & WEINBLATT LLC
800 N. West Street, Third Floor
Wilmington, DE 19801
Telephone: (302) 999-1540
Facsimile: (302) 762-1688
stamoulis@swdelaw.com
weinblatt@swdelaw.com

Of Counsel:
Ronald M. Daignault (*pro hac vice*)*
Chandran B. Iyer (*pro hac vice*)
Zachary H. Ellis (*pro hac vice*)*
rdaignault@daignaultiyer.com
cbiyer@daignaultiyer.com
zellis@daignualtiyer.com

DAIGNAULT IYER LLP
8618 Westwood Center Drive
Suite 150
Vienna, VA 22182
**Not admitted to practice in Virginia*

ATTORNEYS FOR PLAINTIFF