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?

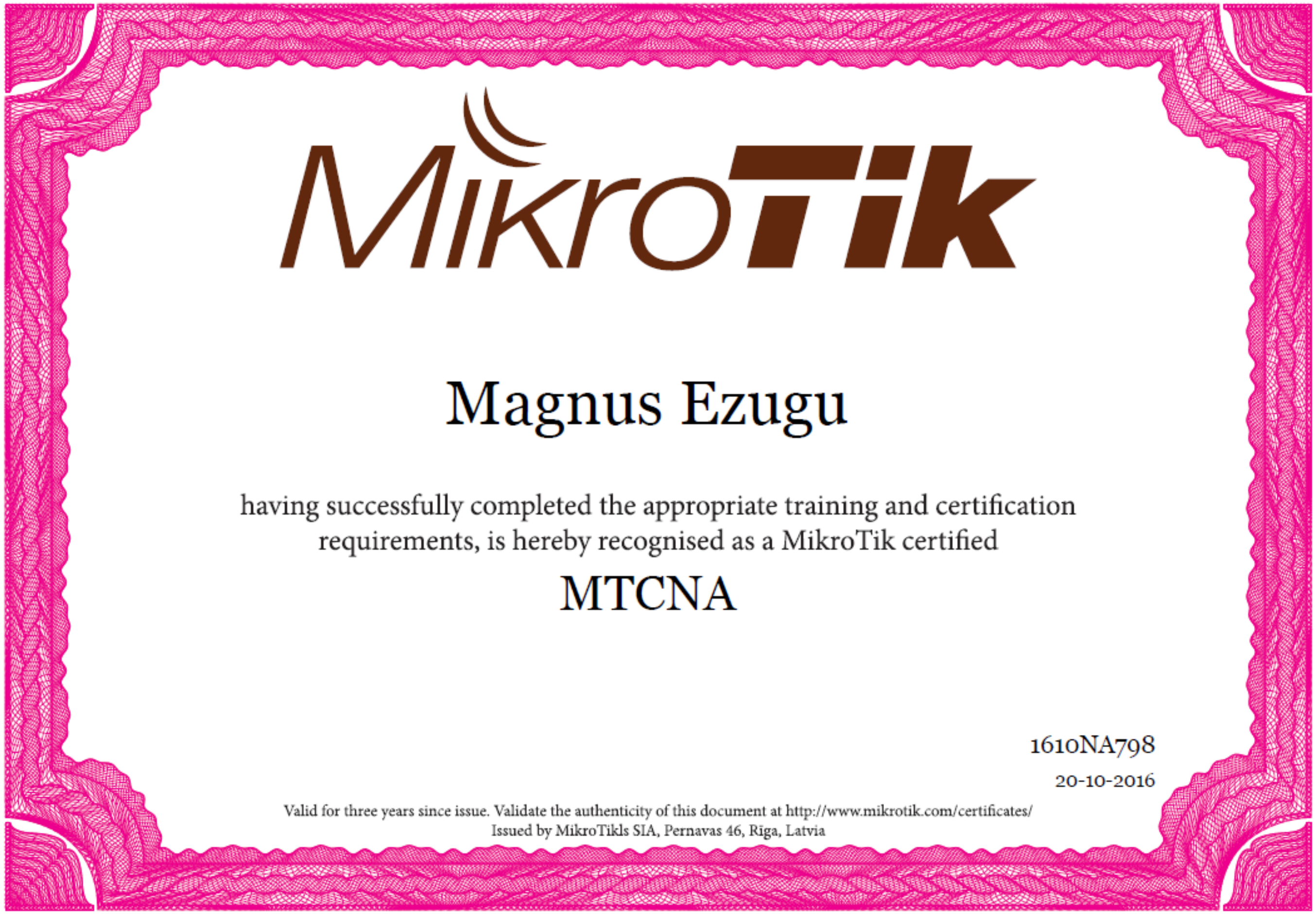
It is an electronic file which enables a secure exchange of information over a network and used to prove the ownership of a public key and identify an entity.

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?



MikroTik

Magnus Ezugu

having successfully completed the appropriate training and certification requirements, is hereby recognised as a MikroTik certified

