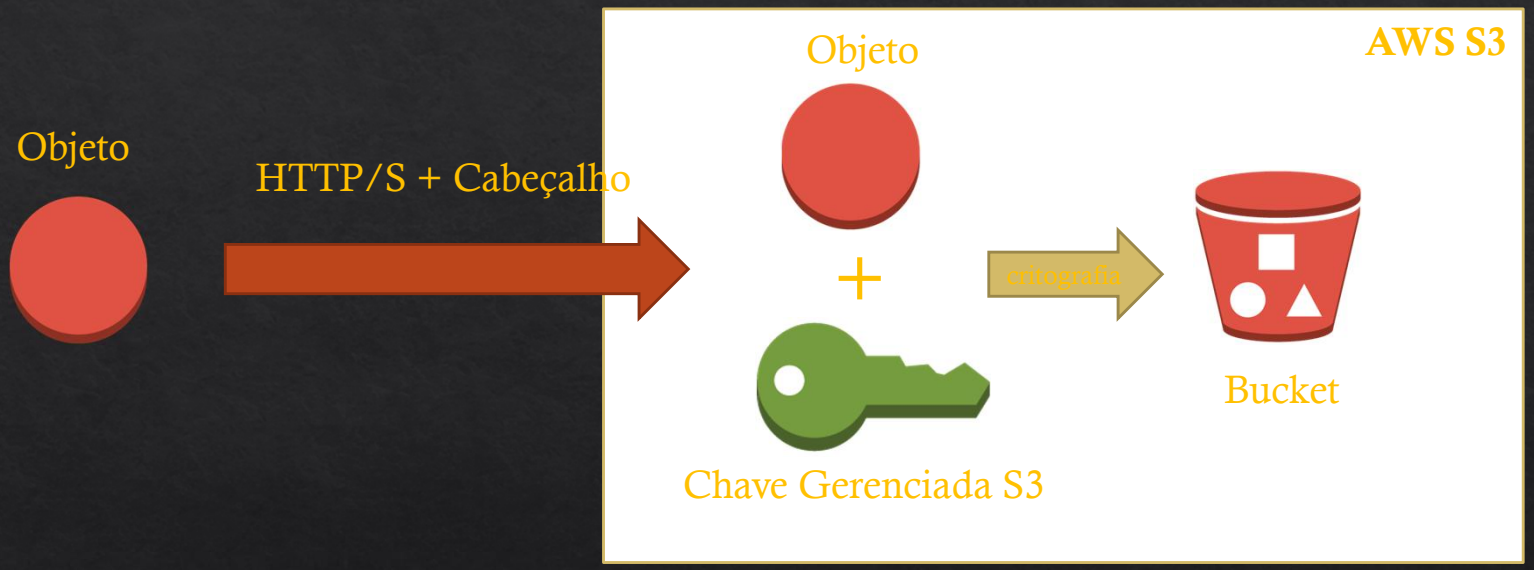
Criptografia S3 para Objetos

- Existem 4 métodos de criptografia para objetos no S3

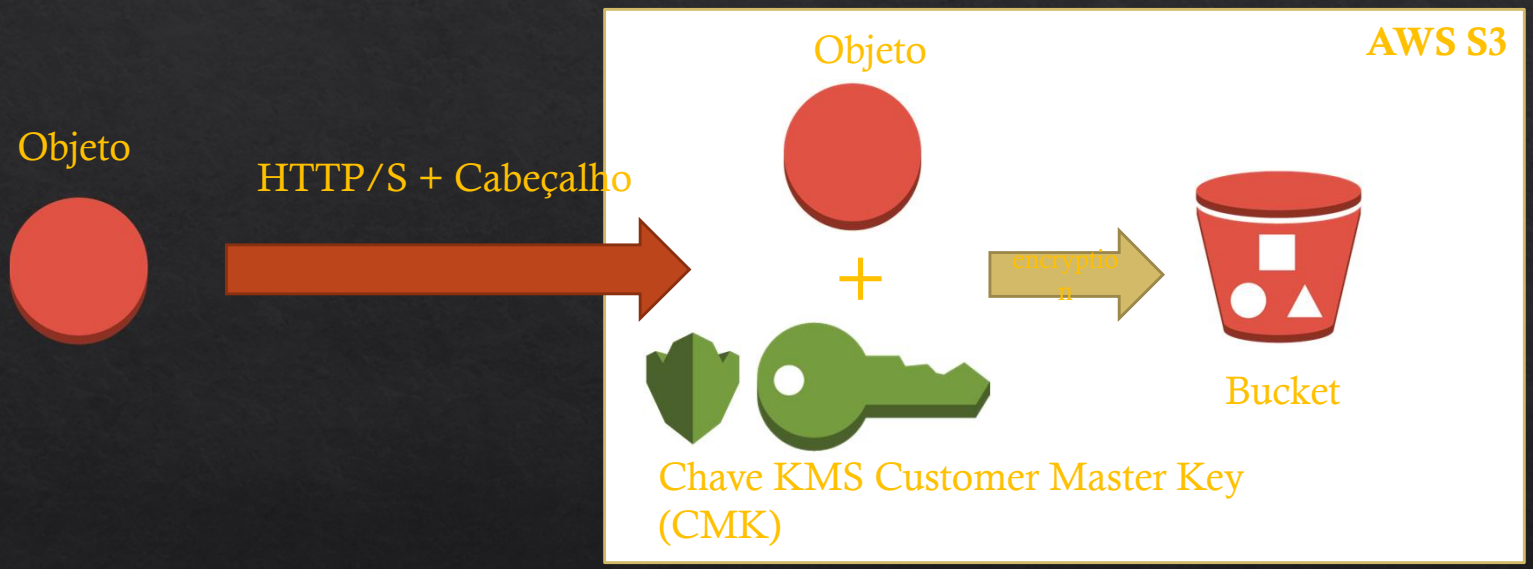
- **SSE-S3:** Criptografa objetos S3 usando chaves criadas e gerenciadas pelo AWS
- **SSE-KMS:** Usa o serviço de Gestão de Chaves do AWS para gerenciar chaves criptográficas
  - Segurança adicional (usuário deve ter acesso a chave KMS)
  - Trilha de auditora para o uso da chave KMS
- **SSE-C:** Quando você quer gerenciar suas próprias chaves
- **Criptografia no cliente**

- **De uma perspectiva de análise de dados, SSE-S3 e SSE-KMS são usadas**

SSE-S3



SSE-KMS



Segurança S3

- Baseada no usuário
  - Políticas IAM - quais chamadas de API devem ser permitidas para usuários específicos

- Baseadas em Recursos
  - **Políticas de Buckets-** regras abrangentes de buckets - permitem contas cruzadas
  - Lista de controle de acesso a objetos (ACL) – controle mais detalhado
  - Lista de controle de acesso ao Bucket (ACL) – menos comum

Políticas de Buckets S3

- Políticas baseada em configuração JSON
  - Recursos: buckets e objetos
  - Ações: definir API para permitir ou negar
  - Efeito: permite / nega
  - Principal: A conta ou usuário que aplica a política

- Use a Política de Bucket S3 para
  - Dar acesso público a um bucket
  - Forçar objetos a serem criptografados no upload
  - Dar acesso a outra conta (conta cruzada)

Segurança S3 - Outros

- Rede **- VPC Endpoint Gateway:**
  - Permite que o tráfico fique dentro de sua VPC (ao invés de ir para a internet pública)
  - Garante que seus serviços privados (AWS SageMaker) possam acessar o S3
- Log e auditoria
  - Logs de acesso do S3 pode ser armazenados em outro bucket S3
  - Chamadas de API podem ser logadas na "AWS CloudTrail"
- Baseados em Tags (combina politicas IAM e politicas do bucket)
  - Exemplo: adicionar a tag Classification=PHI a seus objetos