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.

<u>KLE's needs the following certificates:</u> root.crt \rightarrow file name mandatory server.crt \rightarrow file name mandatory serverkey.pem \rightarrow file name mandatory

<u>Remote users nneed the following certificates</u> root.crt \rightarrow file name mandatory client.p12 \rightarrow 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

<u>http://sourceforge.net/projects/xca</u>. 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.

Bir Brb	
RZA Keys Cechficite againg sequent Certificato Schwarzen Revocation.lists	
Internal name Common name Strind not After Trust side Envocation	New Cechilants
	Export
	[seport]
	Drove Details
	Delete
	Import EXC2012
	Import FigC2#7
	Finit Yew

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*.

28
2
8

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*.

Flexing set is table to the new key and in Key properties	elect the denied keynine
Name mothey	
Keynine 1004 hit	
Keynne 1004 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.

	1	-	¢.		
Scoute of the sub- Internal name	act [zoot	Organization	My Company		
Country code	UE	Organ. mat	MyDivisia		
Shite or Province Call Locality Day	Californie	Conunco asse	KLE CA		
	Dan Acce	E-Mol address	mexice@acycompany.com		
Object Value			Add	Delata	

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.

					•			
Beau Com Type Fach haust	6000	etices A tell	entr			• •	Keyslenit 19 galac 19 Autor	fer t Key Meantler sty Key Meantler
Validity	9					A. Count	Time Kenne	
Not before	10	lan 💌	2006 0	50	13	Nov	10	Yean .
Notable	08	lan •	2016 0	50	13	Nov	IT Hilaght	Apply
leject ellern mer ellerne	ellor tatter lore tatter	[□ Cog	y E-coull with	nu fron reb	ectlas			

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 ...

j		
Key Dage 17 Galed	Ectended Key Unge	
Digital Digital Ngaatan Maa Ropadasica Key Encipherment Dala Sarijaherment Eso A generated Constant Plan Encipher Only Despher Only	TLG Web Server Arthrotecture TLE Web Closed Arthrotecture Code Signing Brinnil Protecture Tune Damping Microsoft Individual Code Signing Microsoft Commented Code Signing Microsoft Commented Code Signing Microsoft Encoder Ordel Cogets Microsoft Encoder Ordel Cogets Microsoft Encoder Ordel Cogets	-
RL dansbeston point (otherity Info Access OCEP +) (otherity Toless		

ddicele listange edemican	
201 Client	
TALL Deriver	
Object Tigning	
III CA	
Ohert Signing CA	
Base USL	
Constration URL	
Cé Deservative WEI	
CA REPORTED GRA	
Centricate processi URL	
CA policy URL	
DL server anne	
Comment Inter certificate	
ALCONT OF	Construction of the second



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*.

ana -	
etificate templete selection	
A	
Signing report IF Sign for Configure signing proved	
Super (* Create a gell signed certificate with the sensil (* Day that Certificate for for signing	net 💽
Templete Templete for the new centilizate Change the defenit primate Change the defenit primate Classific Classific Classific Templete Classific Templete	
Caust	+Bak Bot> Boy

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*.

		28
New k	icy.	
Einen goer Key pas	n more to the new key and pecters	select the denied keysine
Name	ervedey	
Keynne	Name moveckey Keysian 1034 bit	1
Case	e 1	Control 1

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.

	1				
Scutte of the sub Internal name	pect	Organization	HyCompany		
Country code Date or Province Locality	UE Californae Ens Acce	Organ, mat	MyDivasia RLE serves service@ecocompany.com		
		Constant and			
		E-Mul address			
Object Value					

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.

		1	91	PLL.	-17				
			бiс.						
Sheet Con	athints -						Ery de	entire .	and the state
Type End Exity					-	Z Cantol	Subject Key Identifier		
Not before Not after	10 la	• 200	6 0) 0 0)	57	24	Now	[365 □ Malaig	Depti Ad A	• 1969
dian taber	untern sector (
mer siberae	dave same	Copyen	al address fo	rom rubjer	et line				_
	10000000								

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 ...

