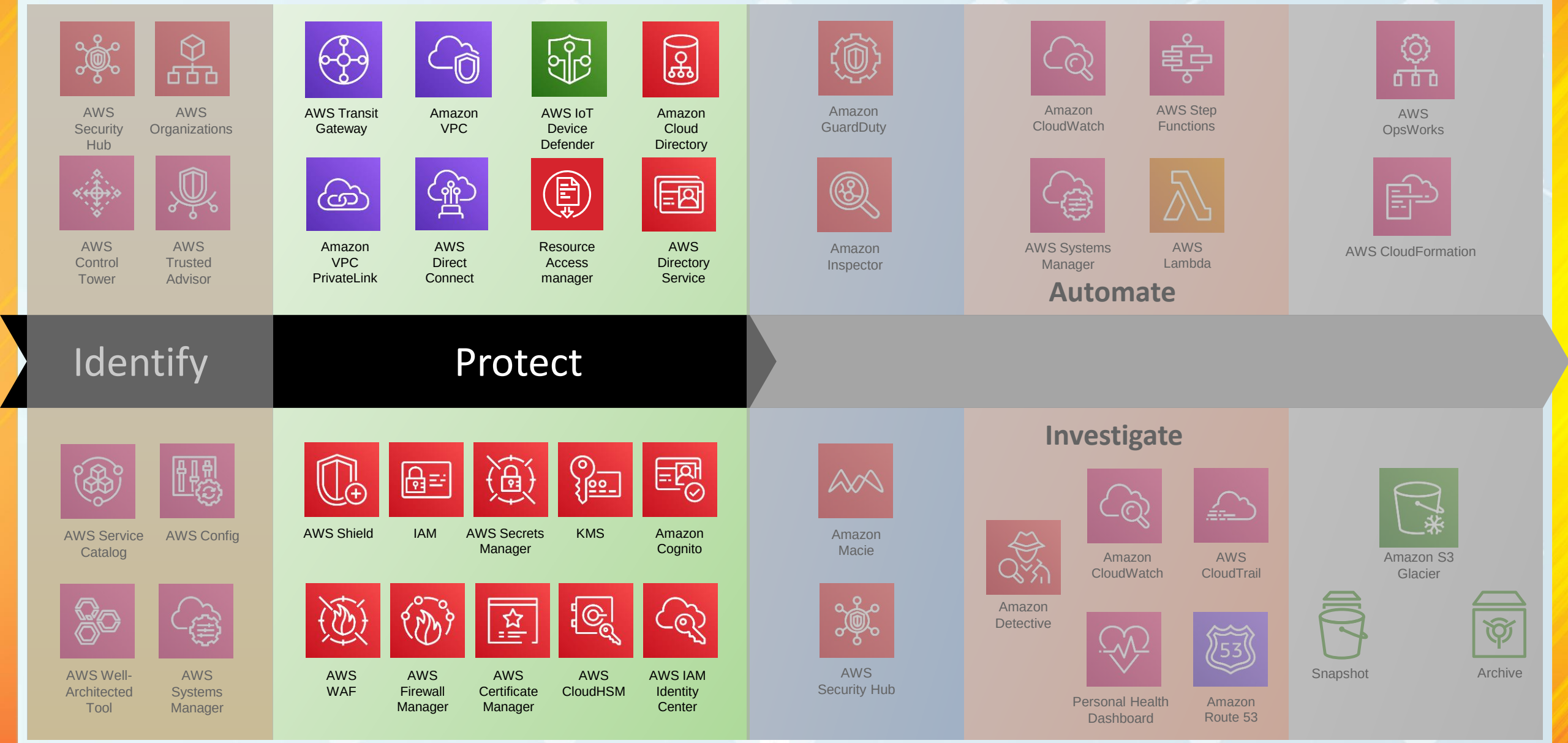
Protect

AWS Foundational and Layered Security Services



Protect your application

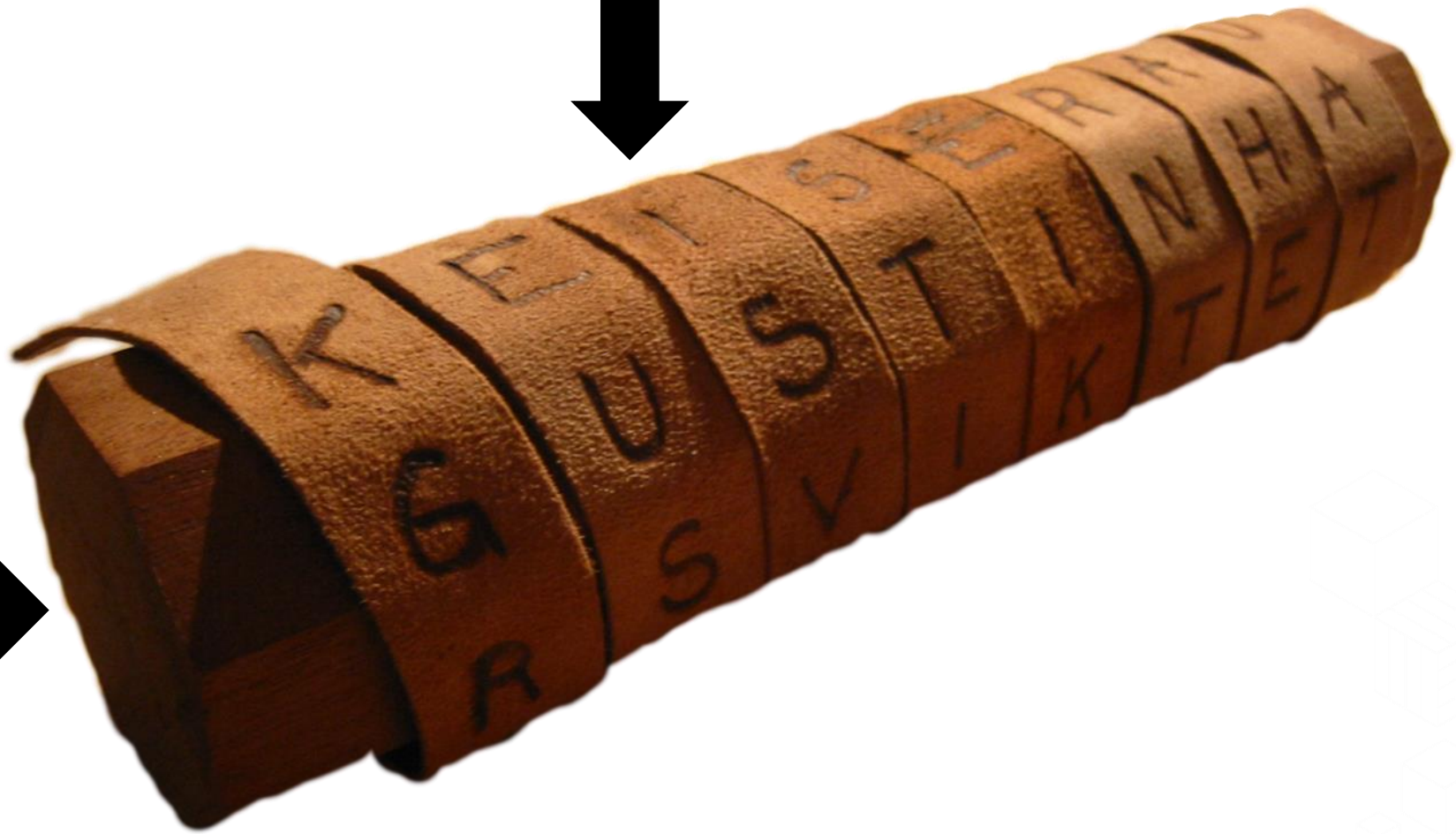
- Encryption
  - AWS Certificate Manager
  - AWS Key Management Service
  - AWS CloudHSM
- Mitigation of DDoS attacks
  - AWS Web Application Firewall (WAF)
  - AWS Shield
  - AWS Firewall Manager
- Authentication & Authorization
  - AWS Directory Service
  - Amazon Cognito
  - AWS Identity and access management (IAM)
  - AWS Identity Center (AWS Single Sign-On)

Encryption Basics

What is this?

- Scytale

Encrypted Message



Key

Encryption Analogy

Pin

4 5 8 2

Key

+ 1 - 1

4 5 8 2 (Plain Text)

+ 1 -1 + 1 - 1

5 4 9 1

Cypher Text

5 4 9 1

Decrypt

5 4 9 1

- 1 +1 - 1 +1

4 5 8 2

Key

+ 1 - 1

+ <Value> - <Value>

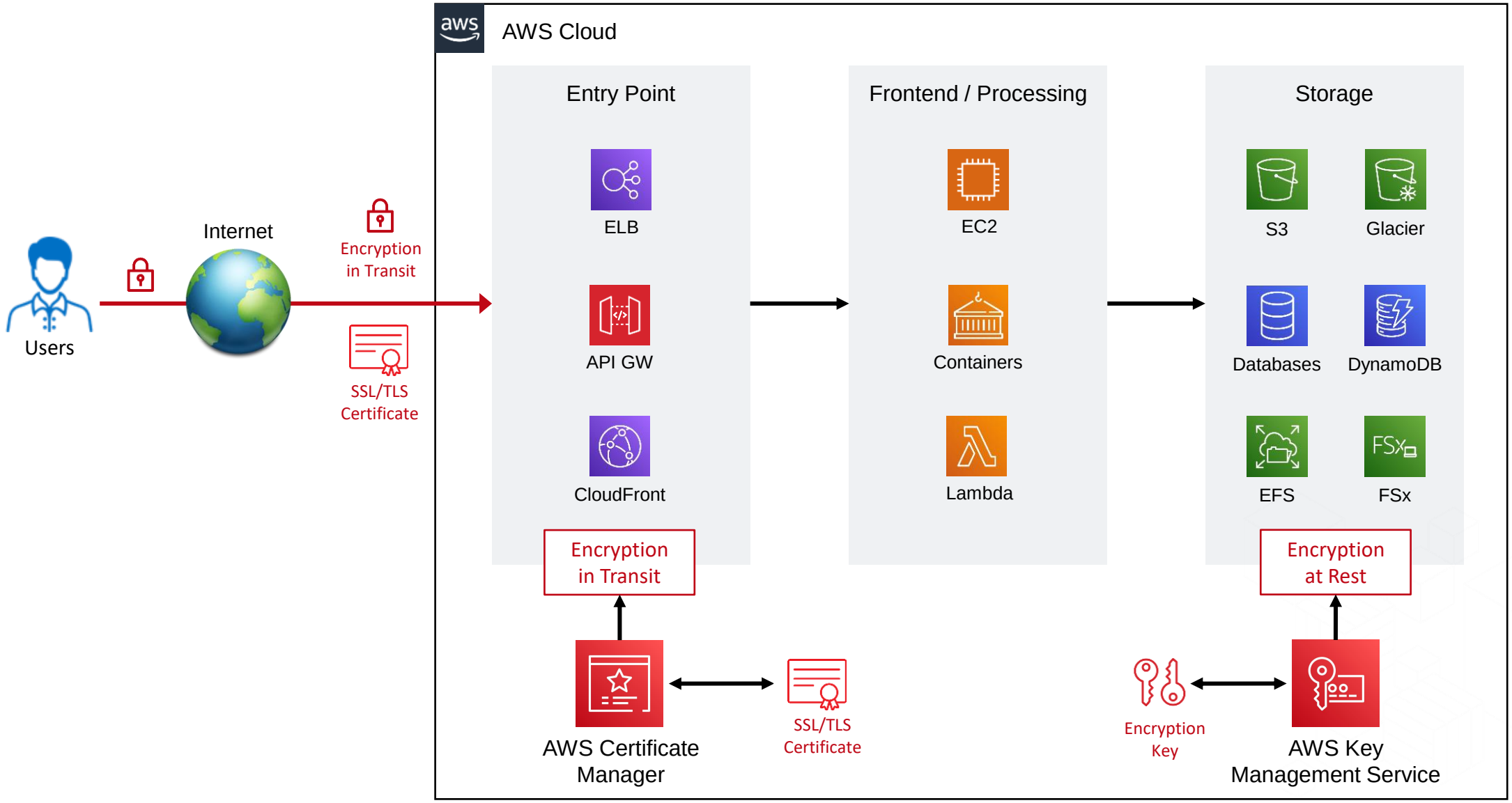
Algorithm

Value = 1

Key Material

Encryption in AWS

Encryption in Transit / Encryption at Rest



AWS Certificate Manager

AWS Certificate Manager

- Easily provision, manage, and deploy public and private SSL/TLS certificate

Provision, Manage & Renew Certificates

Private Certificate Authority (CA)

Free for ACM integrated services

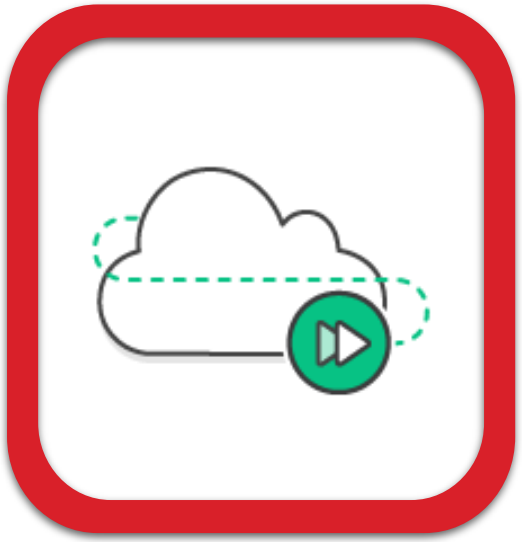
Import 3rd Party Certificates

- AWS Certificate Manager supports a growing number of AWS services.

AWS Key Management Service (KMS)

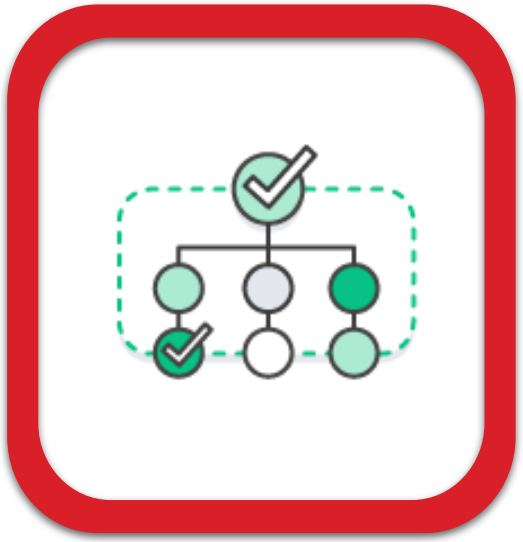
AWS Key Management Service

- Easily create and control the keys used to encrypt or digitally sign your data.



Fully
managed

Built-in
auditing



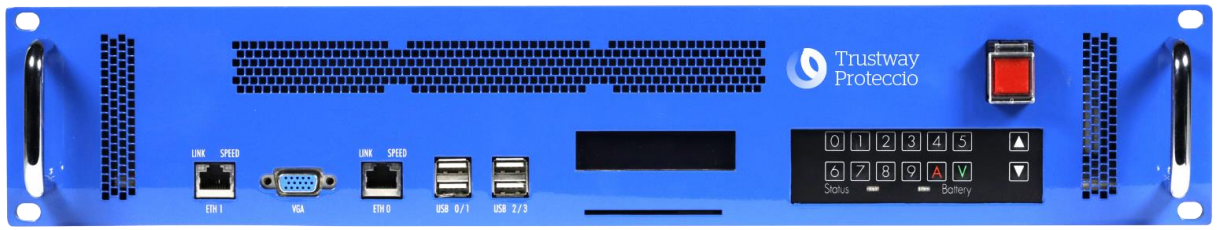
Compliant with
PCI, HIPAA and more

Supports Custom
Key Store

- AWS KMS service stores key material on a device called HSM (Hardware Security Module).

