Using the SSL Toolkit

Secure Sockets Layer (SSL) is a standard protocol used to manage the security of message transmissions in an open communications network, such as the Internet. It uses TCP/IP for its physical communications. In addition, it uses public and private key encryption for both authentication and data encryption keys. These certificates are obtained from a certificate authority.

Note:
The SSL Toolkit is a 32-bit application that runs in both 32-bit and 64-bit environments.

Various organizations, such as VeriSign, act as external certificate authorities for other companies and supply certificates for authentication and encryption as requested by their clients. You can use an external certificate authority to provide your certificates or, *for testing only*, you can use the SSL Toolkit, provided with Encryption for Entire Net-Work, to become your own certificate authority.

The SSL Toolkit allows you to create your own certificate authority (CA) and certificates for C code. It is available in Windows environments only.

▶ **To use the SSL Toolkit:**

1. Collect the information described in *Gathering SSL Toolkit Information*. This information is requested when running the SSL Toolkit.
2. At a command prompt, make the SSL Toolkit directory on your Windows machine the current directory.
3. Create a certificate authority for the Windows machine. For more information, read *Setting Up a Certificate Authority*.
4. Create the certificates you need. For more information, read *Creating Certificates*.
5. When the certificates you need have been created, deploy them on the system on which they are needed. For more information, read *Deploying Certificates*.
6. Update the appropriate target definitions in the Entire Net-Work Client, Kernel, and server target entries or in the Directory Server entries to support secure transmissions. For more information, read *Access and Connection Definition Setup*.

This chapter covers the following topics:

- Gathering SSL Toolkit Information
- Setting Up a Certificate Authority
- Creating Certificates
- Deploying Certificates

Gathering SSL Toolkit Information

When you use the SSL Toolkit, it will prompt you for the information described in the following table. Use the following table to collect this information prior to using the SSL Toolkit. The order in which this information is requested varies by what you attempt to create: a certificate authority (CA) or a certificate and key. All of this information is not necessarily requested during SSL Toolkit processing.

Information Requested	**Description**	**Used to Create**
City or Town (Locality)	The name of your city or town. If a default is provided, it is shown in brackets next to the prompt. This information is used as part of the distinguished name (DN) for a certificate or CA. The contents of the DN for each certificate must be unique; this means that at least one of the fields that comprise the DN for each certificate must be unique.	Certificate authority C certificates
Common Name	Your name or the name of your application. If a default is provided, it is shown in brackets next to the prompt. A maximum of 64 characters can be specified. This information is used as part of the distinguished name (DN) for a certificate or CA. The contents of the DN for each certificate must be unique; this means that at least one of the fields that comprise the DN for each certificate must be unique.	Certificate authority C certificates
Country Name	A two-letter code for your country. If a default is provided, it is shown in brackets next to the prompt. This information is used as part of the distinguished name (DN) for a certificate or CA. The contents of the DN for each certificate must be unique; this means that at least one of the fields that comprise the DN for each certificate must be unique.	Certificate authority C certificates
E-mail Address	Your e-mail address. The default is "Security@YourCompany.com". A maximum of 40 characters can be specified. This information is used as part of the distinguished name (DN) for a certificate or CA. The contents of the DN for each certificate must be unique; this means that at least one of the fields that comprise the DN for each certificate must be unique.	Certificate authority C certificates

Information Requested	Description	Used to Create
Organization Unit	The name of your department within the organization. If a default is provided, it is shown in brackets next to the prompt. This information is used as part of the distinguished name (DN) for a certificate or CA. The contents of the DN for each certificate must be unique; this means that at least one of the fields that comprise the DN for each certificate must be unique.	Certificate authority C certificates
Organization Name	The name of your organization. If a default is provided, it is shown in brackets next to the prompt. This information is used as part of the distinguished name (DN) for a certificate or CA. The contents of the DN for each certificate must be unique; this means that at least one of the fields that comprise the DN for each certificate must be unique.	Certificate authority
PEM Pass Phrase	A Public Encryption Method (PEM) password phrase used by the certificate authority to sign certificates. This PEM password phrase is also requested when you create a certificate. The PEM password you use when setting up the certificate authority should be the same as the PEM password requested when creating a certificate. PEM passwords can be between 4 and 20 alphanumeric characters long, including blanks. They are case-sensitive.	Certificate authority C certificates
State or Province	The name of your state or province. If a default is provided, it is shown in brackets next to the prompt. This information is used as part of the distinguished name (DN) for a certificate or CA. The contents of the DN for each certificate must be unique; this means that at least one of the fields that comprise the DN for each certificate must be unique.	Certificate authority C certificates
Optional Challenge Password	An optional password you can request when you create a C certificate. This password must be different from the PEM password and must be different for each certificate. Challenge passwords can be between 4 and 20 alphanumeric characters long.	C certificates
Optional Company Name	An optional company name	C certificates

