How to Generate KLE Certificates using XCA

This document is intended for those who want to generate their own set of KLE certificates for PKI-authenticated viewer connection instead of obtaining certificates from external Certification Authorities (CA).

KLE offers 3 levels of SSL/PKI Authentication settings in free combination with 3 levels of password policies to be freely adopted according to user's security requirements. Different levels of password/SSL/PKI Authentication combinations should be used conscientiously, taking into consideration of your security concerns and usage convenience. A prior assessment of your security requirements and the practical concern of usage convenience will be helpful in implementing a best security/password connection scheme over your KLE connection.

In order to secure the connections using the awesome power of 1024-bit private/public key encryption, you should obtain an appropriate set of certificates to establish an authenticated connection. KLE uses the certificates issued by an external CA (*Certification Authorities*). Authentication via digital certificates is a much more secure way of remote user identification than only password authentication.

You can use the XCA to

(1) Generate the root certificate (root.crt) and the rootkey (rootkey.pem)
(2) Generate the server certificate (server.crt) -- using the rootkey to sign the server certificate and meanwhile generate a server key
(3) Generate the client certificates (client_name.p12) - using the rootkey to sign the client certificates and meanwhile generate each client key for corresponding client certificates.
(4) Export the certificates and keys for KLE and remote client authentication usage.

KLE's needs the following certificates:
root.crt → file name mandatory
server.crt → file name mandatory
serverkey.pem → file name mandatory

Remote users nneed the following certificates
root.crt → file name mandatory
client.p12 → file name is freely changable
(p12 is a format that is included with a password-protected client private key)


The file name of root.crt, rootkey.pem, server.crt, serverkey.pem are all mandatory, while the file name of client certificates might vary according to user's choice. If you already have certificates appropriate for use with KLE, you could change the file names to be adapted to KLE authentication use.


You could use the default set of certificates (could be found on CD-ROM) to practice making some PKI-authenticated connections as long as your network safety is not jeopardized. We advise that it is better to do the practices within your Local Area Network, which is supposed to be well secured with adequate firewall

and other due precautions against network intrusions. Or if you have already obtained a set of certificates with the file names and formats required by KLE, you can then use them for KLE viewer authentication. However, if you simply use the default set of certificates that comes with KLE, anybody who has a copy of the default certificates may establish a connection to your servers. . So we strongly recommend that you obtain your own certificates for KLE or go forth to generate them using software like XCA.....

1.1 Download and Install XCA

The XCA is a freeware that can help you generate your own set of certificates for secure KLE viewer connection. You can download it from http://sourceforge.net/projects/xca. After downloading it, just install it in a Windows computer. The installation program will create an XCA program group in you're the Start/Programs menu. Run the XCA.

1.2 Generate the KLE certificates

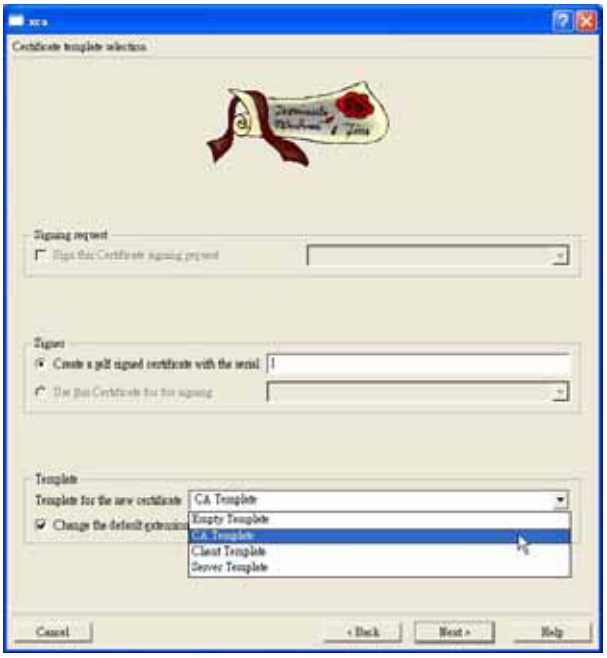
1.2.1 Generate the root certificate and rootkey

The root certificate (later will be exported as *root.crt*) we are going to generate is a self-signed CA certificate that contains the KLE CA's *public key.* (in this case, the KLE CA is the XCA you are using now to generate the certificates).

Step 1. Run the XCA software and Select the *Certificates* tab.

Step 2. Click the *New Certificate* button. If this is your first-time installation of the XCA, you should see a prompt box appears to request you for the password that will encrypt the private key in the XCA database. Just enter the password as you choose and confirm it again. Click OK.

and the *Certificate Template Selection* dialog box appears. The serial number of the root certificate should appear as *1.* Then select the template type to be *CA template*.



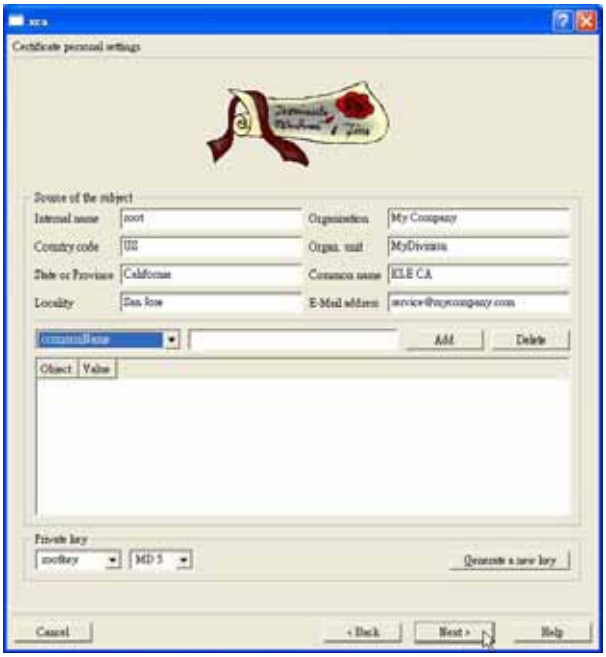
Click *Next*, and the *New Key* dialog box appears.

