A unique opportunity for you to be mentored by Amazonians

BeSA

Become a Solutions Architect

Week 7
29-Oct-2022

Agenda

Technical Track (40 Mins)

- AWS KMS
  - › Ashish Prajapati

Serverless Track (30 Mins)

- Observability
  - › James

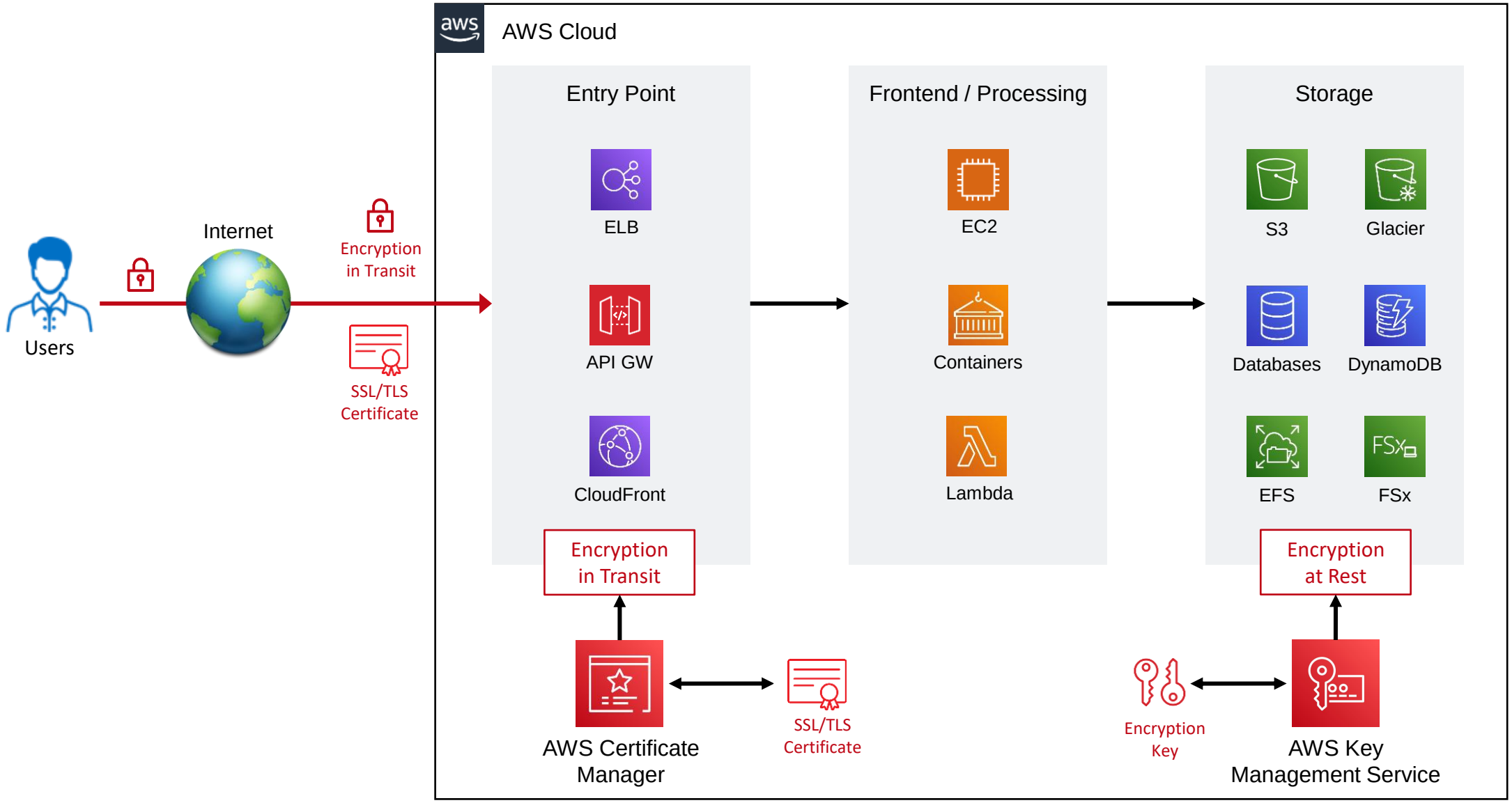
Behavioural Track (15 Mins)

- Guest Speaker
  - › Ashish & James

What is this?

Scytale

Encryption in Transit / Encryption at Rest



AWS Key Management Service (KMS)

Protecting your Pin

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>

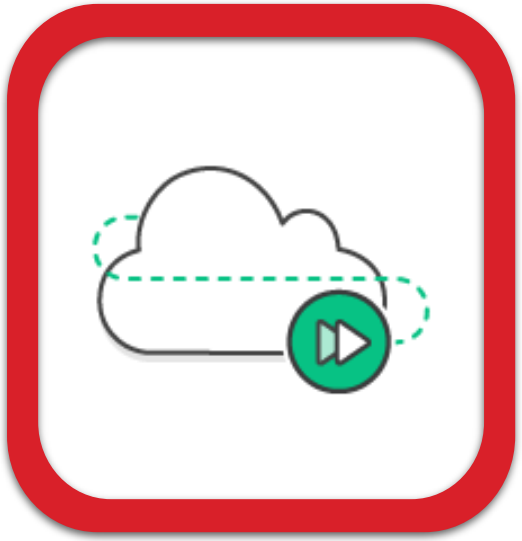
Algorithm

Value = 1

Key Material

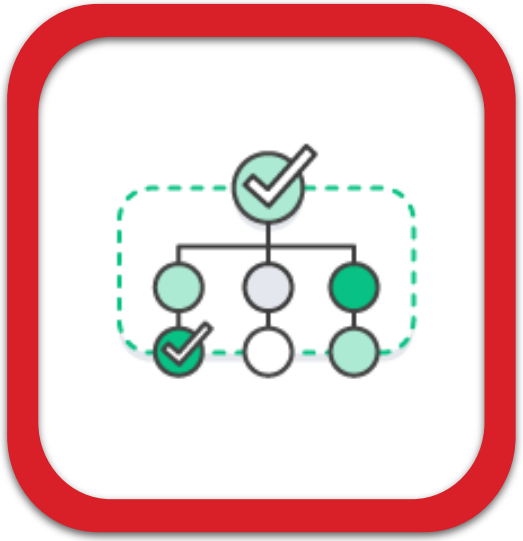
AWS Key Management Service

- 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

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

Role based access control in AWS – KMS

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"