What is a Hardware Security Module (HSM)?

- Hardware Security Module (HSM) is a physical device which is designed to store keys safely.



Role based access control in AWS KMS

- Key Admin vs. Key User

Key Admin

"kms:Create*",
"kms:Describe*",
"kms:Enable*",
"kms:List*",
"kms:Put*",
"kms:Update*",
"kms:Revoke*",
"kms:Disable*",
"kms:Get*",
"kms:Delete*",
"kms:TagResource",
"kms:UntagResource",
"kms:ScheduleKeyDeletion",
"kms:CancelKeyDeletion"

Key User

"kms:Encrypt",
"kms:Decrypt",
"kms:ReEncrypt*",
"kms:GenerateDataKey*",
"kms:DescribeKey"

S3 Permissions and Encryption

- Object Encrypted using - S3 Default Key

User	S3 Permission	Key Permission	Can they read data?
Manager	S3 Full Access	Not Applicable	✔
Dev 1	S3 Read	Not Applicable	✔
Dev 2	S3 Read	Not Applicable	✔
Dev 3	No S3 Permission	Not Applicable	✘

- Object Encrypted using - S3 KMS Key

User	S3 Permission	Key Permission	Can they read data?
Manager	S3 Full Access	Key Administrator	✘
Dev 1	S3 Read	Key User – Encrypt/Decrypt	✔
Dev 2	S3 Read	No Permission	✘
Dev 3	No S3 Permission	Key User – Encrypt/Decrypt	✘

