SSL Certificate

This lesson deals with making the connection between us and our users more secure.

We'll cover the following

A Safer Approach

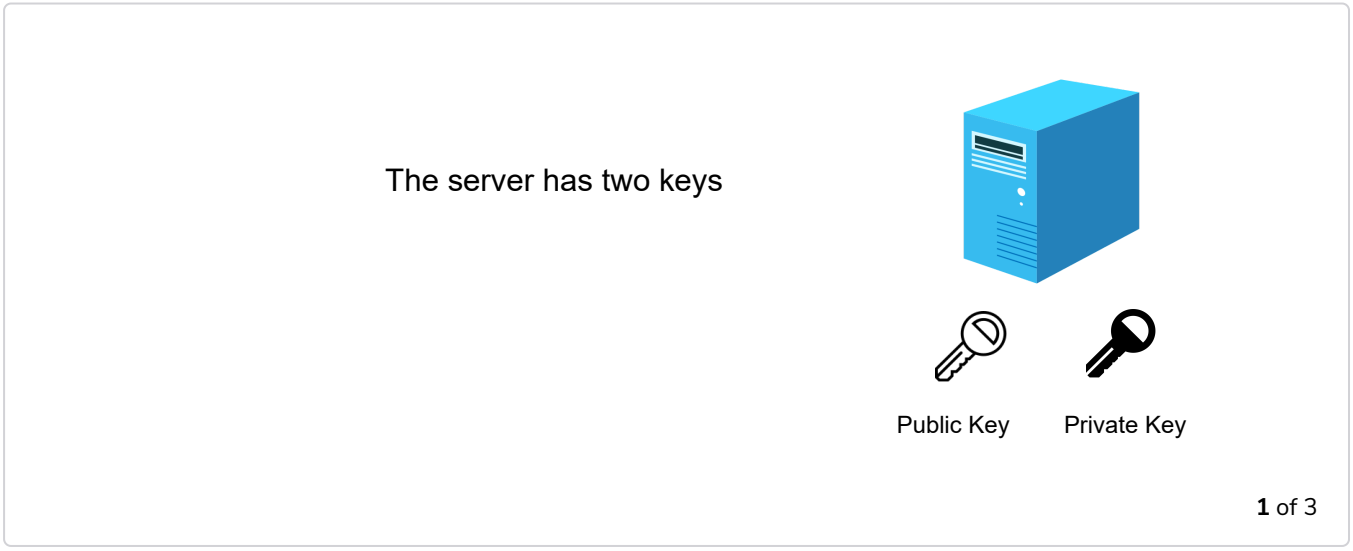
We've finally implemented client-server communication by deploying our website on the web. Till now, our domain name has been preceded by `http://`. However, you might have noticed that many sites follow the `https://` protocol instead. This is because HTTPS, or Hyper Text Transfer Protocol Secure, is the safer form of the HTTP protocol.

How does HTTPS work?

HTTPS uses the private and public keys encryption method to encrypt the communication between the website and the server. As website creators, we acquire two keys, **public** and **private**. These are long strings used to encrypt messages.

Our public key is available to everyone. If a user interacts with our application, his/her data is encrypted by the public key and is transmitted to the server.

The interesting part is that the encrypted data can only be decrypted using the private key, which no one other than us knows. Hence, hackers can get their hands on the encrypted message, but they won't be able to make sense out of it.



Advantages of Using HTTPS

HTTPS ensures that personal information such as passwords and credit card details is transmitted over a secure connection which won't allow anyone else to access it. HTTP was vulnerable to such attacks.

Because of this reason, customers are usually more inclined towards HTTPS websites as they are more secure. This increases traffic as well.

Google, the primary search engine of our generation, ranks a site higher in searches if it follows the HTTPS protocol.

Shifting Over to HTTPS

So how does one shift to HTTPS? This is where the **SSL certificate** comes into play. By acquiring this certificate and installing it on our web server, we can achieve HTTPS status.

achieve HTTPS status.

The certificate is also signed by our public key, which everyone else will use to encrypt communication.

SSL certificates can be purchased (permanently) or acquired for free (usually for a fixed time interval).

We can earn an SSL certificate if we are using a dedicated or cloud host. For VPS and shared servers, we need to ask our server administrator to acquire the certificate.

The process involves submitting a request to a Certified Authority. We must generate a **certificate signing request** (CSR) from our server. This request will contain the information which the Authority will use to grant us an SSL certificate. But before we do that, we need to get familiarized with the different types of SSL certificates.

Types of SSL Certificates

There are three main types of certifications provided by Certified Authors. Let's discuss them one by one.

Domain Validation

This is the simplest and least expensive form of certification. The Certified Author (CA) confirms that we have control over our domain. This can be done by altering our site's domain name in front of the CA, so that it can verify that the domain name is indeed ours. The process isn't ver long and we end up with an HTTPS connection.

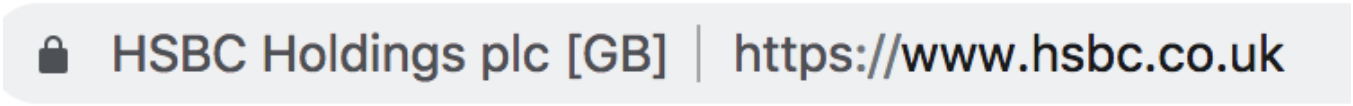
Organization Validation

This is a step higher since the CA validates our basic information as well including the person or company's name and location. These details are displayed on the certificate.

Extended Validation

An extended validation certificate is the highest form of validation our website can receive. Along with all the details verified in the previous methods, the CA will also confirm our legal status. This process can take up to a few weeks. If we opt for this validation, then our website's name will appear

before the URL:



We can opt for any of these forms of validation if we are dealing with a single domain. However, there is another category of SSL certificates we need to understand when working with multiple domains.

Wildcard Certificates

These certificates provide the HTTPS functionality for all subdomains of our domain.

Unified Communications/Subject Alternative Names

These two types of certifications lets us extend the HTTPS tag over multiple domains which we own.

Best Certified Authors

Below, we've listed some of the most popular and reliable CAs.

- GlobalSign
- Cloud Flare (Free)
- Comodo (Paid/Free)
- GeoTrust (Free Trial)
- DigiCert

All of these platforms explain how to install their respective certificates.

Test Your Knowledge!

1 What method does SSL use to ensure data security?

A) The user encrypts data using a private key and the server decrypts it using a public key.

B) The user encrypts data using a public key and the server decrypts it using a private key.

C) There is a single key for encryption/decryption known only to the user and the server.

COMPLETED 0%

1 of 2

Next, we'll compare some of the most popular cloud services.