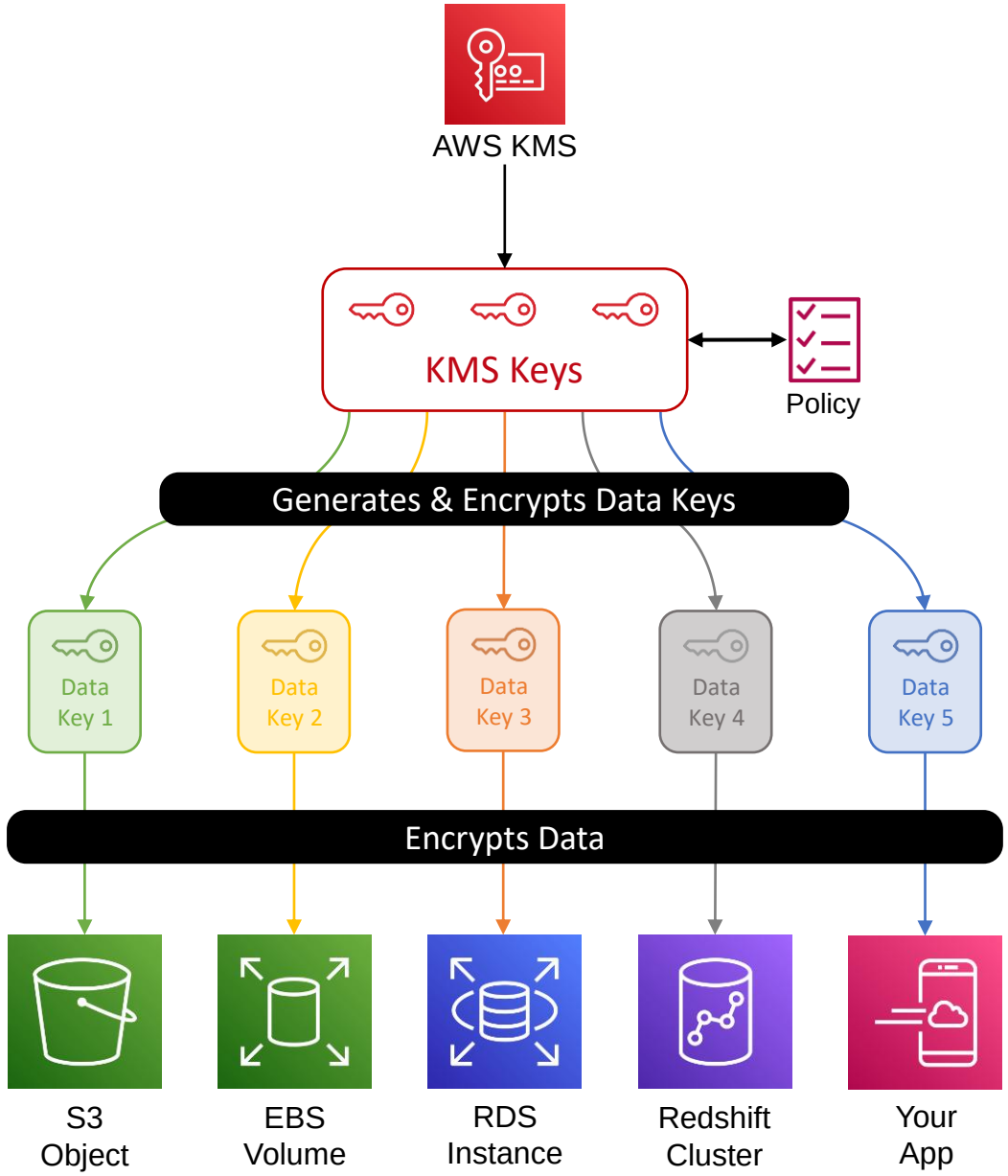
Key User

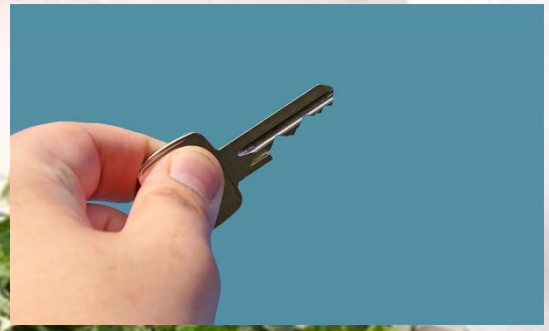
"kms:Encrypt",
"kms:Decrypt",
"kms:ReEncrypt*",
"kms:GenerateDataKey*",
"kms:DescribeKey"

KMS in Action

How AWS Services Integrate with KMS?

- 2-Tiered key hierarch using envelope encryption
- Data keys encrypt customer data
- KMS 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





