AWS Certificate Manager ACM

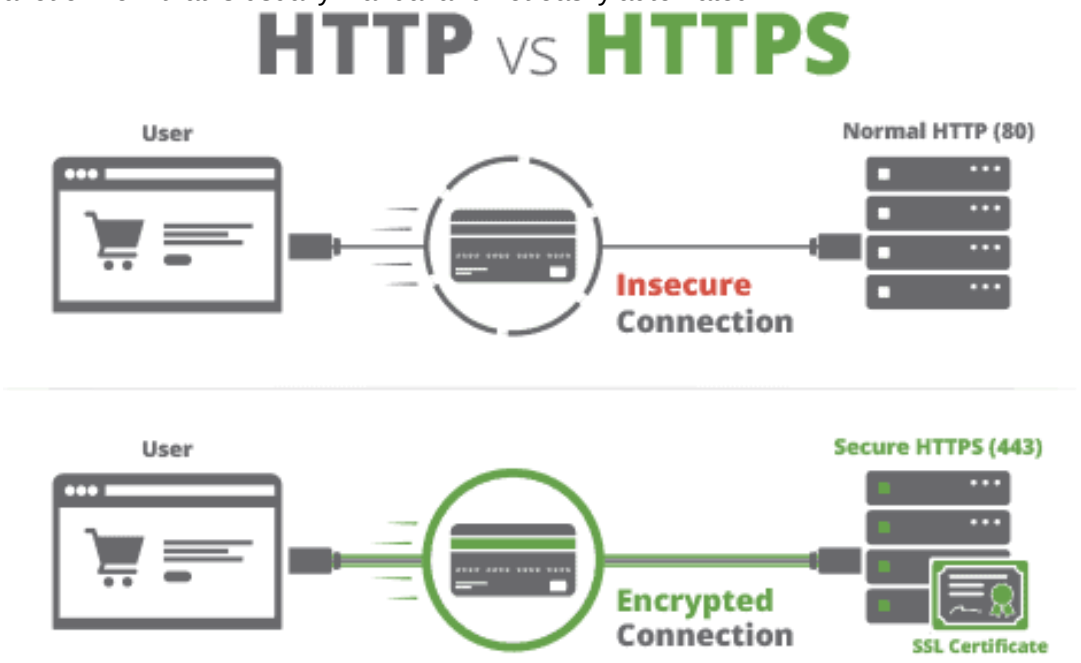
we are going to cover one of the important **AWS security services for data protection .ie. AWS Certificate Manager ACM** which provides free SSL/TLS Certificates.
AWS Certificate Manager (ACM) is designed to simplify and automate many of the tasks traditionally associated with provisioning and managing SSL/TLS certificates. ACM takes care of the complexity surrounding the provisioning, deployment, and renewal of digital certificates for no extra cost!

Before deploying a web application we should understand the basic concept of **Secure Socket Layer (SSL)**, what are they, and how to request them for free using Amazon Certificate Manager.

Overview of SSL/TLS Certificates

An SSL certificate is like an ID card or a badge that proves someone is who they say they are. SSL certificates are stored and displayed on the Web by a website's or application's server.

SSL (Secure Socket Layer) is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral. Secure Sockets Layer/Transport Layer Security (SSL/TLS) is a must-have whenever sensitive data is moved to and from a website. For instance, sites that require to fulfil compliance requirements such as PCI-DSS, FedRAMP, and HIPAA make extensive use of SSL/TLS. Unfortunately, provisioning and managing SSL/TLS certificates can entail a lot of work that is usually manual and not easily automated.

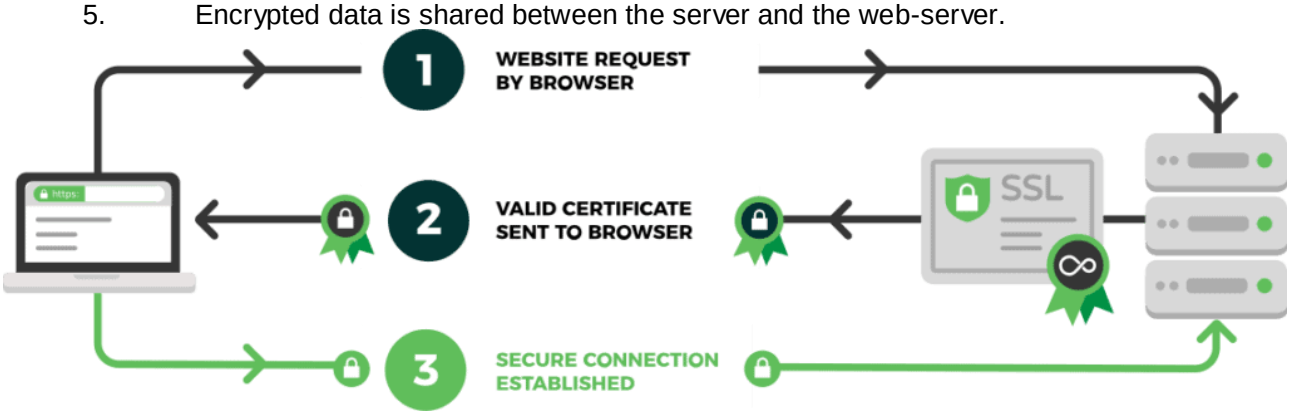


Are SSL and TLS identical?