MTCNA

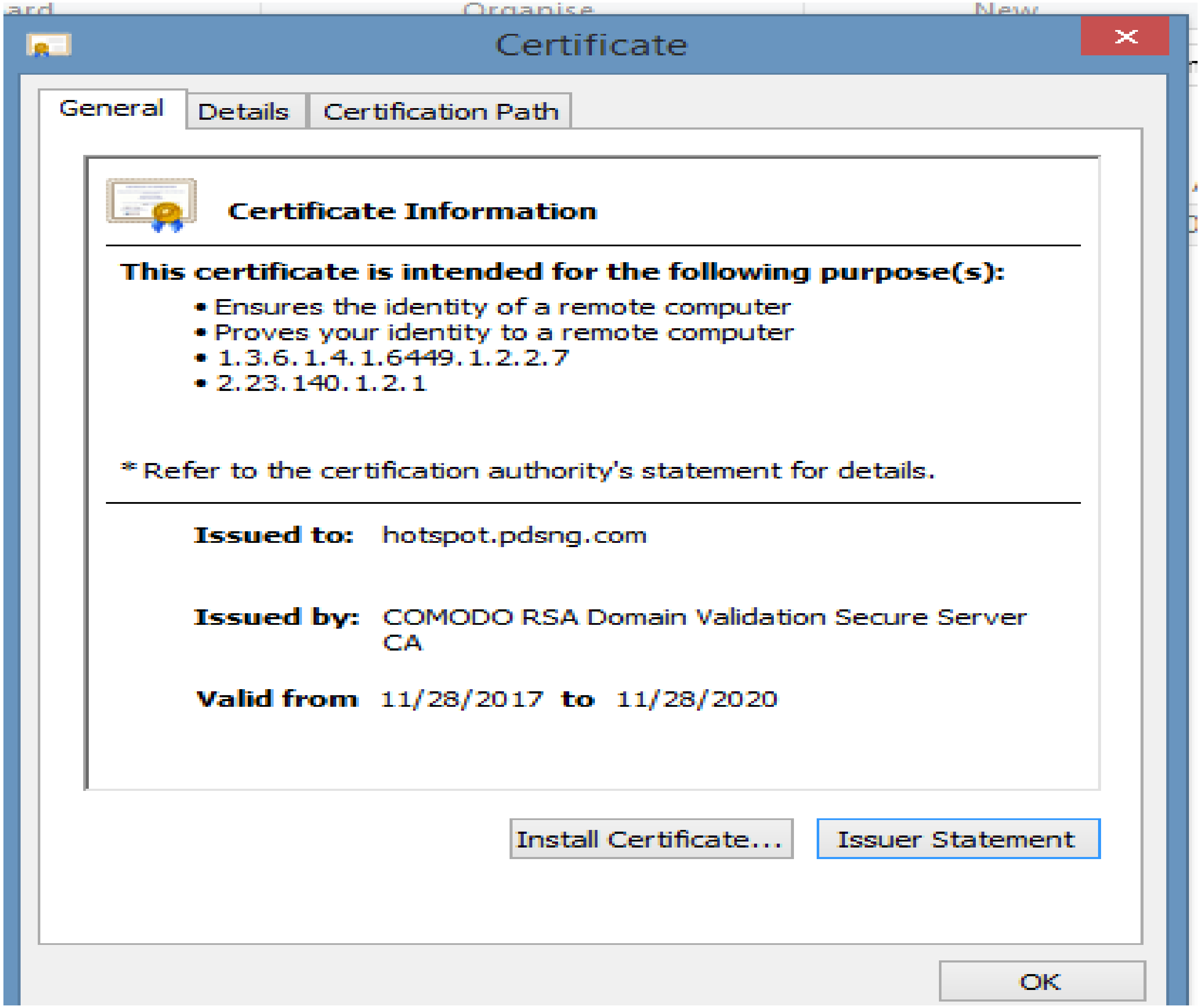
1610NA798

20-10-2016

Valid for three years since issue. Validate the authenticity of this document at http://www.mikrotik.com/certificates/
Issued by MikroTikls SIA, Pernavas 46, Rīga, Latvia

Introduction to Digital Certificate

What is a Digital Certificate?



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
- 1.3.6.1.4.1.6449.1.2.2.7
- 2.23.140.1.2.1

* Refer to the certification authority's statement for details.

Issued to: hotspot.pdsng.com

Issued by: COMODO RSA Domain Validation Secure Server CA

Valid from 11/28/2017 **to** 11/28/2020

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

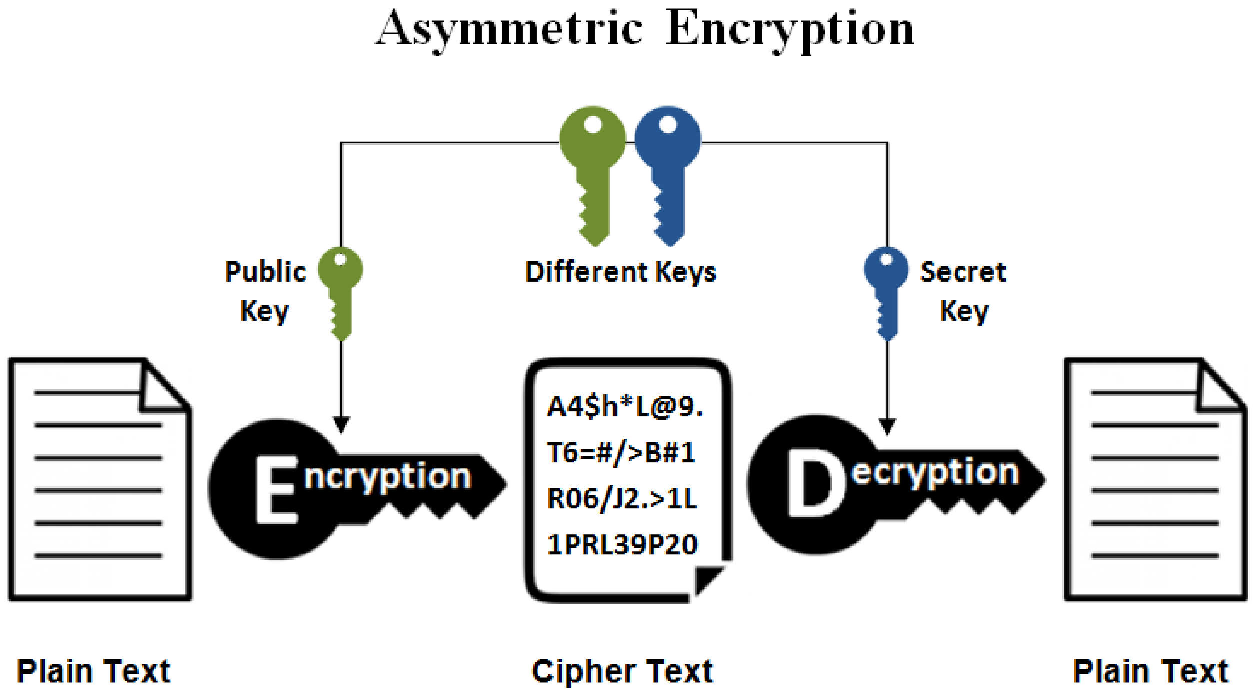
Why do we need certificate:

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:



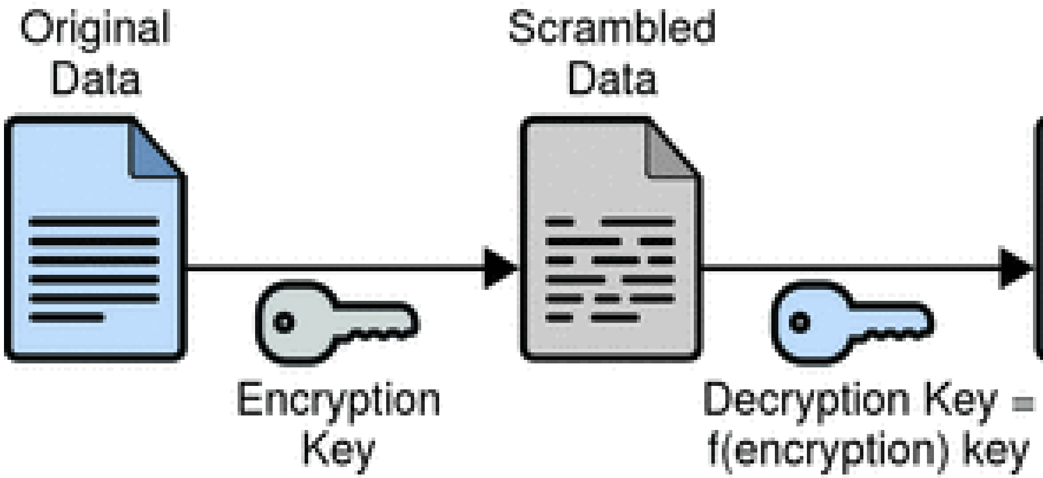
Courtesy ssl2buy.com

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

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

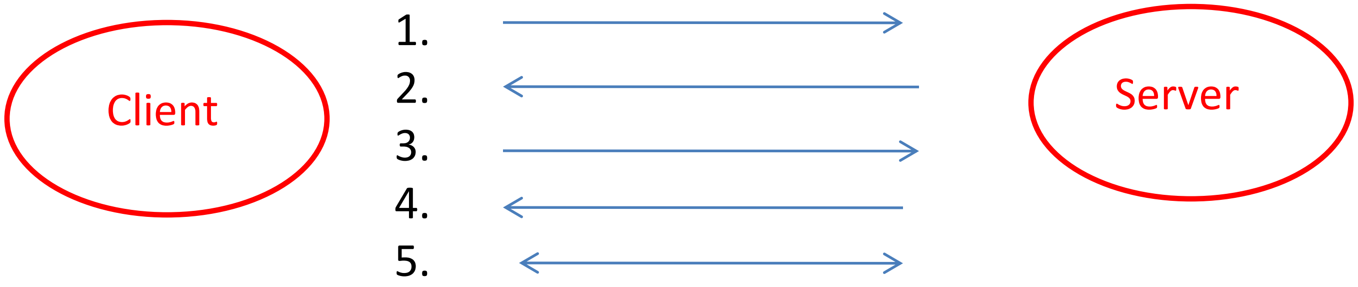
There are various schemes for issuance of a digital certificate which helps to certify the identity and establish trust in the system.