I HIDE DOOR KEY

Protecting your key

Plain Text Data

A B C D
1 2 3 4

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

Encryption Process

Plain Text Data

A B C D
1 2 3 4

Encryption

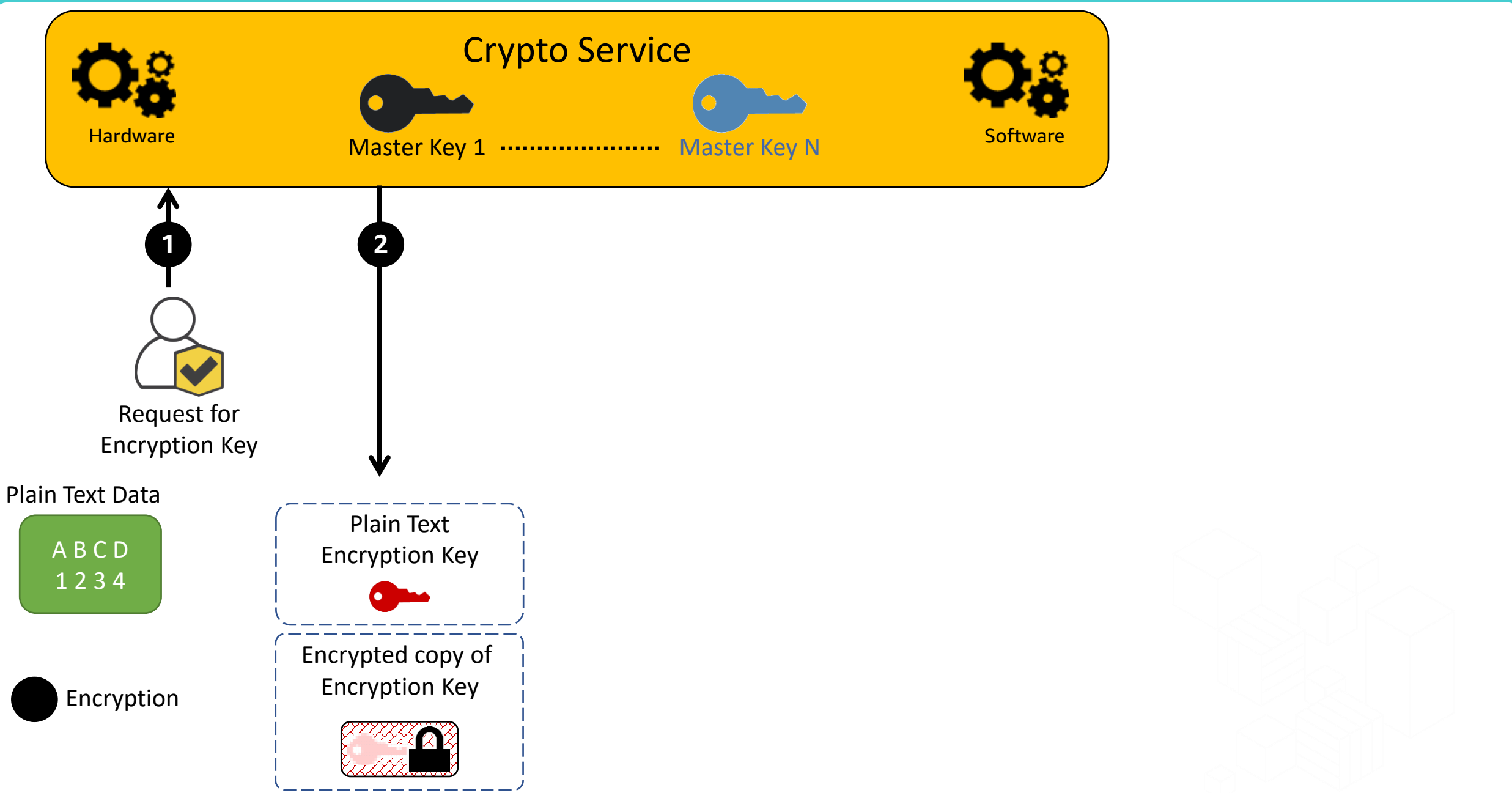
1

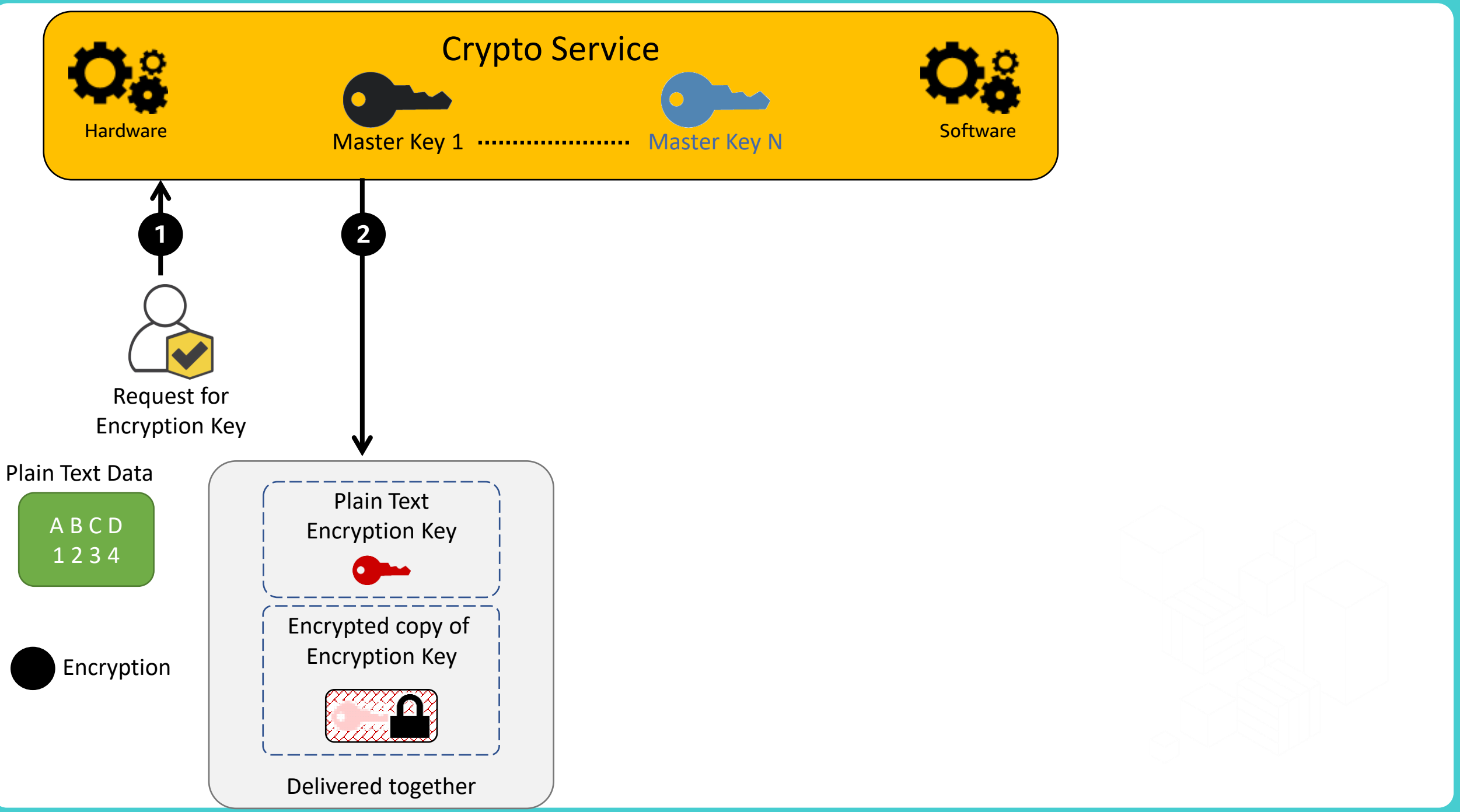
Request for
Encryption Key