Envelope Encryption

I HIDE DOOR KEY

Encryption Process

Plain Text Data

Crypto Service

Plain Text Data

A B C D
1 2 3 4

Crypto Service

Hardware

Software

Plain Text Data

A B C D
1 2 3 4

Plain Text Data

A B C D
1 2 3 4

Plain Text Data

A B C D
1 2 3 4

Encryption

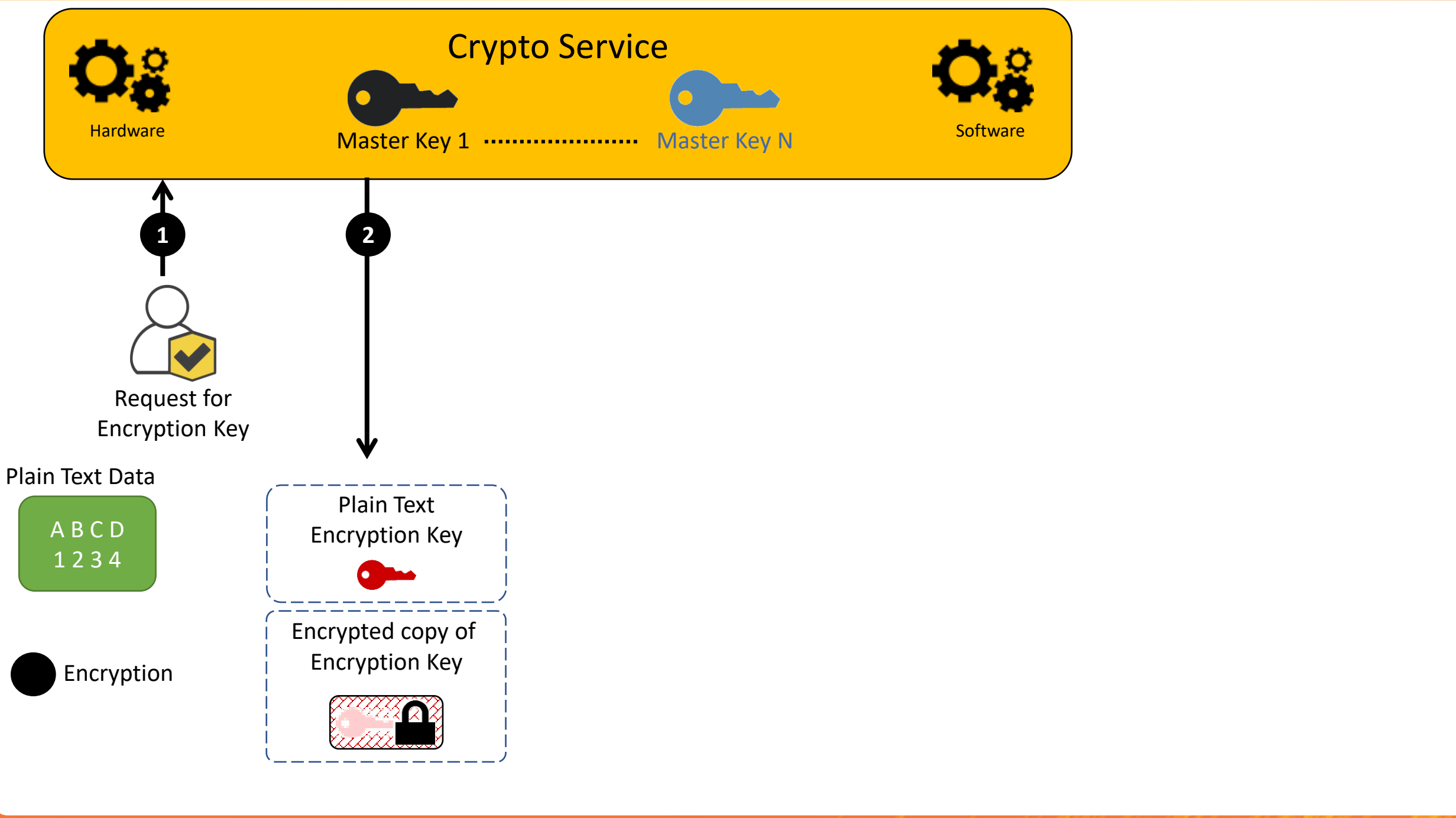
1

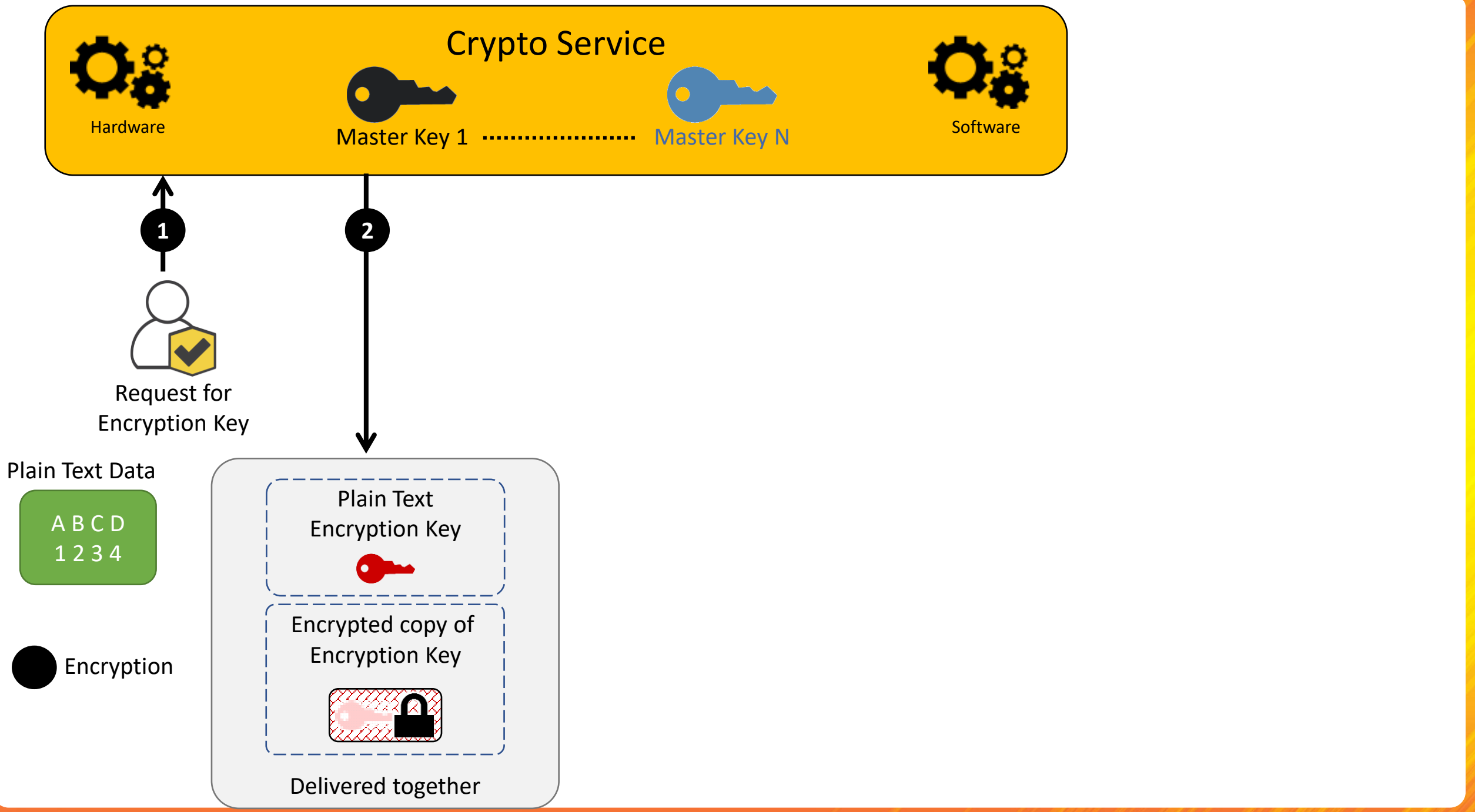
Request for
Encryption Key

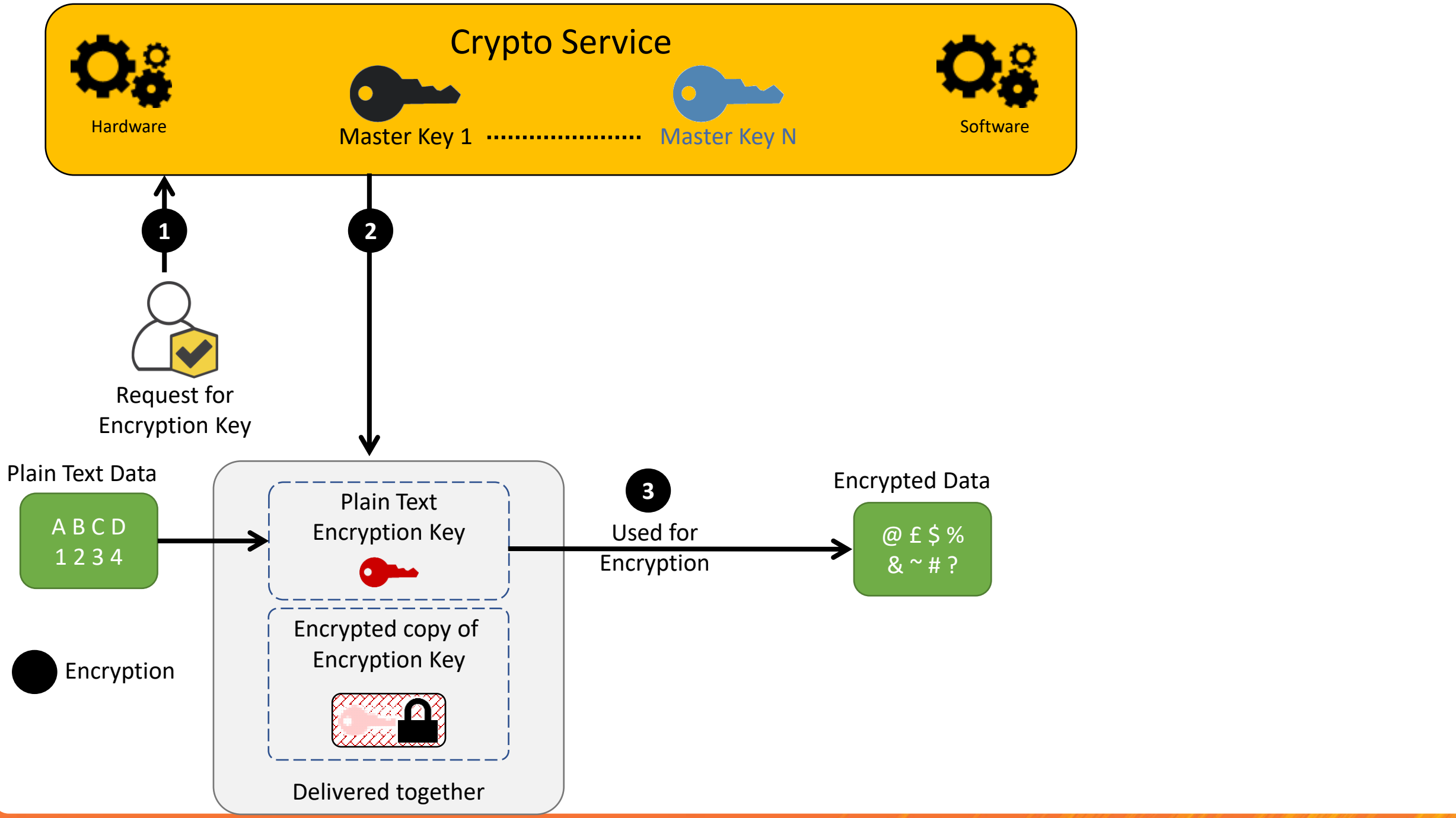
Plain Text Data

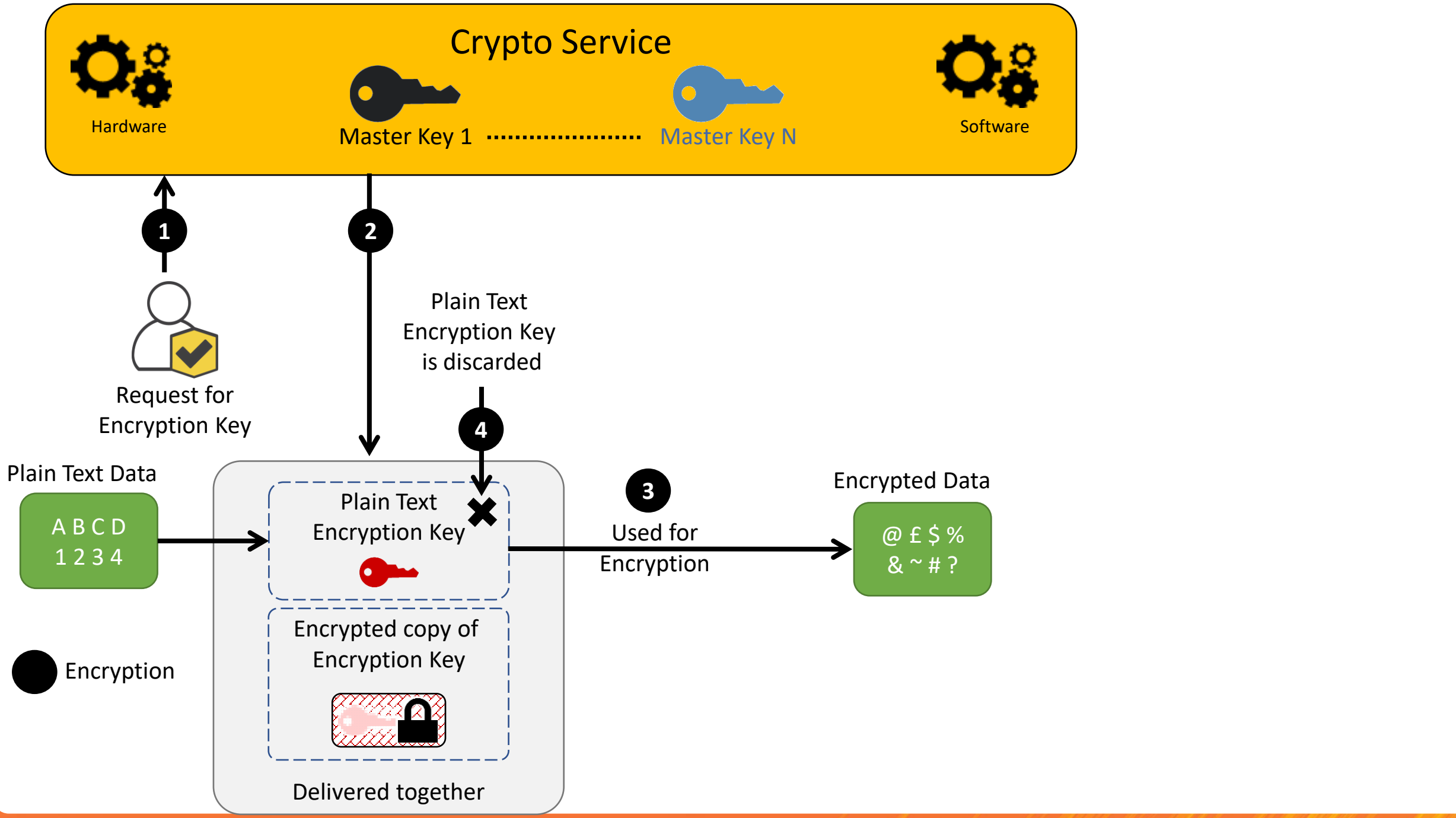
A B C D
1 2 3 4

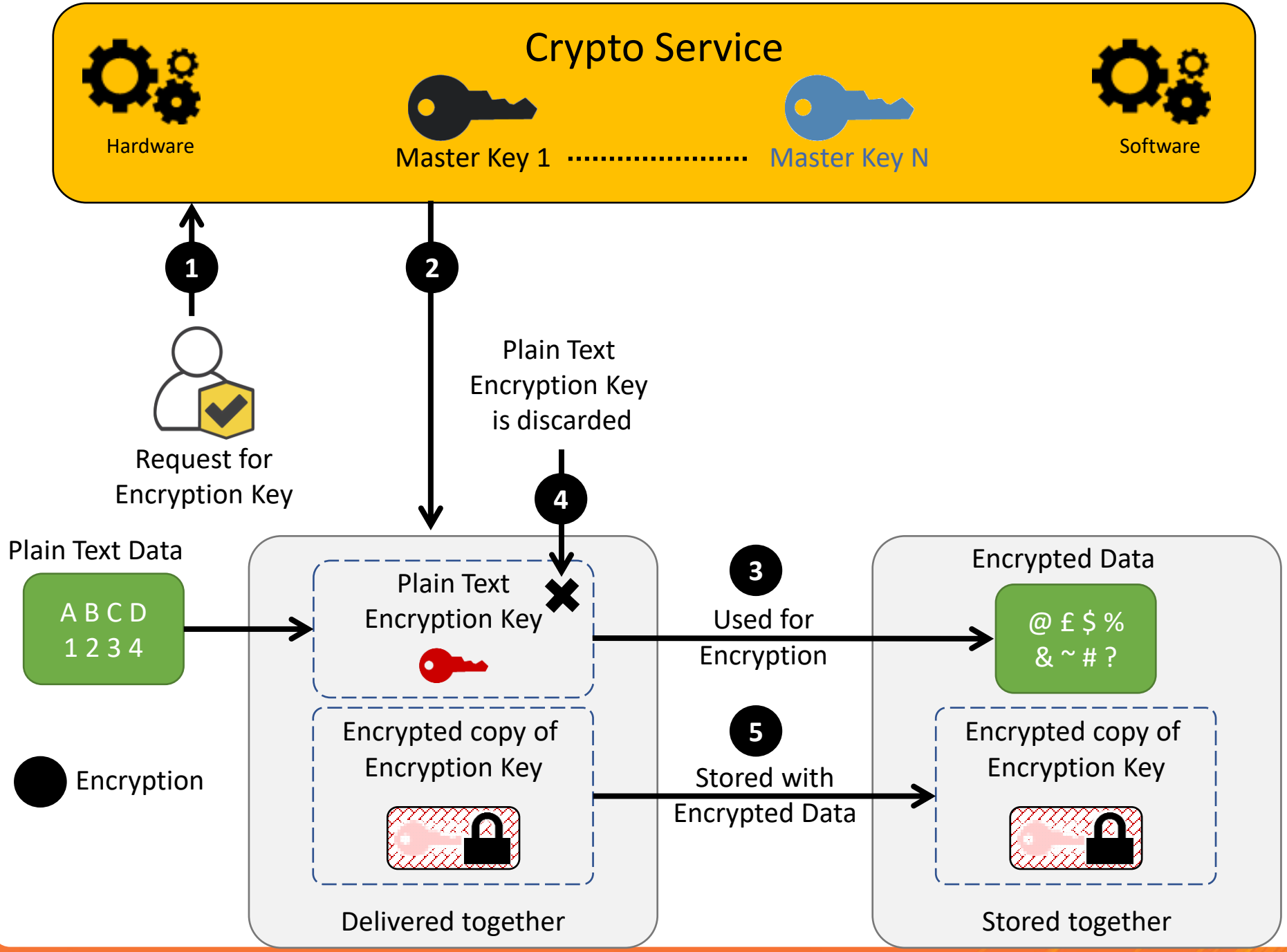
Encryption


Crypto Service
Hardware
Master Key 1
Master Key N
Software
1
2
Request for
Encryption Key
Plain Text Data
A B C D
1 2 3 4
Encryption
Plain Text
Encryption Key
Encrypted copy of
Encryption Key

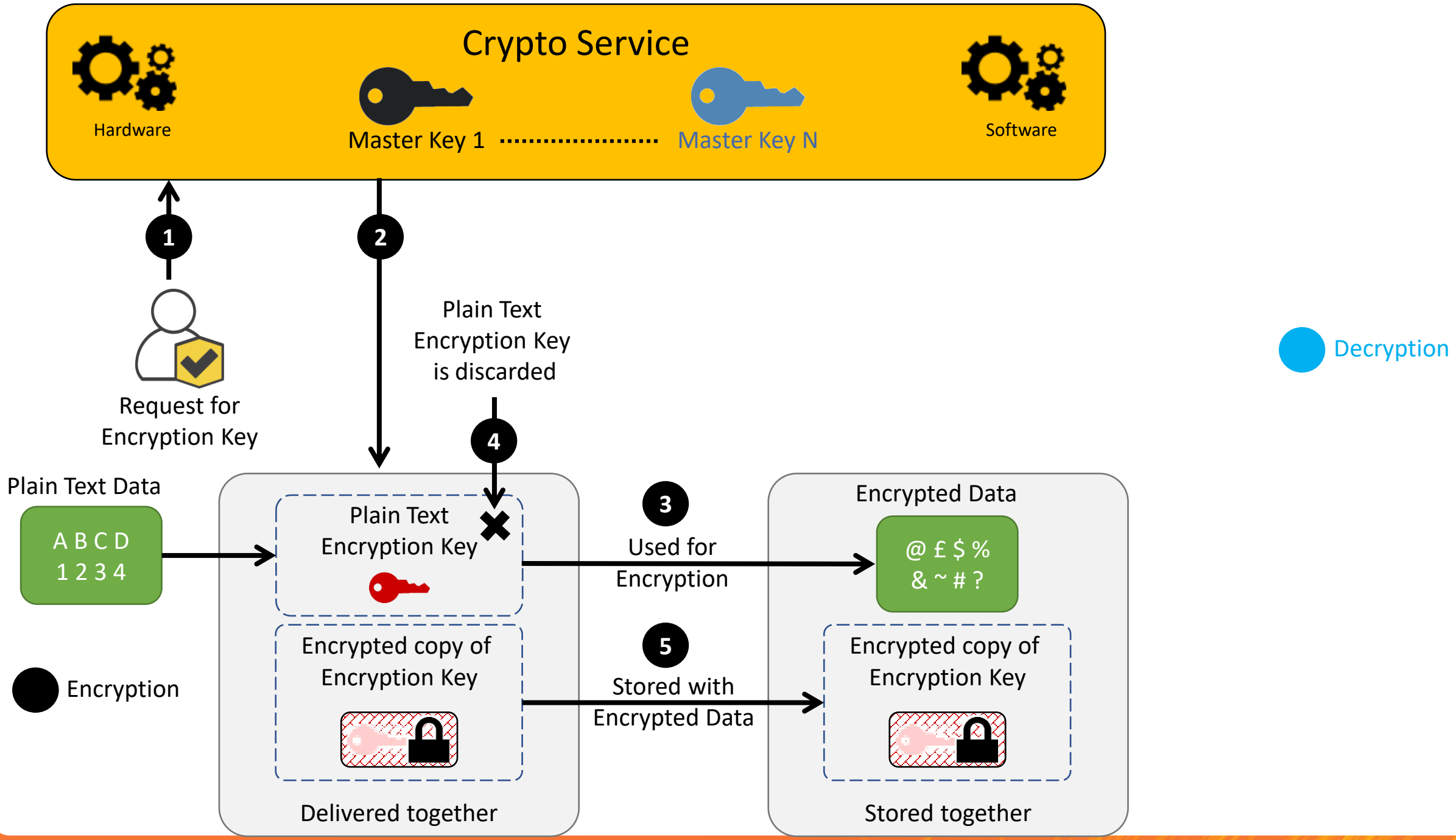

Crypto Service
Hardware
Master Key 1
Master Key N
Software
1
2
Request for
Encryption Key
Plain Text Data
A B C D
1 2 3 4
Encryption
Plain Text
Encryption Key
Encrypted copy of
Encryption Key
Delivered together

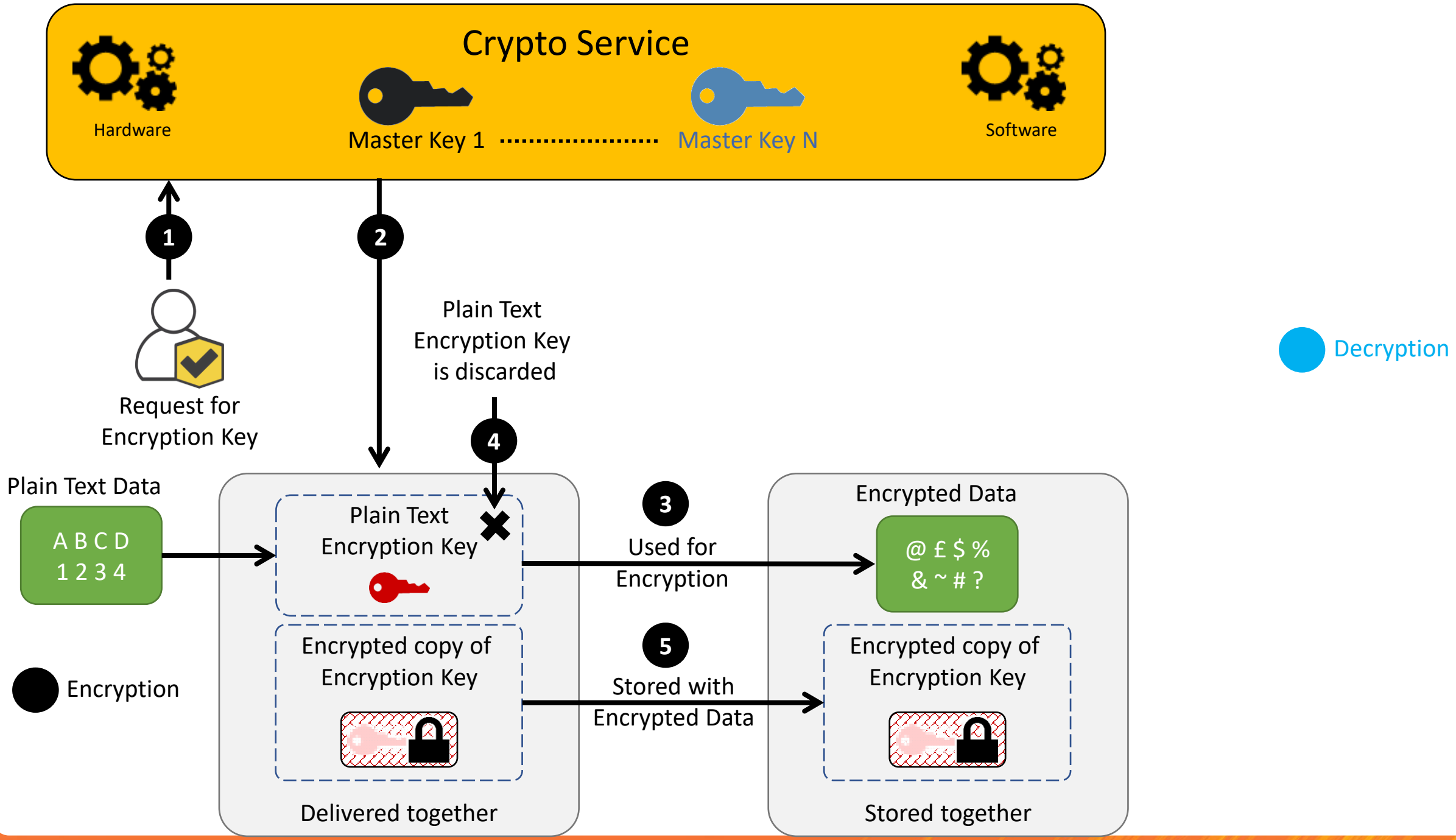

Crypto Service
Hardware
Master Key 1
Master Key N
Software
1
2
Request for
Encryption Key
Plain Text Data
A B C D
1 2 3 4
Plain Text
Encryption Key
Encrypted copy of
Encryption Key
Delivered together
3
Used for
Encryption
Encrypted Data
@ £ $ %
& ~ # ?
Encryption


Crypto Service
Hardware
Master Key 1
Master Key N
Software
1
2
Request for
Encryption Key
Plain Text
Encryption Key
is discarded
4
Plain Text Data
A B C D
1 2 3 4
Plain Text
Encryption Key
Encrypted copy of
Encryption Key
Delivered together
3
Used for
Encryption
Encrypted Data
@ £ $ %
& ~ # ?
Encryption


Crypto Service
Hardware
Master Key 1
Master Key N
Software
1
2
Request for
Encryption Key
Plain Text
Encryption Key
is discarded
4
Plain Text Data
A B C D
1 2 3 4
Plain Text
Encryption Key
3
Used for
Encryption
Encrypted Data
@ £ $ %
& ~ # ?
Encrypted copy of
Encryption Key
5
Stored with
Encrypted Data
Encrypted copy of
Encryption Key
Encryption
Delivered together
Stored together

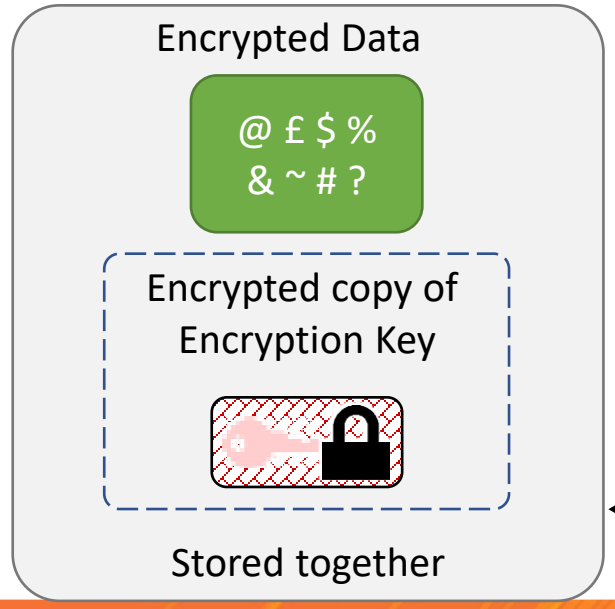
Decryption Process

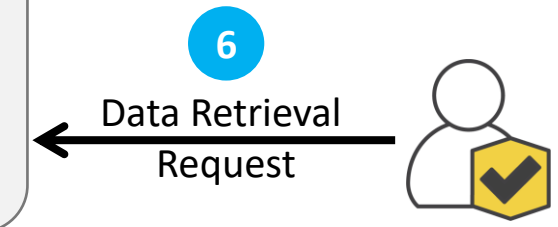

Crypto Service
Hardware
Master Key 1
Master Key N
Software
1
2
Request for
Encryption Key
Plain Text
Encryption Key
is discarded
4
Plain Text Data
A B C D
1 2 3 4
Plain Text
Encryption Key
3
Used for
Encryption
Encrypted Data
@ £ $ %
& ~ # ?
Encrypted copy of
Encryption Key
5
Stored with
Encrypted Data
Encrypted copy of
Encryption Key
Delivered together
Stored together
Encryption
Decryption

