
SSL

What is SSL?

SSL, or Secure Sockets Layer, is a protocol used for secure and encrypted communication between computers. It's indicated by the little green padlock in the address bar of your browser.

Before we talk about SSL, however, we need to cover asymmetric (or public-key) encryption. At its most basic form, key-based encryption requires each party (or person) to generate a public and a private key pair. Think of this like a lock on a door. Locks on doors are rather public. Anyone can walk up to them, inspect them, even try to open them with their keys, but only the right keys will open the lock. In this analogy, the door locks are public keys, because they're visible and public. Private keys are, well, keys, and are used to unlock the public keys. If you know a person's public key, you can encrypt a message using their public key that only they will be able to decrypt and read.

Think about it this way. You have a secret code (a key) that you don't tell anyone. You also have a public code (a lock) that you tell everyone about. The two are linked together and the secret code acts as a key for the public code/lock. Anyone can see your public code and can encrypt messages using it. Once a message is encrypted (locked) with a public code, only the private code can decrypt (unlock) it. For example, if I wanted to send an encrypted photo of a cat to my friend Laura, I'd ask her for her public key. I'd use it to encrypt the cat photo and then send it to her. She would then use her

private key to unlock the cat photo and have a good laugh. Then, she'd take a photo of her cat, encrypt it using my public key, and send it to me. I'd decrypt it with my private key and laugh at how silly her cat is.

Asymmetric encryption is the heart of SSL but with one extra player: a certificate authority, or CA. CAs, such as RapidSSL or InstantSSL, not only issue SSL certificates but also verify their authenticity. You'll need to get a certificate from a certificate authority in order to utilize SSL.

Certificate authorities have what is known as a "root certificate", or what is effectively the "master certificate," under which all issued certificates are signed. If you buy a certificate from RapidSSL, browsers will use RapidSSL's root certificate to check whether or not your certificate is legit when they connect to your server.

An SSL connection works just like a public key exchange but with the addition of the CA to make sure the server you're trying to get data from is legit. Here's what happens during an SSL connection:

1. You (the user) navigate to a secured web page, and your computer reaches out to that server.

2. The server responds with their public certificate (same as a public key).

3. Your computer checks the certificate to make sure it is valid and was issued by a trusted CA.

4. Assuming the certificate is valid and trusted, your computer uses the server's public certificate to generate a random key and encrypts your request (all of the data you want from the website), then sends the request and the randomly generated key to the server.

5. The server decrypts the data and responds in kind by encrypting its message with your randomly generated key.

6. This process repeats until your session is done.

When should I use SSL?

SSL is applicable for many different kinds of websites. Websites that absolutely should implement SSL are any that handle sensitive or private data of any kind. Names, addresses, passwords, and especially financial or credit card information are all examples of sensitive data. If you're working with any kind of website that processes financial transaction, SSL is an absolute must. For more information about payment information and SSL, refer to the PCI compliance guide for your type of website.

How do I implement SSL?

Implementing SSL will depend on your web host, so check with them to determine their implementation practices. At Flywheel, for example, we support SSL certificates but do not issue them ourselves. In order to use SSL with our service, you'll need a certificate issued from a CA which you can use with our services.

Made with love by Flywheel

getflywheel.com