



Securing Connections with Digital Certificates in Router OS

By

Ezugu Magnus

PDS Nigeria

About the Presenter

MikroTik Certifications

- Mikrotik Certified Engineer
(MTCNA,MTCRE,MTCWE,MTCTCE,MTCUME,MTCINE)
- Mikrotik Certified Consultant
- Mikrotik Certified Trainer

My Contact details:

- Email: magnus@pdsng.com
- Skype: ezugumc
- Whatsapp: +234-8174604060

Introduction to Digital Certificate

What is a Digital Certificate?

It is an electronic file which enables a secure exchange of information over a network and used to prove the ownership of a public key and identify an entity.

It contains the following information:

- Name of the certificate holder
- Serial Number
- Expiration date
- Name of the issuer
- Copy of the holders public key
- Digital signature of issuer

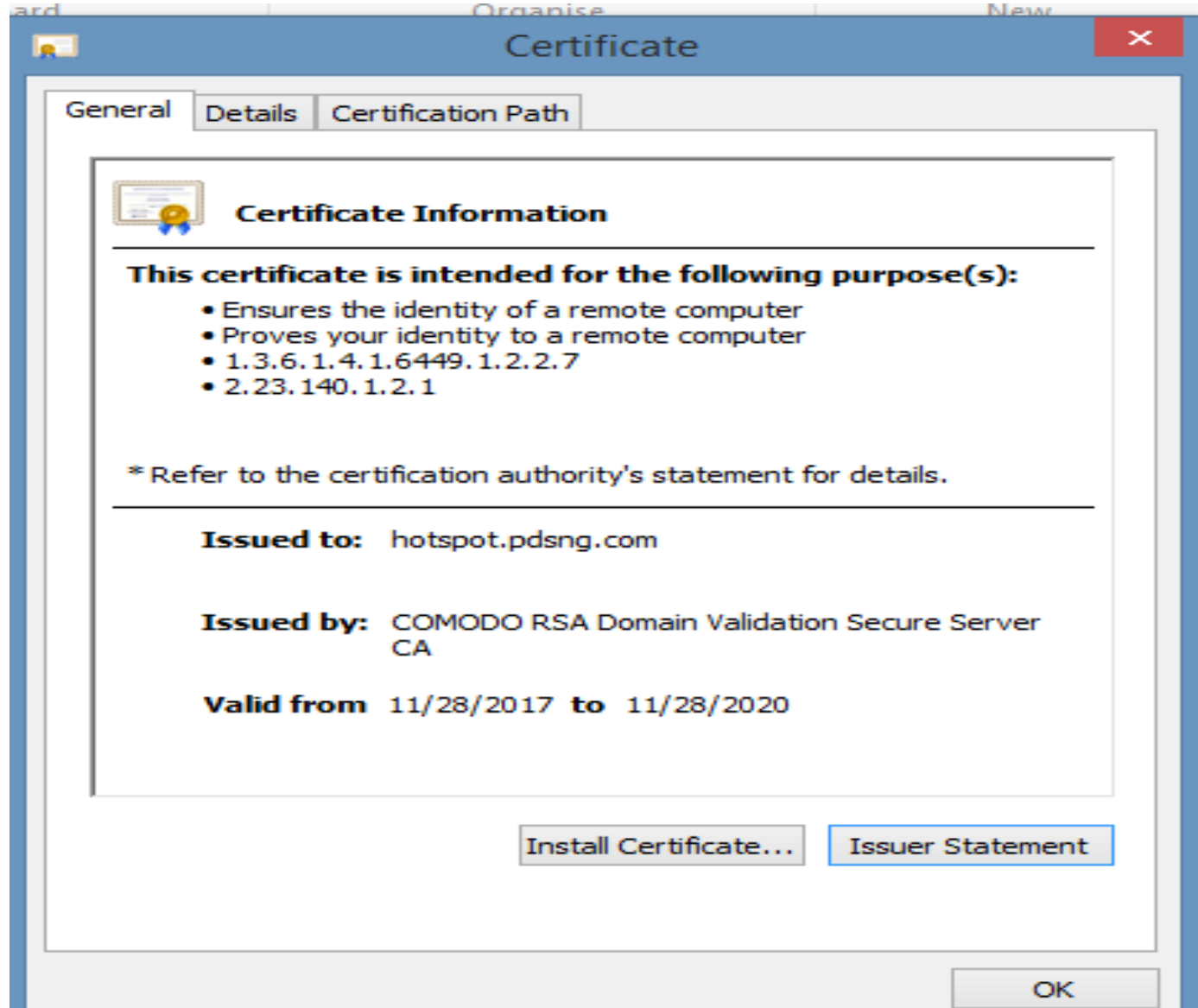
Introduction to Digital Certificate

What is a Digital Certificate?



Introduction to Digital Certificate

What is a Digital Certificate?



Introduction to Digital Certificate

What is a Digital Certificate?

In addition to the identification information, the digital certificate also has the following:

- A public key

- Digital signature

Introduction to Digital Certificate

Why do we need certificate:

1. Encryption

- A way of hiding the data from public view

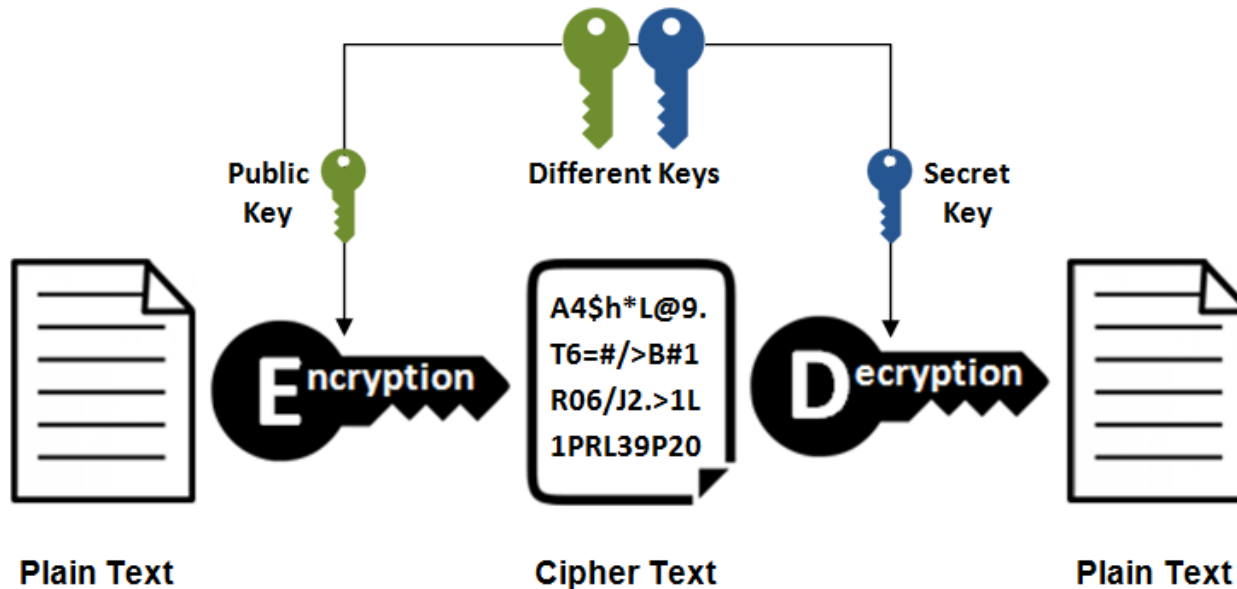
2. Identification & trust

- A way of identifying the recipient of data and confirming if it is trusted

Introduction to Digital Certificate

Two types of Encryption:

Asymmetric Encryption



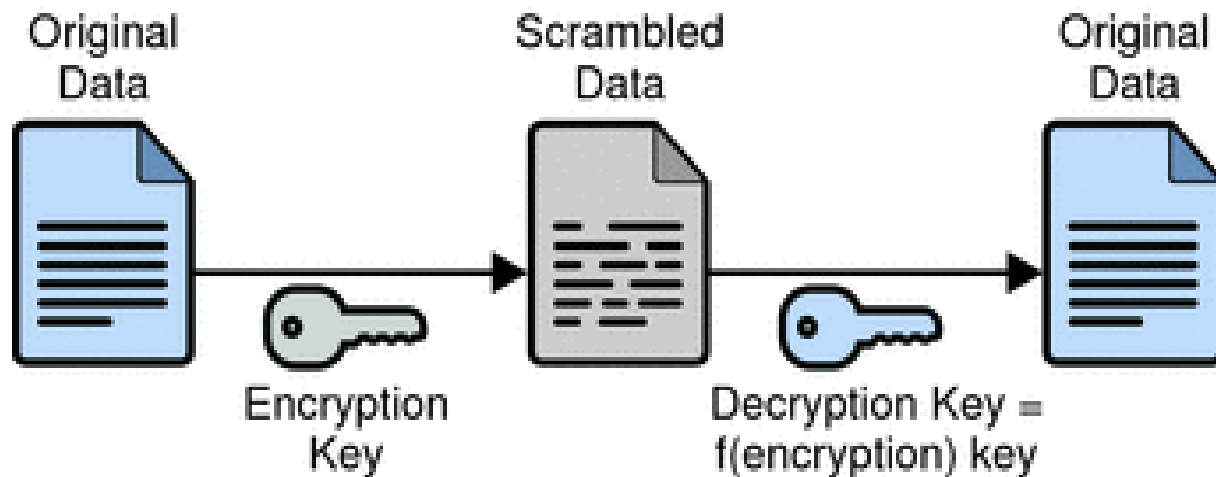
- Larger key size (typically 2048 bits)
- Very slow encoding and decoding process

Courtesy ssl2buy.com

Introduction to Digital Certificate

Two types of Encryption:

Symmetric encryption



- Small key size (typically 256bits)
- Fast encoding and decoding

Introduction to Digital Certificate

Identification & trust

There are various schemes for issuance of a digital certificate which helps to certify the identity and establish trust in the system.

- Public key infrastructure scheme: Here the certificate issuer is the Certificate Authority (CA).
- Web of trust scheme: In this scheme, individual certificate owners sign each others keys directly.

Introduction to Digital Certificate

How does SSL work?



1. **Client** connects to a server secured with SSL. Client requests that the server identify itself.
2. **Server** sends a copy of its SSL Certificate, including the server's public key.
3. **Client** checks the certificate root against a list of trusted CAs and that the certificate is unexpired, unrevoked, and that its common name is valid for the server that it is connecting to. If the client trusts the certificate, it creates, encrypts, and sends back a symmetric session key using the server's public key.
4. **Server** decrypts the symmetric session key using its private key and sends back an acknowledgement encrypted with the session key to start the encrypted session.
5. **Server** and **Client** now encrypt all transmitted data with the session key.

Introduction to Digital Certificate

SSL Client Certificate

This is used to authenticate a client or device connecting to a server. Since authentication is managed by service provider, these certificates are usually issued by the provider for VPN tunnel and not a public CA

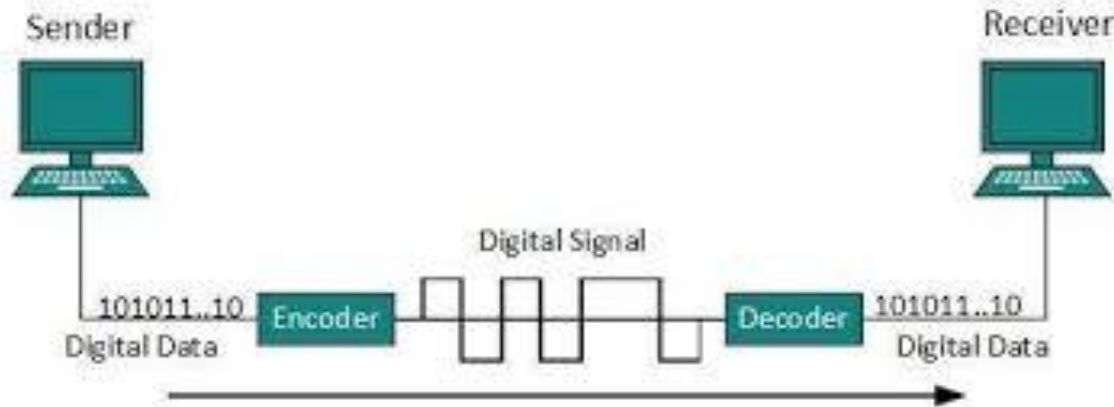
SSL Server Certificate

In SSL, when a client attempts to connect to a server, the server is required to present a certificate in a handshake process. Client checks the certificate and verifies if it is signed by a trusted CA.

Significance of connection security

Data protection

Raw digital data without encryption.