Step 3. Specify the name of the key as *rootkey*, and choose the key size to be *1024-bit*.

Click *Create* to generate a new key named *rootkey*, and go forth with the *Certificate Personal Setting* on the next dialog box.

Note: A cipher strength of 1024 bits is generally considered unbreakable by today's cryptanalyst. Although higher bits give even stronger cipher strength, it involves more computing resources in encryption/decryption.

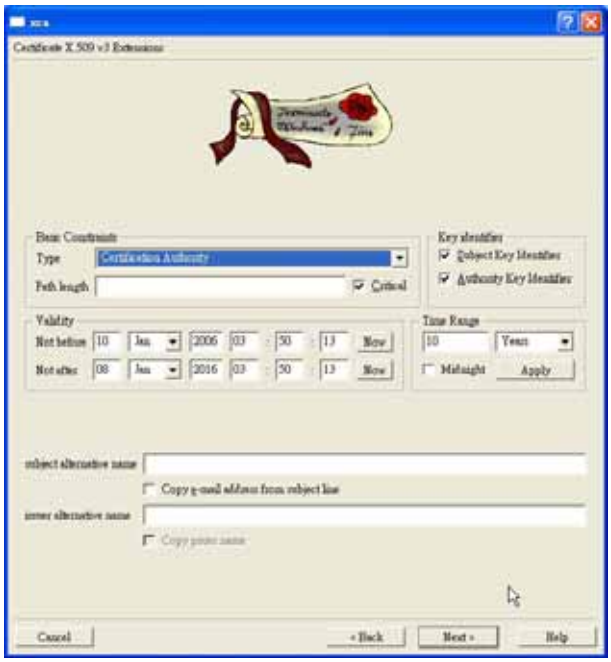
Step 4. Specify the personal information to be bound to the root certificate.



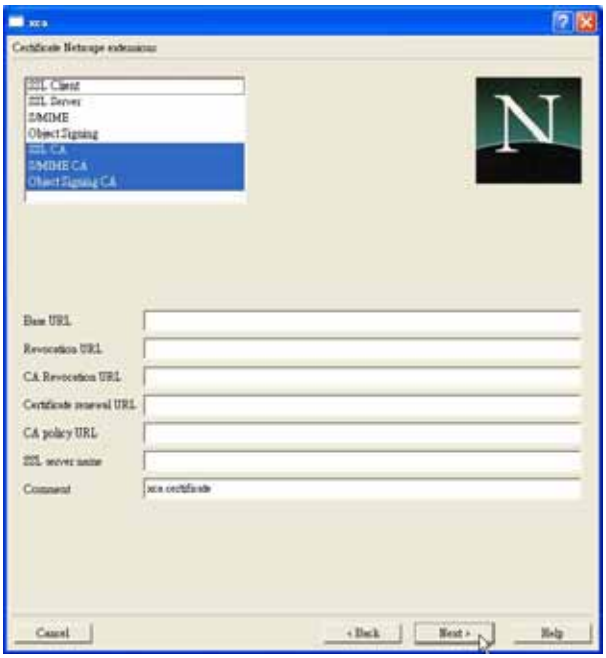
Since a certificate is essentially the binding of personal information and a key, you should here specify the personal information and its binding key (which has already been generated as *rootkey* in previous step) for KLE CA. And it is what you want to specify here for the KLE Certification Authority. The following is an example of personal information for KLE CA:

Internal name: *root (mandatory)*
Country code: *US*
State or Province: *California*
Locality: *San Jose*
Organization: *My Company*
Organization unit: *My Division*
Common name: *KLE CA*
E-mail address: *service@mycompany.com*
Key: *rootkey (mandatory, already appearing in the combo box since we've generated it in previous step)*

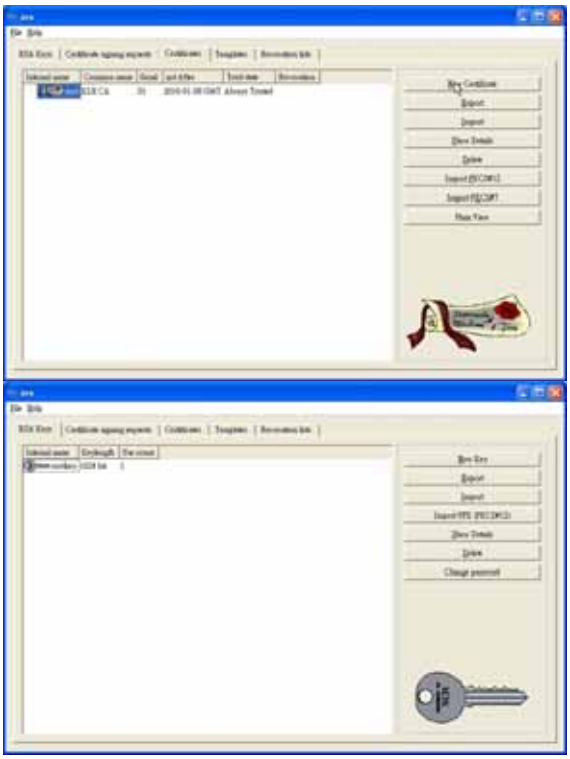
Click *Next*. And then you can set the validity period for the root certificate. In this case, we choose a ten year period from 2006 to 2016. In fact, you can specify a validity period that suits your security policy.



