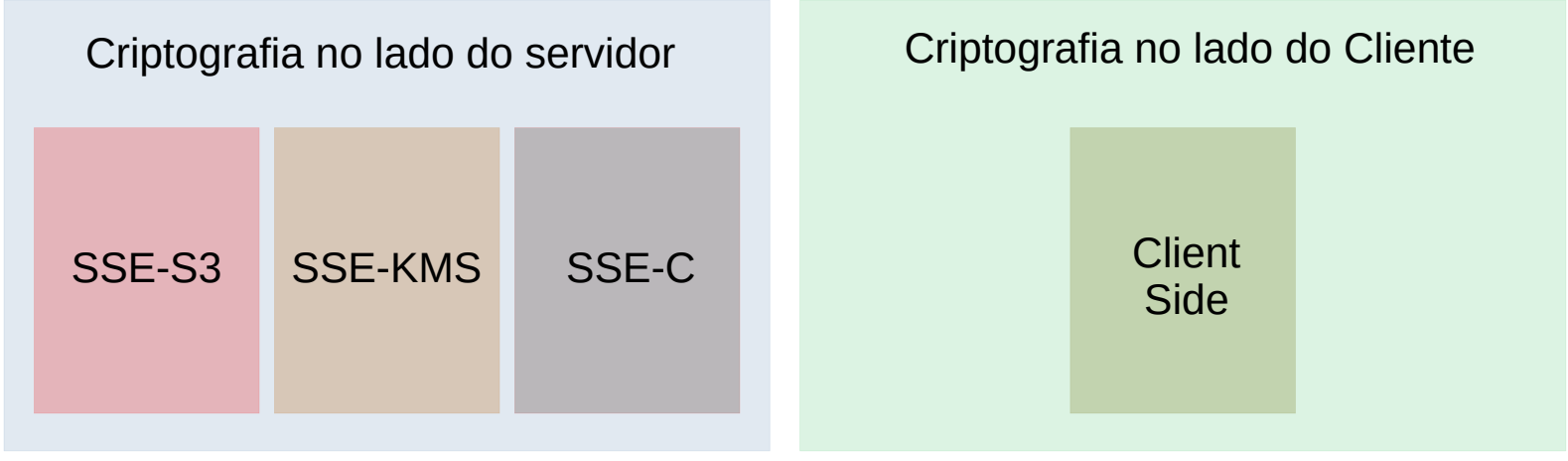

amazon
S3

Criptografia

"... Proteção de dados **protege os dados em trânsito** (à medida que são **transferidos para e do Amazon S3**) **e em repouso** (enquanto estão **armazenados em discos em datacenters do Amazon S3**). Você pode proteger os dados em trânsito usando **Secure Sockets Layer (SSL)** ou **criptografia no lado do cliente**..."

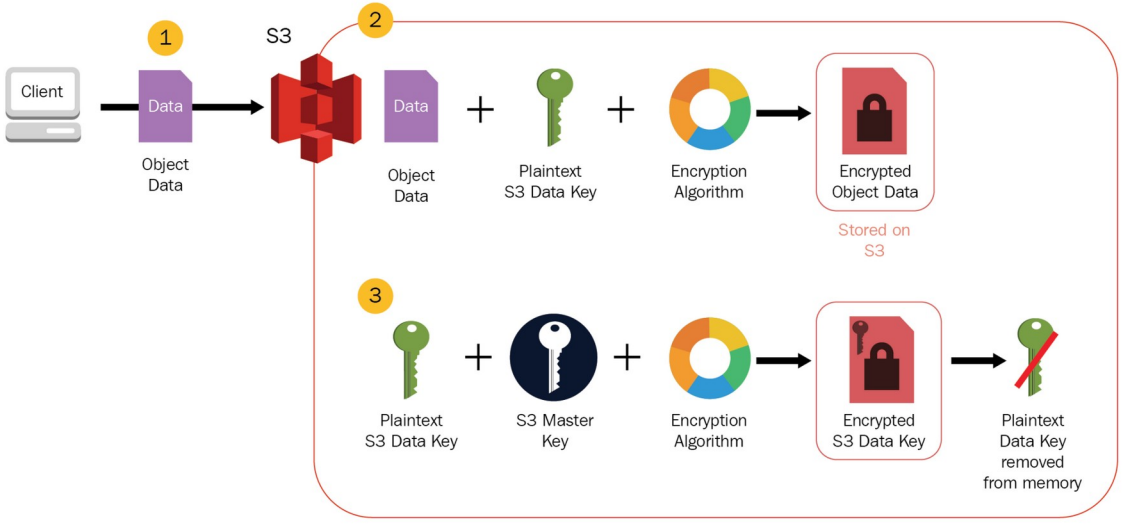
AWS Doc.