- 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

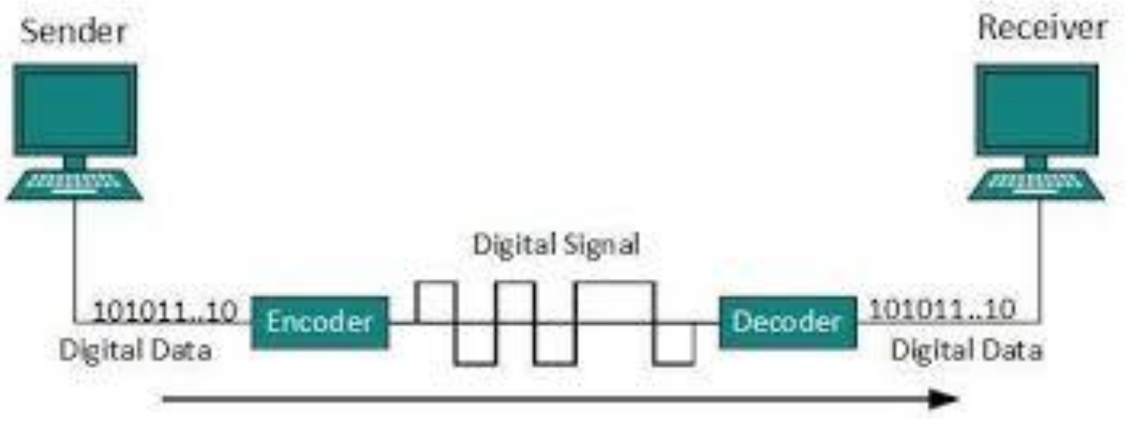
SSL Server Certificate

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.

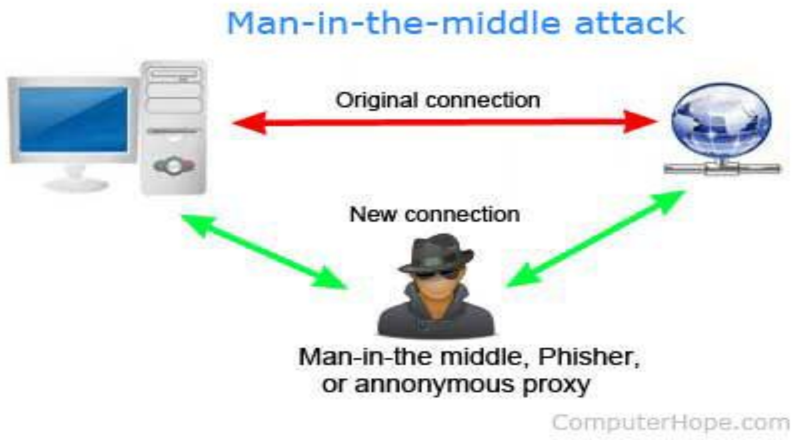


In the absence of SSL or any form of encryption, data is sent as stream of 1s and 0s in a universal encoding format.

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.