For the rest of the settings you can use the defaults provided by XCA. Thus, just click *Next* all the way through to the end …



Before clicking *Finish* for the last step, you can browse the information that will come to be bound with the root certificate. Click *Finish* to complete the root certificate generation.



Now the root certificate and root key have been generated.

Note: As you can see, the personal information is what others can see and will use to identify the entity (i.e. KLE CA, or more specifically, the entity that uses XCA to generate the root certificate) that the certificate comes to represent--here it's the KLE CA, the root certification authority. Also we have generated the root private key, *rootkey*, which we will need later to sign the server certificates and the client certificates.

Note: the internal name, which determine the certificate file naming, and also the name of the key that is bound with the KLE CA certificate, are both mandatory—the KLE CA certificate has to be named *root* (the file name is *root.crt*) and its binding key has to be named *rootkey* (the file name is *rootkey.pem*)

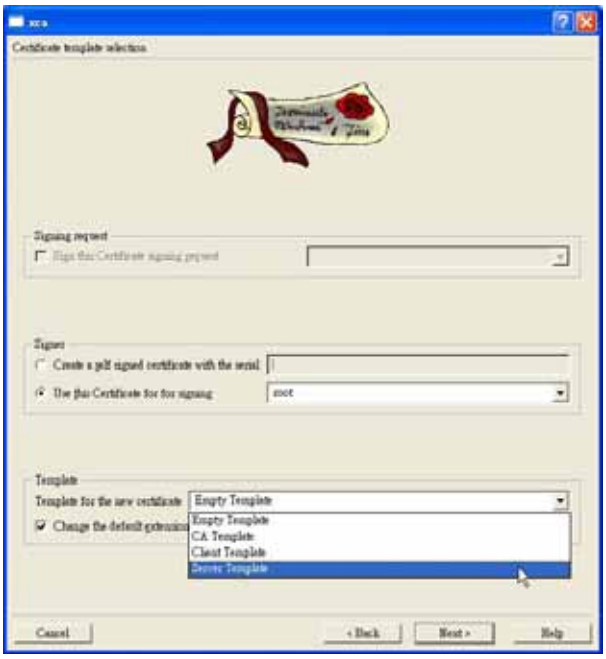
Note: If you want to generate another key, you can press the Generate a new key button. But since the name of the key is mandatory and should be rootkey, we don't actually need to generate any new key here for binding key selection except the rootkey.

Next, we are going to generate the server certificate and key.

1.2.2 Generate the server certificate and server key

The server certificate is required by KLE server (that is, KLE itself) to establish a secure connection with the viewer program on the remote client. The name of the server certificate is mandatory and has to be *server*, and has to be signed by, *rootkey*, the private key of root.

Step 1. Click the *New Certificate* button and the *Certificate Template Selection* dialog box appears. Since server certificate has to be signed by the *rootkey*, we should check the option, *Select Use this certificate for signing,* and select the template type to be *Server template*.

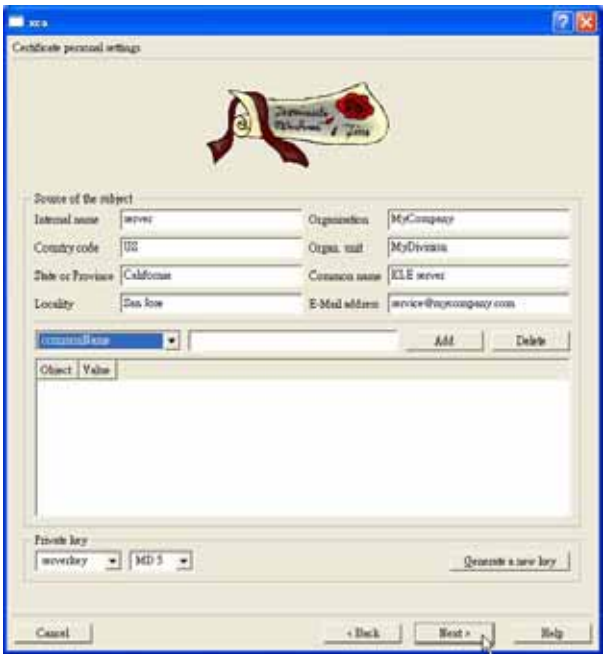


Click *Next*, and the *New Key* dialog box appears.

Step 2. Specify the name of the key as *serverkey*, and choose the key size to be *1024-bit*.

Click *Create* to generate a new key named *serverkey*, and go forth with the *Certificate Personal Setting* on the next dialog box.