Temos duas opções de dados em repouso no Amazon S3:



Criptografia SSE-S3

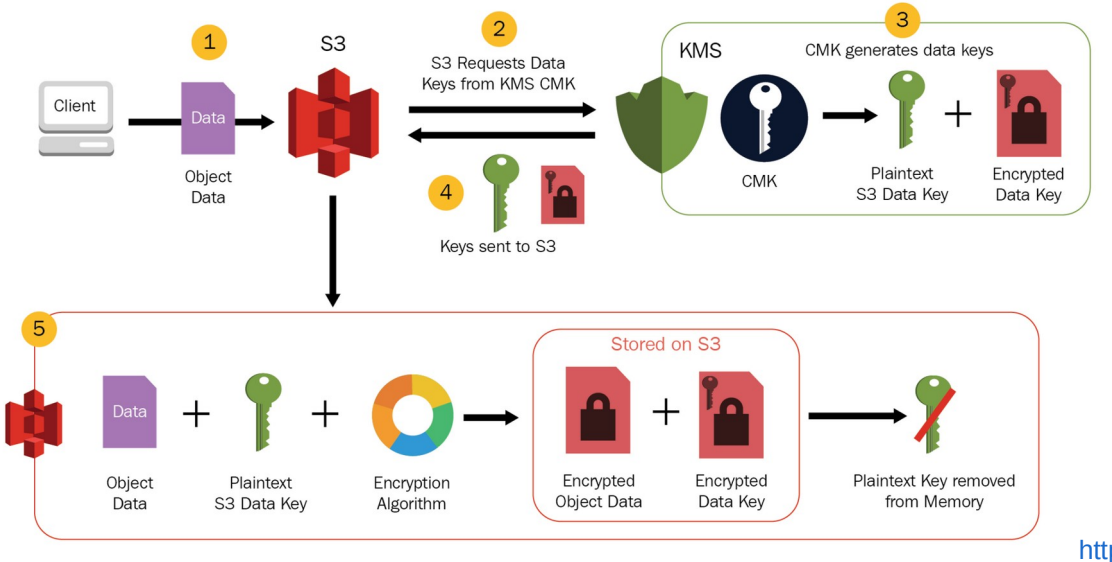
- Criptografia no lado do servidor com **chaves gerenciadas pela AWS**.
- Cada objeto é criptografado com uma chave exclusiva de 256 bits (AES-256).
- Deve configurar no cabeçalho da requisição: **“x-amz-server-side-encryption”:”AES256”**
- Cada chave criada é criptografada por uma **chave mestra**.



https://www.oreilly.com/

Criptografia SSE-KMS

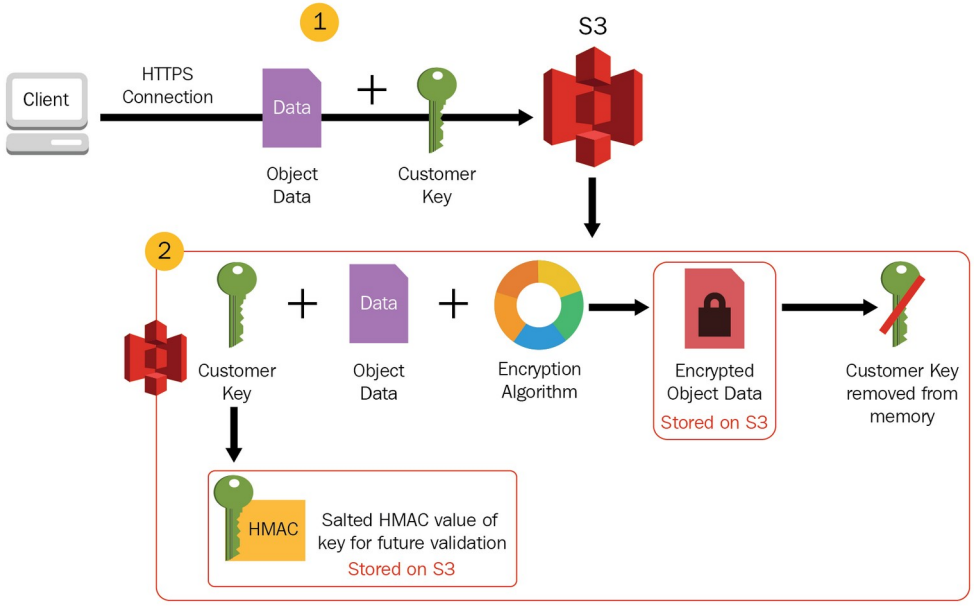
- Criptografia no lado do servidor (semelhando ao SSE-S3) com **chaves gerenciadas pelo KMS**.
- Rastreabilidade e controle com o KMS sobre o CMK (Chave mestra do cliente).
- Deve configurar no cabeçalho da requisição: **“x-amz-server-side-encryption”:”aws:kms”**