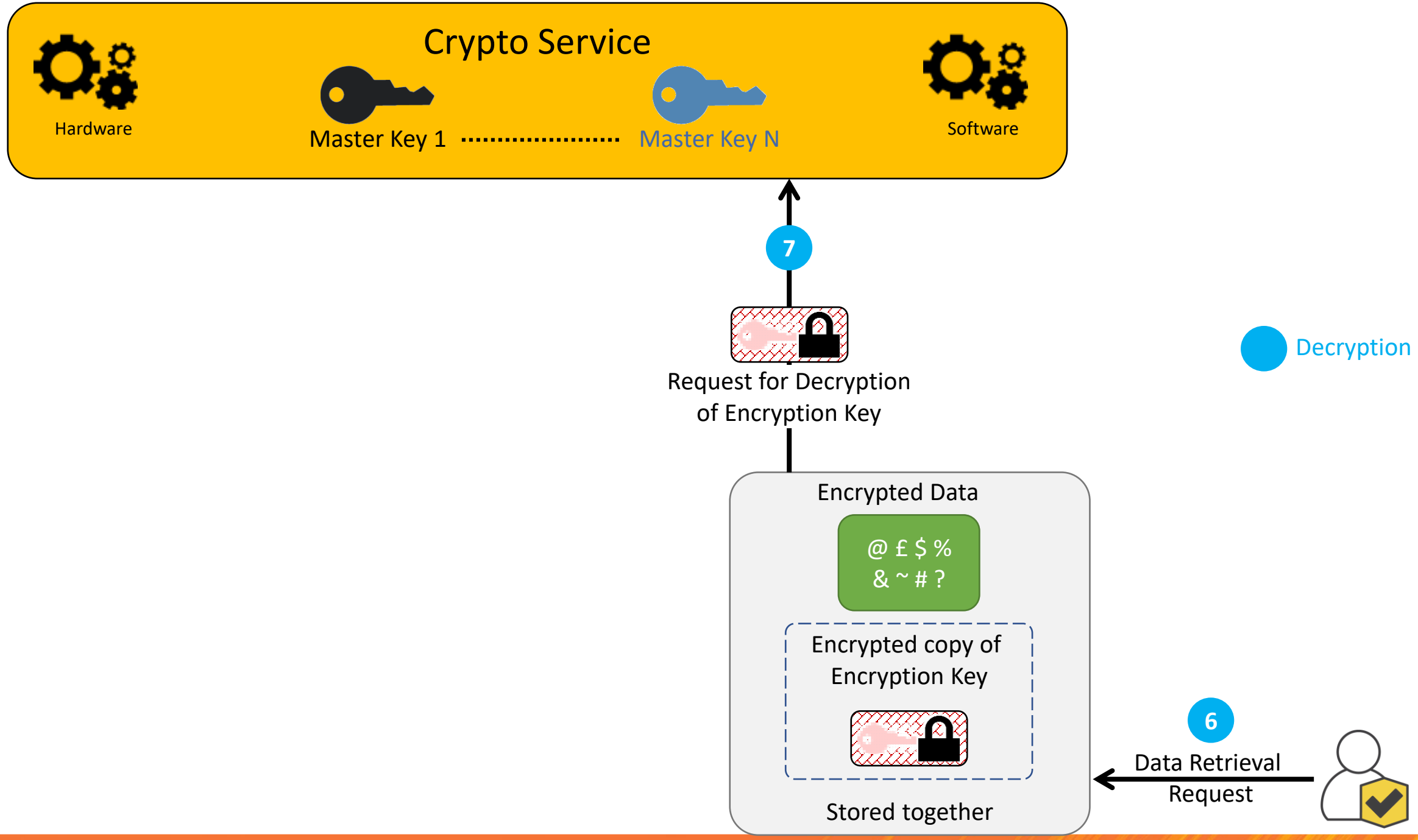

Crypto Service
Hardware
Master Key 1
Master Key N
Software
1
2
Request for
Encryption Key
Plain Text
Encryption Key
is discarded
4
Plain Text Data
A B C D
1 2 3 4
Plain Text
Encryption Key
3
Used for
Encryption
Encrypted Data
@ £ $ %
& ~ # ?
Encrypted copy of
Encryption Key
5
Stored with
Encrypted Data
Encrypted copy of
Encryption Key
Delivered together
Stored together
Encryption
Decryption