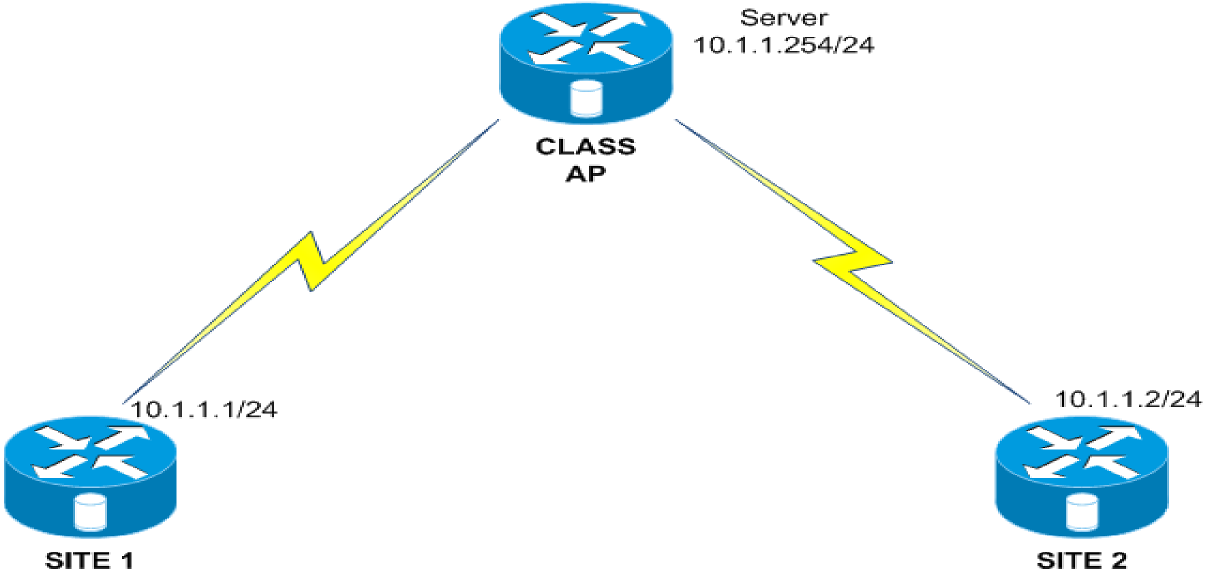
Creating certificates in RouterOs

1. Make certificate templates

2. Sign the certificates and add CRL url

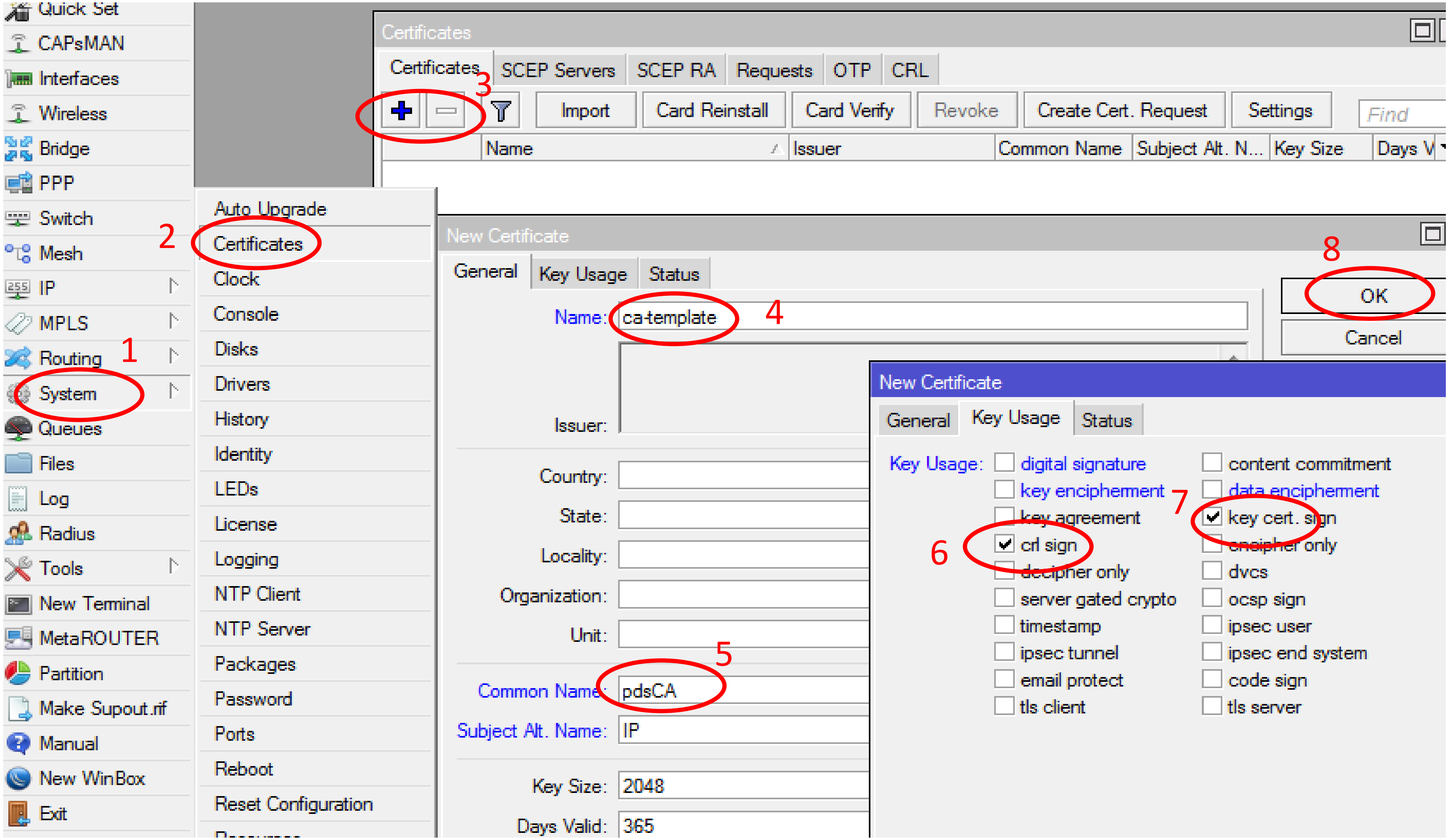
3. Export client certificates with keys and CA certificates and import to client routers

Network Topology:



Creating certificates in RouterOs

Make certificate templates: CA Template



1 System

2 Certificates

3 +

4 Name: ca-template

Issuer:

Country:

State:

Locality:

Organization:

Unit:

5 Common Name: pdsCA

Subject Alt. Name: IP

Key Size: 2048

Days Valid: 365

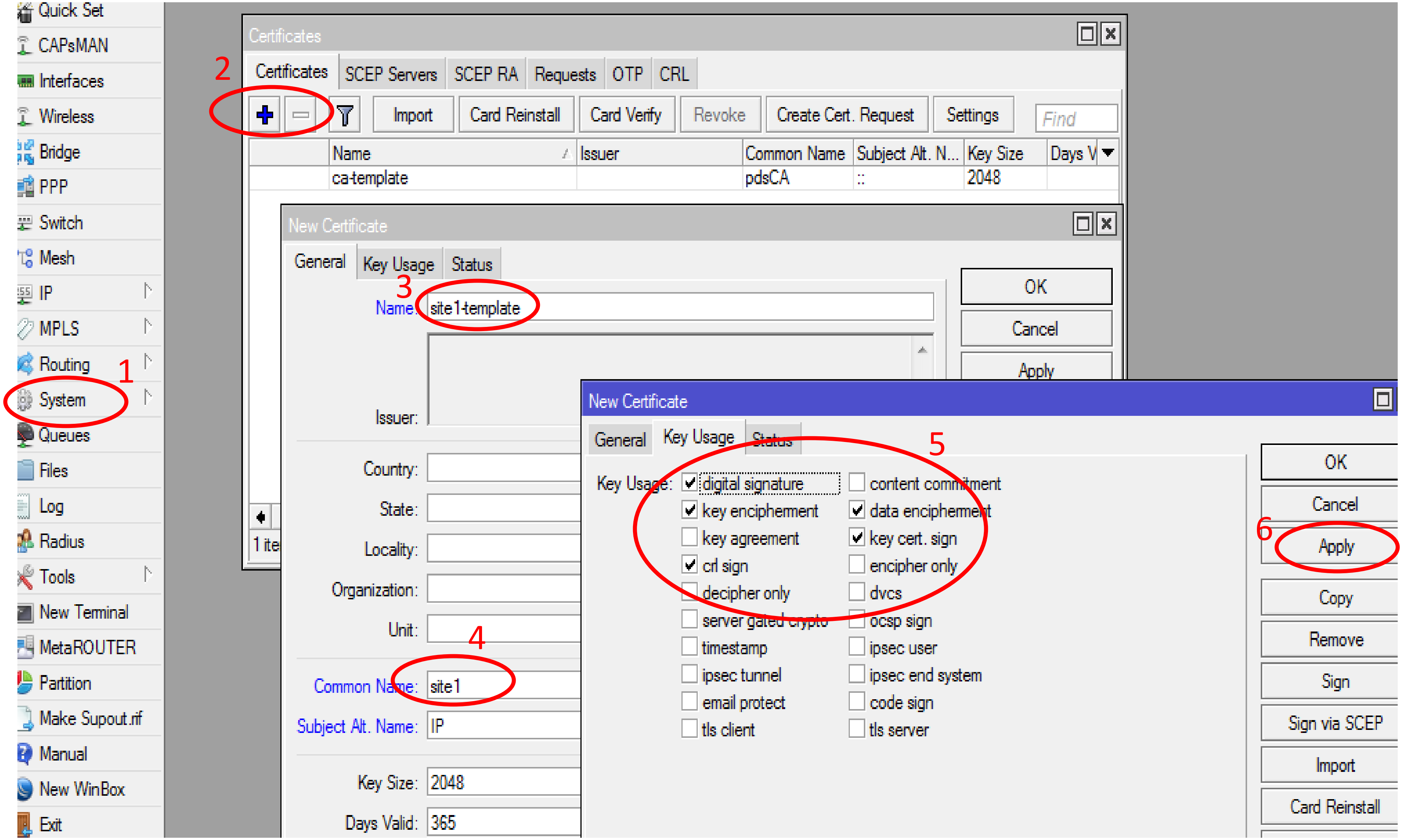
Key Usage:

□ digital signature	□ content commitment
□ key encipherment	□ data encipherment
□ key agreement	7 ☑ key cert. sign
6 ☑ crl sign	□ encipher only
□ decipher only	□ dvcs
□ server gated crypto	□ ocsp sign
□ timestamp	□ ipsec user
□ ipsec tunnel	□ ipsec end system
□ email protect	□ code sign
□ tls client	□ tls server

8 OK

Creating certificates in RouterOs

Make certificate templates: Site1 Template



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

New Certificate — General:

Name: site1-template

Issuer:

Country:

State:

Locality:

Organization:

Unit:

Common Name: site1

Subject Alt. Name: IP

Key Size: 2048

Days Valid: 365

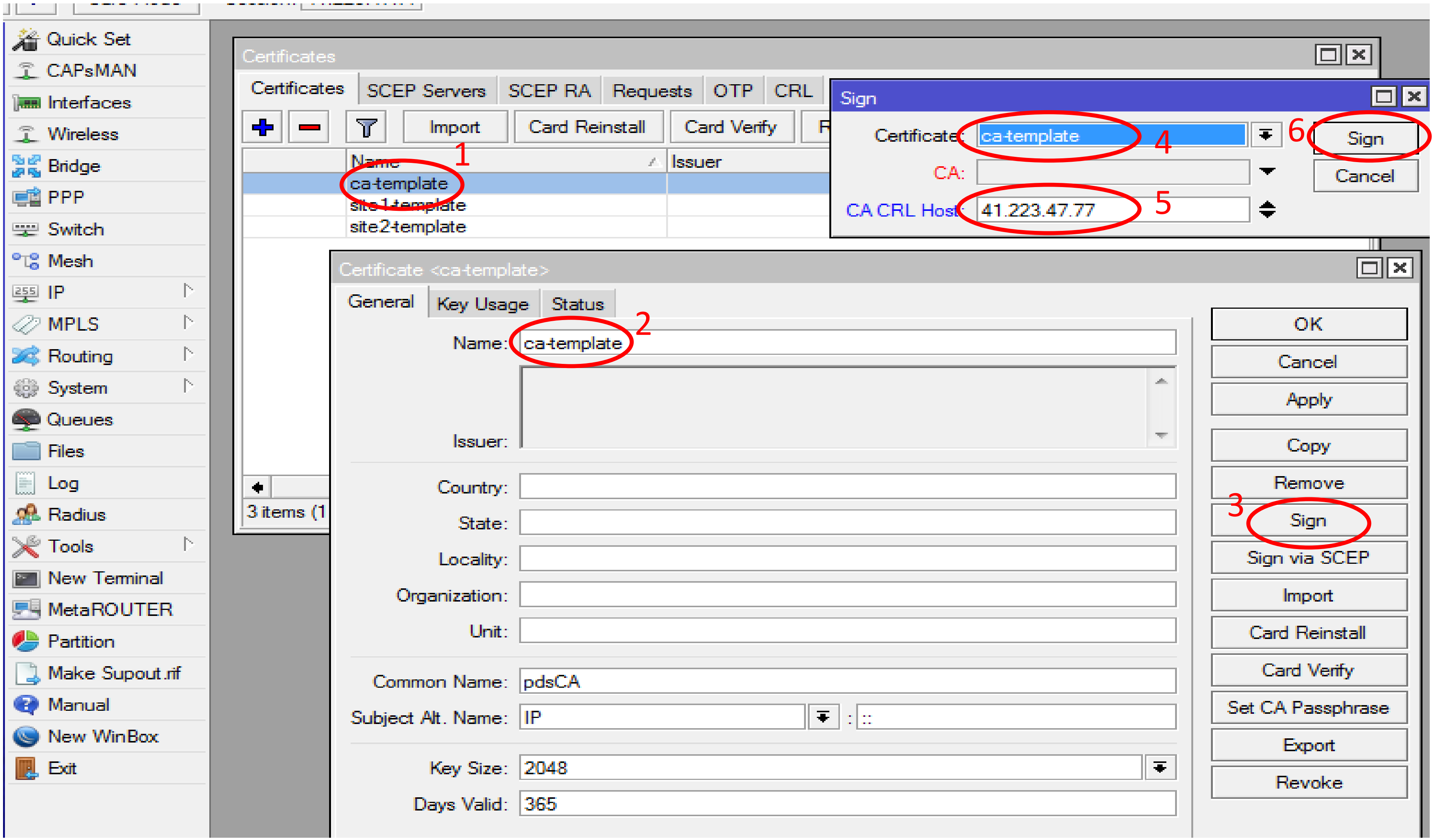
New Certificate — Key Usage:

Key Usage:

☑ digital signature	□ content commitment
☑ key encipherment	☑ data encipherment
□ key agreement	☑ key cert. sign
☑ crl sign	□ encipher only
□ decipher only	□ dvcs
□ server gated crypto	□ ocsp sign
□ timestamp	□ ipsec user
□ ipsec tunnel	□ ipsec end system
□ email protect	□ code sign
□ tls client	□ tls server

Creating certificates in RouterOs

Sign the CA certificate and add CRL url



Certificates: 3 items

Name	Issuer
ca-template	
site1-template	
site2-template	

Certificate <ca-template>

Name: ca-template

Issuer:

Country:

State:

Locality:

Organization:

Unit:

Common Name: pdsCA

Subject Alt. Name: IP : ::