Colificati lary maga antap		
Ery Trup Cannel Capital Countries New Targetowners Tarle Targetowners Tarle Targetowners Confiscer Dans Confiscer Dans Confisc	Extended Key Tage T Gglod TLI We Serier Artheotoxies ULI We Serier Artheotoxies Constitution Constitution Tagent Home Tubering Home Tubering	1. L. I.
OKI Antolesco poet Antoniy Isla Anna (OCP •) Constant Falses		

Internal Internal

Date and the second sec	
and berne	3.7
234348	
III. CA	
ENDIE CA	
Object Signing CA	1
Des 195	
Constraint provide COL	
CA pricy THL	
Ell, anar susa	
Countral and includes	
<u>Sect</u>	ak Net - Seg
	28
tifest Feed Sadel	
	X
Delant (23-628 novel-4828 day Ind II- dahara (24) Space (27-88) Simulation and Alternative Jamer (25-812 (24-616) das Indeland (24) Castrando (24) Caspace (25-66) Simulation (24) Space (24) Space (24) Caspace (25) Space (24) Space	in Dependent on
teed	a _ Peak (j _ Bek
Dant	n Park (j Bay
Deard Page	a Part (100)
Excel du	n Paul 1 Bre
Dented	nBeccele
Decol IR spring seynet: Confinence Despite Rescontino for Communication Decid and The I Rescontino for ELE C.A. II. 216601.00 0041 Along Transf ELE C.A. II. 216601.00 0041 Along Transf ELE server. 22. 2114-01-10-0041 Transidented	n _ hat [_ ho _]
Euse	a Post p Bog
Davel quidg syme Cottleter Conses and David and Alex Davids E28 C.A. = 01 2016/01/2017 March E28 C.A. = 02 2016/01/20 2007 Alexy Transit E28 C.A. = 02 2016/01/20 2007 Transit E28 C.A. = 02 2016/01/20 Z.A. = 02	n Paul Bog
Daved	es Pach [] Boy] mBee Cetter Days Jees Sela Date
Guest	n Rechtlich Bog Ber Cettle Berer Jager John Dabe Sager BC3
tauret 10 suriaj reports Cettioner Deglets Revocation for Consum and Datal just Alls That is a Consum and Datal just Alls That is a Solution of the second sec	n Ber Conto Ber Conto Ber Den Der Den Der Den Der Den Der Den Der Den Der Den

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

How to Generate KLE Certificates using XCA

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 *Amanda, 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.

Contraction of the second	
e serial 1	
foot	
Template	
	e secial [1 zoot

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*.

		Pagminada ()	
	1	- pins		
Source of the subj	ect			
internel neme	client01	Organisation	MyCompany	
Country code	03	Organ. unit	MyDivision	
Itate or Province	Celifornia	Common name	client01	
Locality	San Jose	E-Mail address	service@mytompany	com
common Warms	-		1	Data
Construction of the	2)			LARE
Object Yelse				
Object Value				
Object Yalte				
Object Yaloe				
Object Yaller				
Object Yaller				
Object Yeller				

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)

How to Generate KLE Certificates using XCA

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.

	5	-			
	(Jagmineta			
	1		Time		
	· ·				
Basic Coastra	nts		-	- Key identifier -	Manhfur
15ge	End Endly		-	Authority E	en Mantifier
Peth length			I Cutical	in Garrin a	cy some and
Velidity			1	ime Range	
Not before 1	0 Jan 💌 2006 0	4 : 03 : 16	Now	365 De	yn 💌
Notafter 1	0 Jan - 2016 0	4 : 03 : 16	Now	Midnight	Apply
ubject allectuation	e name				
	Copy g-mail add	pens from subject lane			
cost allectative	name				
	Copy prost nun				

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 ...

Certificate lary mage attap	Permante PL. June 7 700	
Evy Usage Critical Togati Agenetical Ros. Republican Evy Extra because Confinition Tapa Certificate Tapa Certificate Tapa Certificate Tapa Excipater Ouly Decipher Ouly	Extended Key Usage Cptical TLS Web Server Authentication TLS Web Client Authentication Code Signing E-mail Protection Time Description Microsoft Toron and Code Signing Microsoft Toron List Signing Microsoft Toron List Signing Microsoft Exercer Sold Copyto Microsoft Exercer Sold Copyto Microsoft Exercer Sold Copyto	4
CRL distribution point CRL distribution point Authority Info Access Certificate Policies	and I Marcol I	