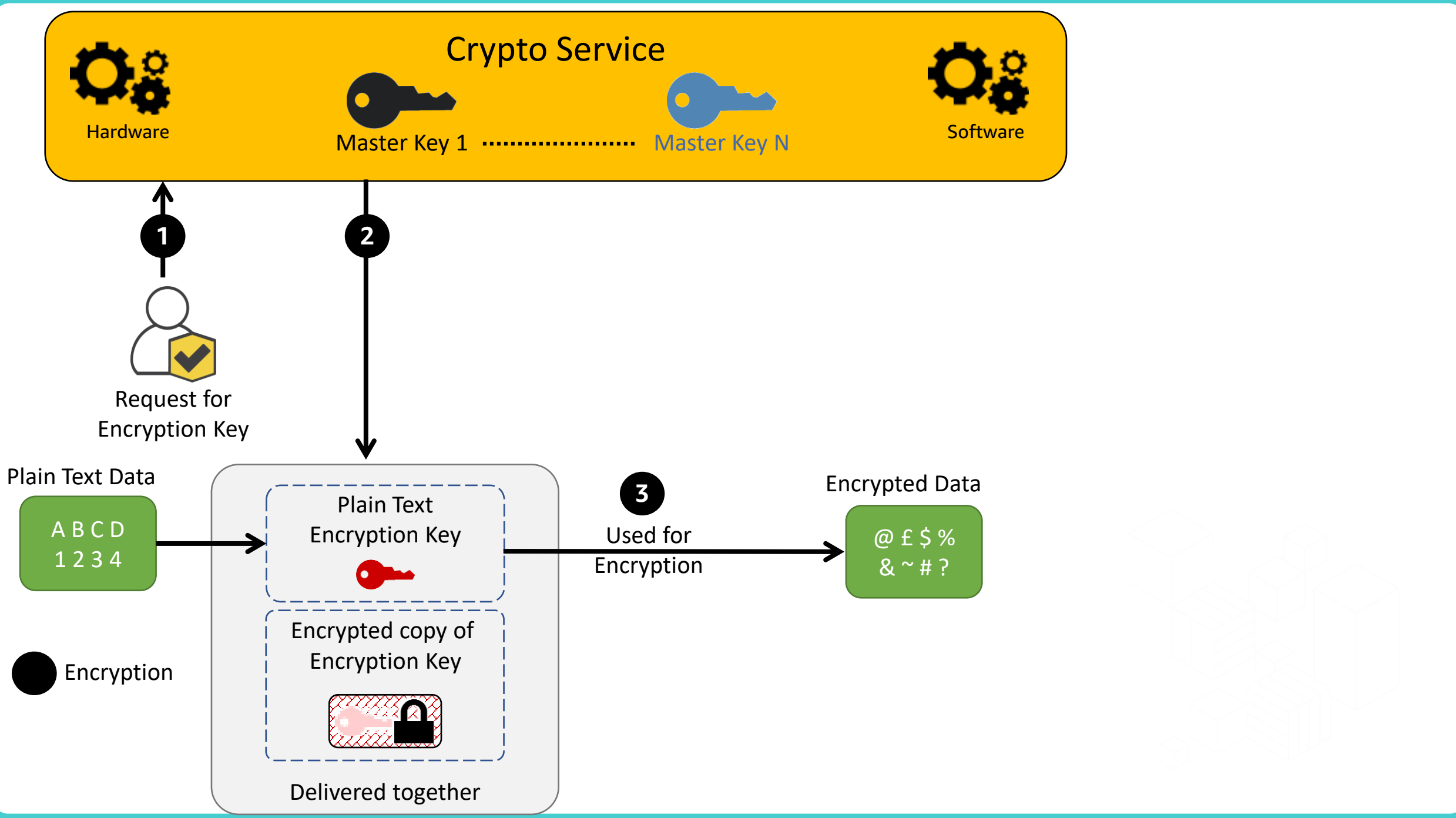
Plain Text Data

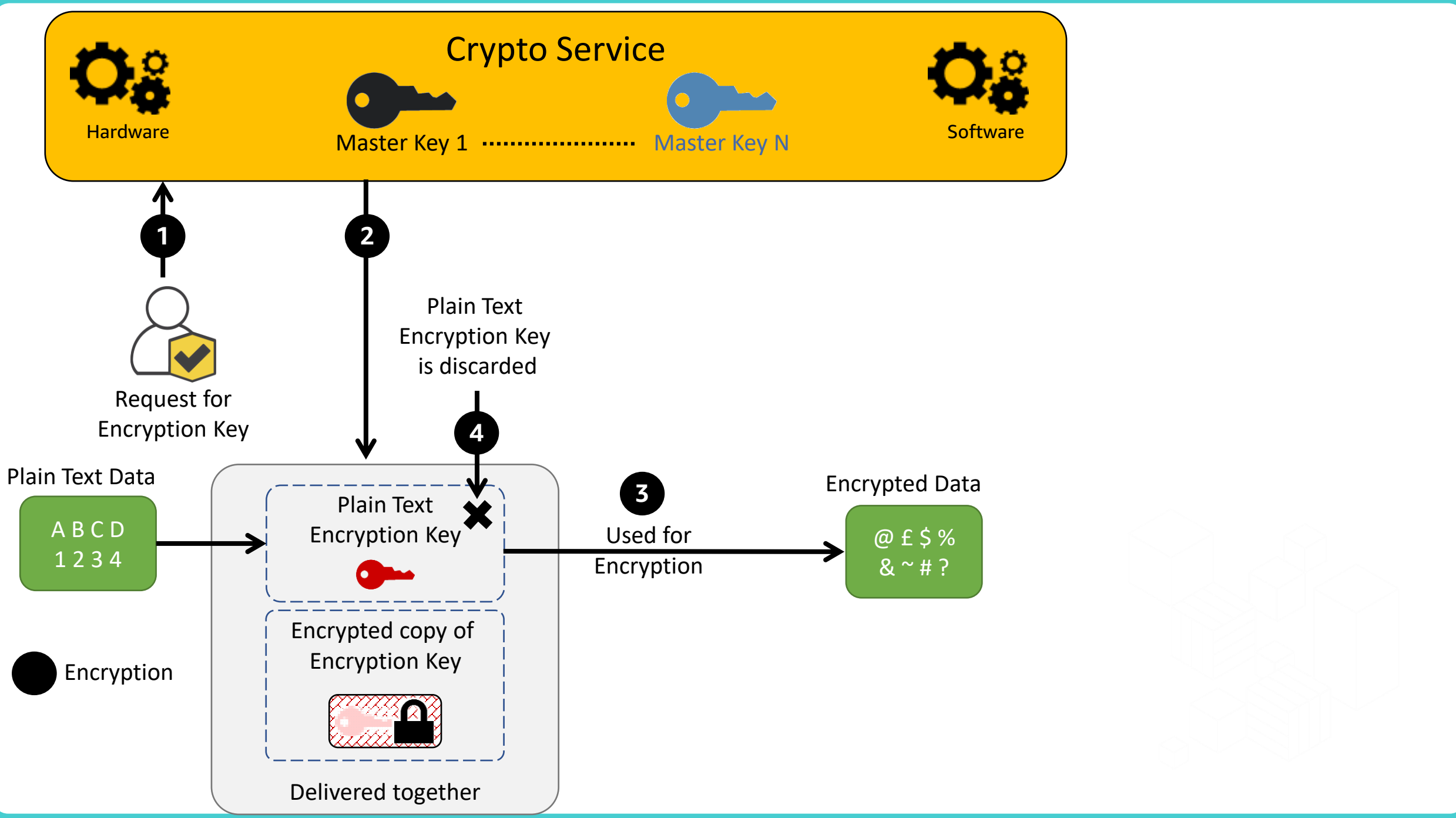
A B C D
1 2 3 4

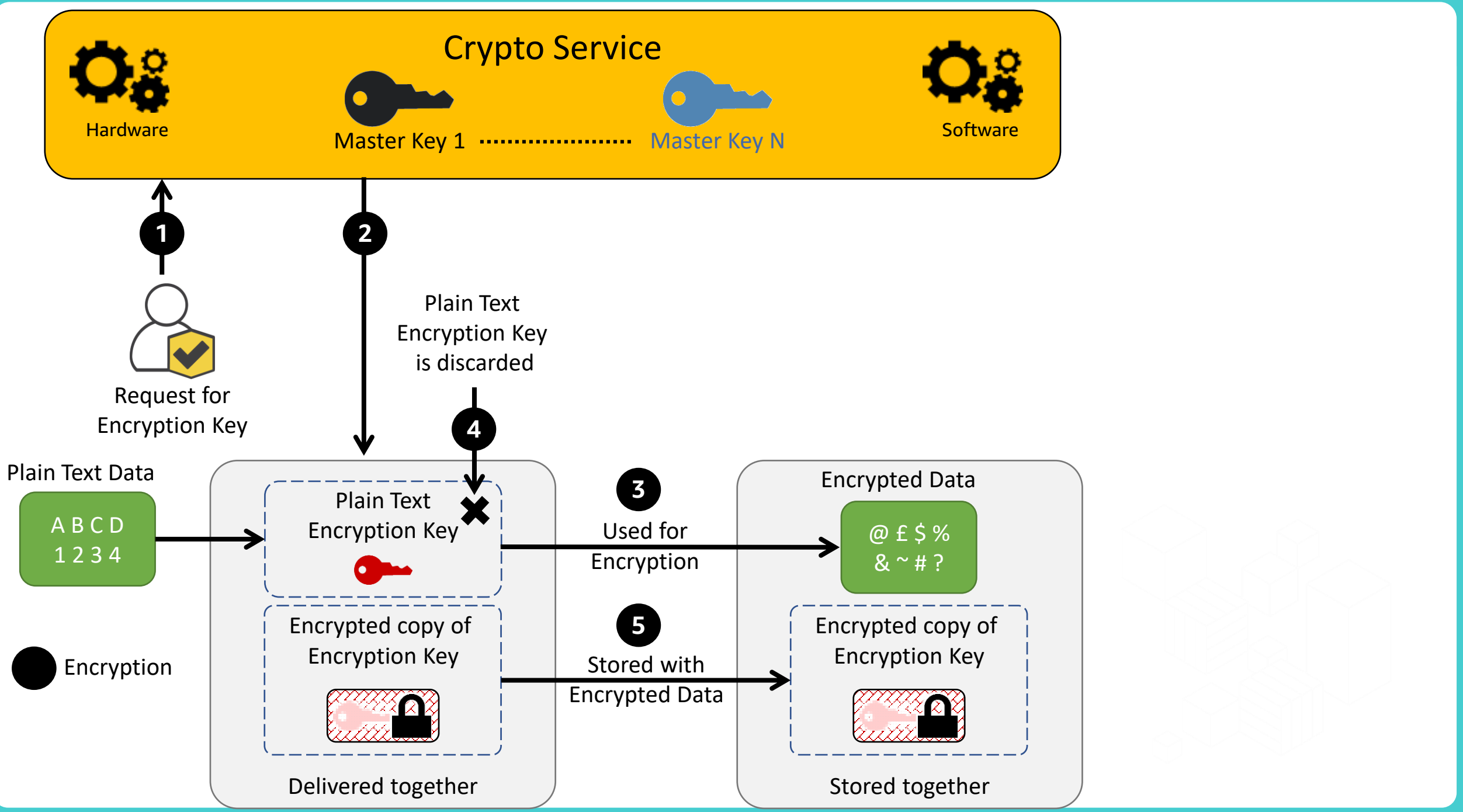
Encryption


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
Plain Text
Encryption Key
Encrypted copy of
Encryption Key
Encryption