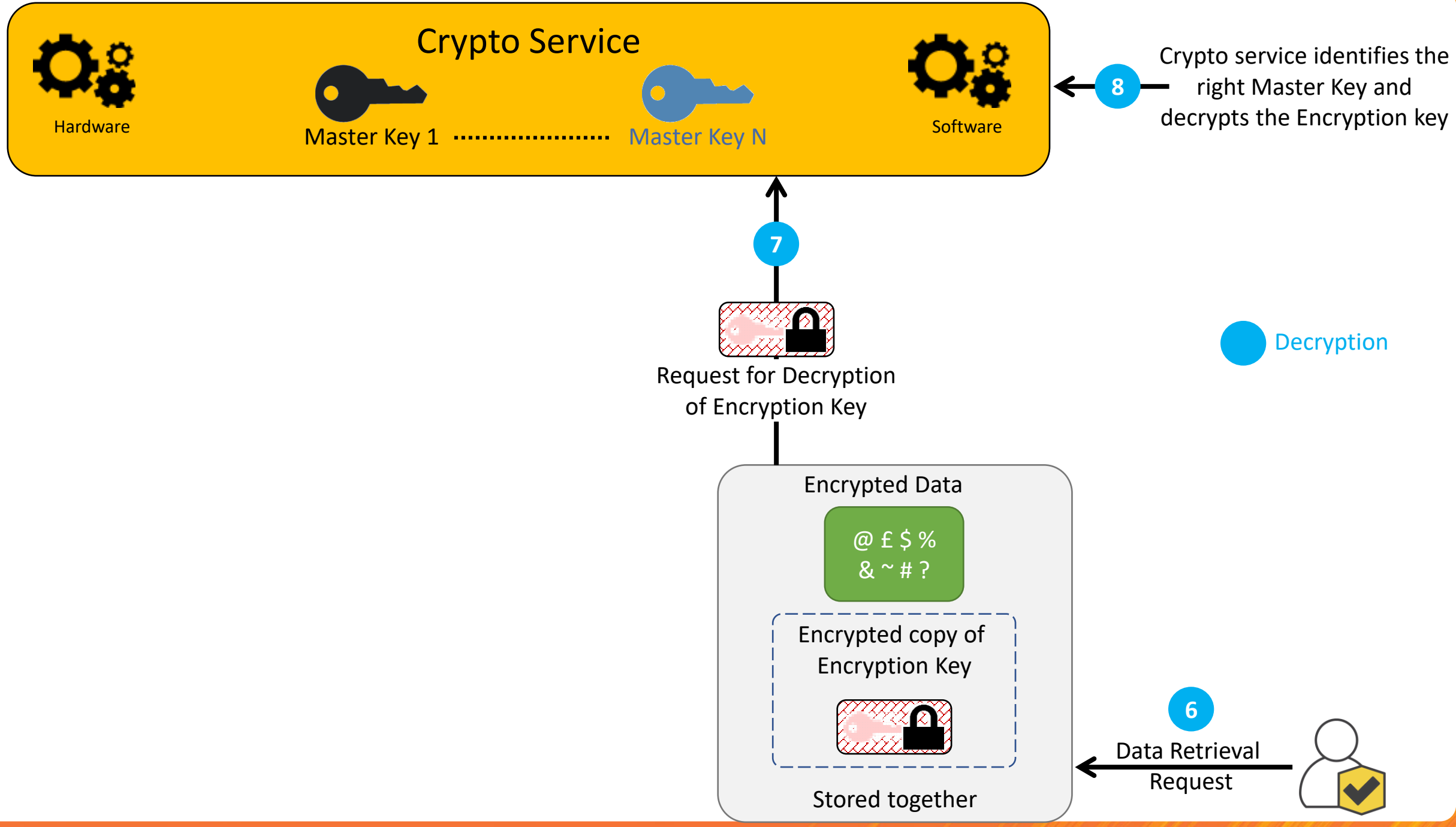

Crypto Service
Hardware
Master Key 1
Master Key N
Software

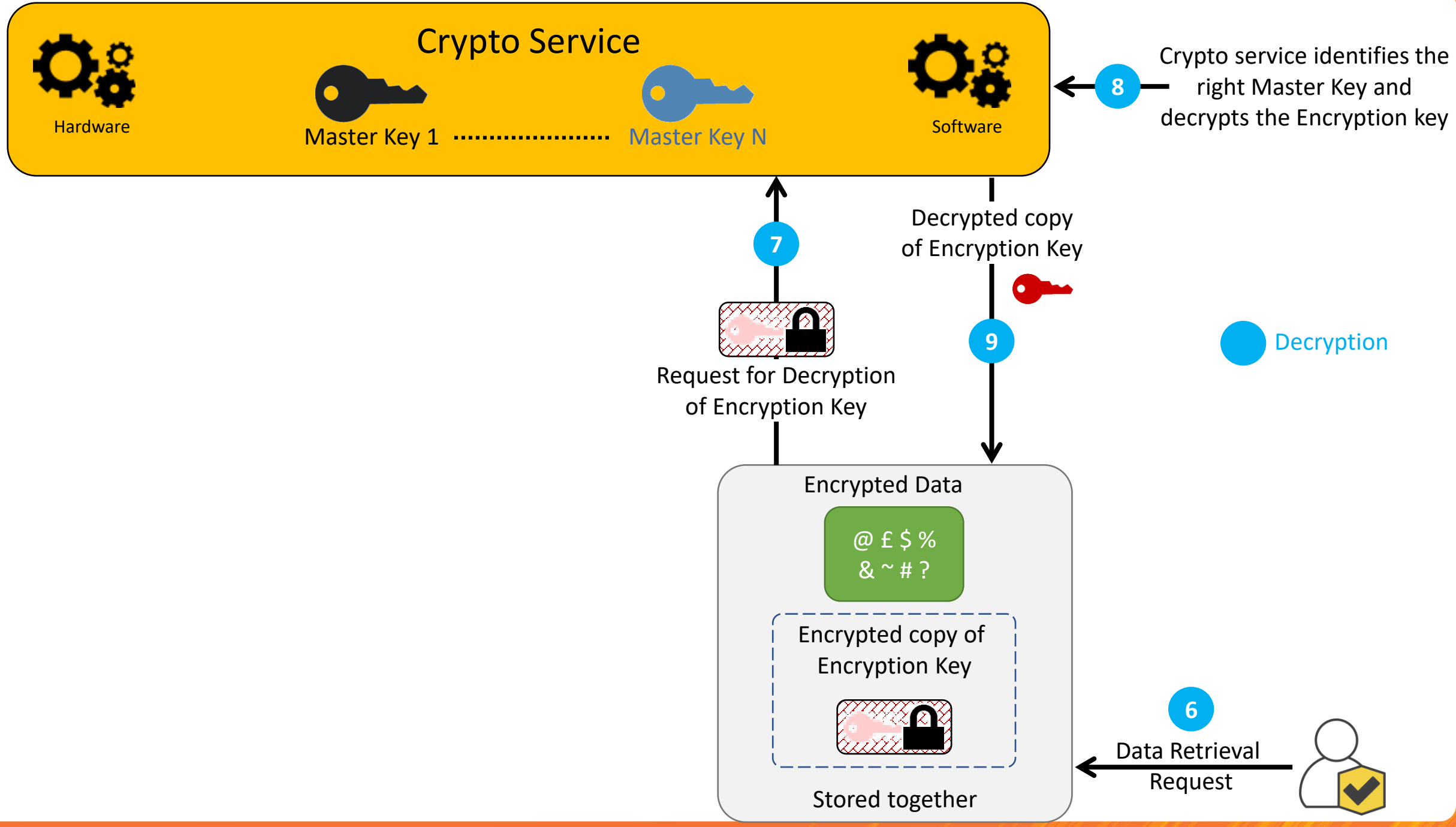
Decryption

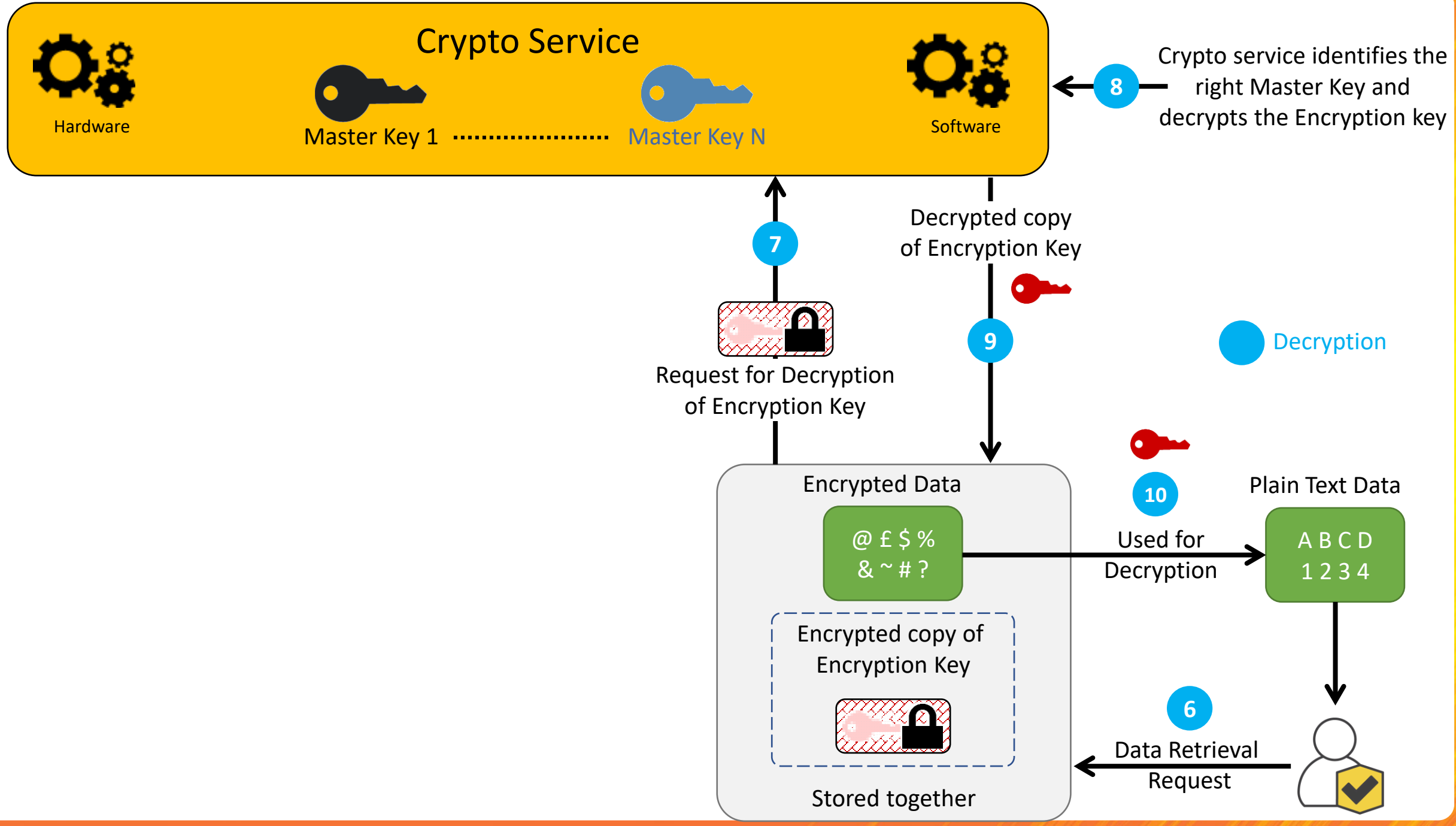

Encrypted Data
@ £ $ %
& ~ # ?
Encrypted copy of
Encryption Key
Stored together


6
Data Retrieval
Request

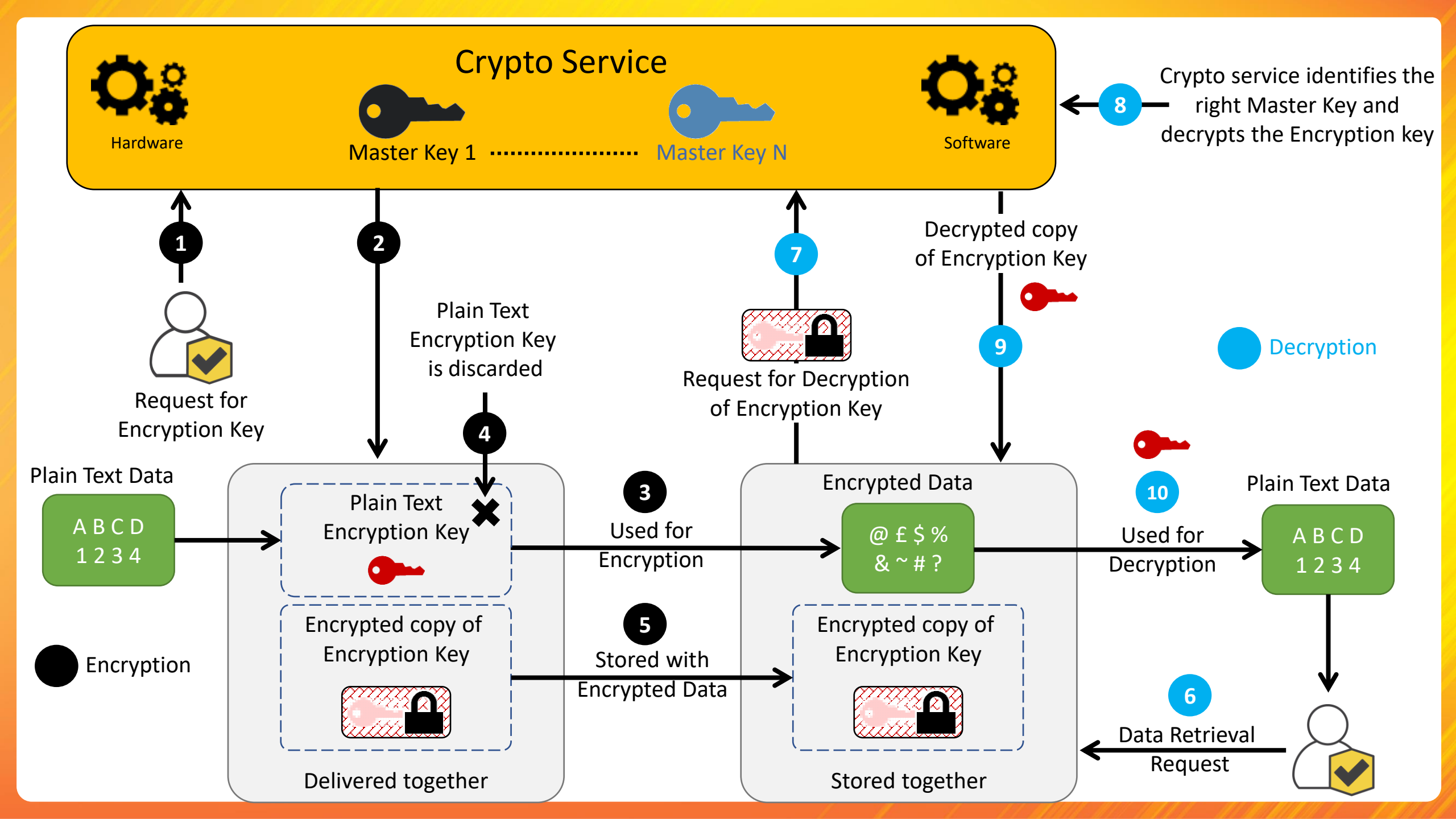

Crypto Service
Hardware
Master Key 1
Master Key N
Software
7
Request for Decryption
of Encryption Key
Decryption
Encrypted Data
@ £ $ %
& ~ # ?
Encrypted copy of
Encryption Key
Stored together
6
Data Retrieval
Request


Crypto Service
Hardware
Master Key 1
Master Key N
Software
8
Crypto service identifies the right Master Key and decrypts the Encryption key
7
Request for Decryption of Encryption Key
Decryption
Encrypted Data
@ £ $ %
& ~ # ?
Encrypted copy of Encryption Key
Stored together
6
Data Retrieval Request


Crypto Service
Hardware
Master Key 1
Master Key N
Software
8
Crypto service identifies the right Master Key and decrypts the Encryption key
7
Request for Decryption of Encryption Key
Decrypted copy of Encryption Key
9
Decryption
Encrypted Data
@ £ $ %
& ~ # ?
Encrypted copy of Encryption Key
Stored together
6
Data Retrieval Request

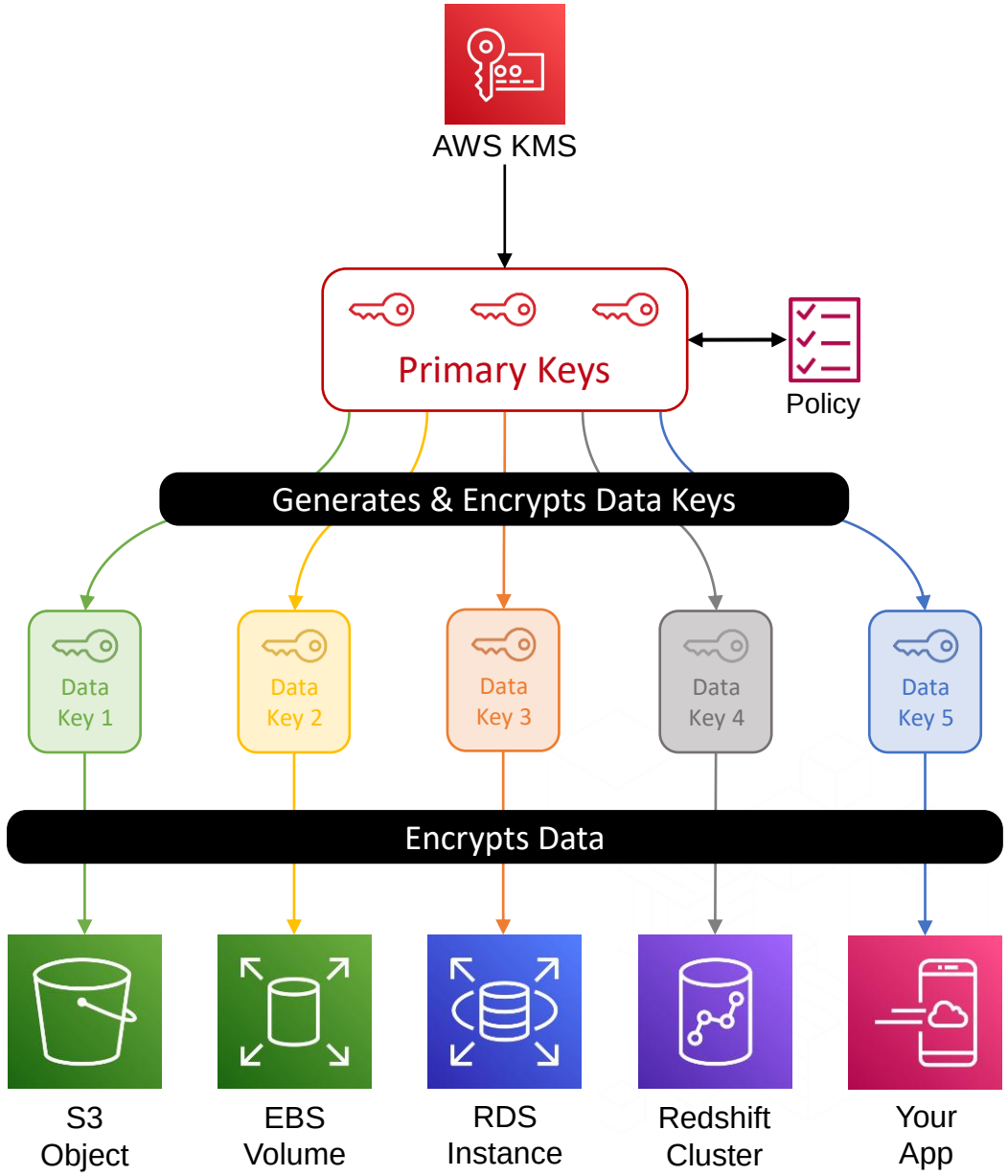

Crypto Service
Hardware
Master Key 1
Master Key N
Software
8
Crypto service identifies the right Master Key and decrypts the Encryption key
7
Request for Decryption of Encryption Key
Decrypted copy of Encryption Key
9
Decryption
Encrypted Data
@ £ $ %
& ~ # ?
Encrypted copy of Encryption Key
Stored together
10
Used for Decryption
Plain Text Data
A B C D
1 2 3 4
6
Data Retrieval Request

Complete Encryption Decryption Process


Crypto Service
Hardware
Master Key 1
Master Key N
Software
8
Crypto service identifies the right Master Key and decrypts the Encryption key
1
2
7
Decrypted copy of Encryption Key
9
Decryption
Request for Encryption Key
Plain Text Encryption Key is discarded
4
Request for Decryption of Encryption Key
Plain Text Data
A B C D 1 2 3 4
Plain Text Encryption Key
3
Used for Encryption
Encrypted Data
@ £ $ % & ~ # ?
10
Used for Decryption
Plain Text Data
A B C D 1 2 3 4
Encrypted copy of Encryption Key
5
Stored with Encrypted Data
Encrypted copy of Encryption Key
Encryption
6
Data Retrieval Request
Delivered together
Stored together

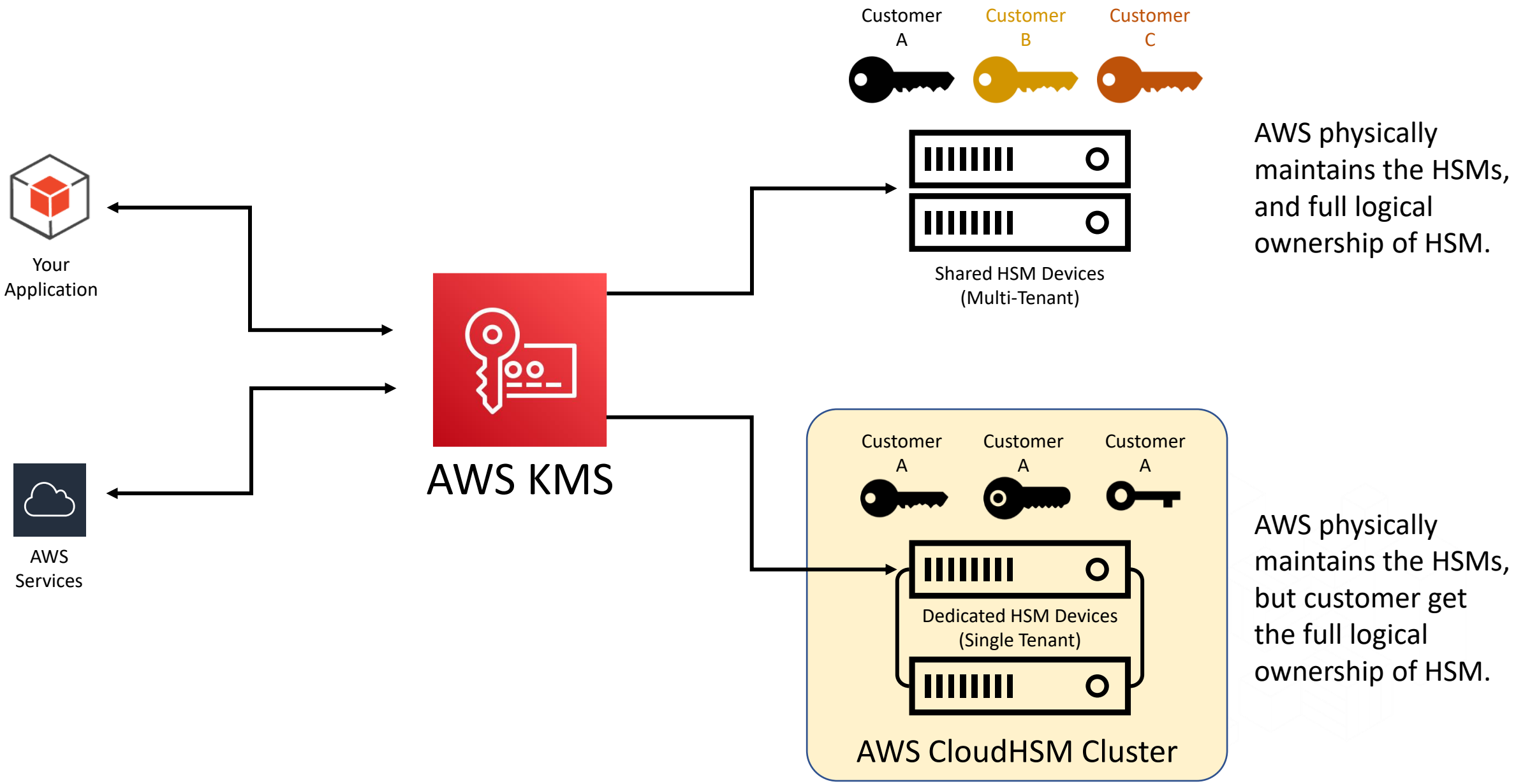
How AWS Services Integrate with KMS?

- 2-Tiered key hierarch using envelope encryption
- Data keys encrypt customer data
- KMS master keys encrypt data keys
- Benefits:
  - Limit blast radius of compromised resources and their keys
  - Easier to manage a small number of keys than billions of resource keys
  - Better performance



AWS CloudHSM

AWS CloudHSM



AWS physically maintains the HSMs, and full logical ownership of HSM.

AWS physically maintains the HSMs, but customer get the full logical ownership of HSM.

When to use CloudHSM?

