Data Security with OpenSSL



Afzaal Ahmad Zeeshan

Developer Advocate

@afzaalvirgoboy | www.afzaalahmadzeeshan.com



Creator: Eric A. Young and Tim J. Hudson

A project forked from the original SSLeay library to provide an encryption and cryptography toolkit as an open-source library. OpenSSL is a battle-test cryptographic library that works with Transport Layer Security (TLS) protocol, previously known as Secure Socket Layer (SSL).

OpenSSL

Cryptography toolkit

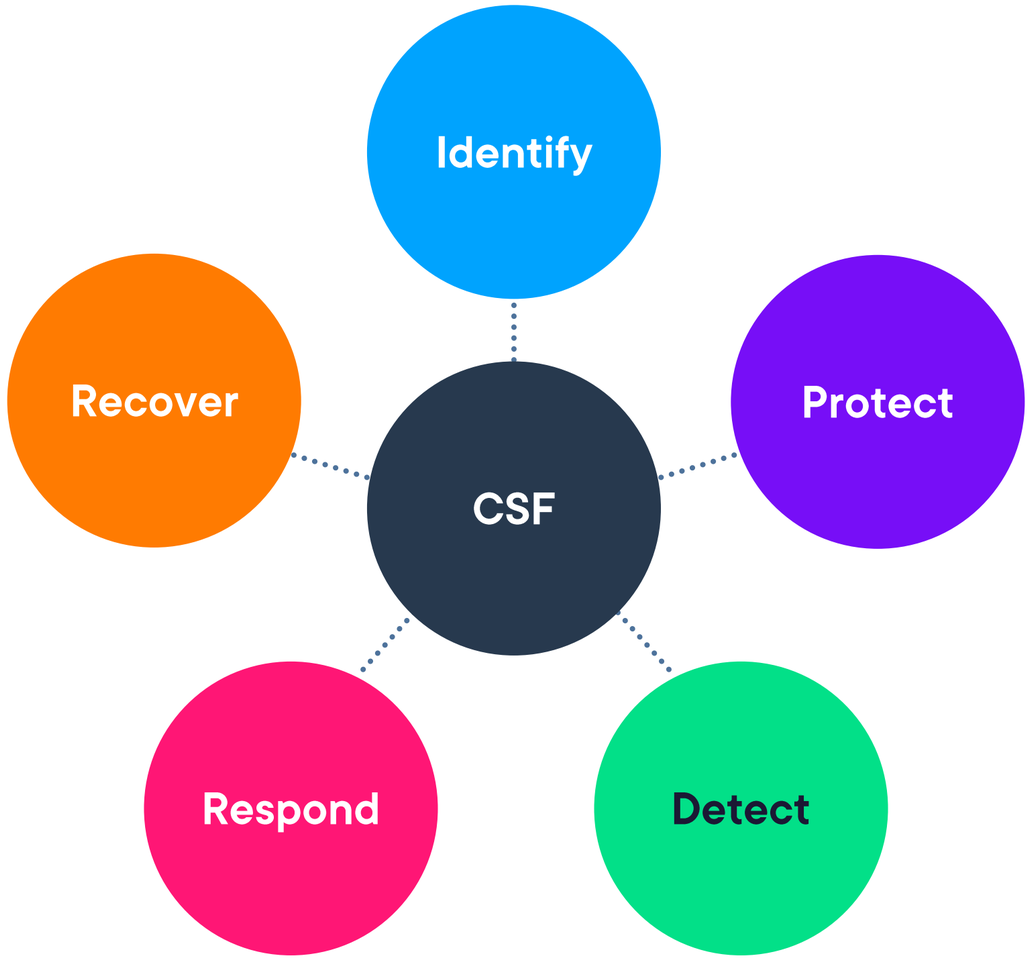
Open source, available from GitHub

Feature-complete and battle-tested

Widely used for SSL/TLS

- Most practically used for HTTPS

NIST Cybersecurity Framework



NIST Cybersecurity Framework



Transport Layer Security



Builds on top of the Secure Socket Layer protocol



Uses certificates from trusted and third-party certificate authorities



Globally used by websites and Internet-connected devices



TLS 1.3 is the latest version being used on the Internet

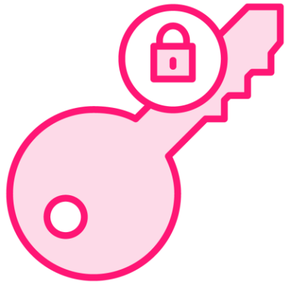
Scope of OpenSSL

OpenSSL generates certificates that can be used to validate the authenticity of a software and protect the data-in-transit.



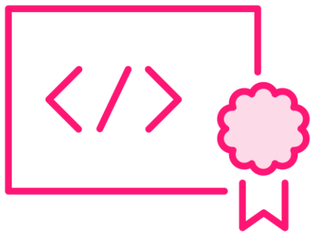
Cryptography

Supports generation of data hash and random numbers



Encryption

Data protection ciphers for encryption and decryption



Certificates

Creating private keys, public certificates, and signing requests

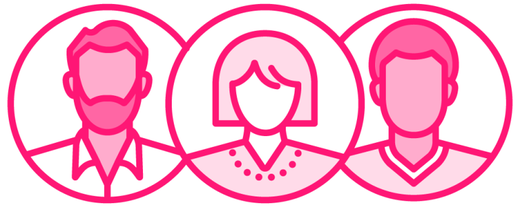
Cross-platform OpenSSL



Primary



Secondary



Community

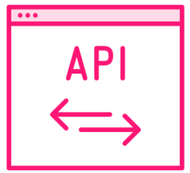
Cross-platform OpenSSL



The file path and directories and their permissions



Configuration of OpenSSL is handled using .cnf files



OpenSSL CLI integration with operating system

In This Course



Using OpenSSL CLI to generate certificates



Configuring OpenSSL CLI for certificates



Verifying the certificates of the software

Demo



Install and verify OpenSSL

Demo



Configuring OpenSSL

- openssl.cnf

Demo



Creating a certificate with OpenSSL

Demo



Certificate validation with OpenSSL

- Server certificate validation

Demo



Certificate validation with OpenSSL

- Verify certificate authority