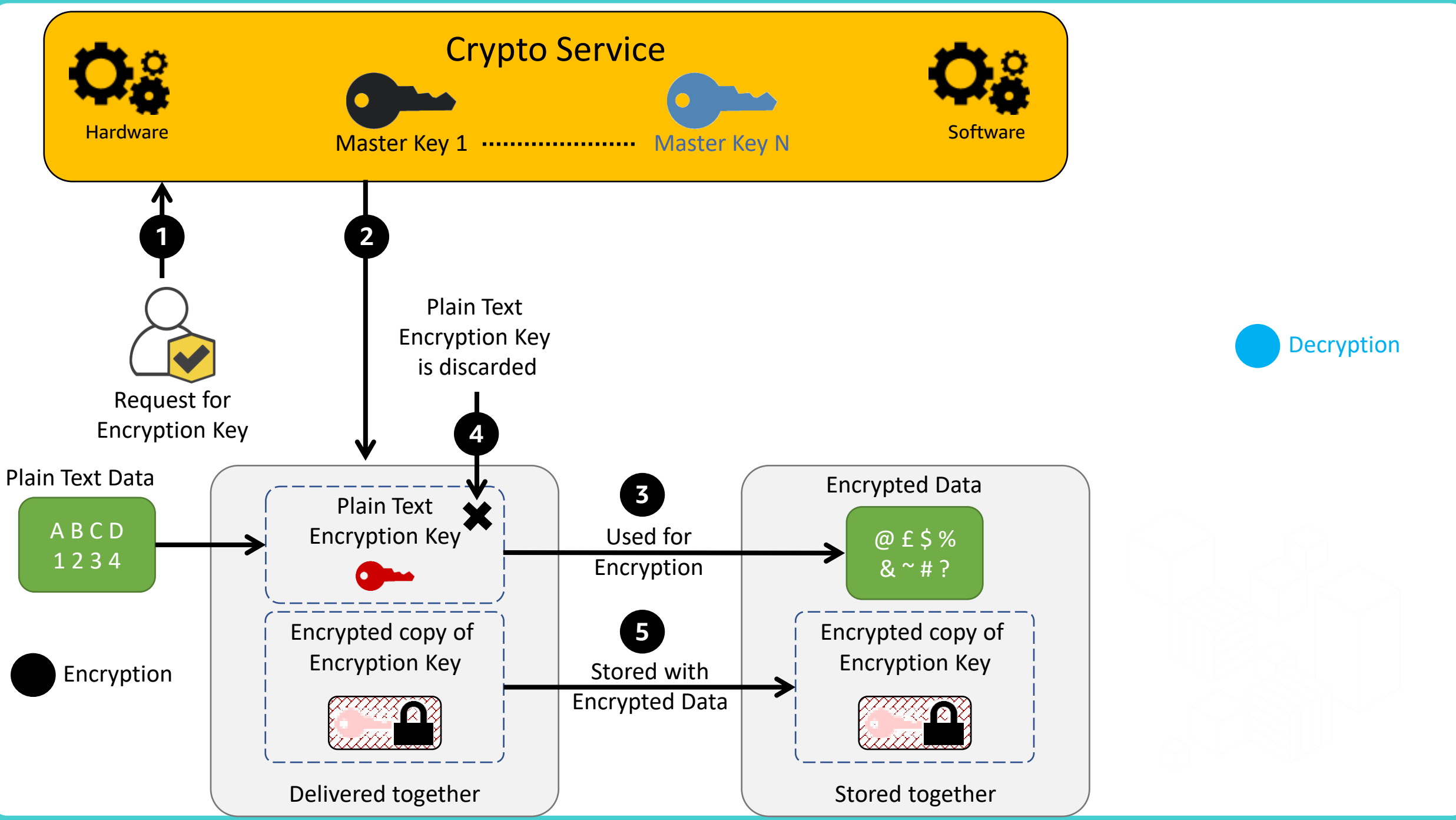

Crypto Service
Hardware
Master Key 1
Master Key N
Software
1
2
Request for
Encryption Key
Plain Text Data
A B C D
1 2 3 4
Encryption
Plain Text
Encryption Key
Encrypted copy of
Encryption Key
Delivered together

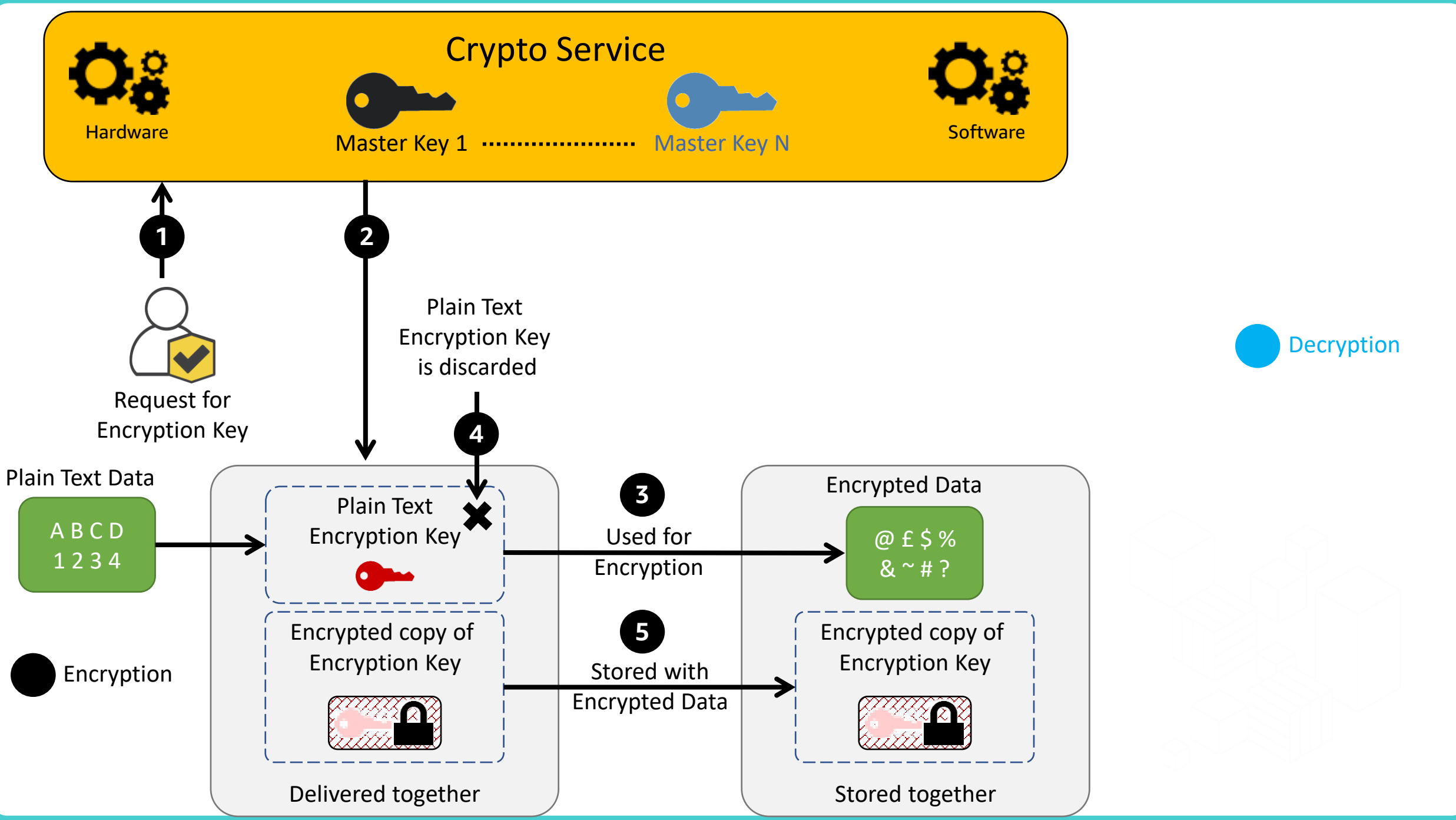

Crypto Service
Hardware
Master Key 1
Master Key N
Software
1
2
Request for
Encryption Key
Plain Text Data
A B C D
1 2 3 4
Plain Text
Encryption Key
Encrypted copy of
Encryption Key
Delivered together
3
Used for
Encryption
Encrypted Data
@ £ $ %
& ~ # ?
Encryption


