Create an mTLS Cert Package

Building mutual TLS (mTLS) certificates using a local Certificate Authority (CA) involves several steps. Here's a general guide to help you through the process:

Step 1: Set Up Your Local Certificate Authority

Create a Private Key for the CA

```
openssl genrsa -out ca.key 2048
```

Create a Self-Signed Certificate for the CA

```
openssl req -x509 -new -nodes -key ca.key -sha256 -days 1024 -out ca.crt
```

You will be prompted to enter information for the certificate.

Step 2: Generate Server and Client Certificates

For the Server Certificate:

Create a Private Key for the Server

```
openssl genrsa -out server.key 2048
```

Create a Certificate Signing Request (CSR) for the Server

```
openssl req -new -key server.key -out server.csr
```

Sign the Server CSR with the CA

```
openssl x509 -req -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial \
-out server.crt -days 500 -sha256
```

For the Client Certificate:

Create a Private Key for the Client

```
openssl genrsa -out client.key 2048
```

Create a Certificate Signing Request (CSR) for the Client

```
openssl req -new -key client.key -out client.csr
```

Sign the Client CSR with the CA

```
openssl x509 -req -in client.csr -CA ca.crt -CAkey ca.key \
-CAcreateserial -out client.crt -days 500 -sha256
```

Step 3: Verify the Certificates

You can verify the certificates to ensure they are correctly signed

Verify the Server Certificate

```
openssl verify -CAfile ca.crt server.crt
```

Verify the Client Certificate

```
openssl verify -CAfile ca.crt client.crt
```

Step 4: Configure Your Server for mTLS

Depending on the server software you are using (e.g., Nginx, Apache, etc.), you will need to configure it to require client certificates and to trust your CA.

Step 5: Test the mTLS Setup

Start your server with the configured certificates. **Use a client** (like `curl` or a custom application) to connect to the server, providing the client certificate and key.

Example using `curl`

```
curl -v --key client.key --cert client.crt \
--cacert ca.crt https://your-server-url
```

Conclusion

This process sets up a basic mTLS configuration using a local CA. Make sure to adjust the configurations based on your specific requirements and security policies.

From:
https://kb.unixservertech.com/ - **Unix Server Tech Knowledge Base**

Permanent link:
https://kb.unixservertech.com/software/tls/mtlsgen

Last update: **2025/07/23 20:38**