Certificate Authority (CA)

A **Certificate Authority (CA)** is a trusted entity that issues digital certificates used to verify the identity of individuals, organizations, and servers, either over the internet (i.e., public certificates like SSL/TLS) or within private networks (i.e., private certificates). These certificates are essential for establishing secure communication by encrypting data and confirming the authenticity of the communicating parties. There are two services in AWS primarily used when dealing the type of digital certificates mentioned above, **AWS Private Certificate Authority (AWS Private CA)** and **AWS Certificate Manager (ACM)**. Both services are discussed briefly below:

AWS Private Certificate Authority (AWS Private CA) is a proprietary service offered by AWS that helps manage and issue digital certificates within a private AWS environment. It plays a crucial role in securing communications between AWS resources, ensuring encrypted data transfer, and verifying the identities of the parties involved in internal transactions.

Now, while AWS Private CA primarily focuses on issuing and managing private certificates for AWS resources, they are not the dominant type of digital certificates, and we may face situations where might need to integrate external certificates (e.g., SSL/TLS certificates issued by third-party providers) with our pre-existing AWS resources.

AWS allows us to import these external certificates via **AWS Certificate Manager (ACM)** rather than AWS Private CA. However, these imported certificates have limitations. For example, while AWS-issued certificates can be automatically renewed, external certificates imported into AWS must be manually rotated, and requiring more effort to maintain in general.

There are ways though to make the process of handling external certificates in ACM slightly more convenient, for example AWS Config has a managed rule named `acm-certificate-expiration-check` which can automatically check for expiring certificates, reminding us to rotate the certificate manually whenever the expiration date of the certificate approaches near.