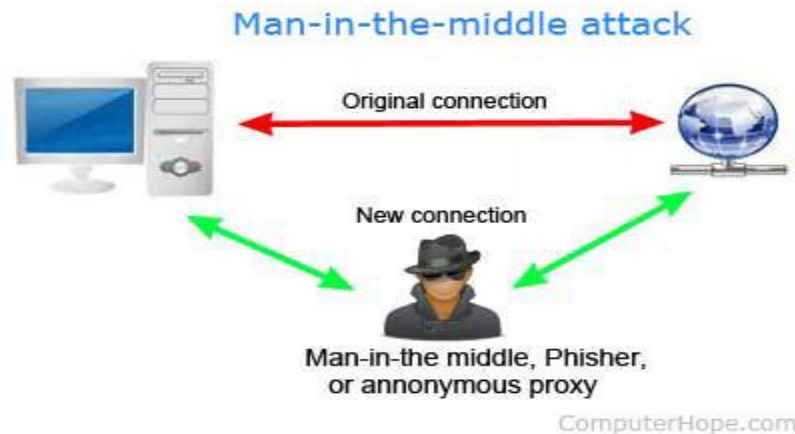


In the absence of SSL or any form of encryption, data is sent as stream of 1s and 0s in a universal encoding format.

Significance of connection security

Data protection

- Data go through various un-trusted networks while moving from source to destination
- Evil people can easily listen in and view the conversation in clear text. These are known as man in the middle.



- The man in the middle can read/store the data and possibly modify traffic between the source and destination
- Attacker can have access to sensitive information such as credit card details if sent through such communication medium.

Significance of connection security

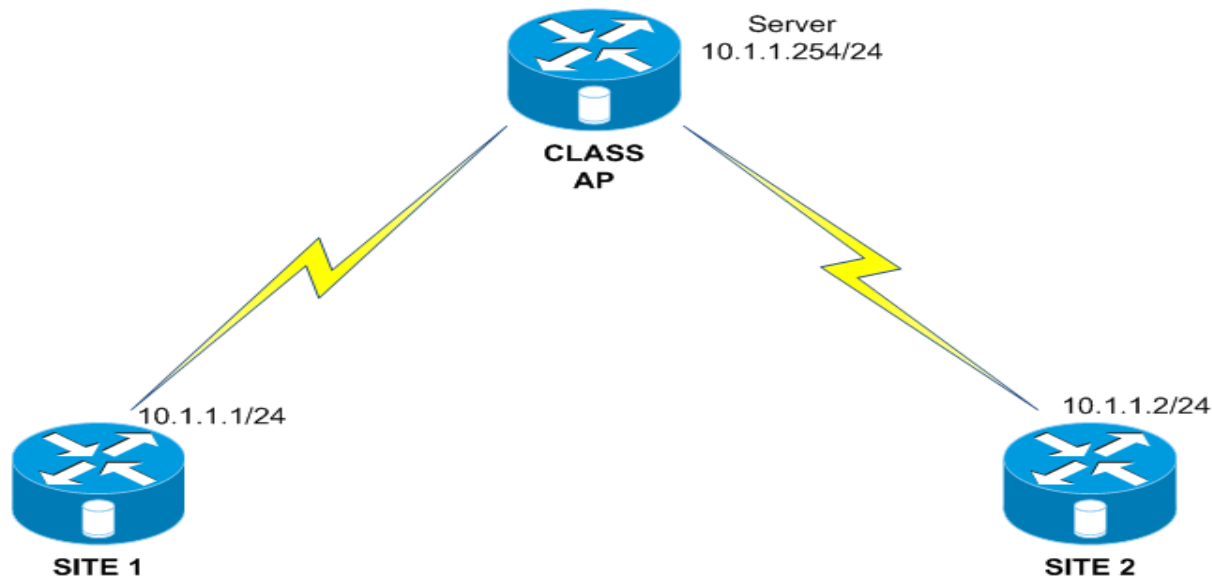
Attack mitigation

- With SSL, this will hardly happen, or practically will take a massive computational capacity to break the keys to decrypt the data.
- The use of digital certificates will eliminate the possibility of man in the middle attack as such attackers will have a tough time breaking the connection between a source and the destination devices.
- The use of certificates on CAP to CapsMan connections will eliminate the possibility of having a rogue Access Point on a network which in-turns reduces the possibility of an attacker eavesdropping or impersonating a wireless user.

Creating certificates in RouterOs

1. Make certificate templates
2. Sign the certificates and add CRL url
3. Export client certificates with keys and CA certificates and import to client routers

Network Topology:



Creating certificates in RouterOs

Make certificate templates: CA Template

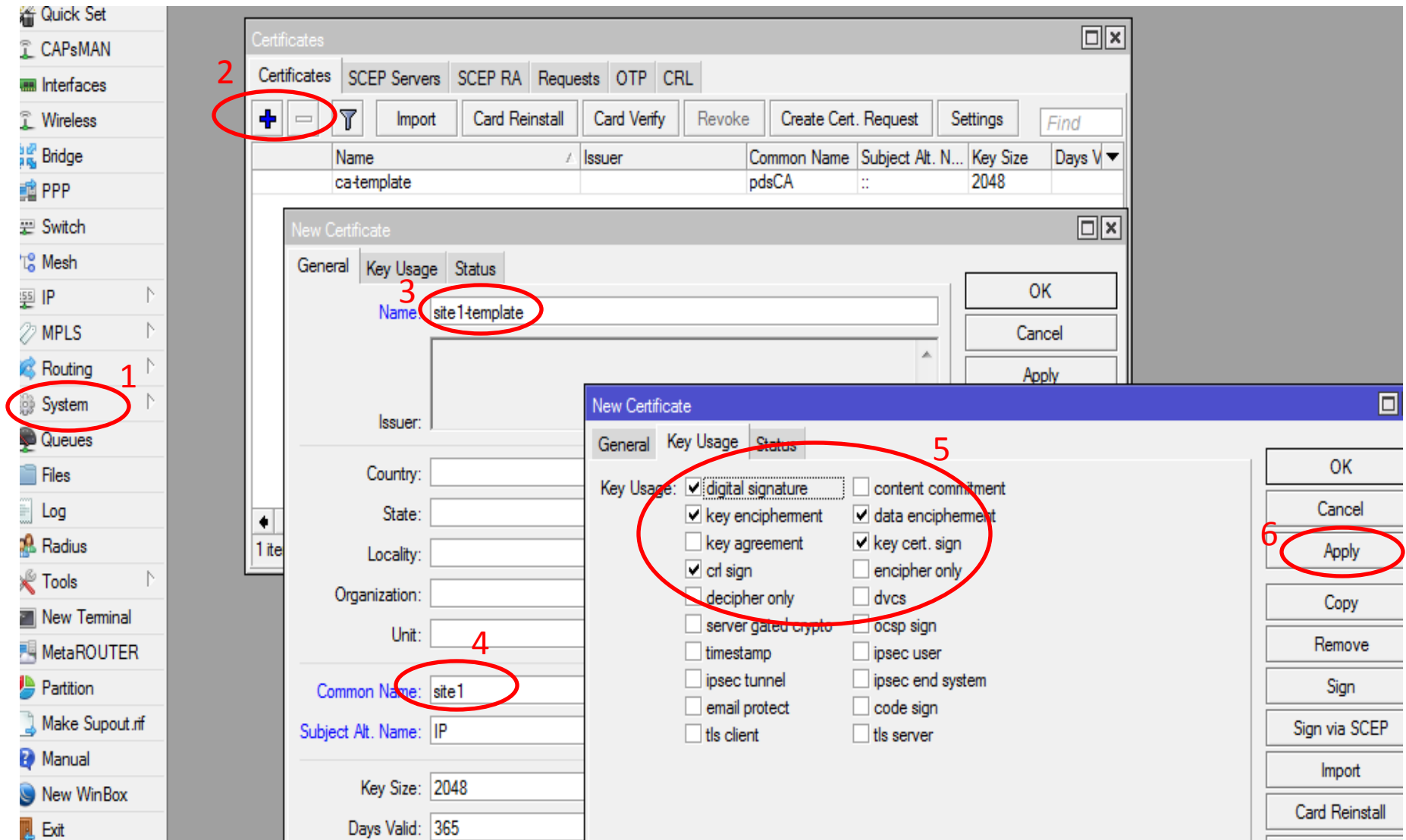
The image shows the MikroTik WinBox interface with several windows and menu items highlighted by red circles and numbered 1 through 8, illustrating the steps to create a CA template certificate.

- 1:** The **System** menu item in the left sidebar is highlighted.
- 2:** The **Certificates** sub-menu item is highlighted.
- 3:** The **+** button in the Certificates window is highlighted.
- 4:** The **Name** field in the **New Certificate** window is highlighted, containing the text **ca-template**.
- 5:** The **Common Name** field in the **New Certificate** window is highlighted, containing the text **pdsCA**.
- 6:** The **Key Usage** section in the **New Certificate** window is highlighted, showing the **crf sign** checkbox checked.
- 7:** The **key cert. sign** checkbox in the **Key Usage** section is highlighted.
- 8:** The **OK** button in the **New Certificate** window is highlighted.

The **Certificates** window shows tabs for Certificates, SCEP Servers, SCEP RA, Requests, OTP, and CRL. The **New Certificate** window has tabs for General, Key Usage, and Status. The **Key Usage** section includes checkboxes for digital signature, key encipherment, key agreement, crf sign, decipher only, server gated crypto, timestamp, ipsec tunnel, email protect, tls client, content commitment, data encipherment, key cert. sign, encipher only, dvcs, ocsp sign, ipsec user, ipsec end system, code sign, and tls server.

Creating certificates in RouterOs

Make certificate templates: Site1 Template

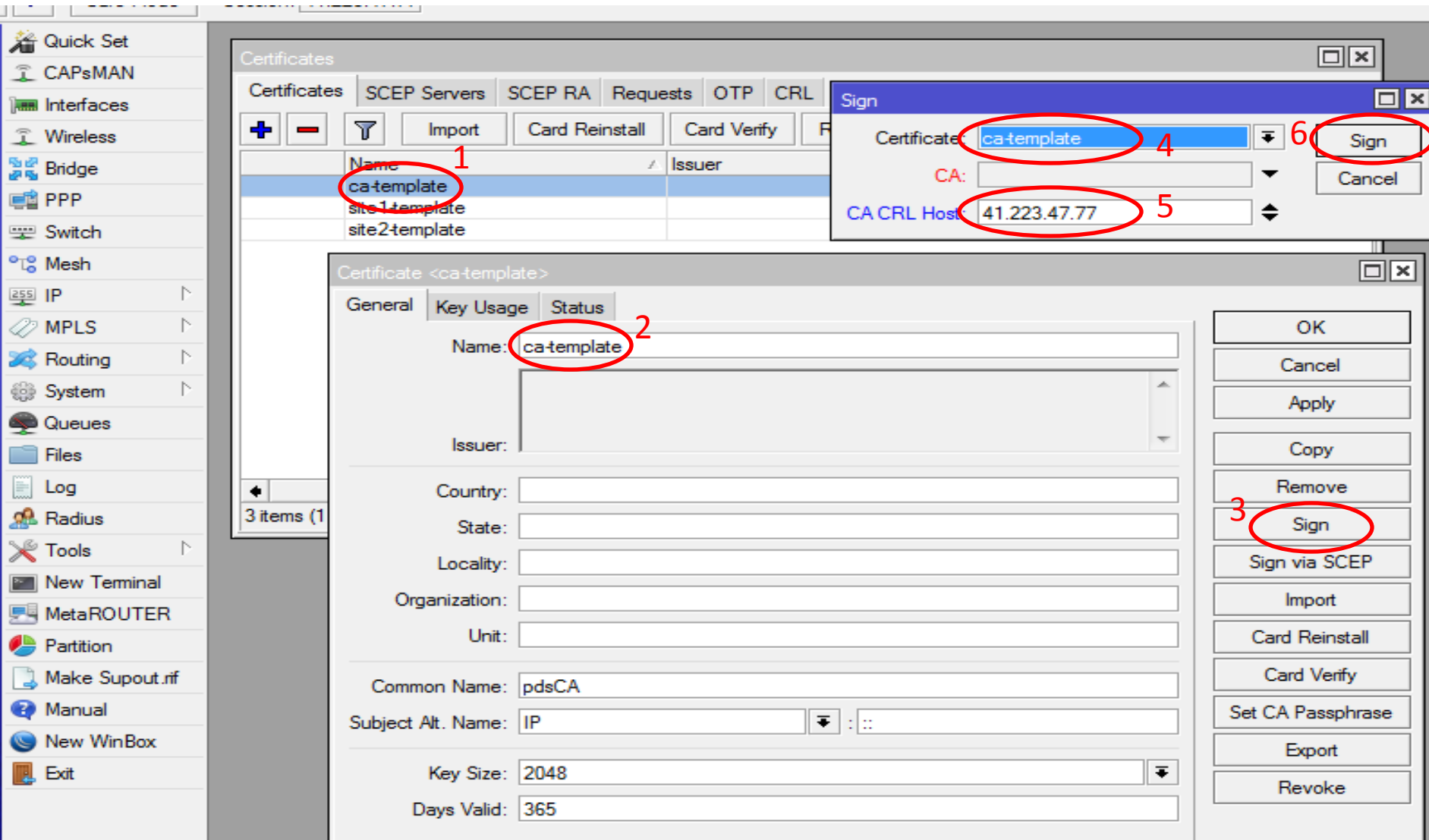


The screenshot illustrates the steps to create a certificate template in MikroTik WinBox:

- 1**: The **System** menu is selected in the left sidebar.
- 2**: The **Certificates** window is open, showing a list of certificates. The **+** button is highlighted to add a new certificate.
- 3**: The **New Certificate** dialog is open, showing the **General** tab. The **Name** field is set to **site1-template**.
- 4**: The **Common Name** field is set to **site1**.
- 5**: The **Key Usage** tab is selected, showing various options. The **digital signature** option is checked.
- 6**: The **Apply** button is highlighted to save the certificate template.