	AWS KMS	CloudHSM
Scope	AES-256 and RSA encrypt; RSA and ECC sign	Most general-purpose HSM functions (encrypt, sign /verify, derive, hash, wrap)
Secrets / keys stored in	Shared FIPS-validated HSM	Single-tenant FIPS-validated HSM in customer VPC
HSM controlled by	AWS	Customer
Scalability managed by	AWS	Customer
Keys managed by	AWS	Customer
Key access by	AWS IAM / resource policies	Customer-defined credentials
Integrated with AWS services	Yes	No
Secret / key operations implemented with	AWS CLI / SDK or Encryption SDK	Customer-built application
Rotation executed by	AWS [not for BYOK and CKS]	Customer

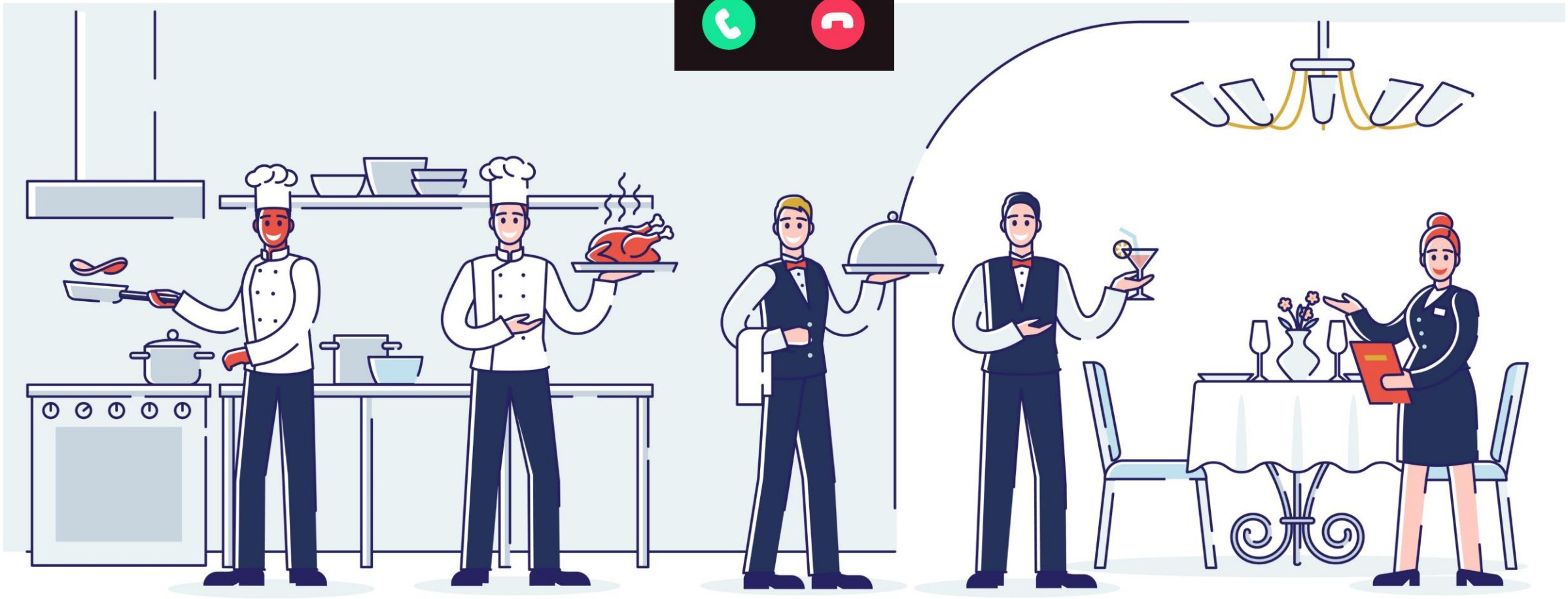
AWS KMS custom key store: best of two worlds

	AWS KMS	KMS custom key store (CloudHSM)
Where keys are generated	HSMs controlled by AWS	HSMs controlled by you
Where keys are stored	HSMs controlled by AWS	HSMs controlled by you
Where keys are used	HSMs controlled by AWS	HSMs controlled by you
How to control key use	JSON key policies you define	JSON key policies you define
Responsibility for performance / scale	AWS	You
Integration with AWS services?	Yes	Yes
Pricing model	$1/key + usage	$1/key + usage; hourly charge for each HSM

Mitigation of DDoS attacks

What is a DDoS attack?

- A restaurant at work



What is a DDoS attack?

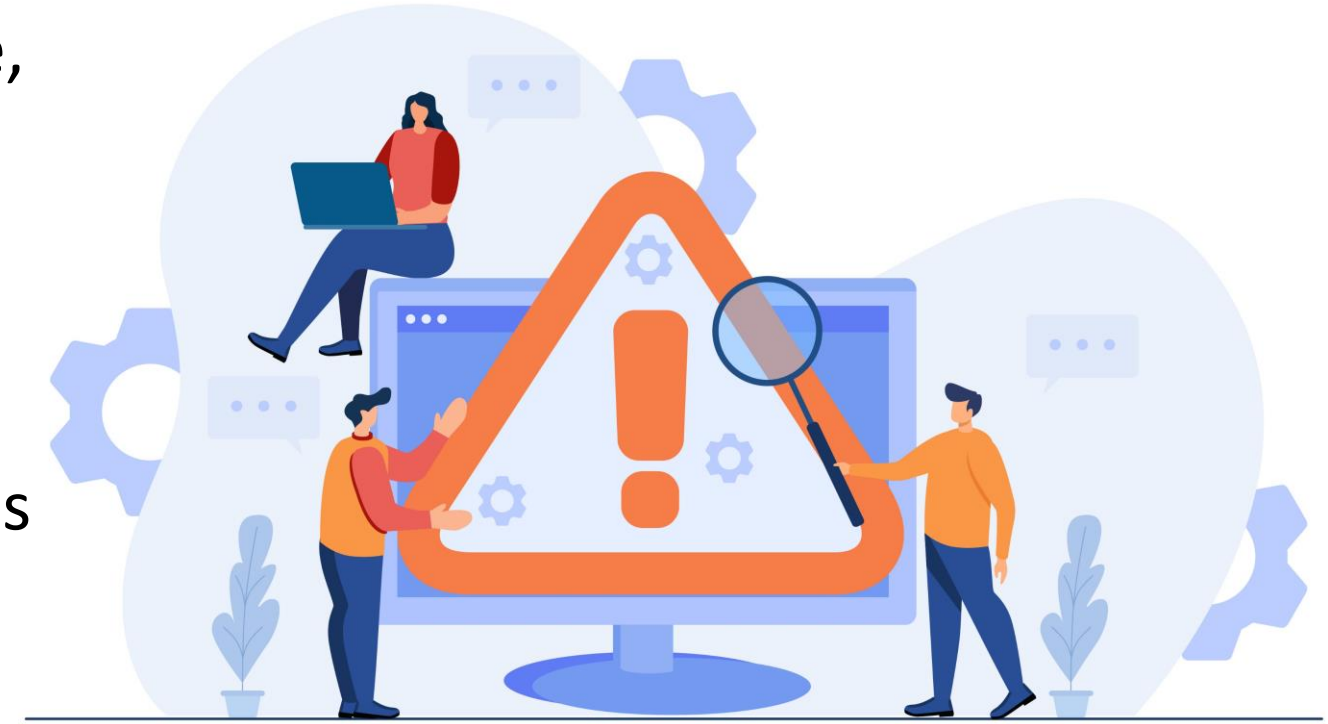
- A restaurant ~~at work~~

What is a DDoS attack?

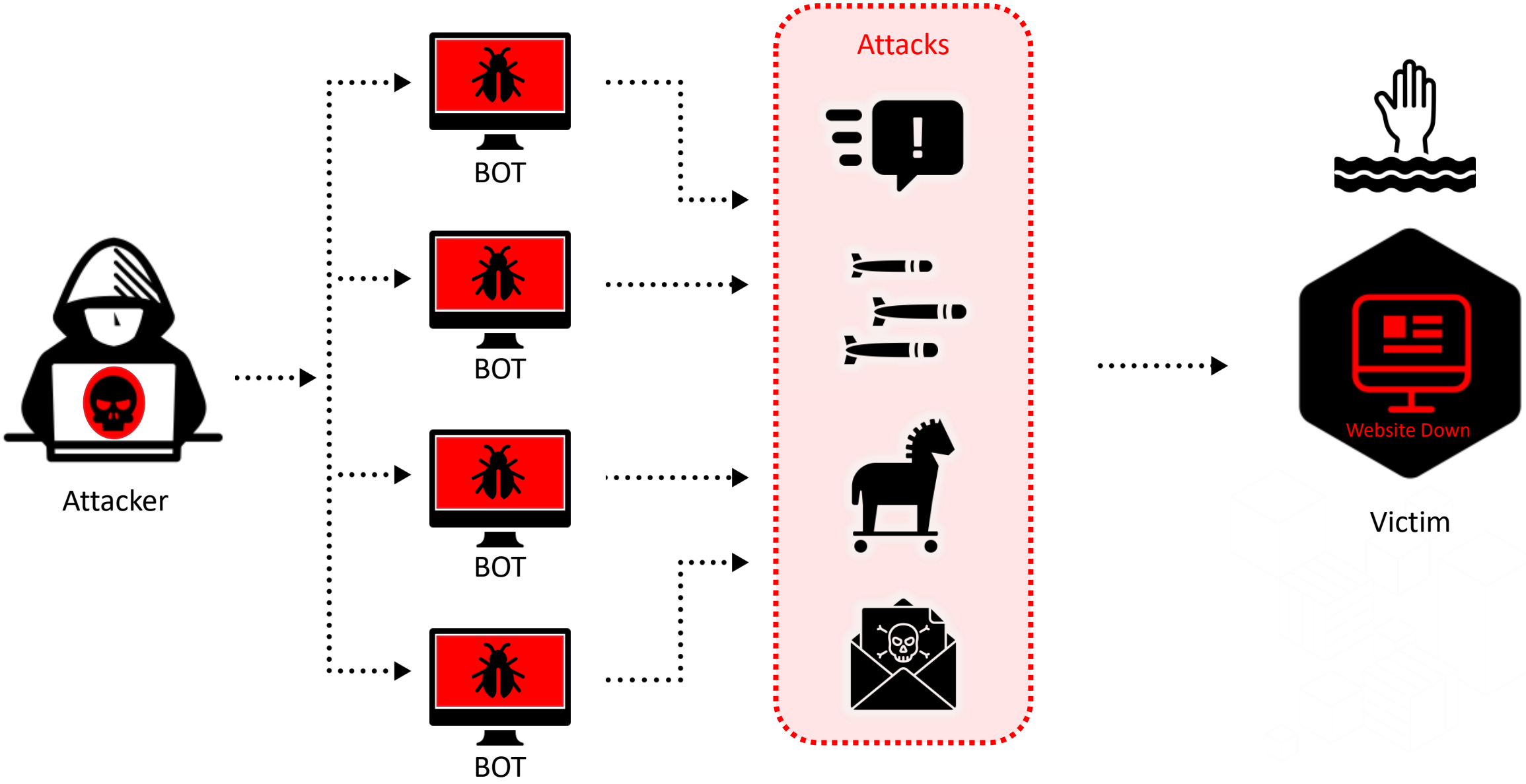
- A distributed denial-of-service (DDoS) attack occurs when a group of systems flood a server with fraudulent traffic.

- Eventually, the server is overwhelmed, causing it to either go down, or become unresponsive, even to legitimate requests.

- A DDoS attack is launched from numerous compromised devices, often distributed globally in what is referred to as a botnet.



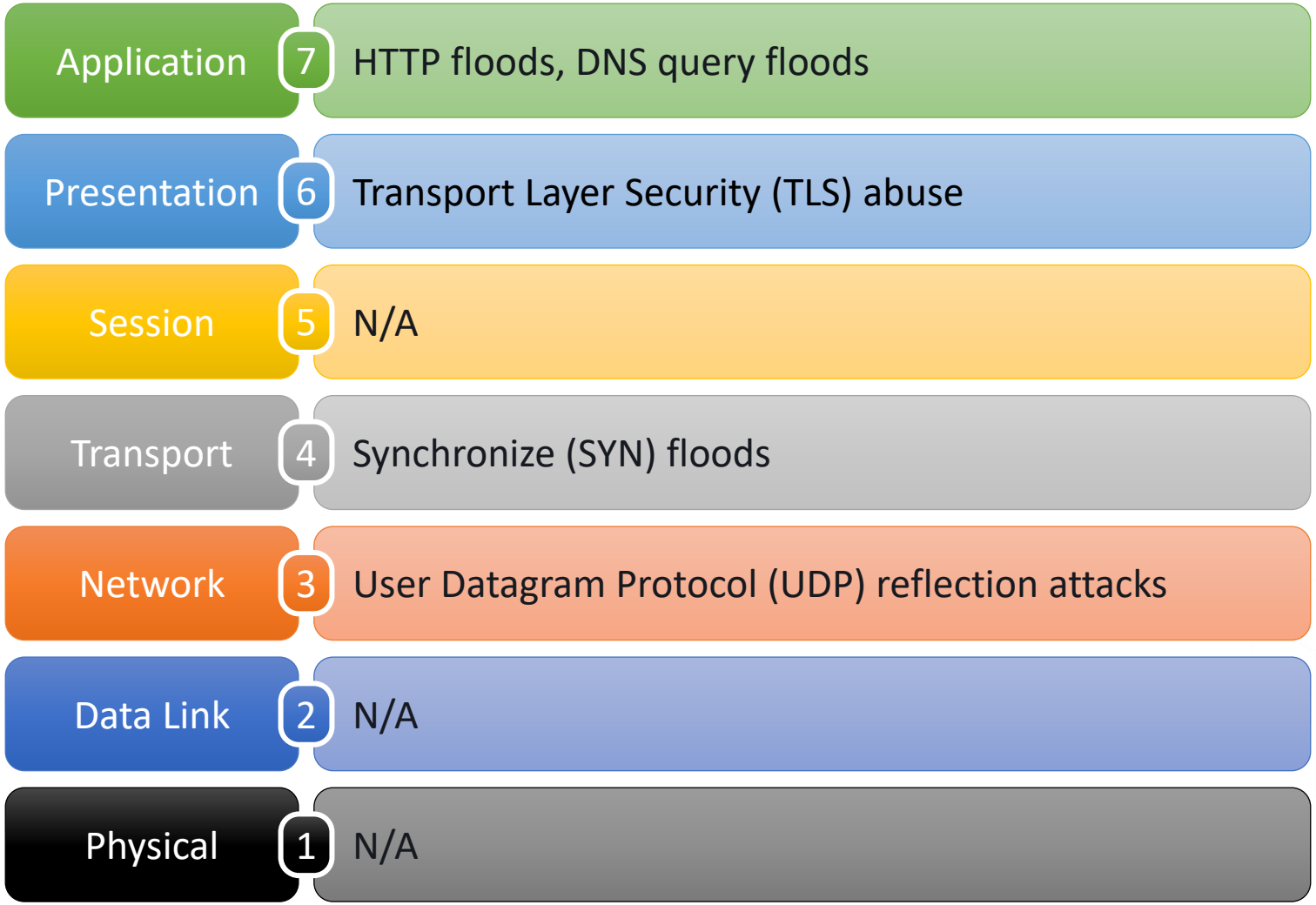
What is a DDoS attack?



Type of DDoS Attack

- Volume Based Attacks
  - Includes UDP floods, ICMP floods, and other spoofed-packet floods. The attack's goal is to saturate the bandwidth of the attacked site, and magnitude is measured in bits per second (Bps).
- Protocol Attacks
  - Includes SYN floods, fragmented packet attacks, Ping of Death, Smurf DDoS and more. This type of attack consumes actual server resources, or those of intermediate communication equipment, such as firewalls and load balancers, and is measured in packets per second (Pps).
- Application Layer Attacks
  - Includes low-and-slow attacks, GET/POST floods, attacks that target Apache, Windows or OpenBSD vulnerabilities and more. Comprised of seemingly legitimate and innocent requests, the goal of these attacks is to crash the web server, and the magnitude is measured in Requests per second (Rps).