You can set defaults for some of these values in the *genca.template* file located in the SSL Toolkit directory. However, the defaults you specify in this file only pertain to setting up a certificate authority or generating C certificates.

⚠ **Warning:**
Before you change the *genca.template* file, be sure to save a copy of the original for later reference.

Setting Up a Certificate Authority

Only one certificate authority can be set up on a single Windows machine. If you run the procedure described in this document more than once on the same machine, the new certificate authority overwrites the old one.

▶ **To set up a certificate authority:**

1. At a DOS command prompt, make the SSL Toolkit directory on your Windows machine the current directory. Then enter the following command:

   ```
   makeca
   ```

   The certificate authority setup process is started. You are prompted to answer a number of questions, as described in the remaining steps.

2. At the PEM password phrase prompt, enter the PEM password phrase you want to use for this certificate authority. The password phrase is used by the certificate authority to sign C certificates. For more information about PEM password phrases, read *Gathering SSL Toolkit Information*.

3. When you are prompted to repeat the PEM password phrase, enter it again exactly as you did in Step 2. Remember that PEM password phrases are case-sensitive.

   The PEM password phrase you enter in this step is compared and verified using the one PEM password phrase you entered in Step 2. If a mismatch occurs, you are prompted to enter the original PEM password phrase (Step 2) and to verify it (Step 3) again.

4. At the country prompt, enter a two-letter country code you want used when creating a distinguished name (DN) for use by the certificate authority. If you press Enter without specifying a value, the default shown in brackets is used.

5. At the state or province prompt, enter the name of the state or province you want used for the distinguished name (DN) for the certificate authority. If you press Enter without specifying a value, the default shown in brackets is used.

6. At the city or town prompt, enter the name of the city or town you want used for the distinguished name (DN) for the certificate authority. If you press Enter without specifying a value, the default shown in brackets is used.

7. At the organizational name prompt, enter the name of your organization. This name is used for the distinguished name (DN) for the certificate authority. If you press Enter without specifying a value, the default shown in brackets is used.
8. At the organization unit prompt, enter the name of your department within the organization. This name is used for the distinguished name (DN) for the certificate authority. If you press Enter without specifying a value, the default shown in brackets is used.
9. At the common name prompt, enter your name or the name of your application. This name is used for the distinguished name (DN) for the certificate authority.
10. At the e-mail address prompt, enter the e-mail address you want used for the distinguished name (DN) for the certificate authority. If you press Enter without specifying a value, the default shown in brackets is used.

    The certificate authority is set up. You can now use it to create certificates.

When you complete these steps, three new subdirectories are added in the SSL Toolkit directory: *cacerts*, *certs*, and *newcerts*.

Subdirectory Name	**Use**
cacerts	Stores certificate authority files.
certs	Stores certificate files, signed or unsigned.
newcerts	For internal use only. Used during the SSL Toolkit certificate creation process.

In addition, the following files are created in the *cacerts* subdirectory:

- *cacert.mf* : A CA certificate that can be used on mainframe systems.
- *cacert.pem* : CA certificate that can be used on open systems.
- *cakey.pem*: A CA key file that can be used on open systems.

Creating Certificates

Once you have set up a certificate authority, you can create C code certificates and their associated keys using the SSL Toolkit.