Creating certificates in RouterOs

Sign the CA certificate and add CRL url



The screenshot displays the MikroTik WinBox interface for managing certificates. The left sidebar shows the navigation menu with options like Quick Set, CAPsMAN, Interfaces, Wireless, Bridge, PPP, Switch, Mesh, IP, MPLS, Routing, System, Queues, Files, Log, Radius, Tools, New Terminal, MetaROUTER, Partition, Make Supout.rtf, Manual, New WinBox, and Exit.

The main window is titled 'Certificates' and contains a table with columns 'Name' and 'Issuer'. The table lists three items: 'ca-template', 'site1-template', and 'site2-template'. The 'ca-template' entry is highlighted, and a red circle with the number 1 is around it.

A 'Sign' dialog box is open, showing the 'Certificate' field with 'ca-template' (4) and the 'CA CRL Host' field with '41.223.47.77' (5). The 'Sign' button is circled in red with the number 6.

The 'Certificate <ca-template>' window is also open, showing the 'Name' field with 'ca-template' (2). The 'Sign' button in this window is circled in red with the number 3.

Other fields in the 'Certificate <ca-template>' window include 'Issuer', 'Country', 'State', 'Locality', 'Organization', 'Unit', 'Common Name' (pdsCA), 'Subject Alt. Name' (IP), 'Key Size' (2048), and 'Days Valid' (365).

Creating certificates in RouterOs

Make certificate templates: Server Template

The screenshot shows the MikroTik WinBox interface for creating a certificate template. The 'Certificates' tab is active, displaying a table of existing certificates:

Name	Issuer	Common Name	Subject Alt. N...	Key Size	Days V
KLAT	pdsCA	pdsCA	::	2048	
site1-template		site1	::	2048	
site2-template		site2	::	2048	

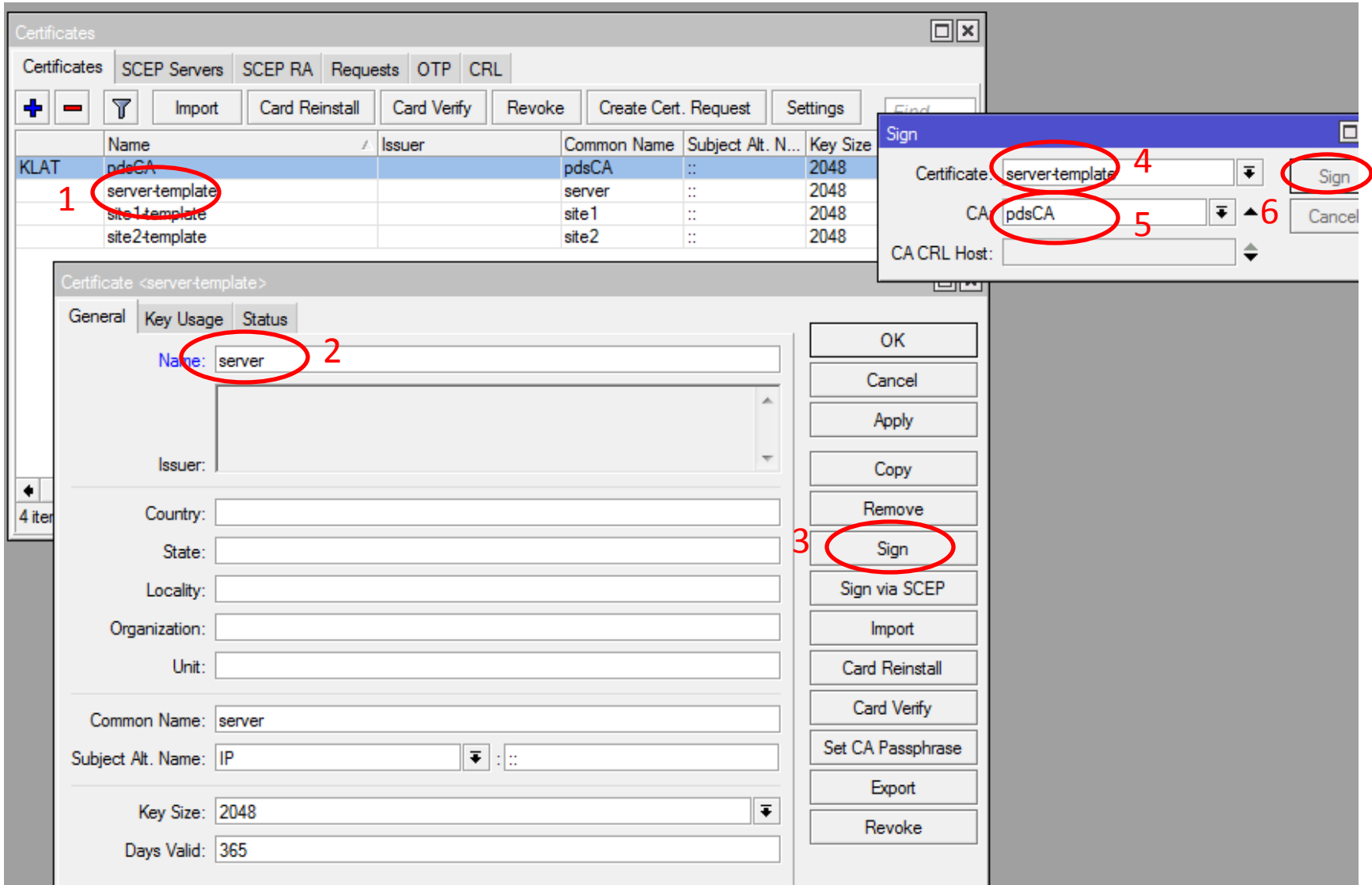
The 'New Certificate' dialog box is open, showing the 'General' tab. The 'Name' field is set to 'server-template'. The 'Common Name' field is set to 'server'. The 'Key Usage' section is checked for 'digital signature', 'key encipherment', 'key agreement', 'crl sign', 'data encipherment', and 'key cert. sign'. The 'Apply' button is highlighted.

Numbered steps in the image:

1. Clicking 'System' in the sidebar.
2. Clicking the '+' button in the 'Certificates' tab.
3. Entering 'server-template' in the 'Name' field.
4. Entering 'server' in the 'Common Name' field.
5. Selecting 'digital signature', 'key encipherment', 'key agreement', 'crl sign', 'data encipherment', and 'key cert. sign' in the 'Key Usage' section.
6. Clicking the 'Apply' button.

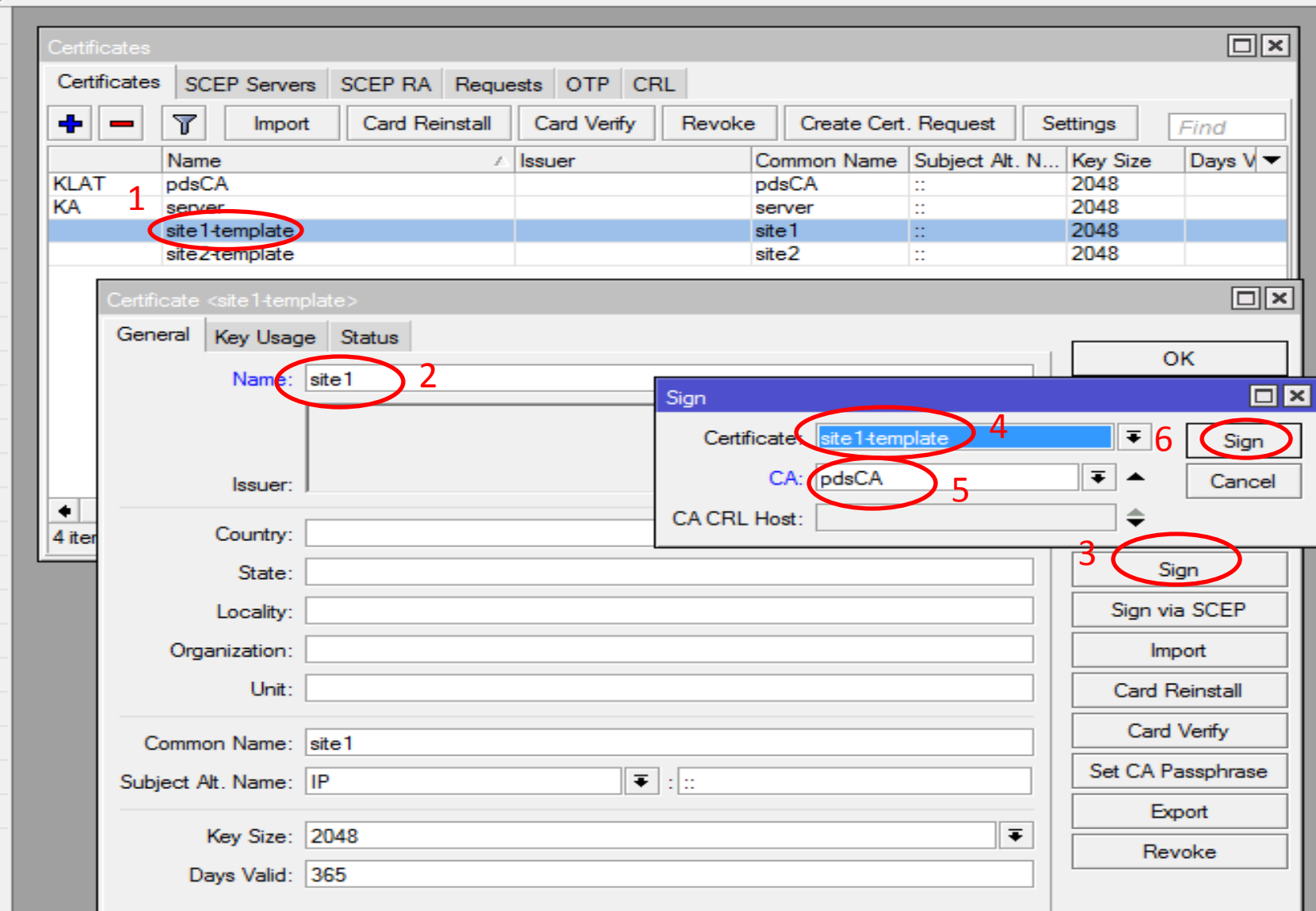
Creating certificates in RouterOs

Sign certificate templates: Server Template



Creating certificates in RouterOs

Sign certificate templates: Site1 Template



Creating certificates in RouterOs

Sign certificate templates: Site2 Template

The screenshot shows the RouterOS 'Certificates' window. The 'Certificates' tab is active, displaying a list of certificates. The 'site2-template' certificate is selected, indicated by a red circle and the number 1. The 'Sign' dialog is open, showing the 'Certificate' field set to 'site2-template' (red circle 4) and the 'CA' field set to 'pdsCA' (red circle 5). The 'Sign' button in the dialog is circled in red (red circle 6). The 'General' tab of the certificate details is visible, showing the 'Name' field set to 'site2' (red circle 2). The 'Issuer' field is empty. The 'Common Name' is 'site2', and the 'Subject Alt. Name' is 'IP'. The 'Key Size' is '2048' and the 'Days Valid' is '365'. The 'Sign' button in the main window is also circled in red (red circle 3).