Key Size: 2048

Days Valid: 365

Sign

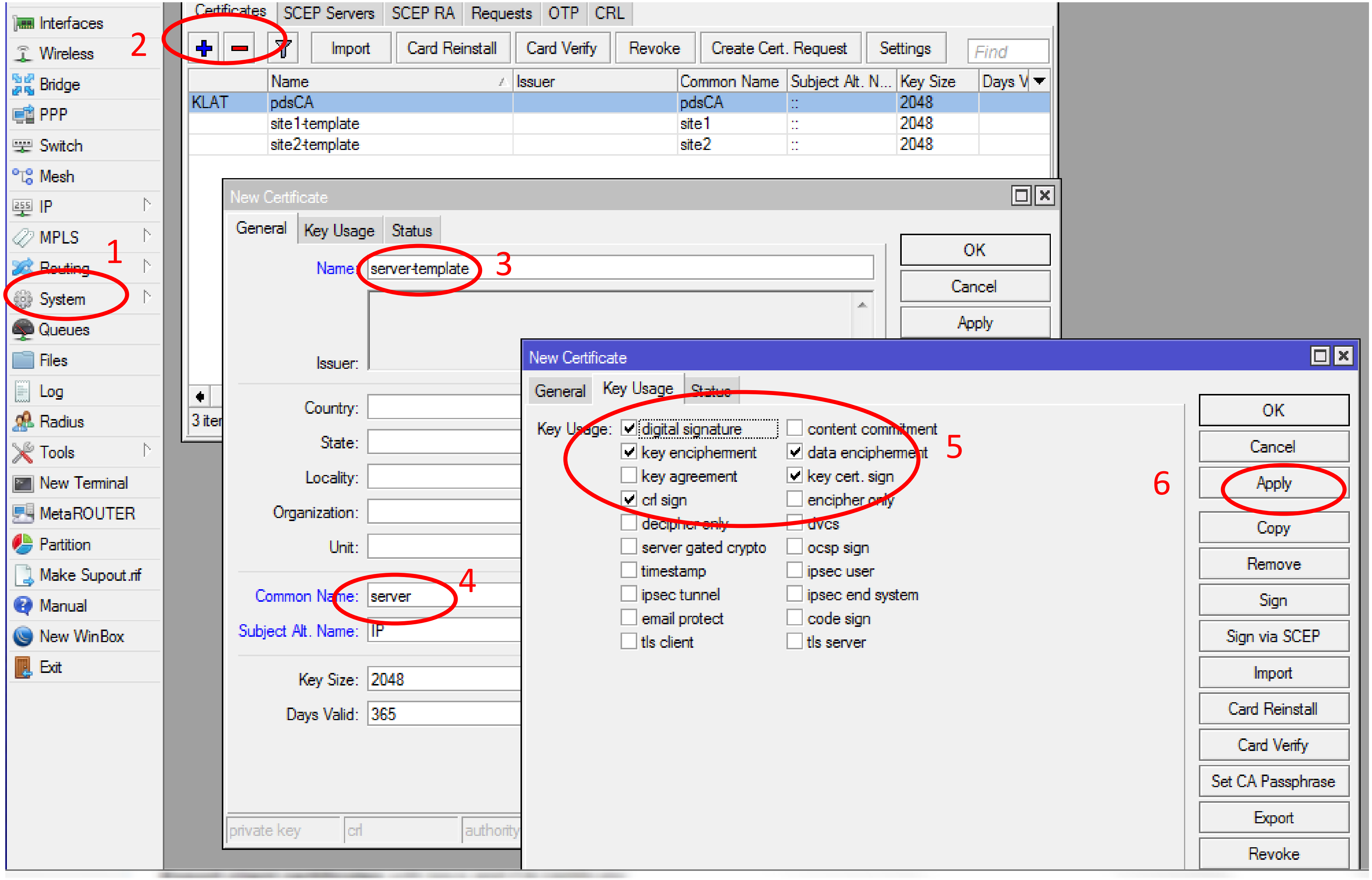
Certificate: ca-template

CA:

CA CRL Host: 41.223.47.77

Creating certificates in RouterOs

Make certificate templates: Server Template



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

New Certificate — General

Name: server-template

Issuer:

Country:

State:

Locality:

Organization:

Unit:

Common Name: server

Subject Alt. Name: IP

Key Size: 2048

Days Valid: 365

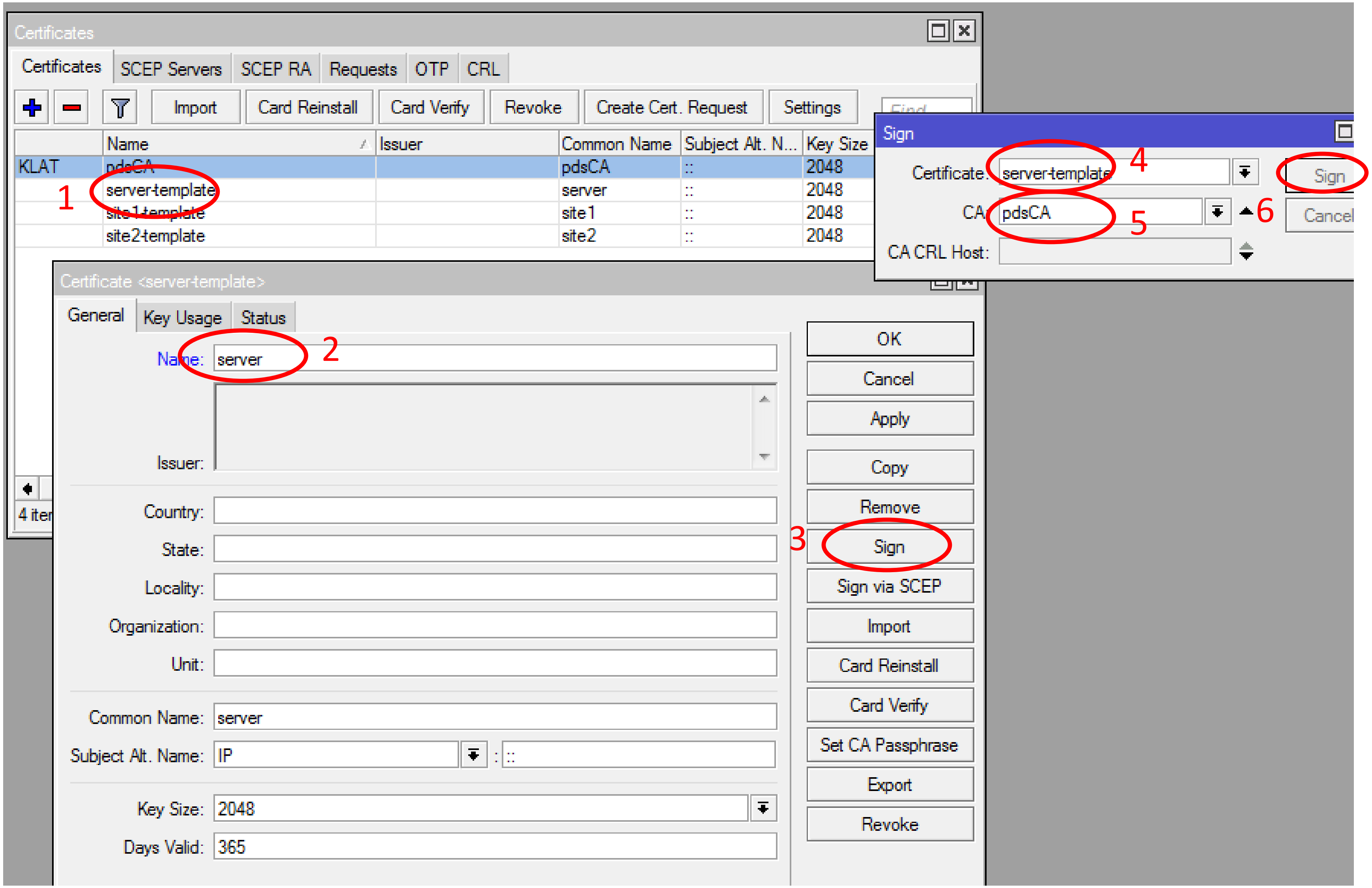
New Certificate — Key Usage

Key Usage:

