openssl

To quote Wikipedia “OpenSSL is a software library for applications that provide secure communications over computer networks against eavesdropping, and identify the party at the other end. It is widely used by Internet servers, including the majority of HTTPS websites. … OpenSSL is available for most Unix-like operating systems (including Linux, macOS, and BSD), Microsoft Windows and OpenVMS.”

From the openssl man page (man 1 openssl)

===

The openssl program is a command line tool for using the various cryptography functions of OpenSSL's crypto library from the shell. It can be used for

- Creation and management of private keys, public keys and parameters
- Public key cryptographic operations
- Creation of X.509 certificates, CSRs and CRLs
- Calculation of Message Digests
- Encryption and Decryption with Ciphers
- SSL/TLS Client and Server Tests
- Handling of S/MIME signed or encrypted mail
- Time Stamp requests, generation and verification

===

The function most commonly known to end users for SSL is securing web sites so that traffic between a user and the web server is secure and validated (you know that the site you're going to is who they say they are).

Generally, a **Certificate of Authority** (commonly called a **CA**) is generated by a well known and respected organization with a certificate given to the public. This CA is then used to digitally sign a certificate for a web site, which the systems administrator puts into the web server configuration.

Widely used CA's are installed by default into most operating systems, so do not have to be manually added by the end users.

Currently, smaller web sites can have SSL Certificates for their web sites from LetsEncrypt at no charge. However, we recommend giving a small donation to help them pay the expense of maintaining the system.

Daily Data uses LetsEncrypt certificates on all our public facing platforms.

However, public SSL certificates will not work on internal (LAN) networks as the issuer (the owner of the CA) must be able to verify ownership of a service. If you want to secure internal web sites/e-mail/ftp sites, see the article LAN SSL Certificates.