	Name	Issuer	Common Name	Subject Alt. N...	Key Size	Days V
KLAT	pdsCA		pdsCA	::	2048	
KA	server		server	::	2048	
KA	site1		site1	::	2048	
	site2-template		site2	::	2048	

Certificate <site2-template>

General | Key Usage | Status

Name: site2

Issuer:

Country:

State:

Locality:

Organization:

Unit:

Common Name: site2

Subject Alt. Name: IP

Key Size: 2048

Days Valid: 365

Sign

Certificate: site2-template

CA: pdsCA

CA CRL Host:

Sign

Copy

Remove

Sign

Sign via SCEP

Import

Card Reinstall

Card Verify

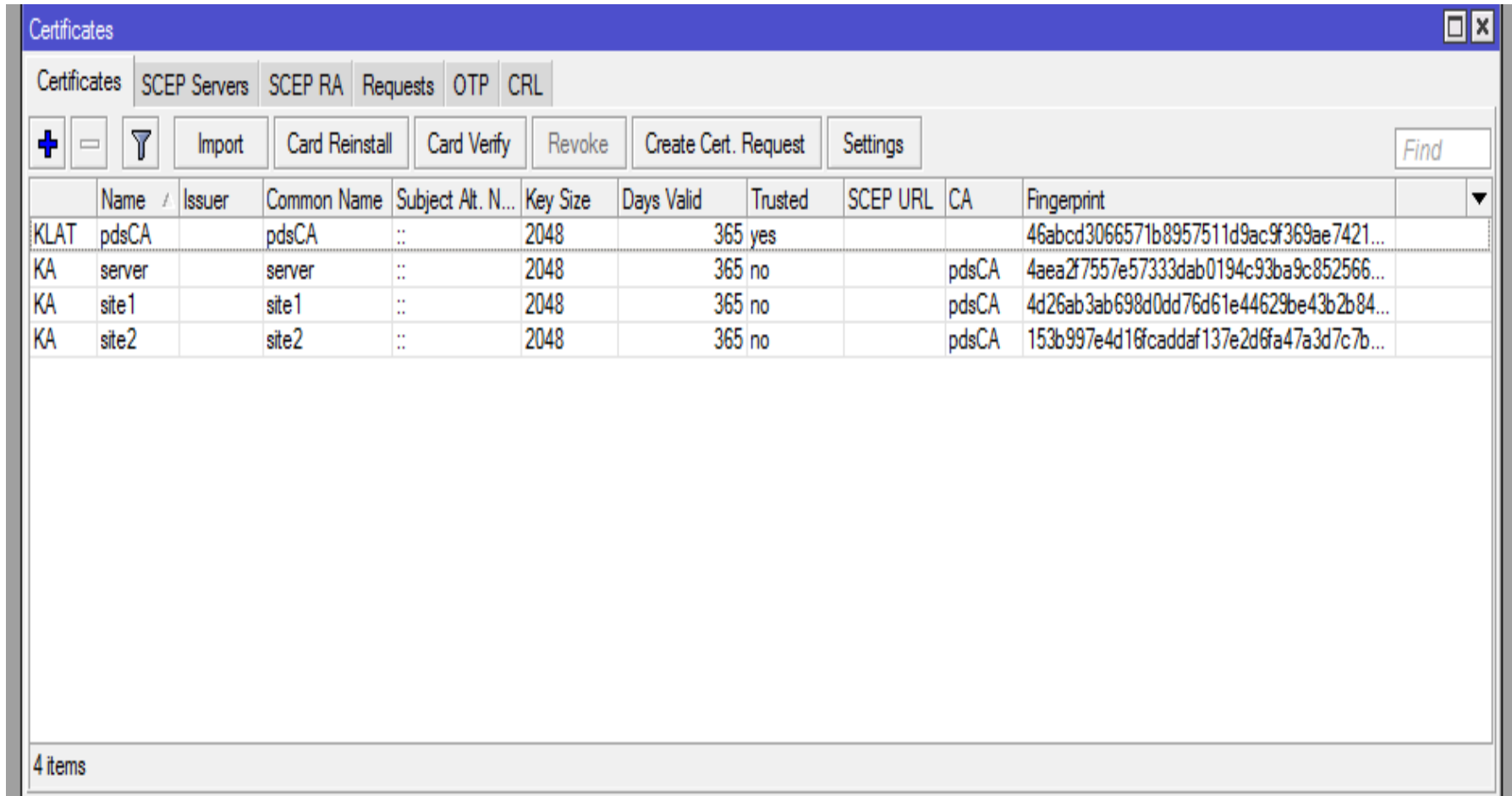
Set CA Passphrase

Export

Revoke

Creating certificates in RouterOs

The results after creating and signing certificate



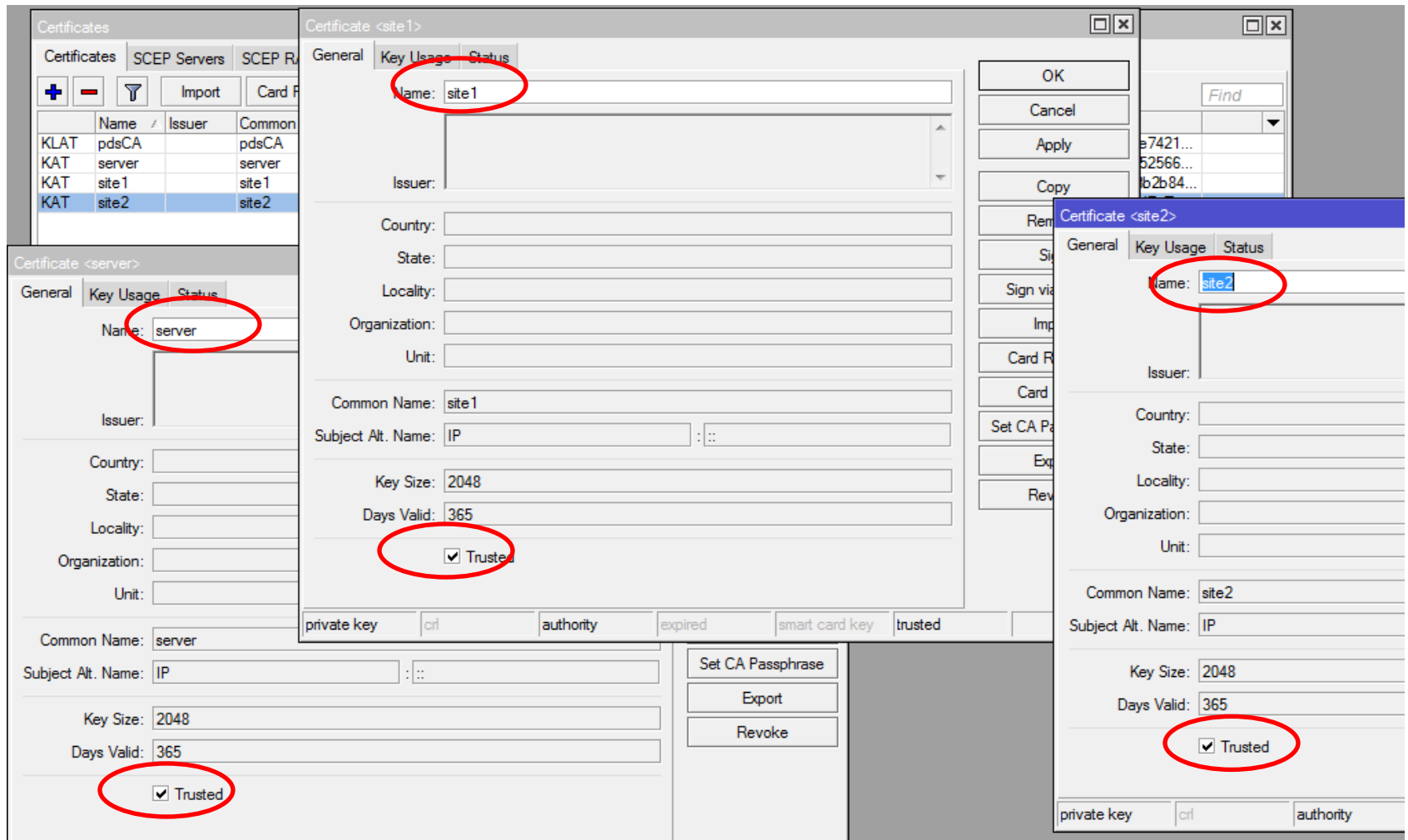
The screenshot shows the 'Certificates' window in RouterOS. The window has a title bar 'Certificates' and a menu bar with 'Certificates', 'SCEP Servers', 'SCEP RA', 'Requests', 'OTP', and 'CRL'. Below the menu bar is a toolbar with buttons: '+', '-', a funnel icon, 'Import', 'Card Reinstall', 'Card Verify', 'Revoke', 'Create Cert. Request', and 'Settings'. There is also a 'Find' search box. The main area contains a table with the following columns: Name, Issuer, Common Name, Subject Alt. N..., Key Size, Days Valid, Trusted, SCEP URL, CA, and Fingerprint. The table lists four certificates: KLAT (issuer pdsCA, common name pdsCA, trusted yes), KA server (issuer pdsCA, common name server, trusted no), KA site1 (issuer pdsCA, common name site1, trusted no), and KA site2 (issuer pdsCA, common name site2, trusted no). The status bar at the bottom indicates '4 items'.

Name	Issuer	Common Name	Subject Alt. N...	Key Size	Days Valid	Trusted	SCEP URL	CA	Fingerprint
KLAT	pdsCA	pdsCA	::	2048	365	yes			46abcd3066571b8957511d9ac9f369ae7421...
KA server		server	::	2048	365	no		pdsCA	4aea2f7557e57333dab0194c93ba9c852566...
KA site1		site1	::	2048	365	no		pdsCA	4d26ab3ab698d0dd76d61e44629be43b2b84...
KA site2		site2	::	2048	365	no		pdsCA	153b997e4d16fcaddaf137e2d6fa47a3d7c7b...