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

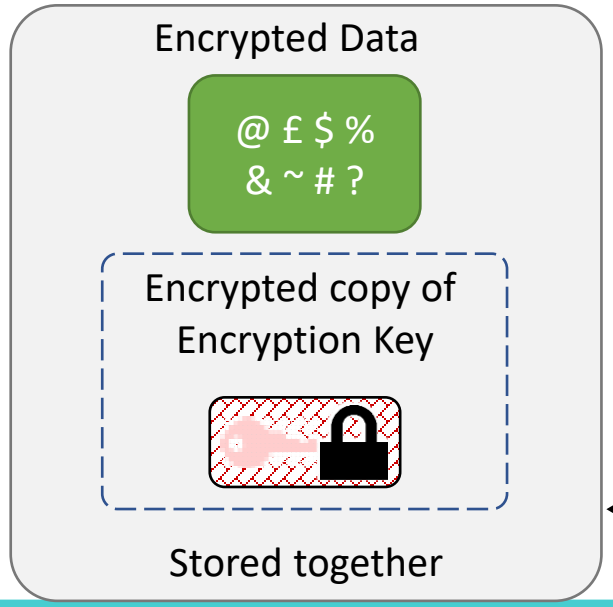
Decryption Process

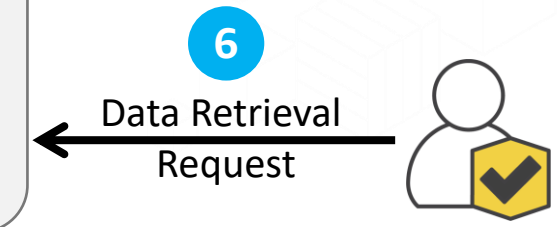

Crypto Service
Hardware
Master Key 1
Master Key N
Software
1
2
Request for
Encryption Key
Plain Text
Encryption Key
is discarded
4
Plain Text Data
A B C D
1 2 3 4
Plain Text
Encryption Key
3
Used for
Encryption
Encrypted Data
@ £ $ %
& ~ # ?
Encrypted copy of
Encryption Key
5
Stored with
Encrypted Data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

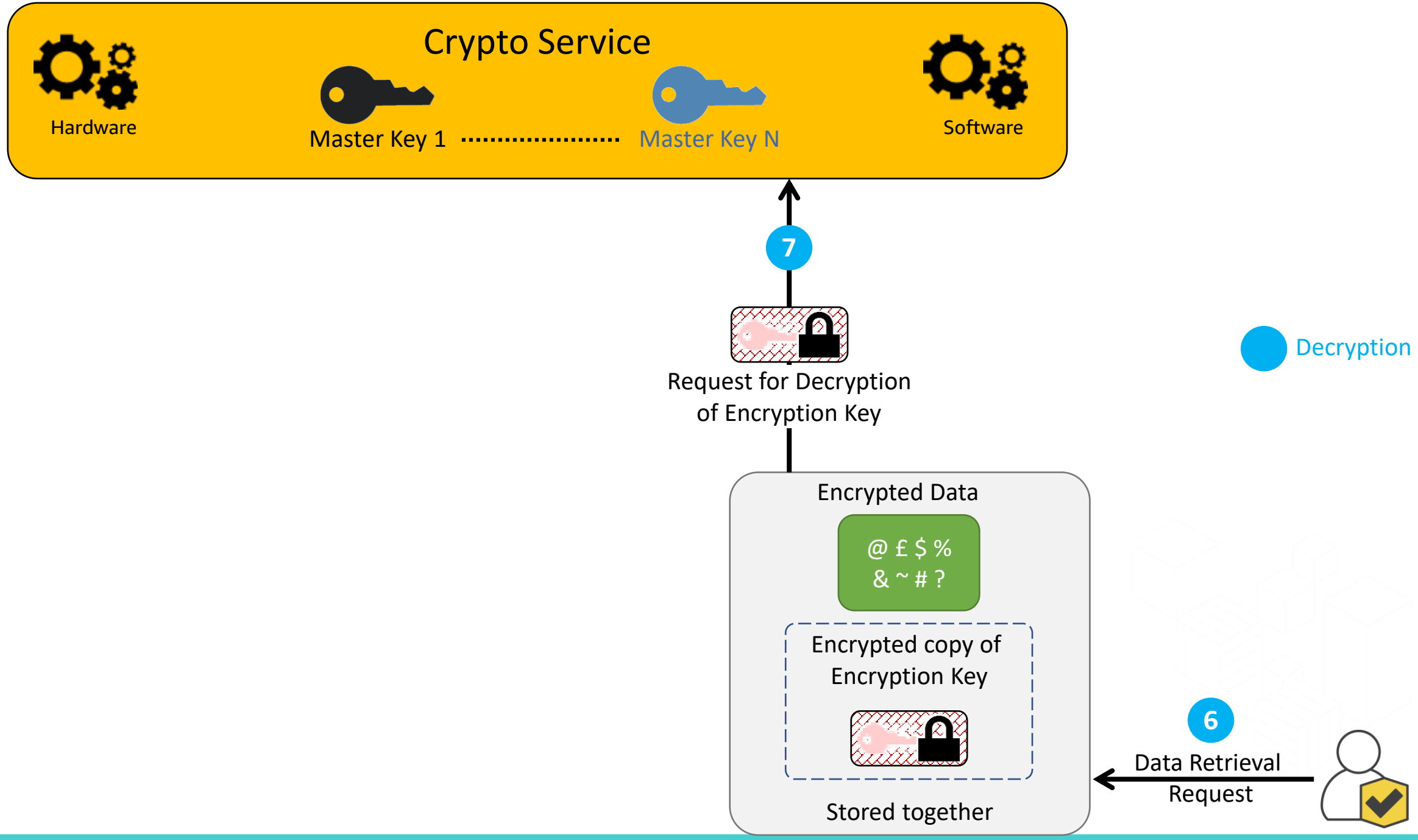

Crypto Service
Hardware
Master Key 1
Master Key N
Software
1
2
Request for
Encryption Key
Plain Text
Encryption Key
is discarded
4
Plain Text Data
A B C D
1 2 3 4
Plain Text
Encryption Key
3
Used for
Encryption
Encrypted Data
@ £ $ %
& ~ # ?
Encrypted copy of
Encryption Key
5
Stored with
Encrypted Data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