☑ digital signature	□ content commitment
☑ key encipherment	☑ data encipherment
□ key agreement	☑ key cert. sign
☑ crl sign	□ encipher only
□ decipher only	□ dvcs
□ server gated crypto	□ ocsp sign
□ timestamp	□ ipsec user
□ ipsec tunnel	□ ipsec end system
□ email protect	□ code sign
□ tls client	□ tls server

Creating certificates in RouterOs

Sign certificate templates: Server Template



Certificates

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

4 iter

Certificate <server-template>

Name: server

Issuer:

Country:

State:

Locality:

Organization:

Unit:

Common Name: server

Subject Alt. Name: IP : ::

Key Size: 2048

Days Valid: 365

Sign

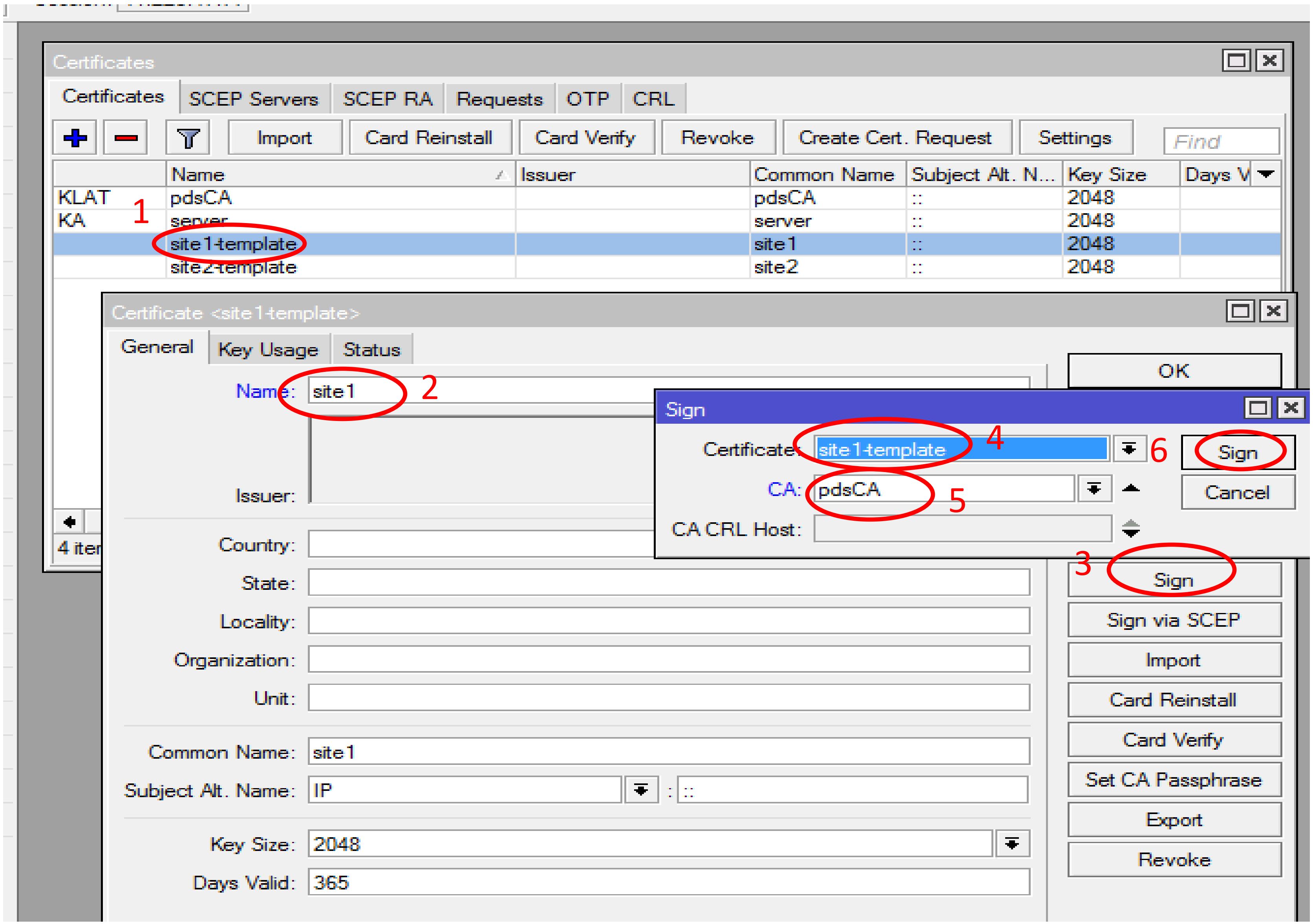
Certificate: server-template

CA: pdsCA

CA CRL Host:

Creating certificates in RouterOs

Sign certificate templates: Site1 Template



Certificates

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

4 iter

Certificate <site1-template>

Name: site1

Issuer:

Country:

State:

Locality:

Organization:

Unit:

Common Name: site1

Subject Alt. Name: IP : ::

