Certificates and Certification process

1. Certification Process

The certificates are delivered by the Certificates Authorities (CA). This is a 3-step process.

a) The generation of a Key Pair or Private Key in standard RSA 2048 bits. This key will be used to generate a CA Request based on it.

b) The CA Request generated is transmitted to the CA. It contains all the necessary information in order for the provider to deliver a certificate (Country Name 2 letters code, State or Province Full Name, Locality Name, Organization Name e.g. Company, Organization Unit Name e.g. Section, valid email address and Common Name (CN) e.g. MyDomainName.com).

c) The Certificate authority verifies the information you transmitted and returns the certificate, and eventually also intermediate certificates that are required to access your certificate.

The certificate also contains the CA Reply (the validated Private Key). Once you have the certificate, the CA reply, its key pair (private key), and the intermediates certificates, they must be imported in the key store handled by Terminal Service Plus.

2. The Certificates

The delivery usually contains several files. Each file is a certificate. As said previously, the authority delivers the certificate of your Domain name and intermediate Certificates that are mandatory to access to your certificate.

The common format file is .cer or .crt. These extensions are recognized by the OS which associates the certificate Icon.

Organize 💌 Include in library 💌 Share with 💌 New Folder						
	Name	Date modified	Type ^			
Computer	📄 cert.jks	30/03/2015 20:08	JKS File			
Local Disk (C:) My Web Sites on MSN	P. portecle	23/07/2012 02:26	PNG image			
	AddTrustExternalCARoot	30/05/2000 10:48	Security Certificate			
💶 Network	COMODORSAAddTrustCA	30/05/2000 10:48	Security Certificate			
1	COMODORSADomainValidationSecureServerCA	12/02/2014 00:00	Security Certificate			
	属 MyDomainName	29/03/2015 00:00	Security Certificate			

In our example above, we received 4 files (.crt). The first, second and third are intermediate certificates (CARoot, TrustCA, DomainValidationCA).

The fourth is our Certificate which certifies our domain name MyDomainName.crt. They all have to be installed together.

For a better understanding of how to proceed, let's examine the certificates.

3. Certificates Properties

The properties of the certificate CA Root show its path. Each certificate has a path from the root to the certificate of your domain name.

TS REMOTEACCESS

Certificate	×			
General Details Certification Path	1			
Certificate Information				
This certificate is intended for the following purpose(s):				
 Ensures the identity of a remote computer Proves your identity to a remote computer Protects e-mail messages Ensures software came from software publisher Protects software from alteration after publication Allows data to be signed with the current time 				
Issued to: COMODO RSA Certification Authority				
Issued by: AddTrust External CA Root				
Valid from 30/ 05/ 2000 to 30/ 05/ 2020				
Learn more about <u>certificates</u>	nent			
	ок			

TS REMOTEACCESS

Certificate	×
General Details Certification Path	
	1
Certification path	
COMODO RSA Certification Authority	
	Ulau Cartificata
	view Cercificate
Certificate status:	
This certificate is OK.	
Learn more about <u>certification paths</u>	
	ОК

Certificate 🗙				
General Details Certification Path				
Certificate Information				
This certificate is intended for the following purpose(s):				
Ensures the identity of a remote computer Proves your identity to a remote computer				
* Refer to the certification authority's statement for details.				
Issued to: www.setting.com				
Issued by: COMODO RSA Domain Validation Secure Server CA				
Valid from 29/03/2015 to 29/03/2016				
Install Certificate Issuer Statement Learn more about <u>certificates</u>				
ОК				

Certification Path	ity on Secure Server CA M
Certification path USERTrust COMODO RSA Certification Authori COMODO RSA Domain Validatio	ity on Secure Server CA M
COMODO RSA Certification Authori COMODO RSA Certification Authori COMODO RSA Domain Validatio	ity on Secure Server CA M
	View Certificate
Certificate status:	
This certificate is OK.	
earn more about certification paths	

The properties of our certificate show all the general informations about the certificate (purposes, addresses, issued to CN), issued by and validity.

What is important to notice is the certification path. It includes the entire path needed to access our certificate. It displays all the intermediate certificates that are included inside ours.

This is a simple process. You must import this entire certification path, plus the Key Pair in the Terminal Service Plus Key store file.

Use Windows certificate manager to import keypair and all certificates into Windows keystore as described in Certificates and Certification process (make keypair exportable when importing!) and then export that key back from Windows keystore by checking the option "Include all certificates in the certification path if possible". For the format choose per example *.p12 Now create a new keystore in JKS format on Portecle, and go to Tools>Import Key Pair and import that *.p12 file:

TO	TSPLUS	Remote Access Management Console			
命 	HOME APPLICATIONS PRINTER	Generate a free valid HTTPS certificate Image: Senerate a free valid HTTPS certificate Image: Senerate a free valid HTTPS certificate Image: Senerate a free valid HTTPS certificate			
S	WEB Web Portal HTTPS	Image: C.\Program Files (x86)\TSplus\Clients\webserver\key* - Portecle — Elle Iools Examine Help Image: Clients Webserver\key* @ Image: Clients Webserver\key* - Portecle Image: Clients Webserver\key* @ Image: Clients Webserver\key* - Portecle —	п	×	
∎⊡	Web Server	Alias Name Last Modified key.p12			
୦ ୧୦	SYSTEM TOOLS				
න ස	ADVANCED ADD-ONS				
ন্ত	LICENSE	Keystore type: PKCS #12, provider: BC, size: 1 entry			

4. Important notice about the Key Pair (Private Key)

The key Pair is the RSA 2048 Bit key generated for the CA Request of the certificate. It has been generated either in the Portecle add-on we provide, or with another available generator like openssl, IIS, online sites, or CA provider's applications.

You must keep this Private Key. It is either a flat file text format unsecured .pem or a secured format .p12 or .pfx. The Private Key generated is mandatory to be able to generate the certificates correctly.

Back to HTTPS, SSL & Certificates Tutorial Summary