LAN SSL Certificates

The procedures described here are generally used for local networks. In only limited cases would this be useful for any public service. For example, you would not use this to secure your public web/mail/ftp site. This is only used for internal, LAN based services which have no public access.

Most SSL Certificates are used on public facing devices and are provided by large organizations which specialize in this. For example, this web site uses an SSL certificate provided by https://letsencrypt.org/Let's Encrypt, an organization the provides free SSL Certificates and is supported by donations.

In many cases it is useful to have SSL certificates in your Local Area Network (LAN), and these can not readily be provided by the public SSL organizations. They are designed for situations where you can prove ownership of a publicly visible service, like a web site or mail server.

There are a few companies which provide a service for internal networks, but the cost generally exceeds what most businesses are willing to spend, and as an alternative, it is easy to simply create your own Certificate of Authority (CA), add the generated certificate to all of your internal computers, and use that CA to generate certificates for your internal services.

We will use openssl to generate the CA's and Server Certificates. The following articles walk you through doing this. Since, at Daily Data we use this for some of our clients and for ourselves, we have created a set of script that will make the process simpler. These scripts are written in Perl and released under the FreeBSD license. They can be viewed in our Subversion repository or checked out with the following command.

```
svn co http://svn.dailydata.net/svn/sysadmin_scripts/trunk/ssl_certs
```

Note: openssl has a built in command, ca, which was written as a sample minimal CA application. I chose not to use that since our needs (a dozen services, at most) and due to the warnings at the bottom of the man page (man 1 openssl-ca).

I have attempted to create a system which uses the recommended steps for such a small setup as of Fall 2025. You may find other articles saying to do things a different way. For example, an RSA private key can be created with any of these commands:

- openssl genrsa
- openssl req (with the -newkey parameter)
- openssl genpkey

I chose to go with *openssl genpkey* as that is the recommended way as of this date. But, be aware, there are multiple ways to achieve the result using openssl.

Basic Procedure

The steps to implementing a private, LAN based set of certificates is fairly straight forward.

1. Install OpenSSL on a computer
    1. Almost all Unix systems (Linux, BSD, MacOS) have it pre-installed
    2. Windows systems, I'm not sure about since it is a cracker paradise. I'll try to put whatever I can find in SSL Program for Windows
2. Create a configuration file
3. Create a private Certificate of Authority
4. Install the CA created above onto all machines which will be making a connection.
5. For each service you need secure
    1. Create a site certificate and sign it with the CA above
    2. Copy the site certificate files to the servers containing the service

At this point, you should be able to access all services using SSL (https, smtps, ftps, imaps).