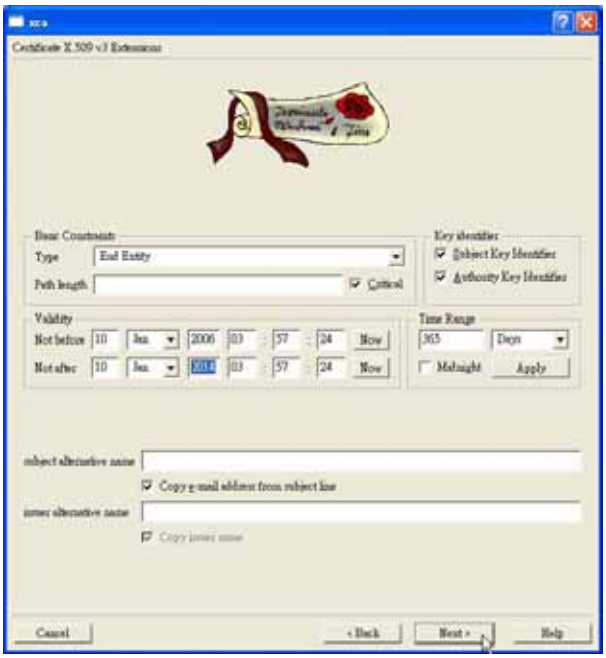
Step 3. Specify the personal information to be bound to the server certificate.



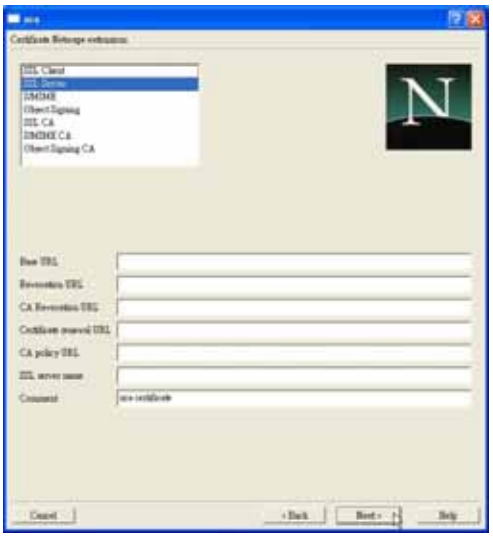
Since a certificate is essentially the binding of personal information and a key, you should here specify the personal information and its binding key (which has already been generated as *serverkey* in previous step) for KLE server. And it is what you want to specify here for the KLE server itself. The following is an example of personal information for KLE server:

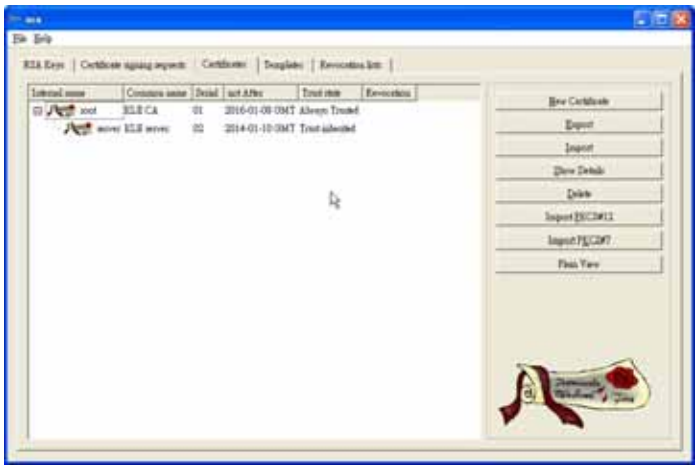
Internal name: *server (mandatory)*
Country code: *US*
State of Province: *California*
Locality: *San Jose*
Organization: *My Company*
Organization unit: *My Division*
Common name: *KLE Server*
E-mail address: *service@mycompany.com*
Key: *serverkey (mandatory, already appearing in the combo box since we've generated it in previous step)*

Click *Next*. And then you can set the validity period for the server certificate. In this case, we choose an eight year period from 2006 to 2014. In fact, you can specify a validity period that suits your security policy. However, the validity period of a server certificate should never exceed that of a root certificate.



For the rest of the settings you can use the defaults provided by XCA. Thus, just click *Next* all the way through to the end …





The KLE server certificate has been generated as you can see appearing on the list.

To install *root certificate, server certificate and server key* on KLE itself is a preceding step to enable the public key authentication feature. For details, please refer to the *User Guide, Section 4.16*.

Note: the internal name, which determine the certificate file naming, and also the name of the key that is bound with the KLE server certificate, are both mandatory—the KLE server certificate has to be named *server* and its binding key has to be named *serverkey*.

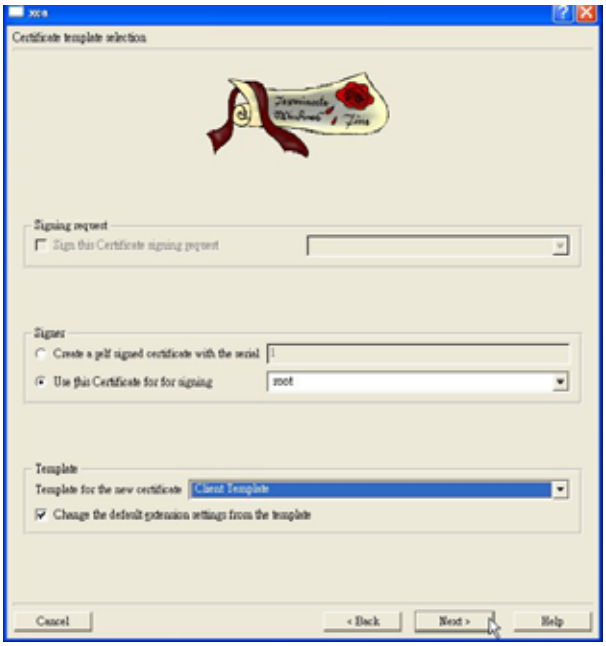
Next, we are going to generate the client certificate and key.