4 items

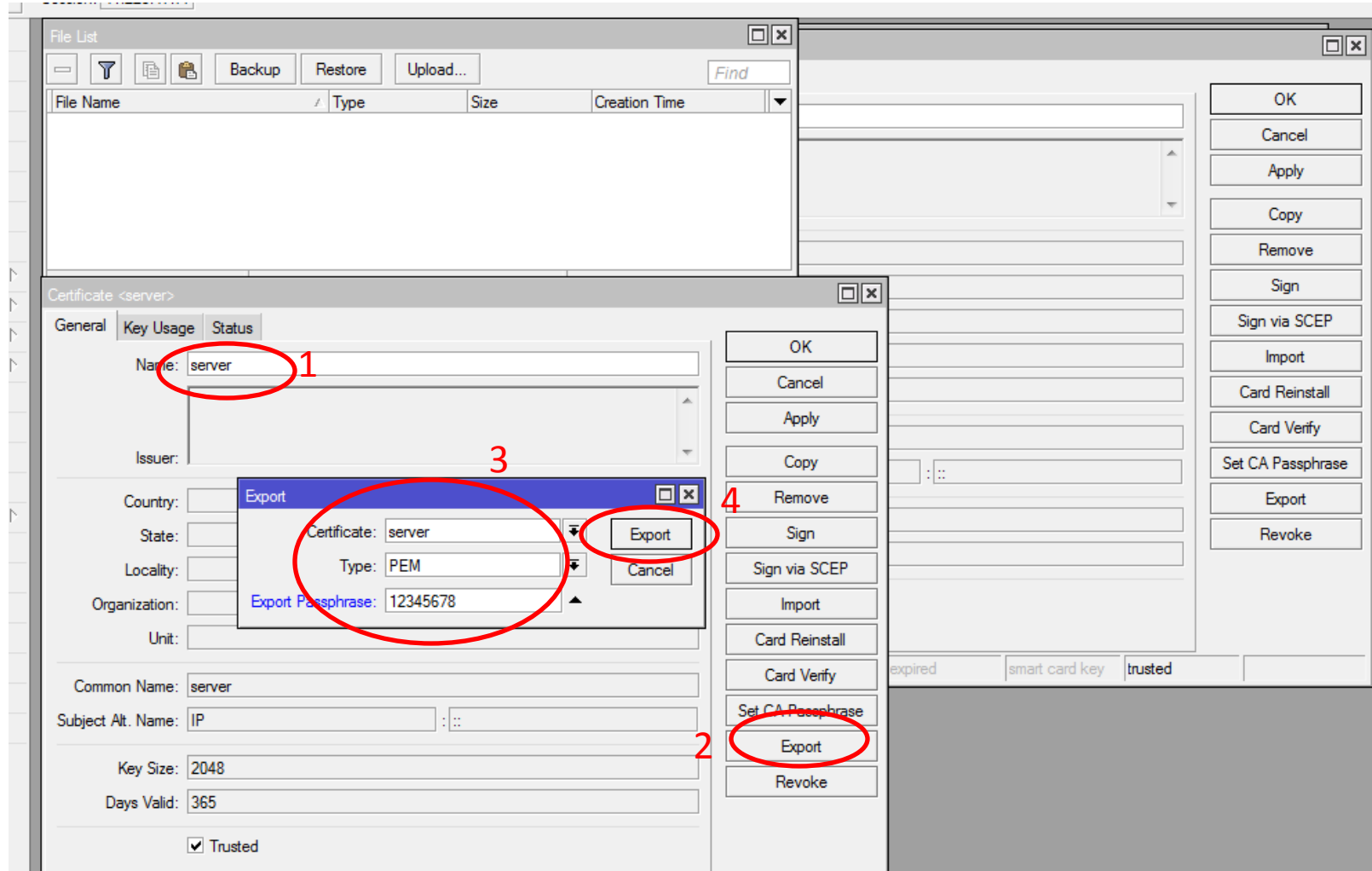
Creating certificates in RouterOs

Set all certificates as Trusted



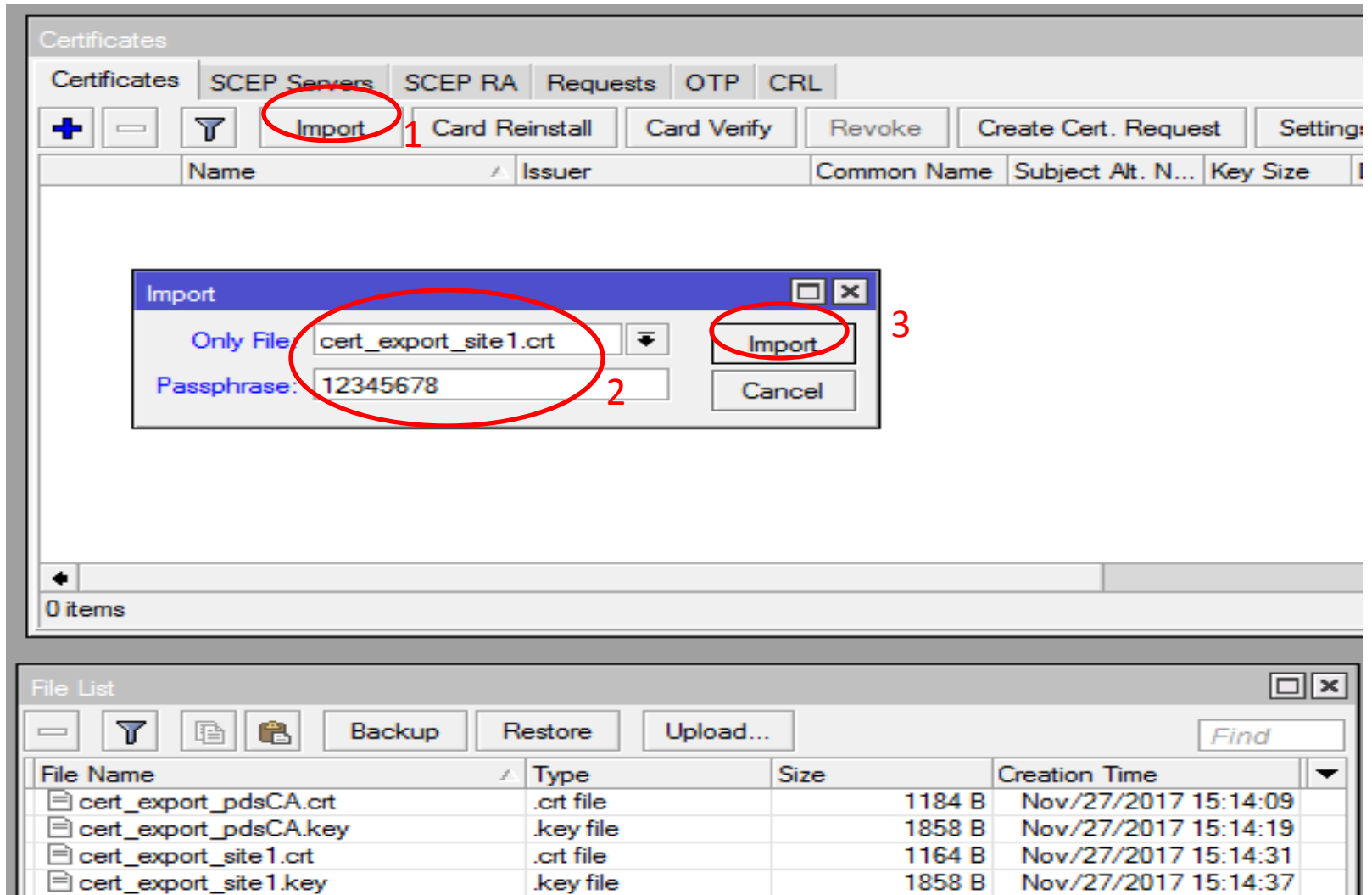
Creating certificates in RouterOs

Export client certificates with keys and CA certificates and import to client routers



Creating certificates in RouterOs

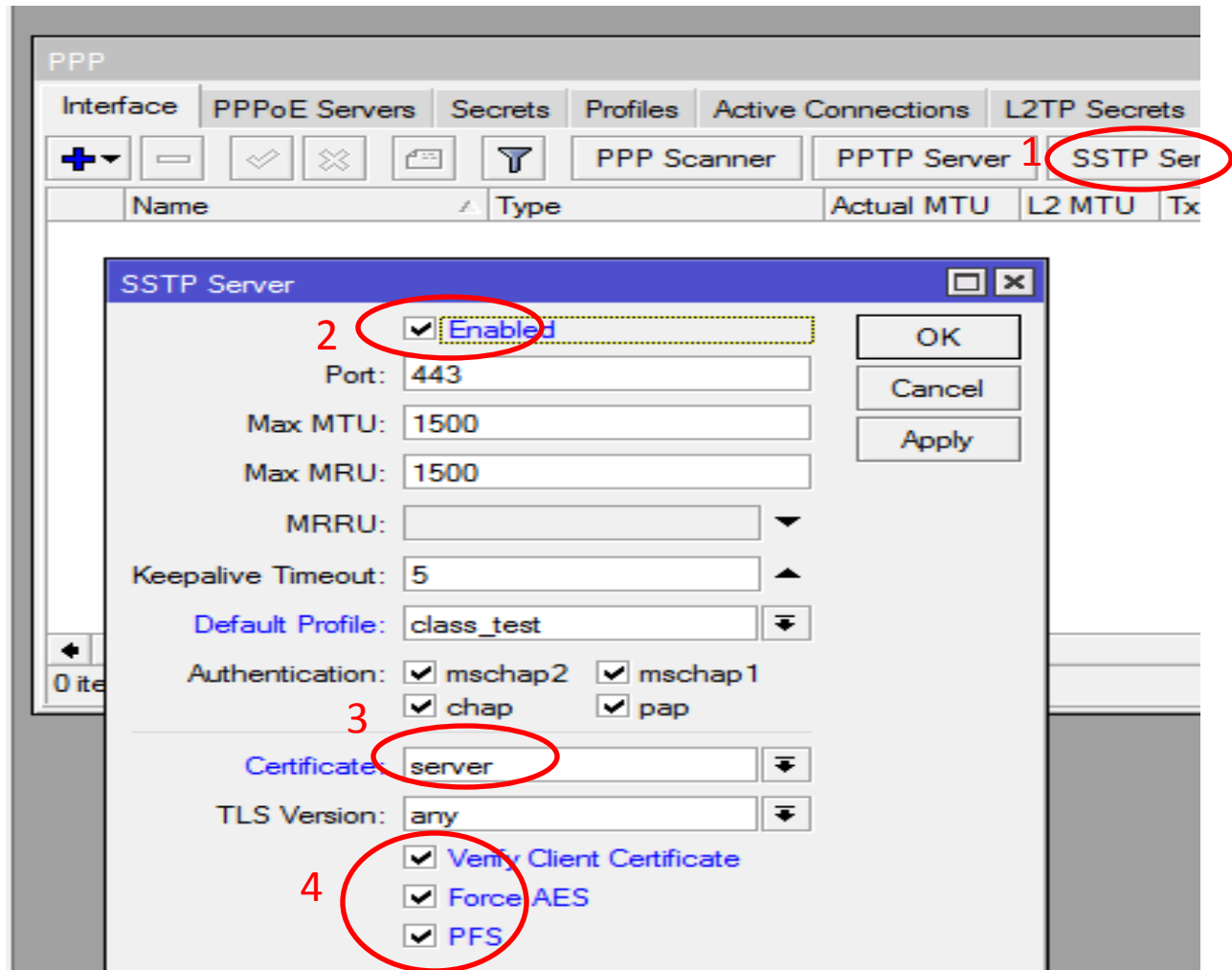
Import client certificates with keys and CA certificates on site1 and site2.



Deploying digital certificates

Using Digital Certificates on SSTP tunnels

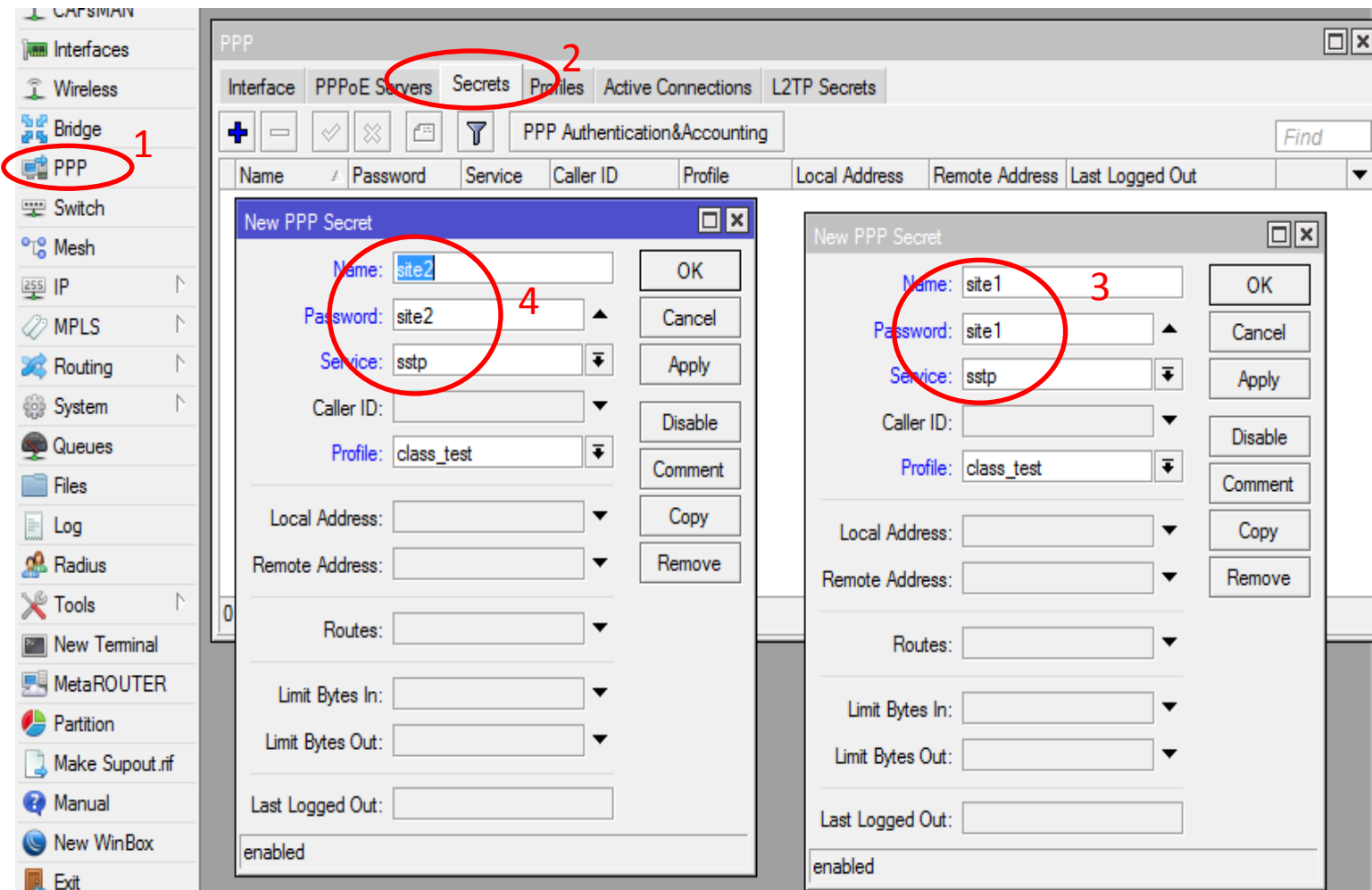
Enable SSTP Server to use Certificate



Deploying digital certificates

Using Digital Certificates on SSTP tunnels

Create credentials for site1 and site2 on SSTP Server



Deploying digital certificates

Using Digital Certificates on SSTP tunnels

Add SSTP client on site1 as below.