Attack vectors



AWS Web Application Firewall (AWS WAF)

Attack vectors

Application	7	HTTP floods, DNS query floods
Presentation	6	Transport Layer Security (TLS) abuse
Session	5	N/A
Transport	4	Synchronize (SYN) floods
Network	3	User Datagram Protocol (UDP) reflection attacks
Data Link	2	N/A
Physical	1	N/A

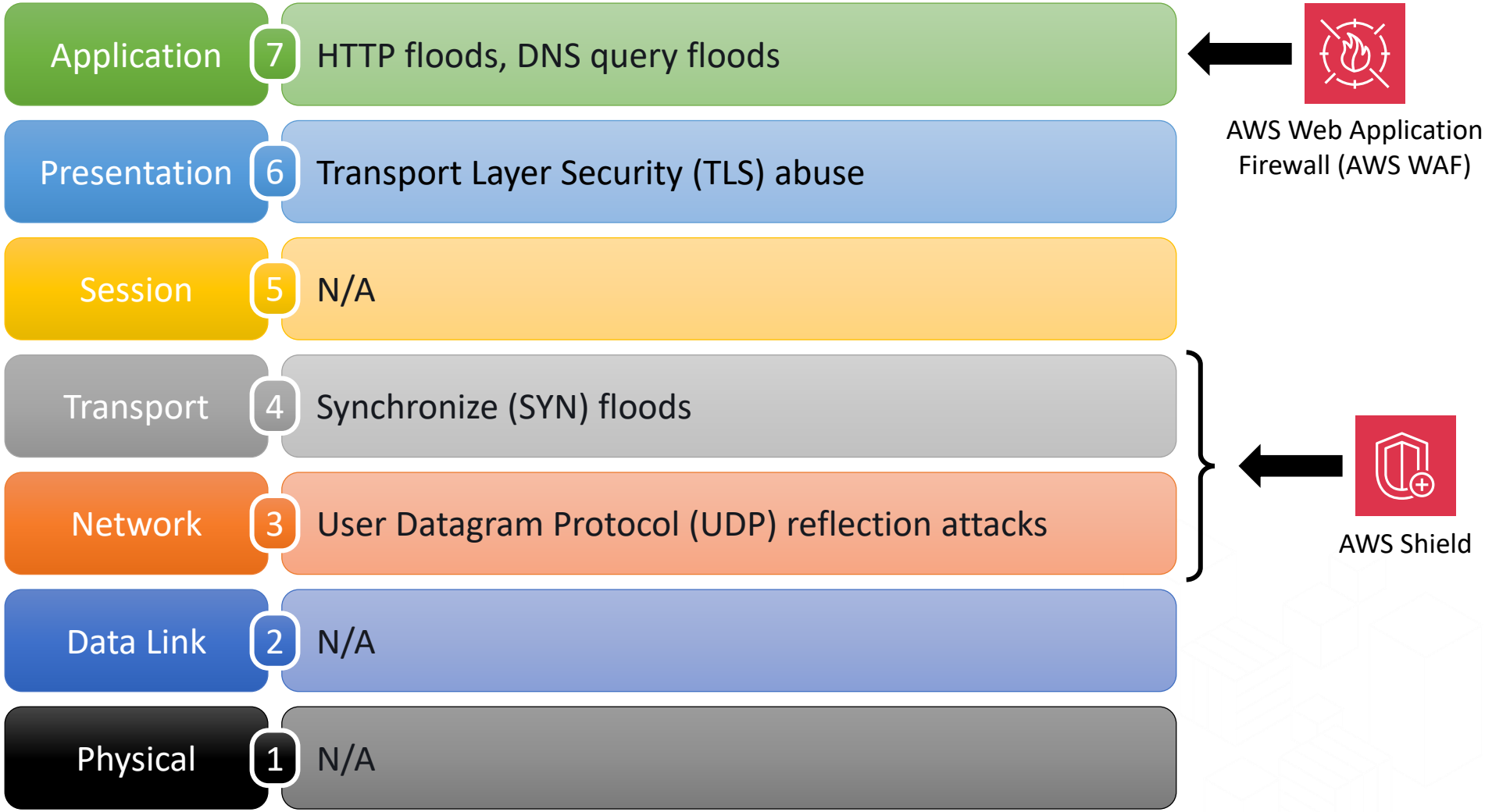
AWS Web Application Firewall (AWS WAF)

AWS Web Application Firewall (AWS WAF)

- AWS WAF protects your web applications from common exploits
- You can create security rules that control bot traffic and block common attack patterns such as SQL injection or cross-site scripting (XSS).
- You do this by defining a web access control list (ACL) and then associating it with one or more web application resources that you want to protect.
- You can protect the following resource types:
  - Amazon CloudFront distribution
  - Amazon API Gateway REST API
  - Application Load Balancer
  - AWS AppSync GraphQL API
  - Amazon Cognito user pool
  - AWS App Runner service
  - AWS Verified Access instance

AWS Shield

Attack vectors



AWS Shield

- AWS Shield is a managed DDoS protection service that safeguards applications running on AWS.
- AWS Shield Standard is automatically enabled to all AWS customers at no additional cost. AWS Shield Advanced is an optional paid service.
- AWS Shield Advanced provides additional protections against more sophisticated and larger attacks for your applications running on Amazon EC2, ELB, Amazon CloudFront, AWS Global Accelerator, and Route 53.
- Customers with Business or Enterprise support can also engage the Shield Response Team (SRT) 24x7 to manage and mitigate their application layer DDoS attacks.

AWS Firewall Manager

AWS Firewall Manager

- AWS Firewall Manager is a security management service that allows you to centrally configure and manage firewall rules across your accounts and applications in AWS Organizations.

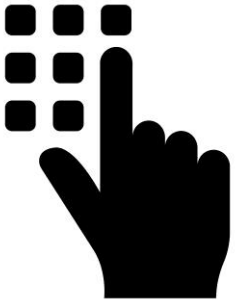
- As new applications are created, Firewall Manager makes it easier to bring new applications and resources into compliance by enforcing a common set of security rules.

- AWS Firewall Manager is integrated with AWS Organizations so you can enable AWS WAF rules, AWS Shield Advanced protections, VPC security groups, AWS Network Firewalls, and Amazon Route 53 Resolver DNS Firewall rules across multiple AWS accounts and resources from a single place.

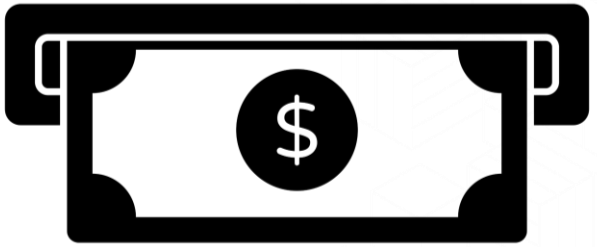
Authentication & Authorization

Authentication & Authorization

Authentication
- Who you are?



Authorization
- What can you do?



Authentication & Authorization

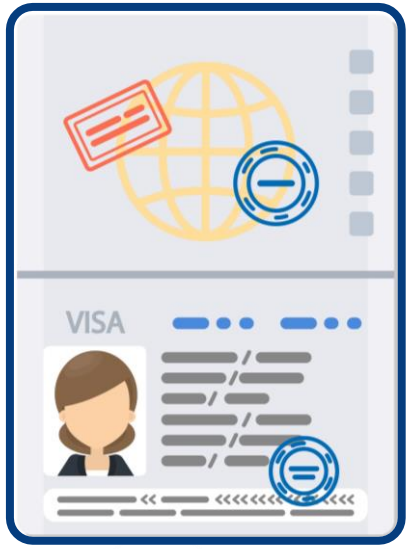
Passport

Authentication

Who you are?

- Name
- Photo
- DOB

visa



Authorization

What can you do?

- Transit
- Work
- Tourism

Directory Services

What is a directory?

- A book containing an alphabetical index of the names and addresses of persons in a city, district, organization, etc., or of a particular category of people.

Directory services in enterprise

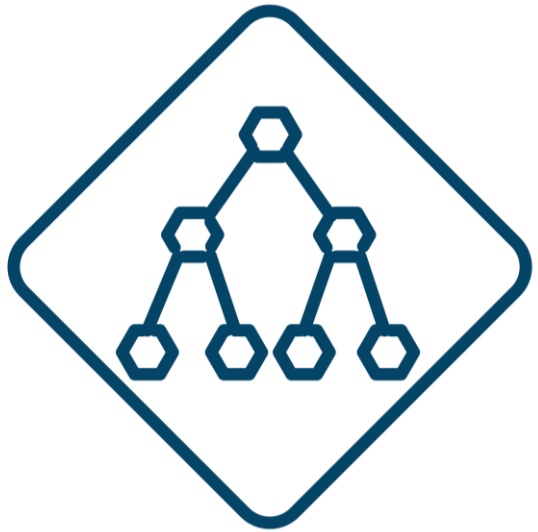
- A directory service is a database for storing and maintaining information about users and resources.
- Directory Services are often referred to as directories, user stores, Identity Stores, or LDAP Directory, and they store information such as usernames, passwords, user preferences, information about devices, and more.

Microsoft Active Directory

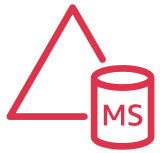
- Microsoft Active Directory, provides the methods for storing directory data and making this data available to network users and administrators.
- For example, it stores information about user accounts, such as names, passwords, phone numbers, and so on.
- Security is integrated with Active Directory through logon authentication and access control to objects in the directory.

Directory Services on AWS

Directory Service
helps you store information and manage access to resources.



AWS Directory Service



AWS Managed Microsoft AD

AD Connector

Simple AD

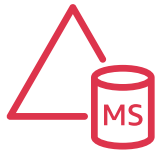
Amazon Cloud Directory

Amazon Cognito

User Pools

AWS Directory Service

AWS Directory Service



AWS Managed Microsoft AD

- **AWS Managed Microsoft AD**
  - With AWS Managed Microsoft AD, you can easily enable your Active Directory-aware workloads and AWS resources to use managed actual Microsoft Active Directory in the AWS Cloud.

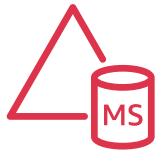
AD Connector

- **AD Connector**
  - AD Connector is a proxy for redirecting directory requests to your existing Microsoft Active Directory without caching any information in the cloud.

Simple AD

- **Simple AD**
  - Simple AD is a standalone managed directory that is powered by a Linux-Samba Active Directory–compatible server.

Which to choose?



AWS Managed Microsoft AD

- Select AWS Directory Service for Microsoft Active Directory (Standard Edition or Enterprise Edition) if you need an actual Microsoft Active Directory in the AWS Cloud.

AD Connector

- Use AD Connector if you only need to allow your on-premises users to log in to AWS applications and services with their Active Directory credentials. You can also use AD Connector to join Amazon EC2 instances to your existing Active Directory domain.

Simple AD

- Use Simple AD if you need a low-scale, low-cost directory with basic Active Directory compatibility that supports Samba 4–compatible applications, or you need LDAP compatibility for LDAP-aware applications.

Amazon Cloud Directory

Amazon Cloud Directory

- Cloud Directory is a high-performance, serverless, hierarchical data store.
- At its core, Cloud Directory is a specialized graph-based directory store that provides a foundational building block for developers.
- Cloud Directory is not a directory service for IT Administrators who want to manage or migrate their directory infrastructure.
- Cloud Directory comes ready with sample schemas for Organizations, Persons, and Devices.

Amazon Cloud Directory

Amazon Cognito

Amazon Cognito User Pools

- Amazon Cognito user pools are a managed service that lets you add secure authentication and authorization to your apps, and can scale to support millions of users.

- A User Pool is your user directory that you can configure for your web and mobile apps. A User Pool securely stores your users' profile attributes.

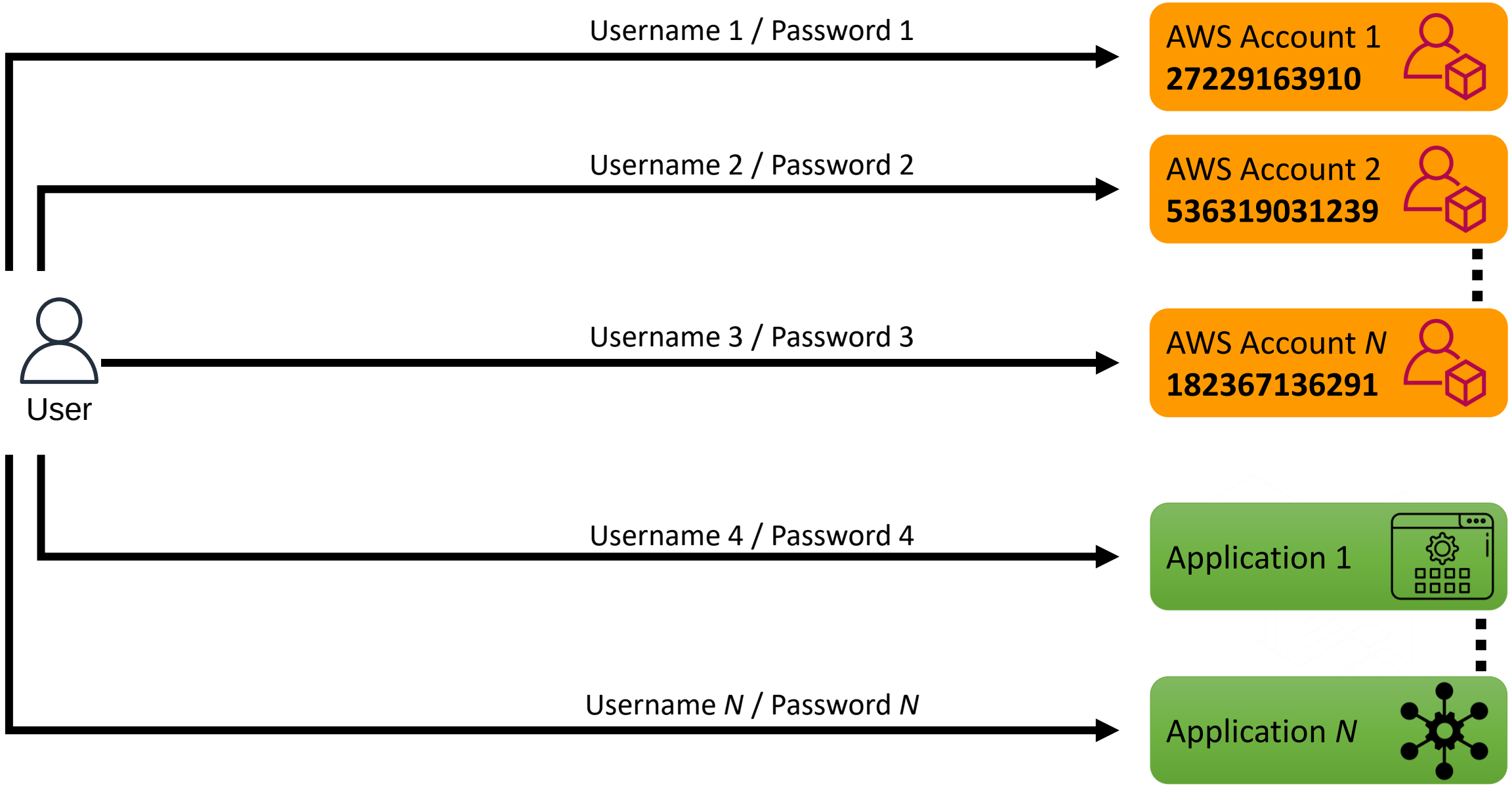
- Use Amazon Cognito if you develop high-scale SaaS applications and need a scalable directory to manage and authenticate your subscribers and that works with social media identities.