1.2.3 Generate the client certificate and client key

The client certificate is required by the remote client computers to establish a secure connection with the KLE server. The name of the client certificate is not mandatory and can be chosen freely to represent the remote user such as A*manda, Tim, client001, myclient,* etc. (Only note that it's case sensitive!), but likewise, they all have to be signed by *rootkey,* the root private key.

Step 1. Click the *New Certificate* button and the *Certificate Template Selection* dialog box appears. Since a client certificate has to be signed by the *rootkey*, we should check the option, *Select Use this certificate for signing,* and select the template type to be *Client template*.

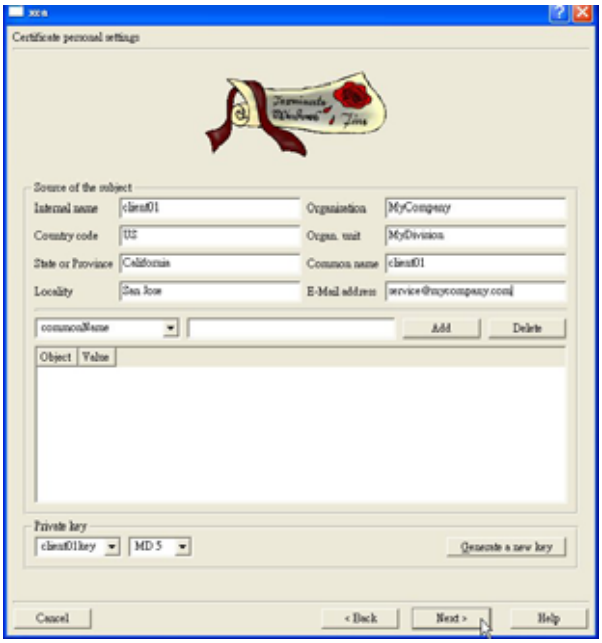
Click *Next*, and the *New Key* dialog box appears.



Step 2. Specify the name of the key as *client01key (the name could be freely chosen, but you'd better choose a name that better corresponds to your client certificate)*, and choose the key size to be *1024-bit*.

Click *Create* to generate a new key named *client01key*, and go forth with the *Certificate Personal Setting* on the next dialog box.

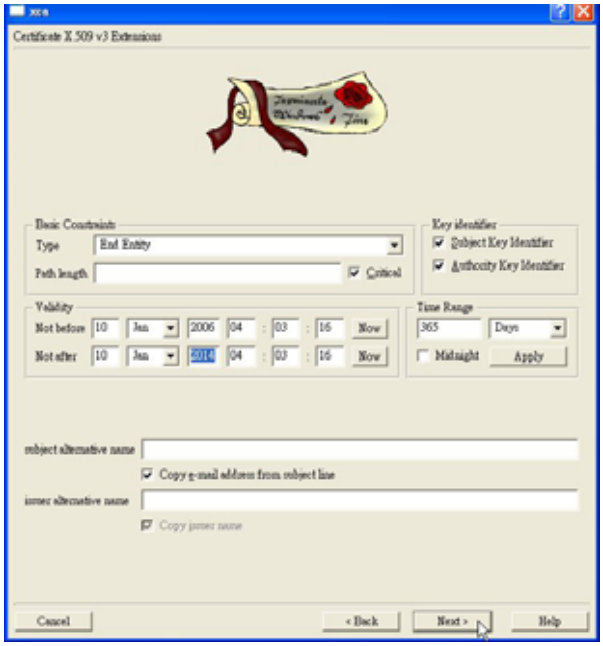
Step 3. Specify the personal information to be bound to the *client01key*.



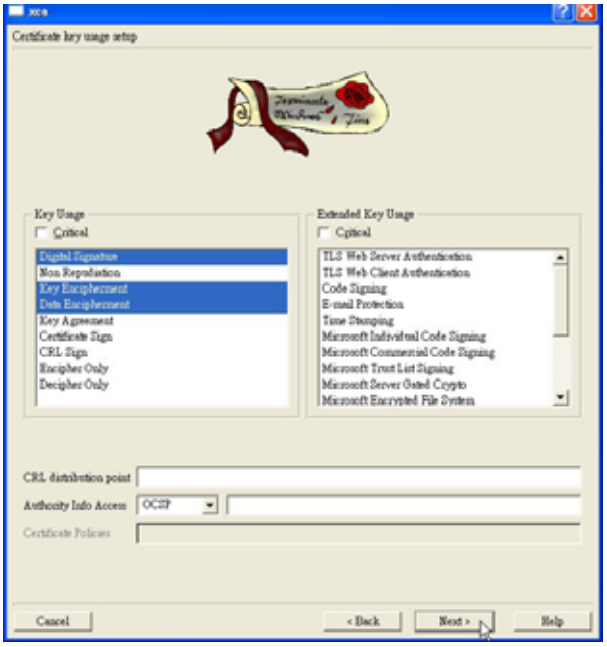
Since a certificate is essentially the binding of personal information and a key, you should here specify the personal information and its binding key (which has already been generated as *client01key* in previous step) for KLE client. And it is what you want to specify here for the client itself. The following is an example of personal information for a KLE client:

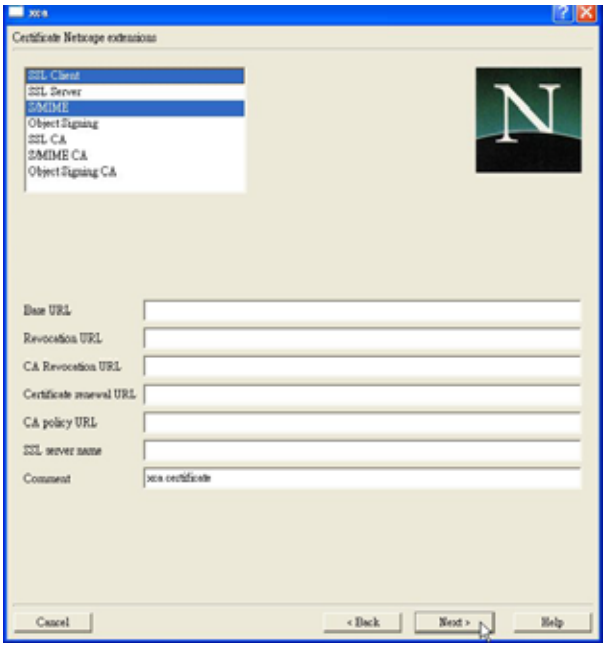
Internal name: *client01 (could be freely chosen to represent the remote client)*
Country code: *US*
State of Province: *California*
Locality: *San Jose*
Organization: *MyCompany*
Organization unit: *MyDivision*
Common name: *client01*
E-mail address: *service@mycompany.com*
Key: *client01key (as already appearing in the combo box since we've generated it in previous step)*

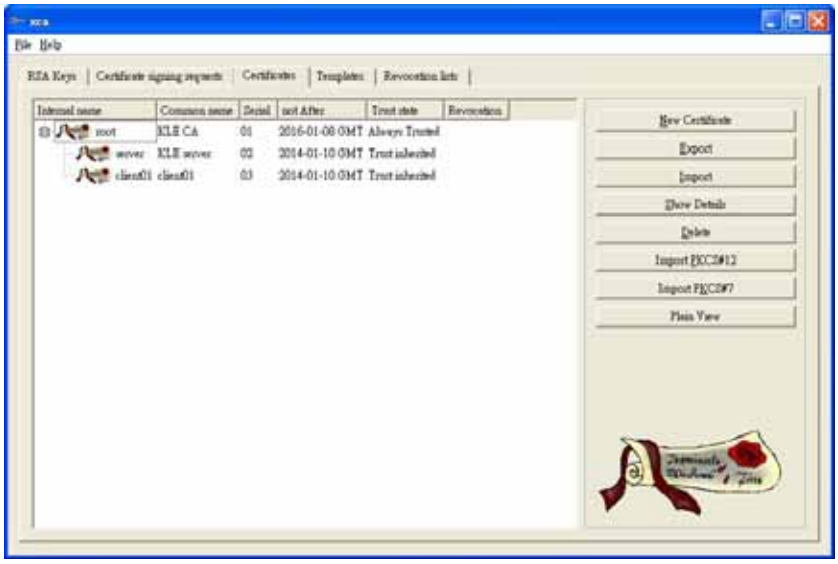
Click *Next*. And then you can set the validity period for the client certificate. In this case, we choose an eight year period from 2006 to 2014. In fact, you can specify a validity period that suits your security policy. However, the validity period of a client certificate should never exceed that of a root certificate.



For the rest of the settings you can use the defaults provided by XCA. Thus, just click *Next* all the way through to the end …







Now a client certificate has been generated for client01 as you can see appearing on the list box.

Note: As you can see, the personal information is what others can see and will use to identify the entity (i.e. a KLE client, or more specifically, a remote user as a KLE client requesting for remote client access) that the certificate comes to represent-- here it's the remote user, client01. Later we will export the client certificate as client01.p12, and give it to a certain client for the authentication of viewer connection.

For the client certificate, the internal name, which determine the certificate file naming, and also the name of the key that is bound with the KLE client certificate, are both freely chosen–could be any name that you think fit to represent the remote client.

Now, we have generated all three types of certificates-root certificate, server certificate and client certificate-- that are needed by authentication before making a secured KLE browser/viewer connection.

Also you can repeat the steps above to generate any number of client certificates prior to exporting them for distribution to the clients. All the client certificates you generated will appear in the listing box and be given with a unique serial number. Note that the serial number will not be freed for further use, even if the certificate is deleted from the XCA database.

1.3 Export KLE Certificates

First, you have to generate the following certificates and keys on XCA. If not, please go back to Section 1.2 to generate all the certificates you need to establish an authenticated viewer connection.

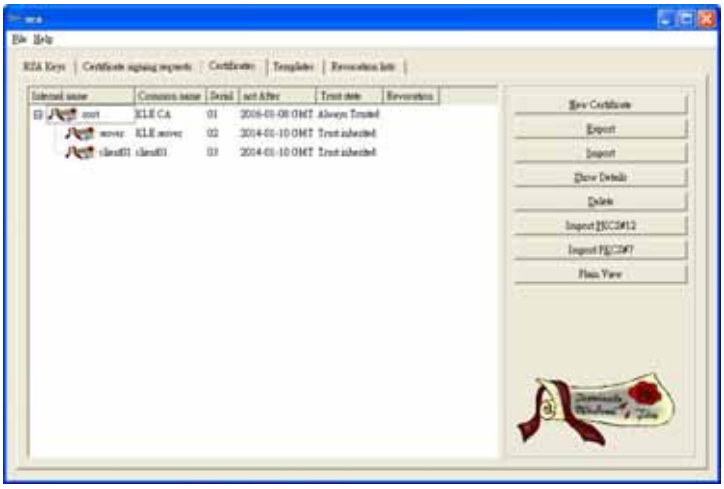
Certificates to be installed on KLE:
(1) the root certificate (*root.crt*)
(2) the server certificate (*server.crt*), and
(3) the server private key (serverkey.pem)

Certificates to be imported to the viewer program on the client computer:
(1) the root certificate (*root.crt*)
(2) the client certificate (*client_name.p12*)

For a remote client, all it takes is the following two files—a root public certificate (*root.crt*) and a client certificate (client.p12)-- which should be handed to the user in a secure way, i.e. either should be handed to the user's hands personally or should employed a secured way of transportation with a temper-proof procedure.