To create C code certificates:

1. At a command prompt, make the SSL Toolkit directory on your Windows machine the current directory. Then enter the following command:

```
makeccerts [prefix]
```

where *prefix* is the prefix you want used in the certificate file names. All of the certificate and key files produced by the `makeccerts` command will begin with the prefix you specify.

The prefix specification is optional. If you do not specify a prefix, the prefix "myapp" is used. If you enter the same prefix twice, the newer certificate and key definitions will overwrite the older certificate and key definitions.

The C certificate and key creation process is started. You are prompted to answer a number of questions, as described in the remaining steps.

2. At the PEM password phrase prompt, enter the PEM password phrase you want to use. This should be the same PEM password phrase you specified when you set up the certificate authority (CA).

   For more information about PEM password phrases, read *Gathering SSL Toolkit Information*.

3. When you are prompted to repeat the PEM password phrase, enter it again exactly as you did in Step 2. Remember that PEM password phrases are case-sensitive.

   The PEM password phrase you enter in this step is compared and verified using the one PEM password phrase you entered in Step 2. If a mismatch occurs, you are prompted to enter the original PEM password phrase (Step 2) and to verify it (Step 3) again.

4. At the country prompt, enter a two-letter country code you want used when creating a distinguished name (DN) for use by the certificate and key. If you press Enter without specifying a value, the default shown in brackets is used.

5. At the state or province prompt, enter the name of the state or province you want used for the distinguished name (DN) for the certificate and key. If you press Enter without specifying a value, the default shown in brackets is used.

6. At the city or town prompt, enter the name of the city or town you want used for the distinguished name (DN) for the certificate and key. If you press Enter without specifying a value, the default shown in brackets is used.

7. At the organizational name prompt, enter the name of your organization. This name is used for the distinguished name (DN) for the certificate. If you press Enter without specifying a value, the default shown in brackets is used.

8. At the organization unit prompt, enter the name of your department within the organization. This name is used for the distinguished name (DN) for the certificate. If you press Enter without specifying a value, the default shown in brackets is used.

9. At the common name prompt, enter your name or the name of your application. This name is used for the distinguished name (DN) for the certificate.

10. At the e-mail address prompt, enter the e-mail address you want used for the distinguished name (DN) for the certificate. If you press Enter without specifying a value, the default shown in brackets is used.

11. Optionally, at the challenge password prompt, enter the challenge password you want used for this certificate.

For more information about challenge passwords, read *Gathering SSL Toolkit Information*.

12. Optionally, enter your company name at the optional company name prompt.

    The basic information for the certificate is complete. The process to sign the certificate is started.

13. At the PEM password phrase prompt, enter the PEM password phrase you selected for the certificate authority (CA) when you set it up.

    If you enter the incorrect CA PEM password phrase, the certificate creation process aborts. Otherwise, the process to sign the certificate continues.

14. You must enter "y" at the Sign the certificate? prompt. If you do not, the certificate will not work.

15. Enter "y" at the commit prompt. If you do not, the certificate will not work.

    The process to sign the C certificate completes. The certificate is certified.

The following files with names in the following formats are created in the */certs* directory:

- *<prefix>*cert.mf: Certificate file that can be used on mainframe systems.
- *<prefix>*cert.pem: Certificate file that can be used on open systems.
- *<prefix>*key.mf: Key file that can be used on mainframe systems.
- *<prefix>*key.pem: Key file that can be used on open systems.
- *<prefix>*Certreq.pem: This file is used internally by the SSL Toolkit for C certificate processing.

where *<prefix>* is the prefix you specified when you ran the makeccerts program in Step 1. For example, if you used the default prefix "myapp", the following files would be created:

- *myappcert.mf*
- *myappcert.pem*
- *myappkey.mf*
- *myappkey.pem*
- *myappCertreq.pem*

Deploying Certificates

▶ **To deploy certificates and their associated keys:**

1. Transport the certificates and key files to the systems where they are to be used. You can use the *ftp* utility to do this. You can also copy and rename certificates and key files as required.

2. Make sure the location of the certificates and keys is clear on the systems where they are being used. If they are not in the current directory, identify their location using the appropriate SSL parameters and settings as described in *Access and Connection Definition Setup*.