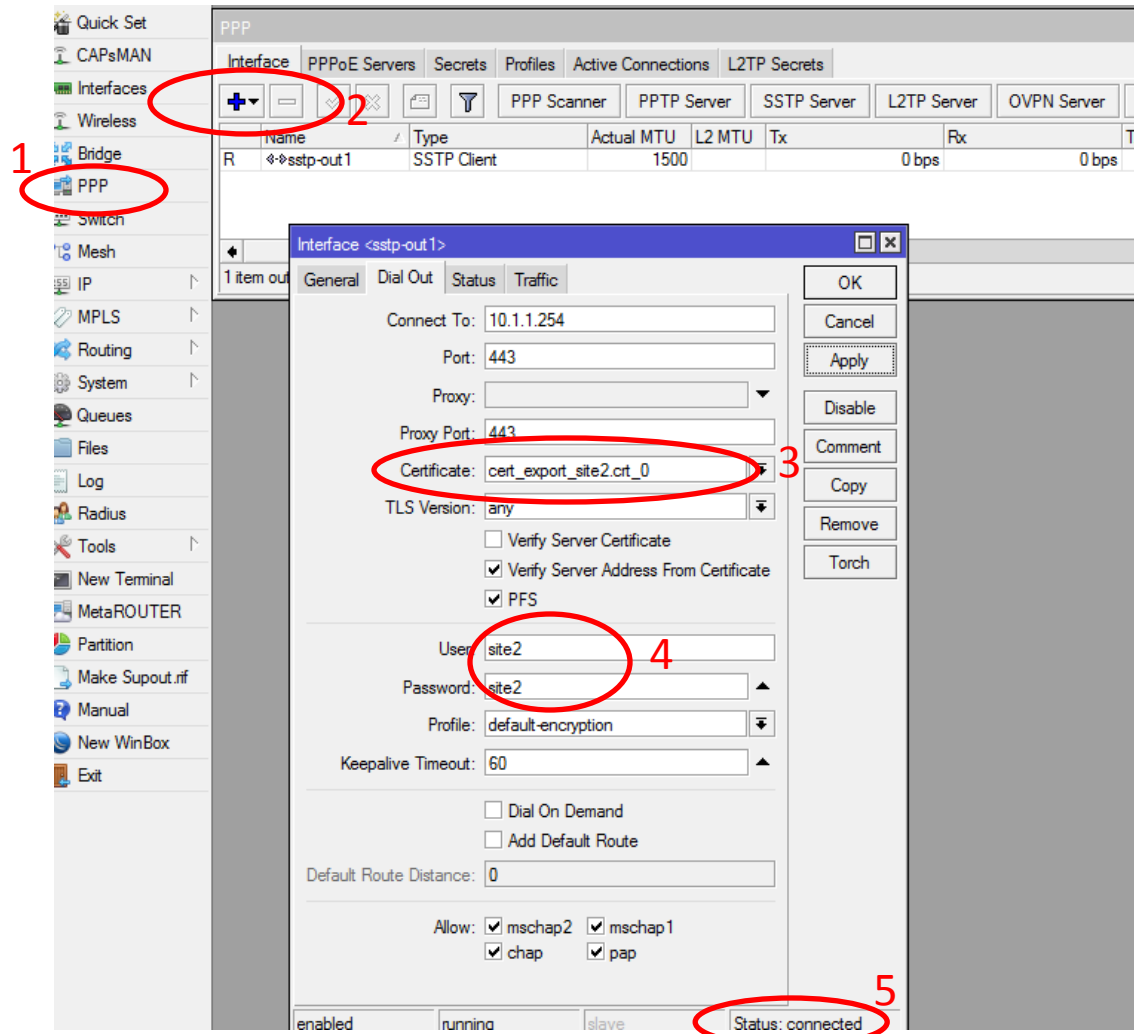
The screenshot displays the MikroTik WinBox interface. On the left sidebar, the 'PPP' menu item is circled in red and labeled with a red '1'. The main window shows the 'Interface <ssstp-out1>' configuration tab. The 'General' sub-tab is active, showing the following settings: 'Connect To' is 10.1.1.254, 'Port' is 443, 'Proxy' is empty, 'Proxy Port' is 443, 'Certificate' is cert_export_site1.crt_0 (circled in red and labeled with a red '3'), 'TLS Version' is any, 'Verify Server Certificate' is unchecked, 'Verify Server Address From Certificate' is checked, 'PFS' is checked, 'User' is site1 (circled in red and labeled with a red '4'), 'Password' is site1, 'Profile' is default-encryption, 'Keepalive Timeout' is 60, 'Dial On Demand' is unchecked, 'Add Default Route' is unchecked, 'Default Route Distance' is 0, and 'Allow' has checkboxes for mschap2, mschap1, chap, and pap, all of which are checked. At the bottom of the configuration window, the status is shown as 'enabled', 'running', 'slave', and 'Status: connected' (circled in red and labeled with a red '5'). Below the configuration window, the 'PPP' section is visible, with the 'Interface' tab selected. A red circle labeled with a red '2' highlights the '+' button in the interface list. The table below shows the configuration for the SSTP client.

Name	Type	Actual MTU	L2 MTU	Tx	Rx
R sstp-out1	SSTP Client	1500		0 bps	0 bps

Deploying digital certificates

Using Digital Certificates on SSTP tunnels

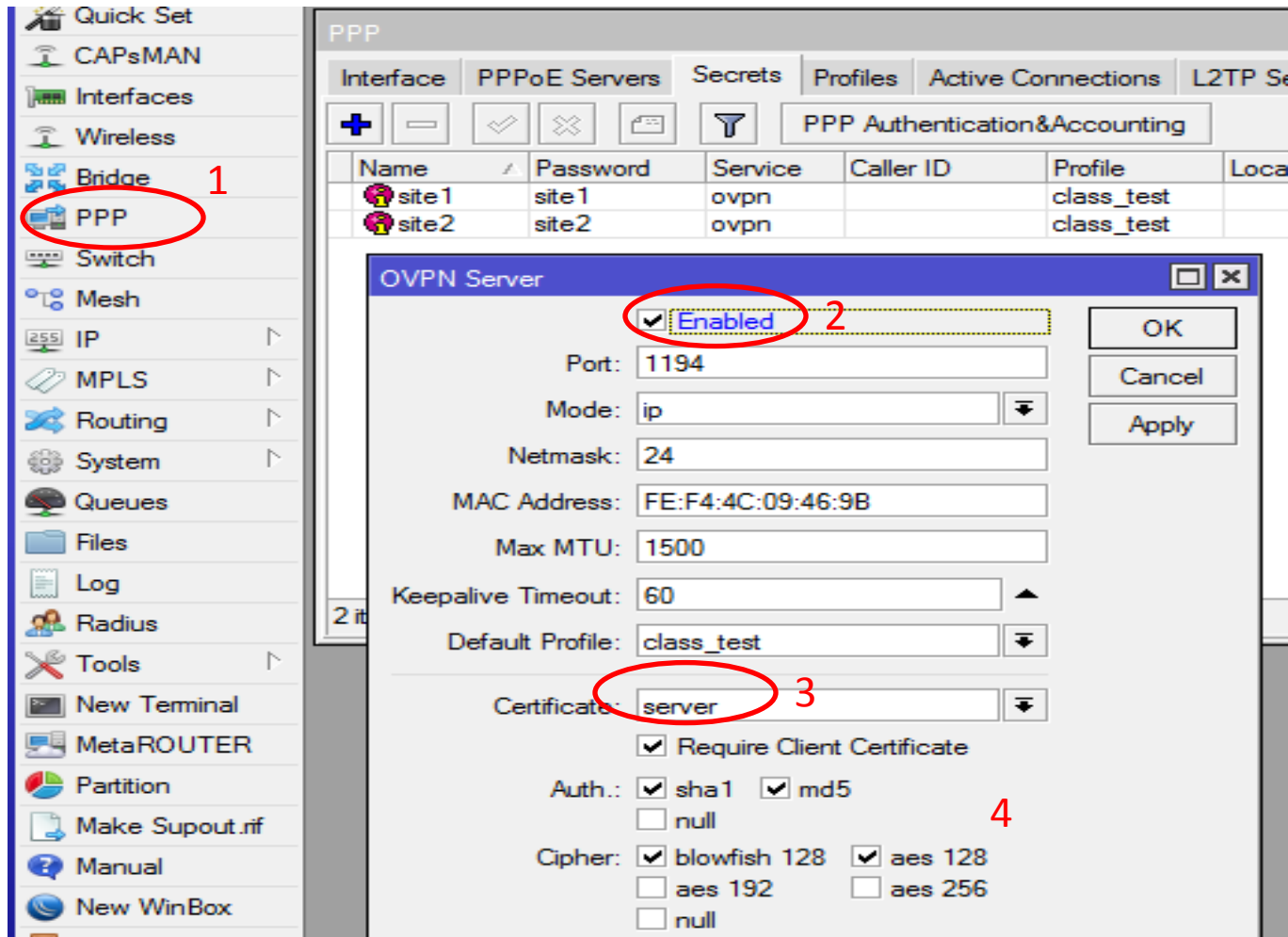
Add SSTP client on site2 as below.



Deploying digital certificates

Using Digital Certificates on OpenVPN tunnels

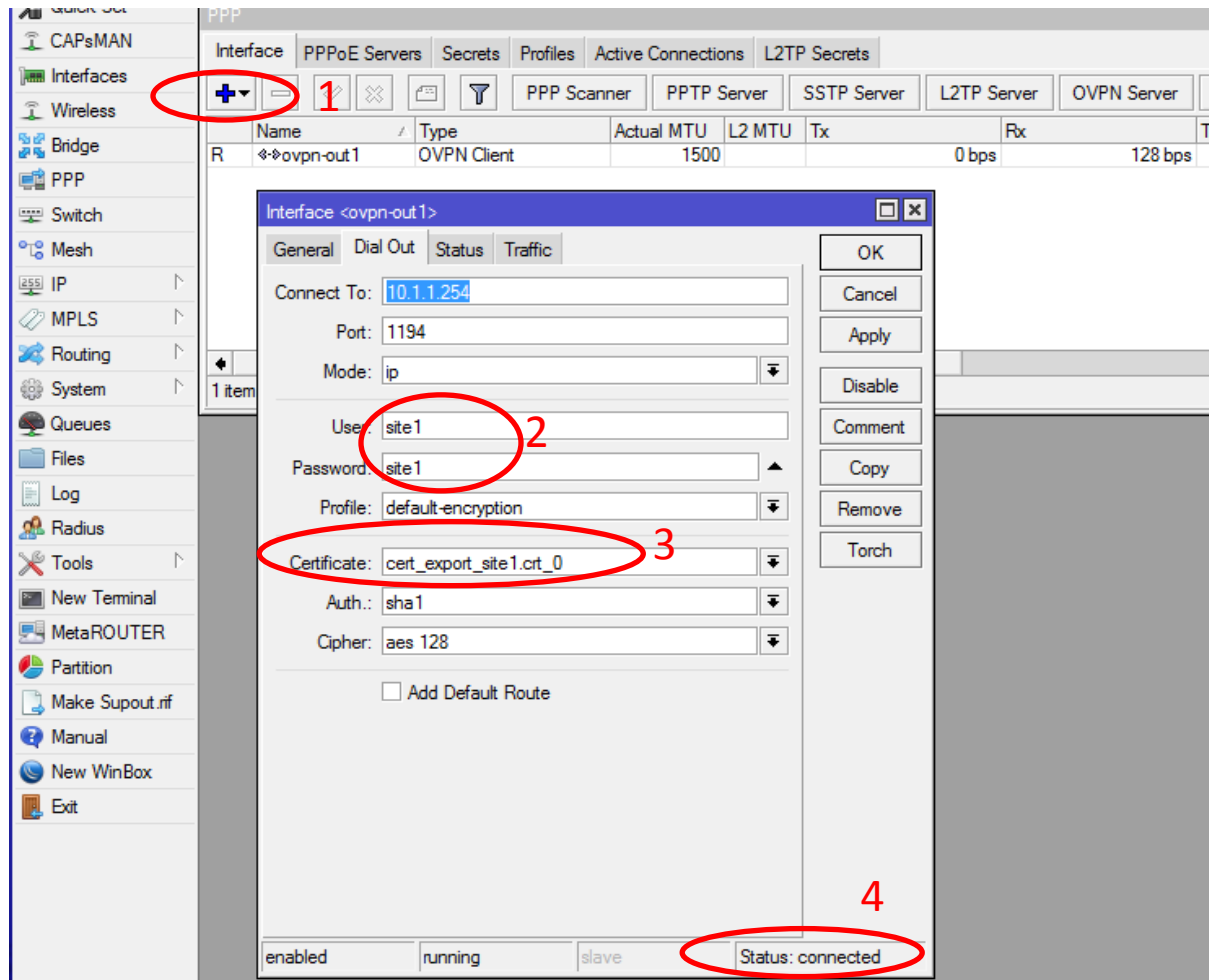
Enable OpenVPN Server to use Certificate