1.3.1 Export the root certificate (*root.crt*)

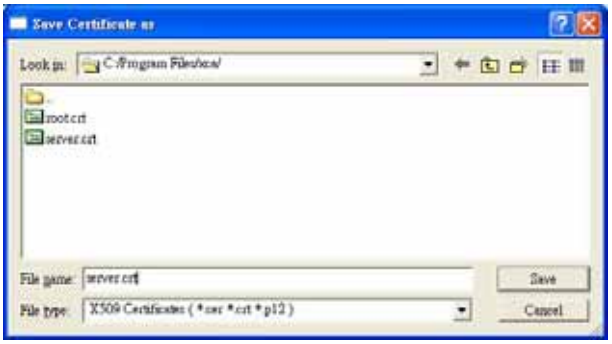
Step 1. Select the *Certificate* tab. Then click to select the *root* certificate listed at the top.



Step 2. Click *Export* and the *Certificate Export* dialog box pops up.

Since the default setting for the file name is already *root.crt*, and the export format is *PEM*, you don't' have to change anything on this page except specifying the location you want to save the exported certificate. Just click the little rectangular

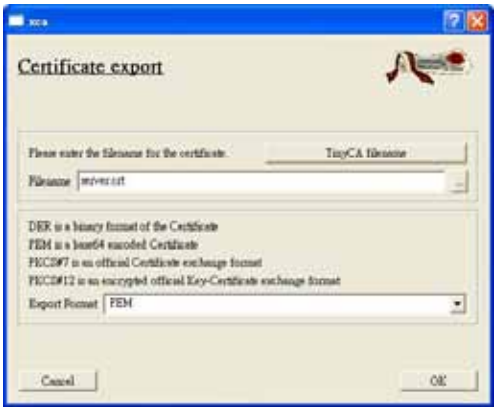
button to the right of the file name box, and the *Save Certificate as..* dialog box appears.



Click *Save* button to specify the export destination path. Then click *OK*. The *root.crt* has been exported to the C:*/Program Files/xca* directory.

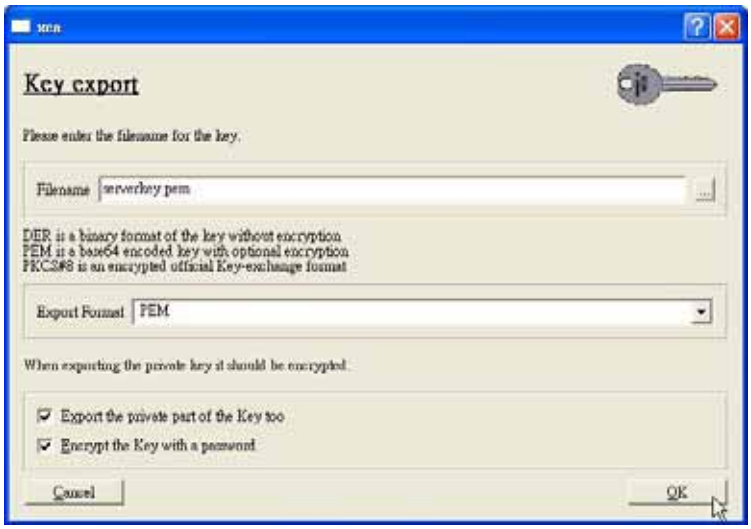
1.3.2 Export the server certificate (server.crt) and server key (serverkey.pem)

To export the server certificate (server.crt) ..
Do the likewise to export the root certificate as in exporting the root certificate …

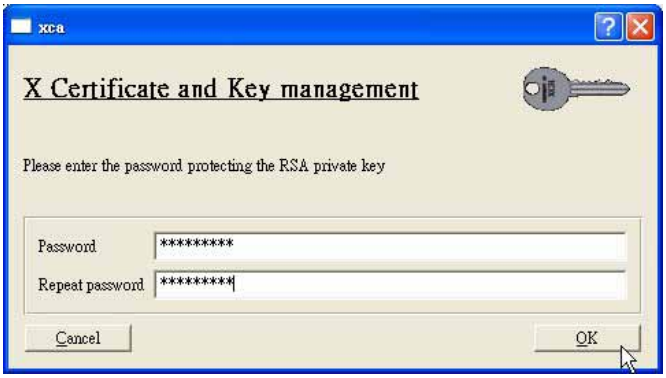


To export the server key (serverkey.pem)..

Step 1. Select the *RSA Keys* tab. Then click to select the *serverkey*. Click *Export* and the *Key Export* prompt box will appear.