X10					2
lectificate Netscope extensio	100				
ant claus	_			_	_
SSL Server					T
SMIME					
Object Signing					
2MIME CA					
Object Signing CA				_	
,					
D					
Base UKL					
Revocation URL					
CA Revocation URL					
Certificate renewal URL					
CA policy URL					
SSL server name	[
Comment	xca certificate				
Cancel			< Back	Next > N	Help
-					
222.0					Ľ
echilacelle Wasaud Essaihed					
			-		
	27	-			
	2	Zegminects			
		and the second second	1 Fins		
	· · · · · · · · · · · · · · · · · · ·				
You are done with enterin	ag all parameters for creat	ting a Certificat	n		
Subject: (CN-client())	C-021-San				
JosefST-California/O-I	eyCompany/OU-MyDiv	inion/eneilAdd	nor-service Output	ompany.com	
Insuer: /CN-KLE CA.	C-USE-San JosefST-Ca	ddomis/O-My	0.00		
Company Company	ACCORDING TO STATE	e a seje company	Art water		

< Dack

Finish

Help

Cancel

How to Generate KLE Certificates using XCA

istermal sense	Common serve	Denal	sol After	Tirest state	Envocation	Bry Cettificate
Aut were	KLE saver	03	2014-01-10 OMT	Trut inherited		Export
Att clientil	clien@1	63	2014-01-10 OMT	Trut inherited		Import
						Dow Details
						Depart
						Import ECC2012
						Import FEC2#7
						Pinis Yaw

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)

<u>Certificates to be imported to the viewer program on the client computer:</u> (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.

mosé saow	Connois same	(Perol	set Afre	Trut de	Beverates -	Sex Codeate
Per ant	RECA	01	2008-03-08 0 MT	Always Truted		Freed
Perit sheefil	deal0	8	204-01-10 OHT	Trat sheeted		
						Dev (while
						Dales
						Import 20C2912
						Impost PECIN7
						Han Yev
						A

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

Certificate export	,∧ e e≉
Please enter the fileneme for the certificate.	TuoyCA filename
Filename root cut	H
DER is a basery format of the Certificate PECM is a basef4 encoded Certificate PECDP7 is no official Certificate exchange format PECDP72 is an encrypted official Key-Certificate exch	enge Somet
Export Format 7EM	<u>.</u>

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.

Save Certificale as	2 🔀
Look ge: 🔄 C-Ringsam Filesbead	. * 🖬 🖝 🖽 🖿
inoten Herecal	
File game: [wover ort]	Save
His type: X509 Certificates (*ser *crt * p12)	• Centrel

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 ...

crtificate export	N.
Fiene sate the Simone for the certificate	TaryCA filenesse
Filesanoe mireraat	-
DER is a hissey format of the Certificate FEM is a basef4 sucoded Certificate FEC207 is an official Certificate on hunge format FEC20712 is an encrypted official Eco-Certificate on	hings format
Export Pornet FEM	2

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.

```
Appendix 1
```

in and the second se	2 🛛
Key export	(i)
Please enter the filename for the key.	
Filename (serverbey pem	
DER is a binary format of the key without encryption FEM is a base64 encoded key with optional encryption FKCS98 is an encrypted official Key-exchange format	
Export Formst FEM	
When exporting the private key it should be encrypted.	
F Export the private part of the Key too	
🔽 Encrypt the Key with a paraword	
Gancel	<u>QK</u>

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.

XCa		? 🛛
K Certifica		
lease enter the pass	word protecting the RSA private key	
Password	*****	
Password Repeat 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.

жса		2
Certific	cate export	
Please ent	er the filename for the certificate.	TinyCA filename
Filename	C:/Program Files/xca/client01.p12	
DER is a l	binary format of the Certificate	N
PEM is a l	base64 encoded Certificate	6
PKCS#7 i	s an official Certificate exchange format	
PKCS#12	is an encrypted official Key-Certificate exc	hange format
Export Fo	rmat PKCS #12	× 1
Cancel		ОК

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

<u>Certificates to be imported to the viewer program on the client computer:</u>
(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

<u>No Password</u> – 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. <u>Global Password</u> – the viewer will prompt you for a global password, which is used by all who want to make viewer connections to **KLE**.

<u>User Password</u> – 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.

<u>Global user password</u> : 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	User-specific
			Password	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) $% \left(\left({{{\rm{CD}}} \right)_{\rm{T}}} \right)$

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.)

