

# Creating a CA in OpenSSL

Joe Haynes of Terra Firma Software Solutions, Inc.

11th January 2005

## 0.1 Why you need a Certificate of Authority

1. Provides control over the certificate creation process
2. Ability to create numerous certificates of a specific type and/or size (2048 bit versus 1024)
3. Much less expensive than creating certificates through an established Certificate of Authority (i.e. VeriSign)

## 0.2 Creation Process

1. Login as root and change to the directory `/etc/ssl/misc`
2. Issue the command: `CA.sh -newca`
3. Just click the Enter key when it asks for a 'CA certificate filename' (this will create a default of `cakey.pem`)
4. Enter a password at the prompt: 'Enter PEM pass phrase:' (***you will need this later to unlock the key when signing certificates***).
5. Follow the questions and enter any locality information (examples: 'US' for United States, 'Montana' for Some-State, 'Helena' for city, Terra Firma Solutions' for the company, 'IT' for Organizational Unit Name, etc.)
6. For the common name use something similar to 'ca.yourbusiness.com' and for the Email Address use and administrative email account.

This will create a directory structure under `/etc/ssl/misc` that contains both the CA certificate and the CA private key.