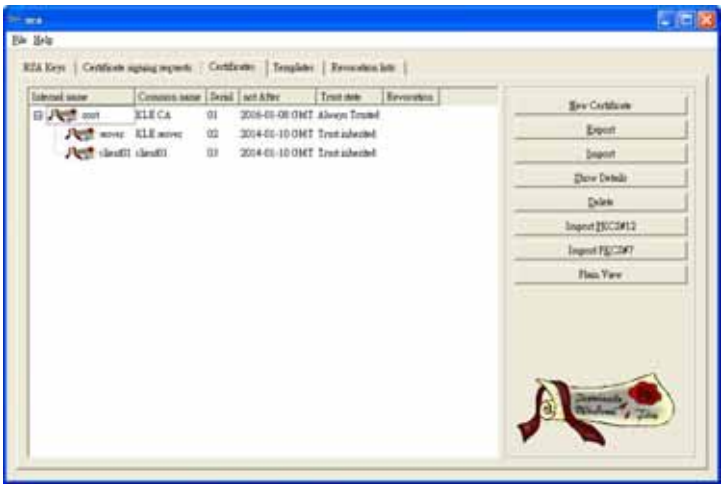
Step 1. Select the *Export format* as *PEM*. Then check both options to *Export the private part of the key too* and to *Encrypt the Key with a password* . Then click *OK*. A password prompt box will appear for you to enter the password that protect the server key. You could enter your own password. Here we enter **serverpwd** as our default server password.



Click *OK* to export.

1.3.3 Export the client certificate

Step 1. Select the *Certificate* tab. Then click to select the client certificate that you want to export--in this case, we select *client01*.



Step 2. Click *Export* and a dialog box such as the following will pop up.

Select the *Export Format* as *PKCS #12, and then specify the location where you want to save the exported file.* Just click the little rectangular button to the right of the file name box, and the *Save Certificate as..* dialog box appears. Click *OK*, and a password management dialog box prompts you to input the password that is going to encrypt this client certificate in *.p12* format.

Choose your password wisely and repeat it again in the second input area.
Click *OK*, and the client certificate, *client01.p12*, is exported to the destination folder you specified.

Now you have all the certificates needed by KLE server and the remote client, client01, to establish both a secure browser connection and a secure viewer connection.

1.4 Install Certificates on KLE

Certificates to be installed on KLE:
(1) the root certificate (*root.crt*)
(2) the server certificate (*server.crt*), and
(3) the server private key (serverkey.pem)

First you have to have these certificates ready on your client computers for uploading to KLE via a Web browser.

To install the certificates on KLE, please refer to the *User Guide, Section 2.7*.

1.5 Import Certificates to the Viewer on Client Computer

Certificates to be imported to the viewer program on the client computer:
(1) the root certificate (*root.crt*)
(2) the client certificate (*client_name.p12*)

To import certificates to the viewer on client computer, please refer to the *User Guide, Section 3.3*

1.6 Select Level 3 Security for Viewer Connection

Step 1. To implement authentication feature on KLE viewer, you have to select Level 3 viewer security connection on the Security page of your KLE browser interface.

Step 2. Then Enter the server password.

Here you should enter the password that has encrypted the *server private key* in the server private key file, *serverkey.pem*. You should enter the correct server password here in order to make successful viewer connection with **KLE** in level 3 security setting. If you use the standard set of certificates provided on the Support CD ROM disc, the password that encrypts the server private key is

serverpwd

However, if you use your own set of certificates, you should get the correct server password from the Certificate Authority that issues those certificates.

Step 3. Go to the *Apply Setting* page and hit the *Apply Setting* button to validate your selection.

1.7 Select a Password Policy

Step 1. Select a User Password Policy.
KLE offers three types of password policies On the drop-down combo box, you can select your password policy for viewer connections:

No Password
Global Password
User Password

No Password – the viewer will prompt you for no password. Anyone who is with the viewer and passes the security level check of the viewer could well establish the connection.
Global Password – the viewer will prompt you for a global password, which is used by all who want to make viewer connections to **KLE**.
User Password – the viewer will prompt you with user-specific password. With this setting, each login user will be checked against his or her corresponding password before allowing viewer connection.

Global user password : If you adopt the Global Password Policy. Here you should enter the password that is used when the global user password setting is enabled as your active password policy.

Step 2. Go to the *Apply Setting* page and hit the *Apply Setting* button to validate your selection.


There are altogether nine (3 x 3) possible combinations of Viewer Security Levels + Password Policies that are available for a flexibility to adapt to your security needs. The administrator can choose an optimized combination of user password policy and the SSL / PKI Authentication according to his security/convenience concern.

	User Password Policy			
SSL / PKI Authentication		No password	Global Password	User-specific Password
	No SSL-No PKI	N – N – N	G – N – N	U – N - N
	SSL – No PKI	N – S – N	G – S – N	U – S - N
	SSL - PKI	N – S – P	G – S – P	U – S - P

G – Global Password U – User-specific Password
S – 128-bit SSL Encryption
P – 1024-bit PKI Authentication
N – Not available

Please note: Either Password Policy or Security Level (SSL/PKI authentication) settings should be used with due precaution: If you adopts No Password Policy and No SSL encryption/No SSL authentication, anyone with a viewer and knowledge of the access IP and port number of KLE can establish a remote connection

Now your KLE is ready for a PKI-authenticated plus SSL-encrypted viewer connection!
All you have to do is to distribute the followings to you remote connection client:

1. Certifidcates: (as you have exported from XCA. They are required only if you select level 3 viewer security)
   root.crt
   client_name.p12. (client_name is freely chosen)

2. Certificate password: (as you have specified for the client certificate when exporting client certificate. It is required only if you select level 3 viewer security)
   clientpwd (if you use the default set of certificate provided on KLE CD-ROM)

3. User account and password: (as you have specified in the *User Management* page. It is required only if you choose User Password Policy)
   Superuser / superu
   Admin / 123456
   User / 123456
   (If you use the default user accounts/passwords)

4. Global Password: (as you have specified in the Security Page. It is required only if you use the Global Password Policy)
   (You will be prompted when choosing it as your password policy on the Security Page.)