Amazon Cognito
User Pools

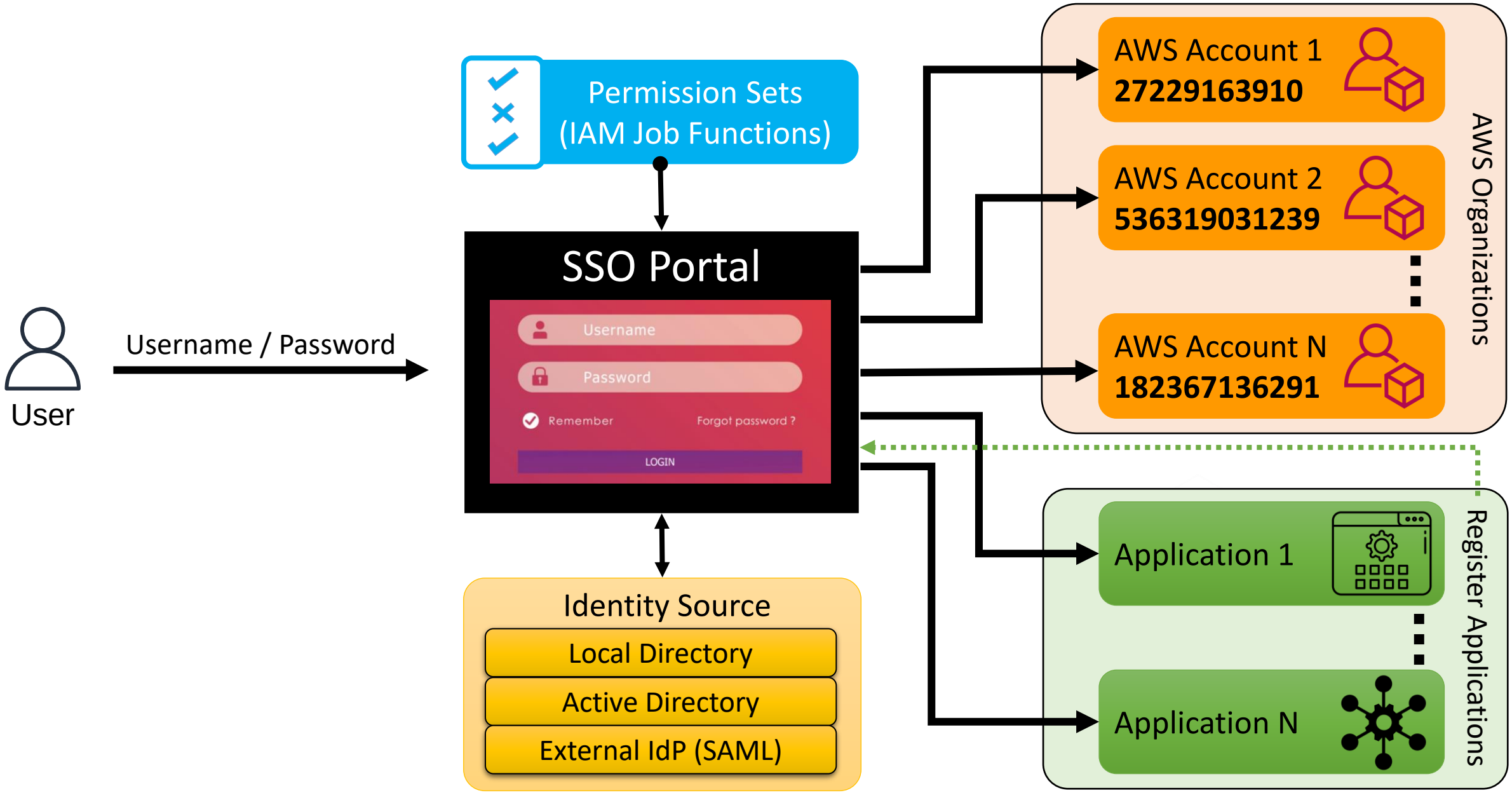
AWS IAM Identity Center

(Previously AWS Single Sign-on)

Accessing AWS accounts and applications **without** AWS IAM Identity Center



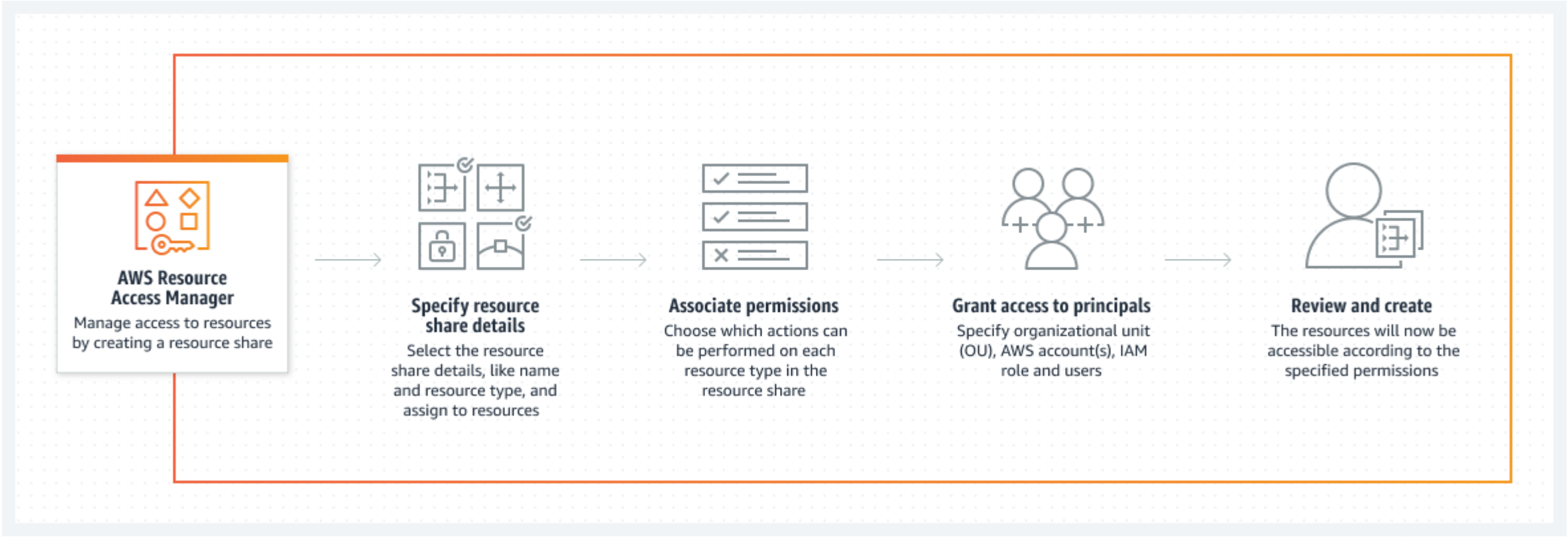
Accessing AWS accounts and applications **with** AWS IAM Identity Center



Resource Access Manager

AWS Resource Access Manager

- AWS RAM helps you securely share your resources across AWS accounts, within your organization or organizational units (OUs), and with IAM roles and users for supported resource types.



AWS Secrets Manager

Without AWS Secrets Manager

Application Code < / >

Access Credentials are hardcoded in the application

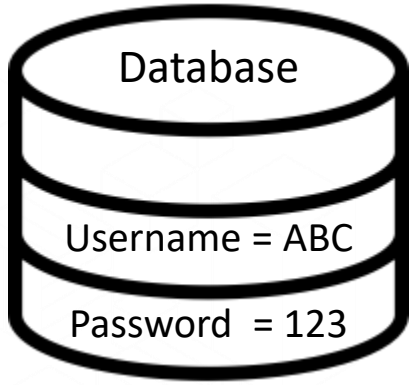
Connect to DB…

- Username = **ABC**
- Password = **123**

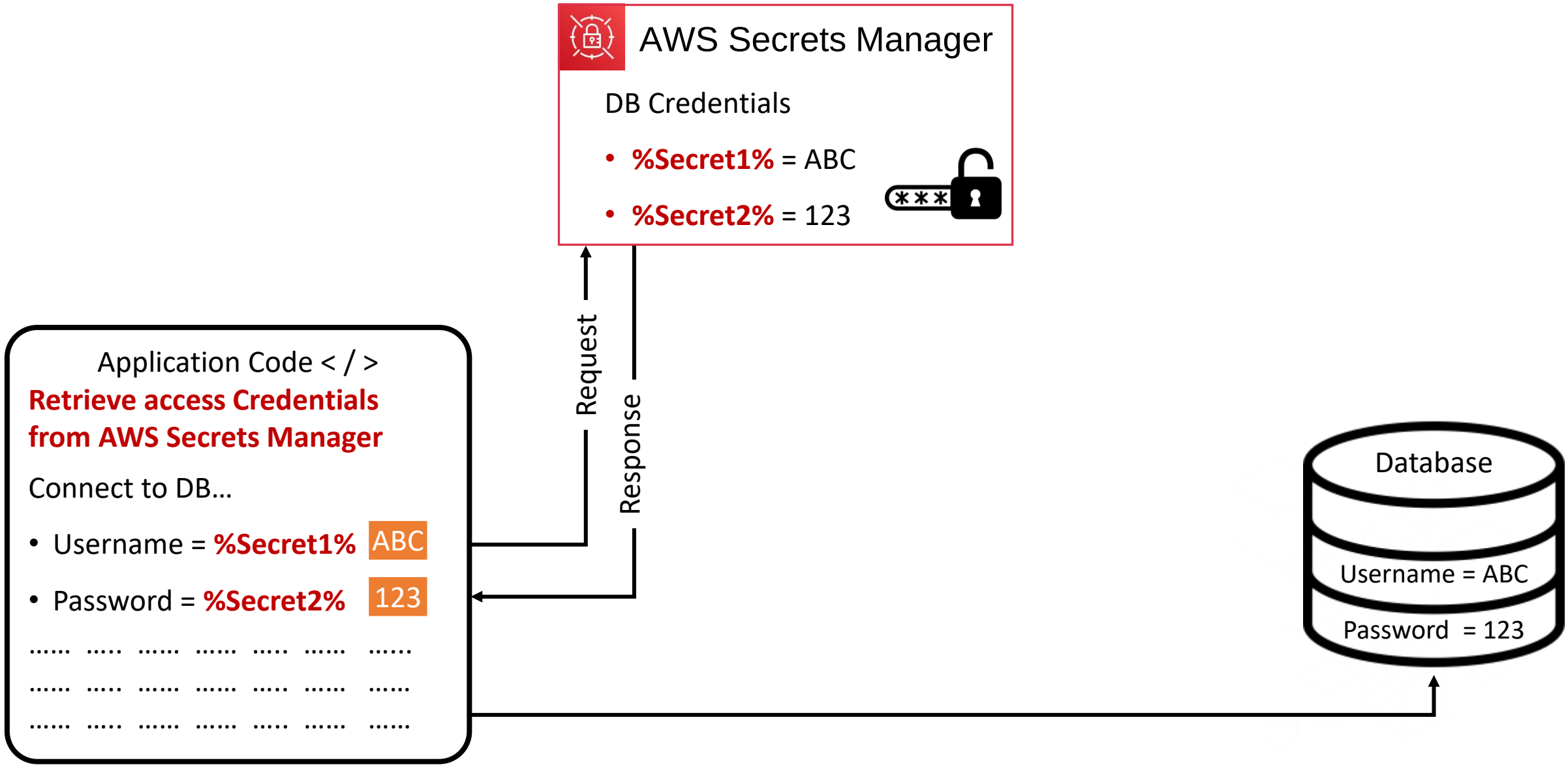
…… ….. …… …… ….. …… ……

…… ….. …… …… ….. …… ……

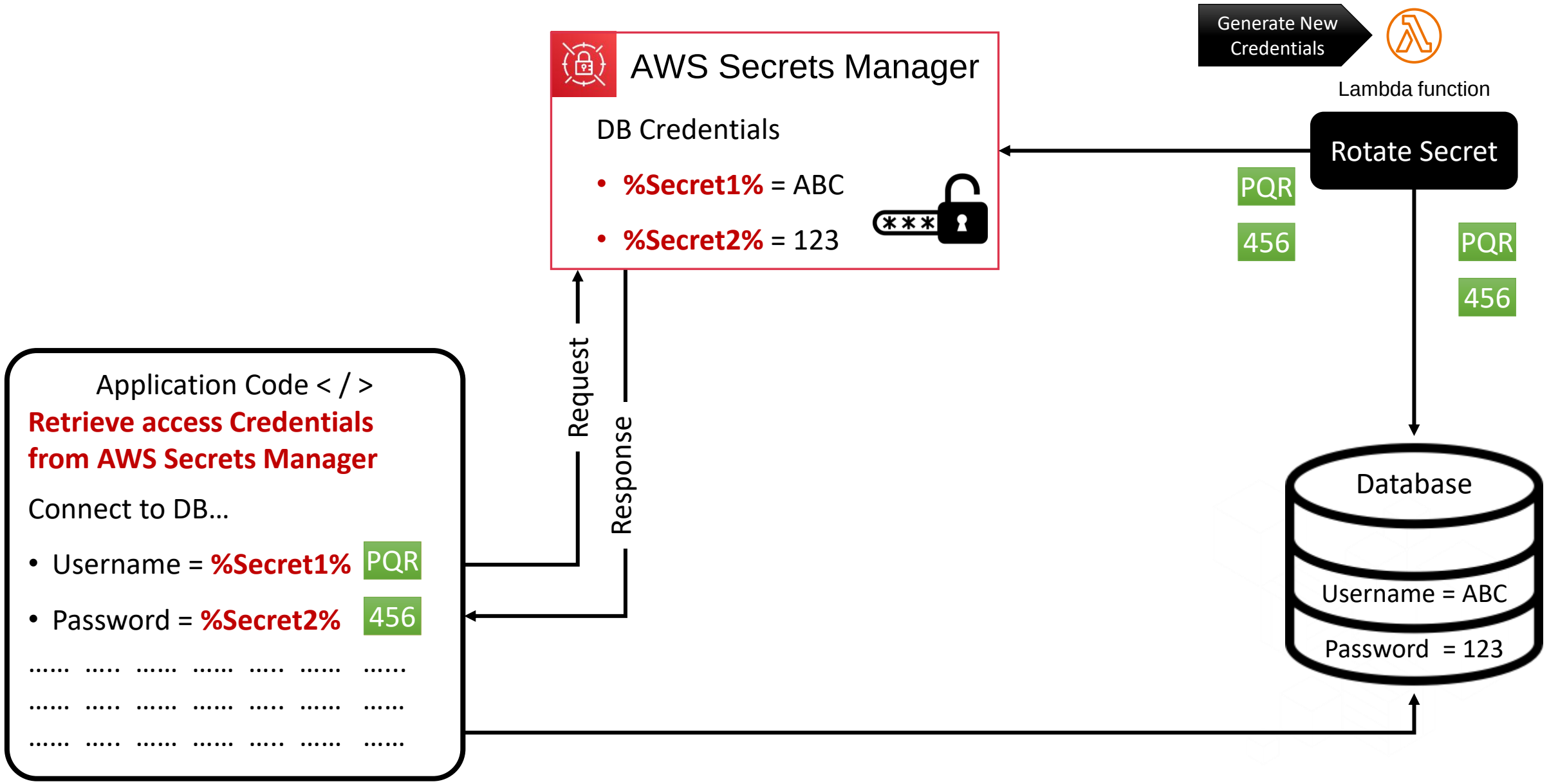
…… ….. …… …… ….. …… ……



With AWS Secrets Manager



With AWS Secrets Manager – Rotate Secrets



AWS Secrets Manager

- AWS Secrets Manager helps you manage, retrieve, and rotate database credentials, application credentials, OAuth tokens, API keys, and other secrets throughout their lifecycles.
- Secrets Manager helps you improve your security posture, because you no longer need hard-coded credentials in application source code.
- You replace hard-coded credentials with a runtime call to the Secrets Manager service to retrieve credentials dynamically when you need them.
- With Secrets Manager, you can configure an automatic rotation schedule for your secrets.

AWS Foundational and Layered Security Services