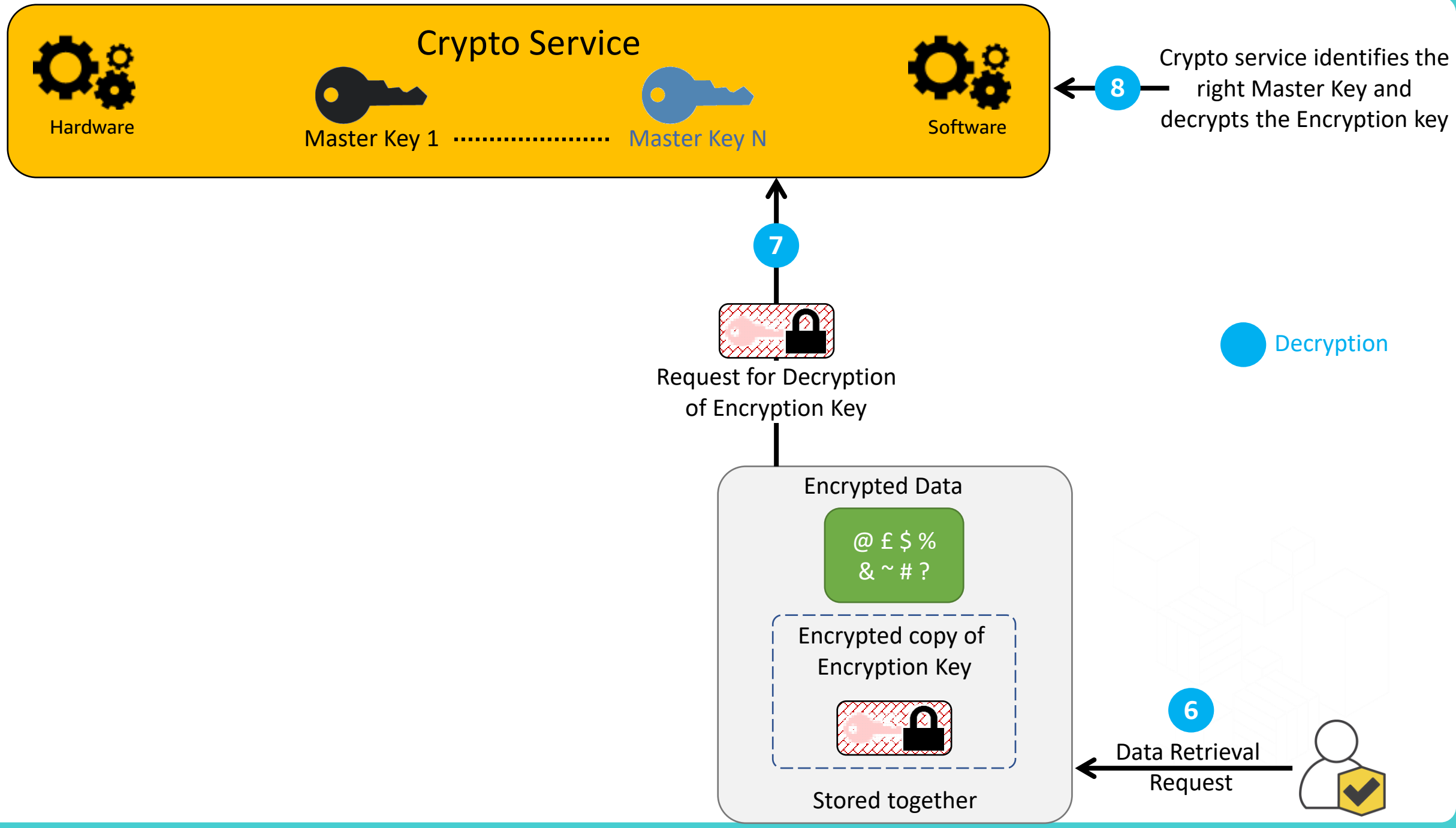

Crypto Service
Hardware
Master Key 1
Master Key N
Software

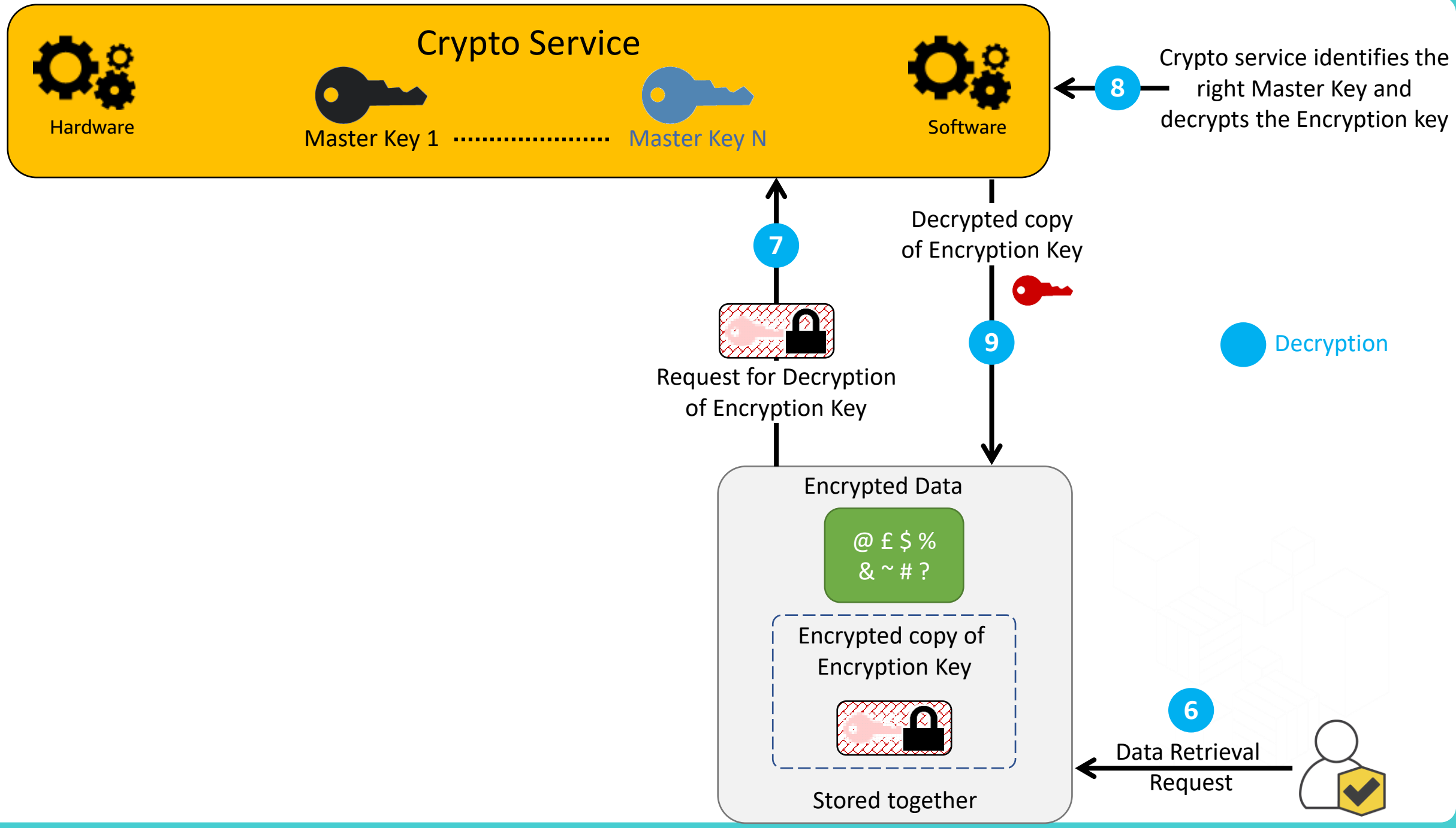
Decryption

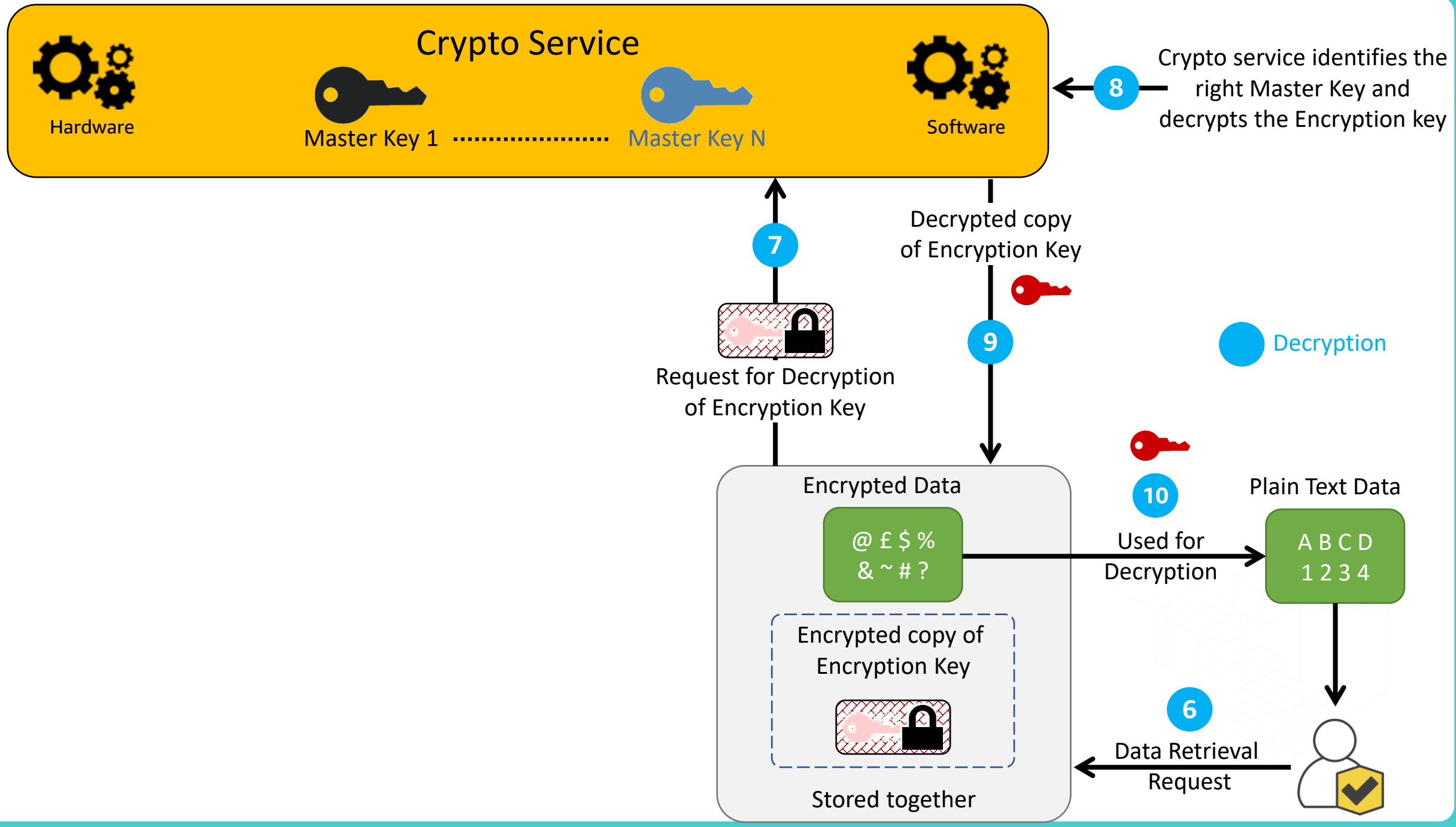

Encrypted Data
@ £ $ %
& ~ # ?
Encrypted copy of
Encryption Key
Stored together


6
Data Retrieval
Request

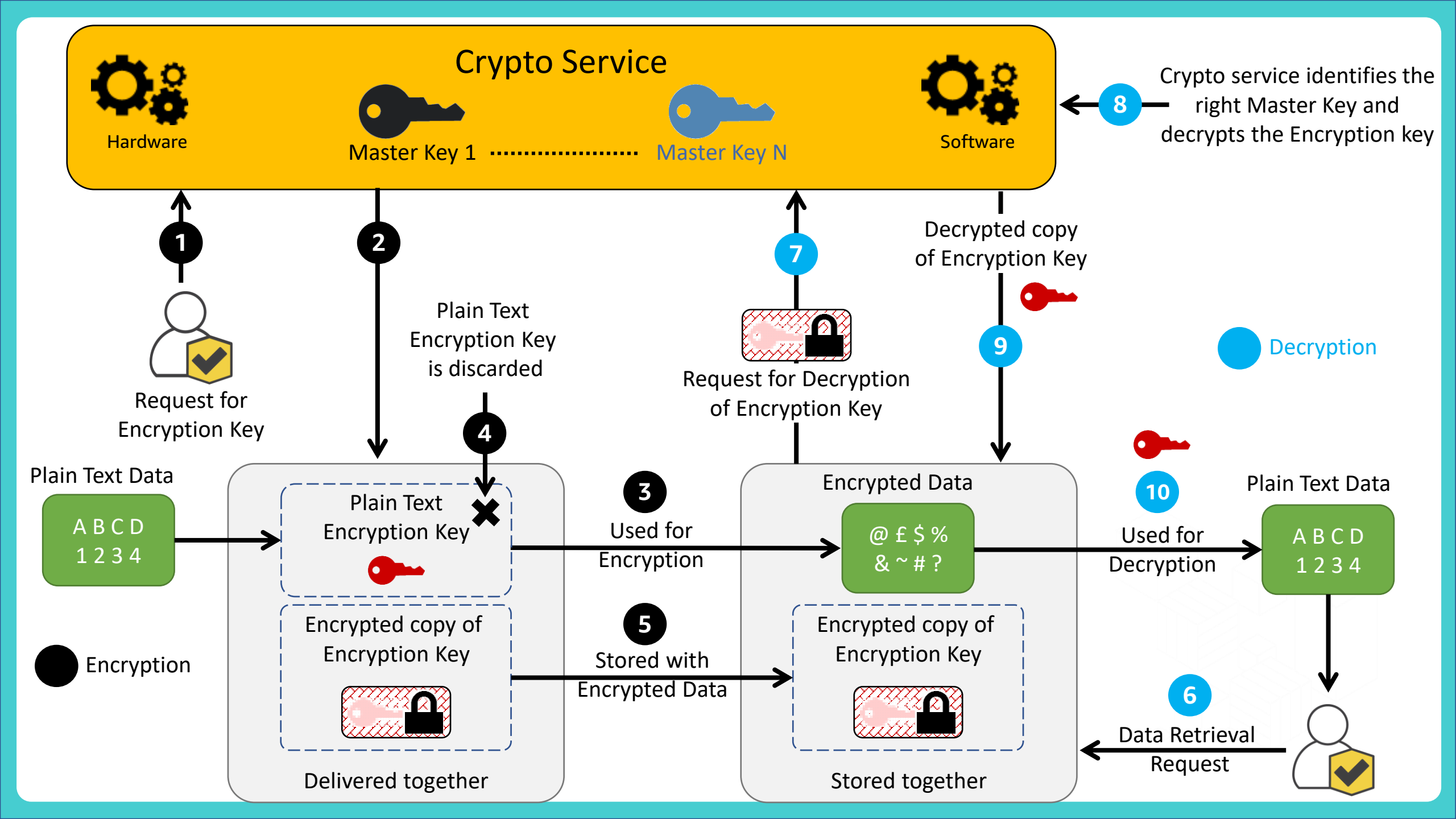

Crypto Service
Hardware
Master Key 1
Master Key N
Software
7
Request for Decryption
of Encryption Key
Decryption
Encrypted Data
@ £ $ %
& ~ # ?
Encrypted copy of
Encryption Key
Stored together
6
Data Retrieval
Request


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

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	✘

Serverless Track

- James Eastham

Guest Speaker

Aisha

- Ashish & James

Thank you.

See you next week.