Transport Layer Security (TLS) is the successor protocol to SSL. TLS is an improved version of SSL. It works in much the same way as the SSL, using encryption to protect the transfer of data and information. The two terms are often used interchangeably in the industry although SSL is still widely used.

How SSL/TLS works

1. A server attempts to connect to a website (i.e. a web-server) secured with SSL. The server requests the web-server to identify itself.
2. The web-server sends the server a copy of its SSL certificate.
3. The server checks to see whether or not it trusts the SSL certificate. If so, it sends a message to the web-server.
4. The web-server sends back a digitally signed acknowledgement to start an SSL encrypted session.
5. Encrypted data is shared between the server and the web-server.



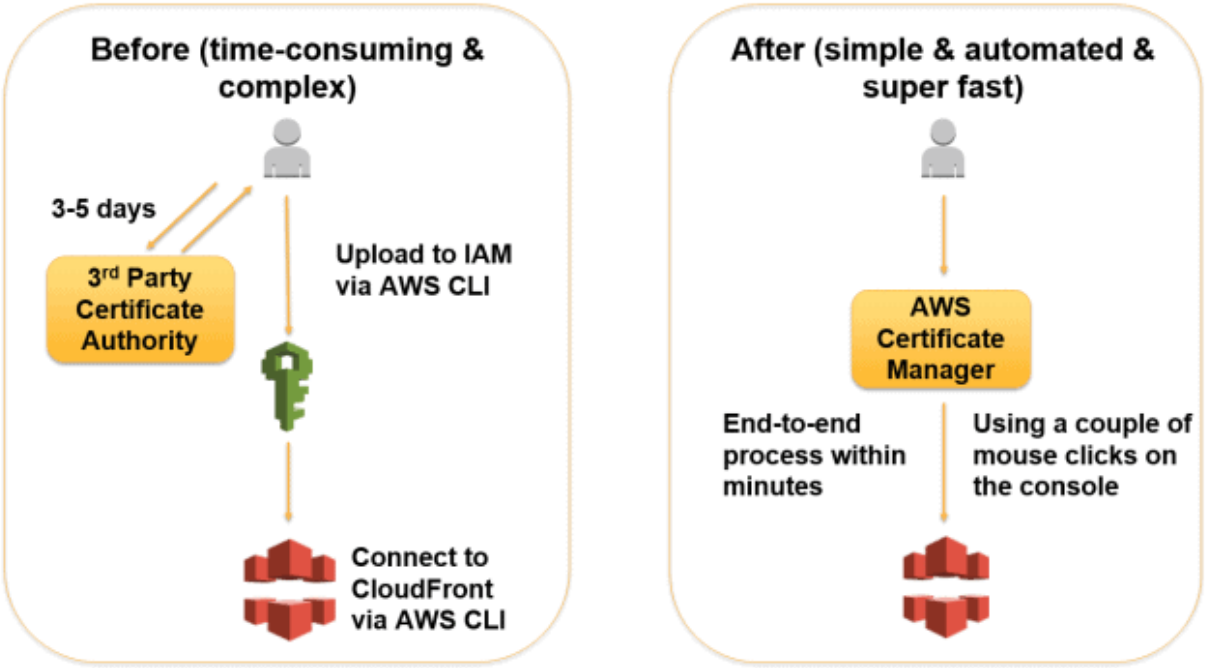
What is AWS Certificate Manager (ACM)?

AWS Certificate Manager is a service that lets you easily provision, manage, and deploy public and private Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates for use with AWS services and your internal connected resources. SSL/TLS certificates are used to secure network communications and establish the identity of websites over the Internet as well as resources on private networks. AWS Certificate Manager removes the time-consuming manual process of purchasing, uploading, and renewing SSL/TLS certificates.

Certificate manager

Why AWS Certificate Manager (ACM)?

ACM makes it easier to enable SSL/TLS for a website or application on the AWS platform. ACM eliminates many of the manual processes previously associated with using and managing SSL/TLS certificates. ACM can also help you avoid downtime due to misconfigured, revoked, or expired certificates by managing renewals. You get SSL/TLS protection and easy AWS certificate management. When you use ACM to manage certificates, certificate private keys are securely protected and stored using strong encryption and key management best practices. ACM lets you use the AWS Management Console, AWS CLI, or AWS Certificate Manager APIs to centrally manage all of the SSL/TLS ACM certificates in an AWS Region.



With AWS Certificate Manager, you will be able to quickly request a certificate, deploy it on ACM-integrated AWS resources, like Elastic Load Balancers, Amazon CloudFront distributions, and APIs on API Gateway, and let AWS Certificate Manager handle certificate renewals.