KMS and Multi-Region Keys

We discussed secrets and AWS Secrets Manager in a previous section, but one of the types of secrets that the mentioned service is not suited for are encryption keys, the cryptographic signatures used to secure stored data.

AWS Key Management Service (KMS) is a vital service for managing cryptographic keys and controlling their use across a wide range of AWS services and applications. In AWS, said keys are usually utilized in order to encrypt/decrypt data either at rest, or during transmission from one service to another. KMS provides us with centralized management of encryption keys, enhancing data security both at rest and in transit. A service that is quite well-integrated into the AWS ecosystem, KMS ensures seamless encryption and decryption across a vast array of AWS services, facilitating strong security measures without adding operational complexity.

KMS supports several types of keys, including:

- **Customer Managed Keys (CMKs)**: Created and managed by the user, offering full control over permissions and lifecycle.
- **AWS Managed Keys**: Automatically created and managed by AWS services such as S3, RDS, and EBS, providing ease of use without manual key management.
- **AWS Owned Keys**: Managed entirely by AWS and used across multiple AWS accounts, offering a simplified, cost-effective solution for less sensitive data.

Also, when utilizing KMS for info stored across AWS regions, we must use the **Multi-Region KMS key**, a variant of the normal KMS key which is designed specifically for dealing with data that spans multiple regions and availability zones.