Deploying digital certificates

Using Digital Certificates on OpenVPN tunnels

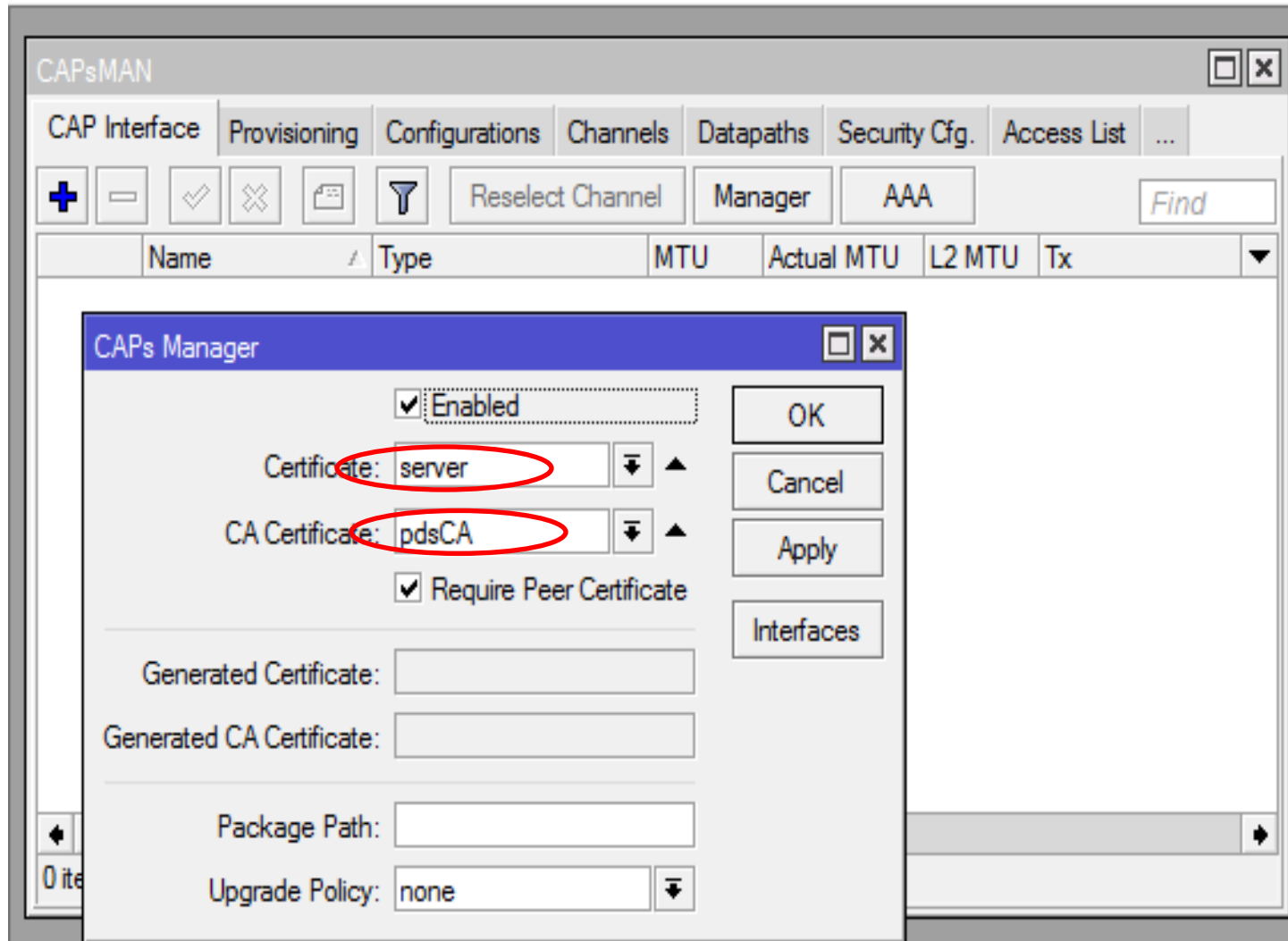
Add OpenVPN client on site1 and site2 as below.



Repeat the setup for site2

Deploying digital certificates

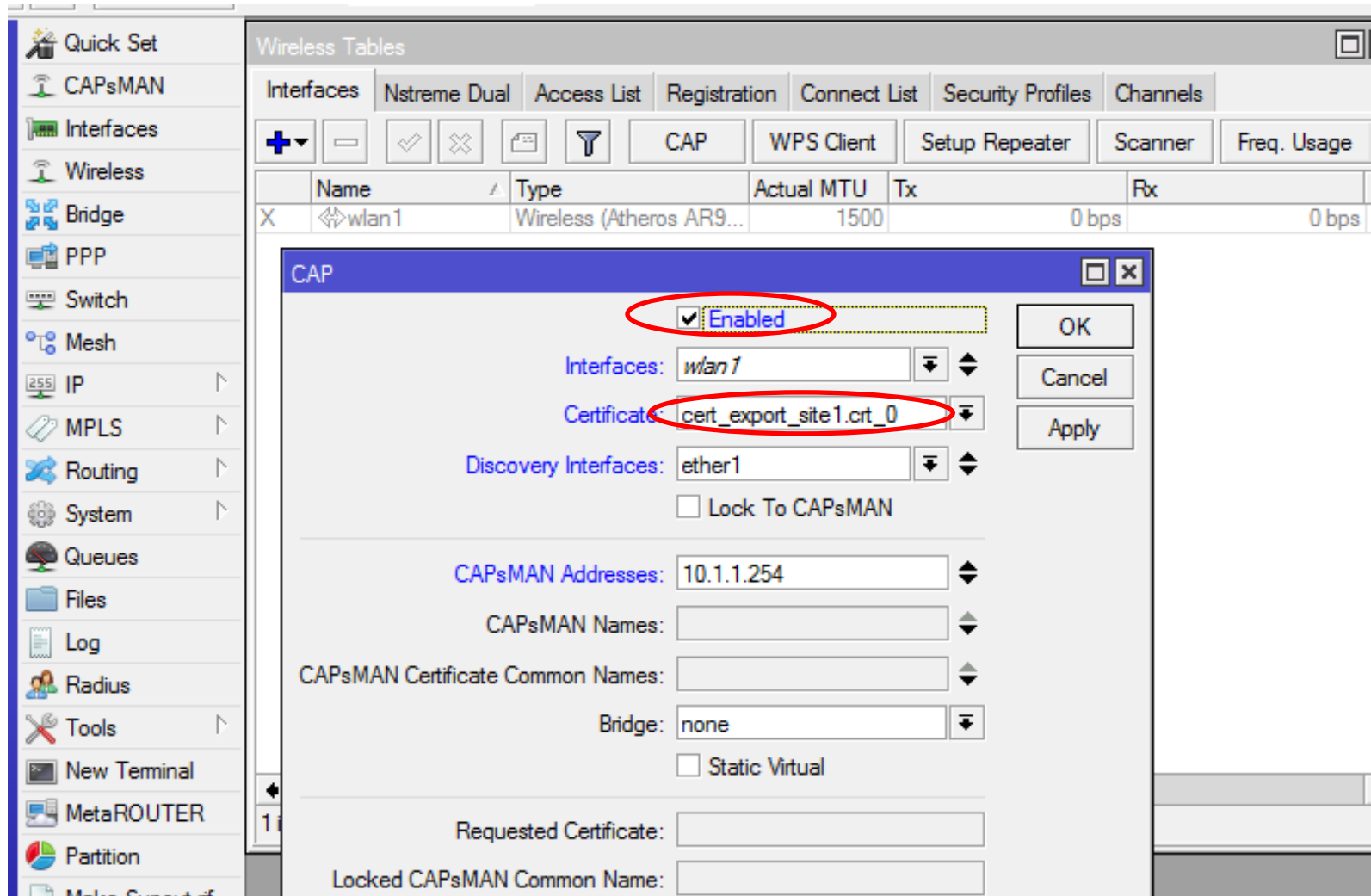
Deploying digital certificates for CAP to CapsMan connections
Enable CapsManager with certificate



Deploying digital certificates

Deploying digital certificates for CAP to CapsMan connections

Enable CAP with certificate:



Deploying digital certificates

Deploying digital certificates for CAP to CapsMan connections
Enable CAP with certificate

The screenshot shows the Mikrotik WinBox interface. On the left is a sidebar with various configuration categories. The main window displays the 'Wireless Tables' configuration for the 'wlan1' interface. A 'CAP' configuration dialog is open, showing settings for enabling CAP on the selected interface.

Wireless Tables Configuration:

Name	Type	Actual MTU	Tx	Rx
--- managed by CAPsMAN				
--- channel: 2427/20-Ce/gn(30dBm), SSID: MUM-Lagos, CAPsMAN forwarding				
X wlan1	Wireless (Atheros AR9...	1500	0 bps	0 bps

CAP Configuration Dialog:

- ☒ Enabled
- Interfaces: wlan1
- Certificate: cert_export_site1.crt_0
- Discovery Interfaces: ether1
- ☐ Lock To CAPsMAN
- CAPsMAN Addresses: 10.1.1.254
- CAPsMAN Names: (empty)
- CAPsMAN Certificate Common Names: (empty)
- Bridge: none
- ☐ Static Virtual
- Requested Certificate: (empty)
- Locked CAPsMAN Common Name: (empty)

Deploying digital certificates

Deploying digital certificates on Hotspots for enhanced security using Public CA issued certificates.

Create a certificate template:

The screenshot shows a Windows 'Certificates' dialog box with the title bar 'Certificates' and a subtitle 'Certificate <hotspot.pdsng.com.tem>'. The 'General' tab is selected, showing the following fields:

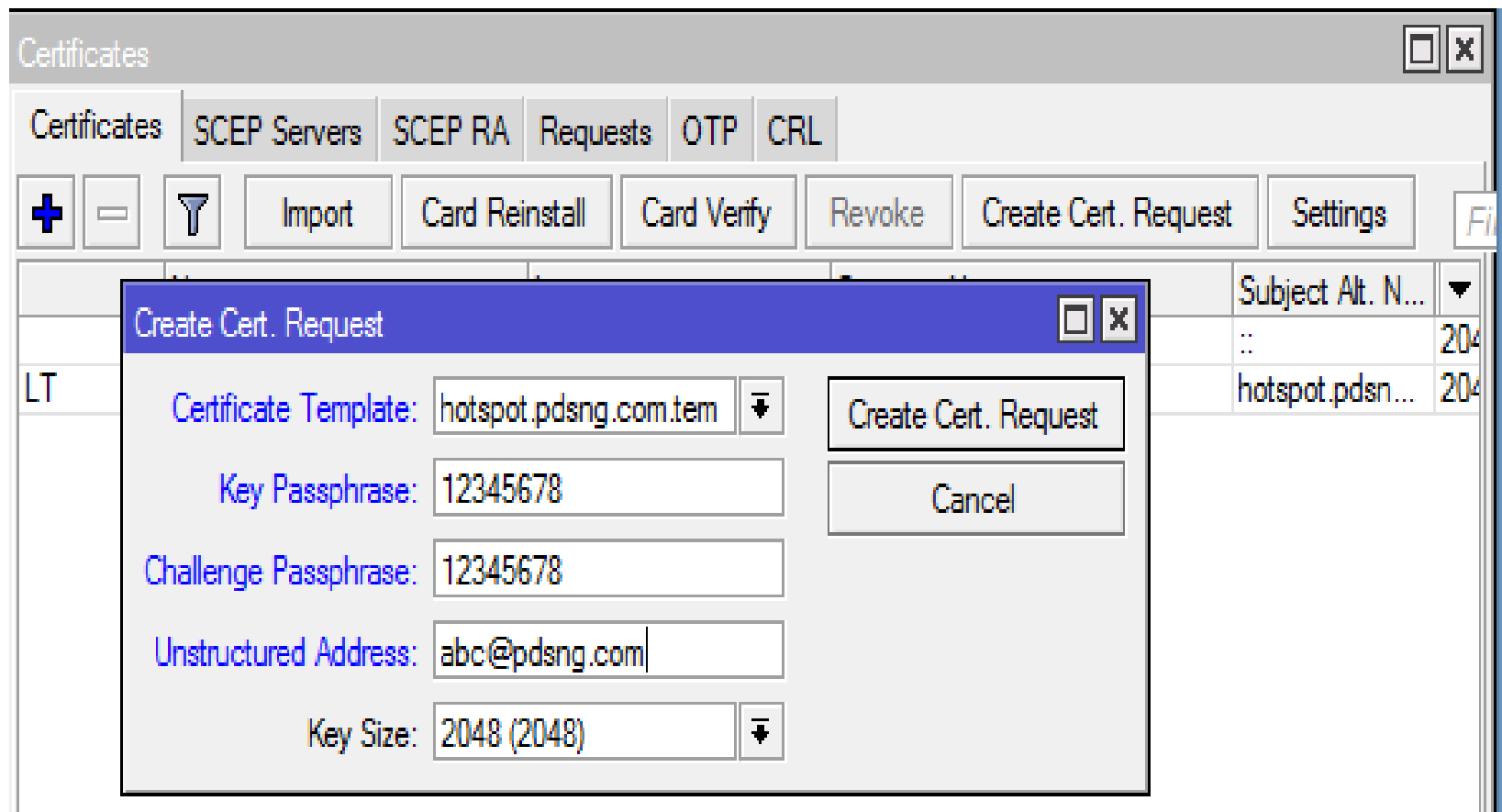
- Name: hotspot.pdsng.com.tem
- Issuer: (empty)
- Country: NG
- State: Lagos
- Locality: Victoria Island
- Organization: Panorama Data Solutions Ltd
- Unit: NOC
- Common Name: hotspot.pdsng.com
- Subject Alt. Name: IP
- Key Size: 2048
- Days Valid: 365

On the right side of the dialog, there is a vertical stack of buttons: OK, Cancel, Apply, Copy, Remove, Sign, Sign via SCEP, Import, Card Reinstall, Card Verify, Set CA Passphrase, Export, and Revoke.