https://www.oreilly.com/

Criptografia SSE-C

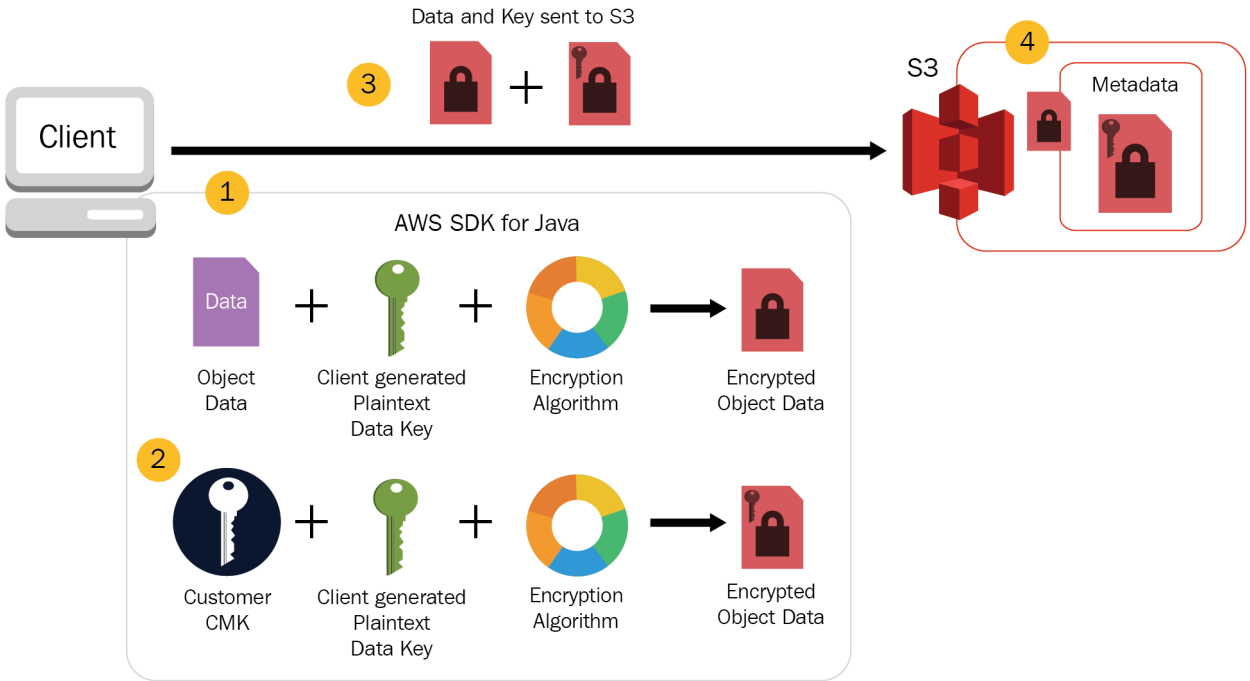
- Criptografia no lado do servidor com **chaves gerenciadas pelo cliente**.
- Amazon S3 não armazenar a chave de criptografia.
- A chave de criptografia é enviada no cabeçalho HTTP em todas requisições (via HTTPS)



https://www.oreilly.com/

Criptografia Client Side

- Criptografia realizada no lado do cliente antes de enviar os dados para o Amazon S3.
- As chaves são gerenciadas pelo próprio cliente.



https://www.oreilly.com/

Links para consulta

https://docs.aws.amazon.com/pt_br/AmazonS3/latest/dev/UsingEncryption.html