Deploying digital certificates

Deploying digital certificates on Hotspots

Create a certificate Signing request:



Deploying digital certificates

Deploying digital certificates on Hotspots

Export the certificate-request.pem and open to get CSR code:

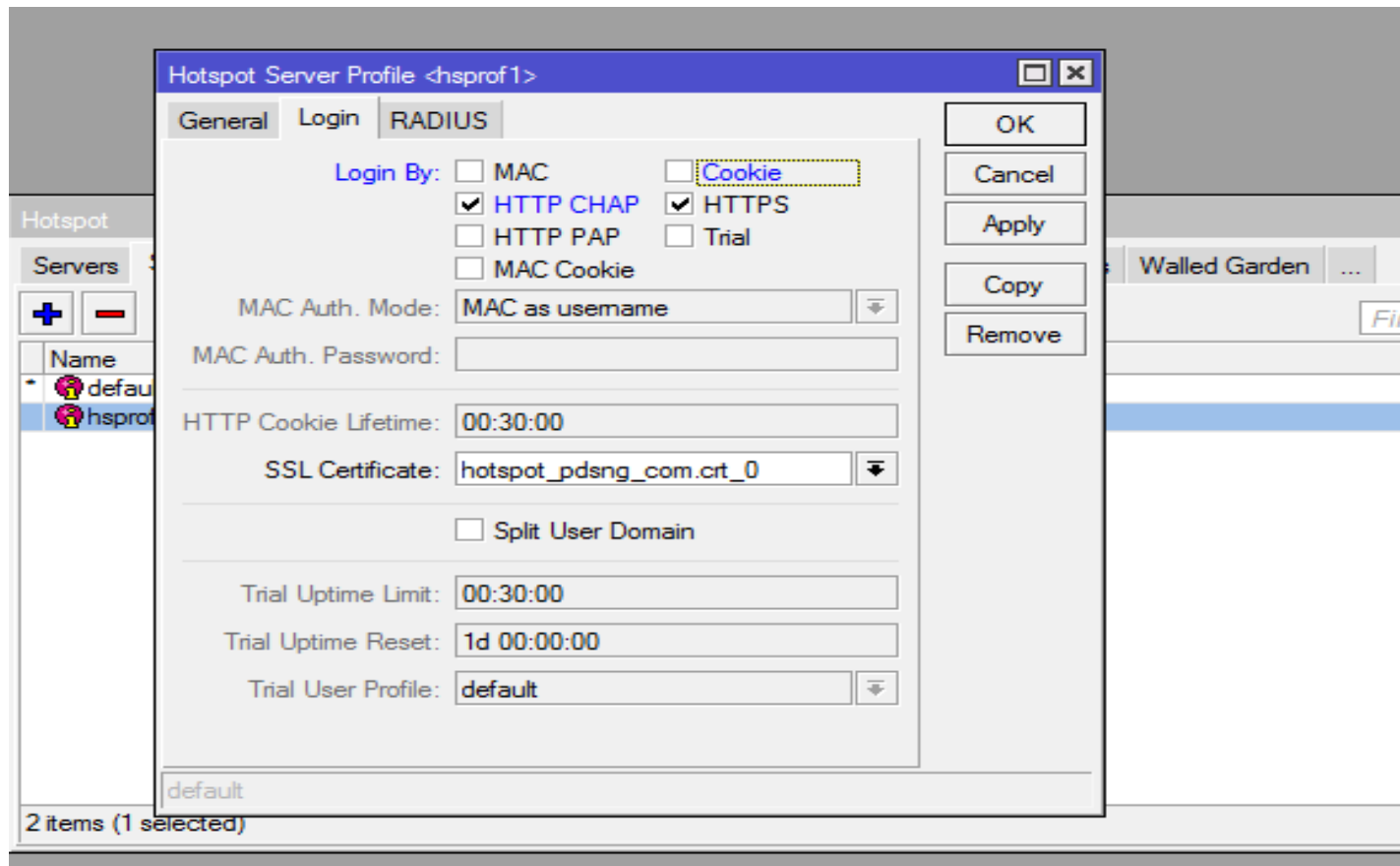
```
-----BEGIN CERTIFICATE REQUEST-----  
MIIDKDCCAACAQIwGycxCzAJBgNVBAYTAk5HMQ4wDAYDVQQIDAVMYWdvczEYMBYG  
A1UEBwwPVmljdG9yaWEgSXNsYW5kMSQwlgYDVQQKBtQYW5vcnFtYSBEYXRhIFNv  
bHV0aW9ucyBMDGQxDDAKBgNVBAsMA05PQzEaMBGGA1UEAwwRaG90c3BvdC5wZHNu  
Zy5jb20wggeiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCzMiohfqTfCNqR  
IW2WUJfN60ikkAIBFZaYxFKjVNn51YDY3F+l2JMqBaVlibnjPpWMtoXVgZN4tZ1  
NHbPYWR32aMrVkjpzmzVNjOhWoFfQ81FJnvucr3Ug7sSAcoeAwCfWY7WAwDjJCY/w  
kF6p648SCK8wja9IDT+mNMPla56kp7ccmzj316QKBOoYGg/l4xf0qH4hAqHJHnuR  
xFG4LyfMLrC10Qx/bAHM2dtRs12bohBQHeunRgTuf59do5ofuw3S5hhQOZYHGw+s  
rC/qxV+seRvI16xK/HdvaFBje0m1mulsasW7Gcnlc+ZCoIC9eoLACgNBFDl6o67z  
8itHKdgrAgMBAAGgWzAXBgkqhkiG9w0BCQcxGgwlcGRzbmcxMjMwHwYJKoZIhvcN  
AQkCMRIMEG1hZ251c0BwZHNuZy5jb20wHwYJKoZIhvcNAQkOMRIwEDAObGNVHQ8B  
Af8EBAMCAbYwDQYJKoZIhvcNAQELBQADggEBAKB8R6aVFBBfZMJz8frB+YUGyxmI  
gQUw5LgcjnblqeJYUMsZqkOzuNfk3Kdh5jrBfqTNNzied8kKTzE82+kcw4trc8P8  
1H7FU8pdRIUHFTxFe/hH5zYKwAjRb4UtCiryjoK1mq62wvK9QJ7fPceWtj46GY7  
n/vkR2BbHrqMVdMhNX0f5V3f/pvwn4C5KvZEUPo80vLDGBX/jXb/k7LaU5NOS4Ro  
I/6O8ep03Ry246VSuc+g64tbGYaB6jzSLy5Mlt31kg8n/18Wv6uBQIapvwQl6xbb  
hS/B01g8elwseatsCRmWxyH6THtcwZmejlgp2F7GuY/IFaMYbAm1F3SAzWs=  
-----END CERTIFICATE REQUEST-----
```

Your Certificate Issuer will require this code

Deploying digital certificates

Deploying digital certificates on Hotspots

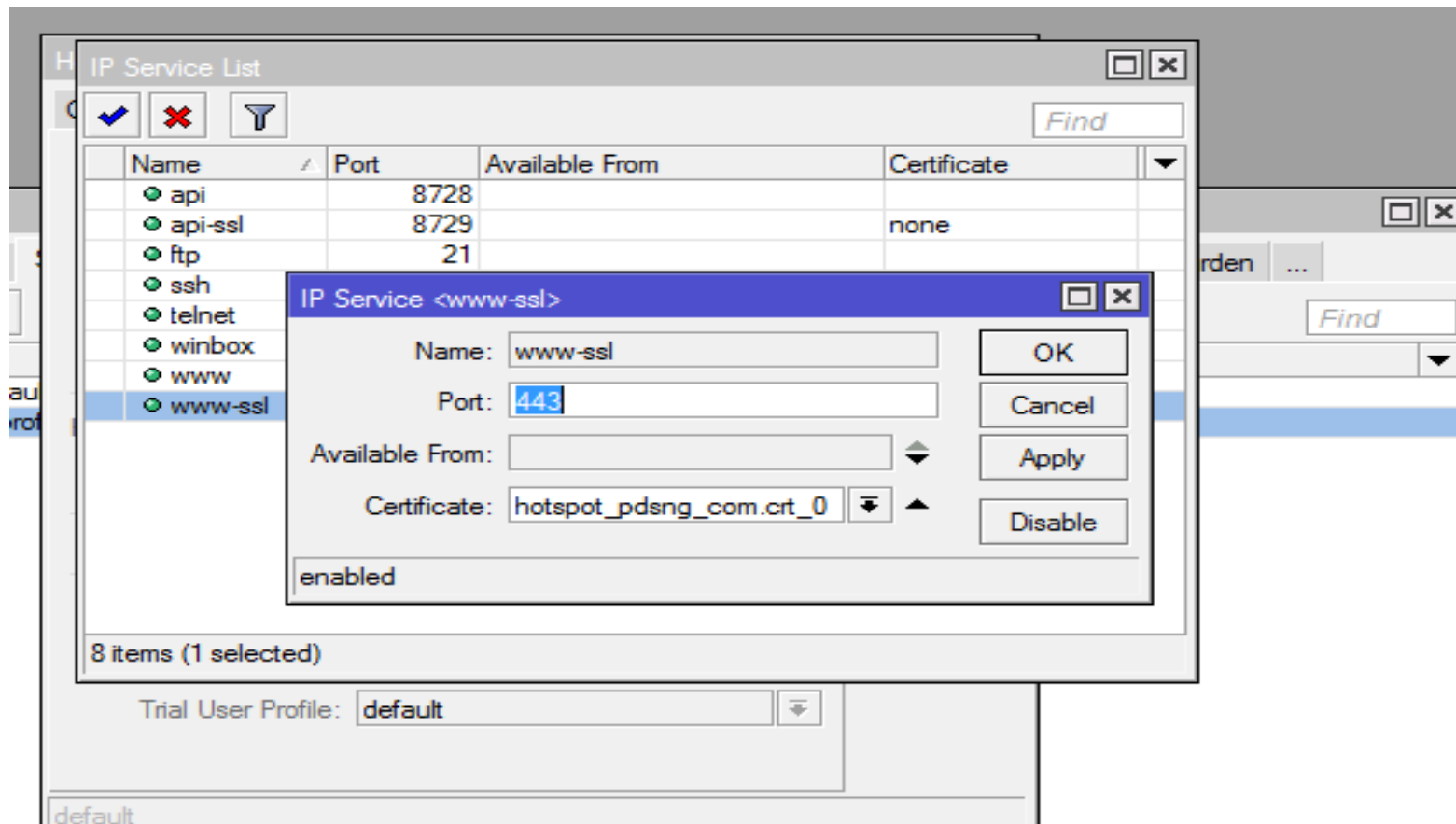
Setup hotspot to use the certificate:



Deploying digital certificates

Deploying digital certificates on Hotspots

Setup www-ssl on IP services with the certificate:



Conclusion

Digital certificates have been shown to be effective in securing different types of data over various kinds of connections. It also allows us to trust online entities when properly deployed.

The presentation has shown a step by step procedure to deploy it over some VPN tunnels and for CAP to CapsMan connection in RouterOS.

Thanks for your attention!

Questions?