Key Size: 2048

Days Valid: 365

Sign

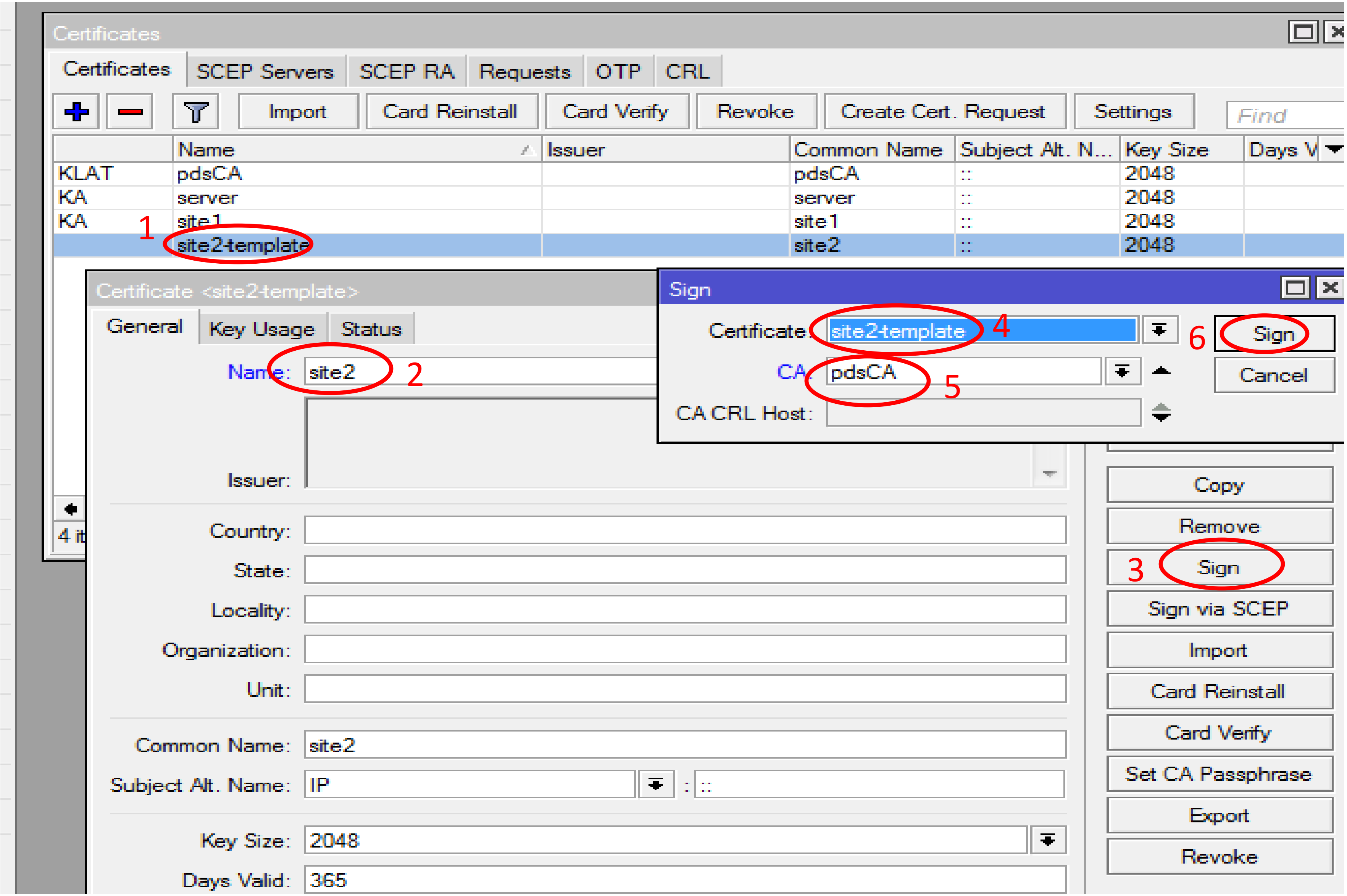
Certificate: site1-template

CA: pdsCA

CA CRL Host:

Creating certificates in RouterOs

Sign certificate templates: Site2 Template



	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

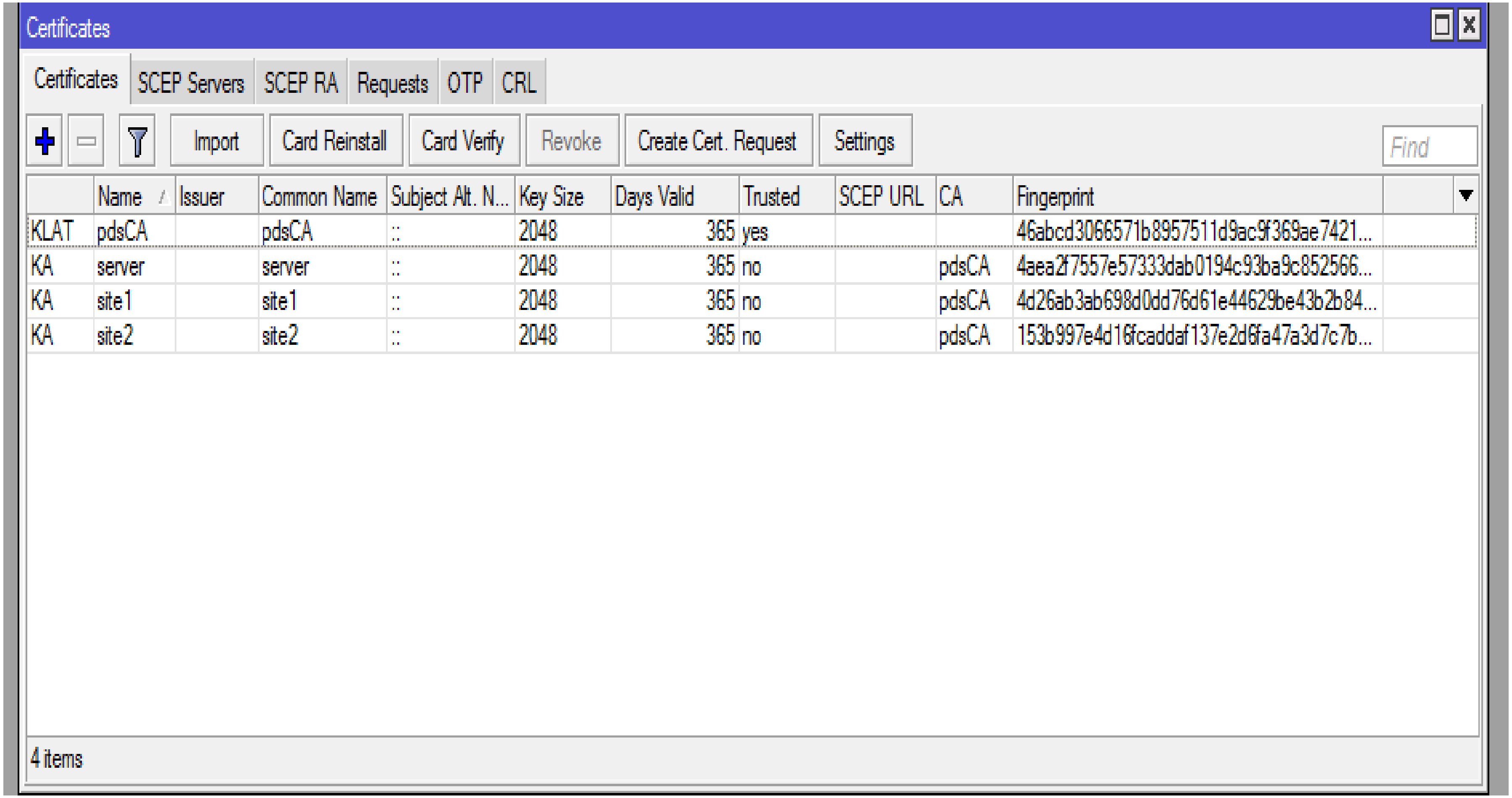
Certificate: site2-template

CA: pdsCA

CA CRL Host:

Creating certificates in RouterOs

The results after creating and signing certificate

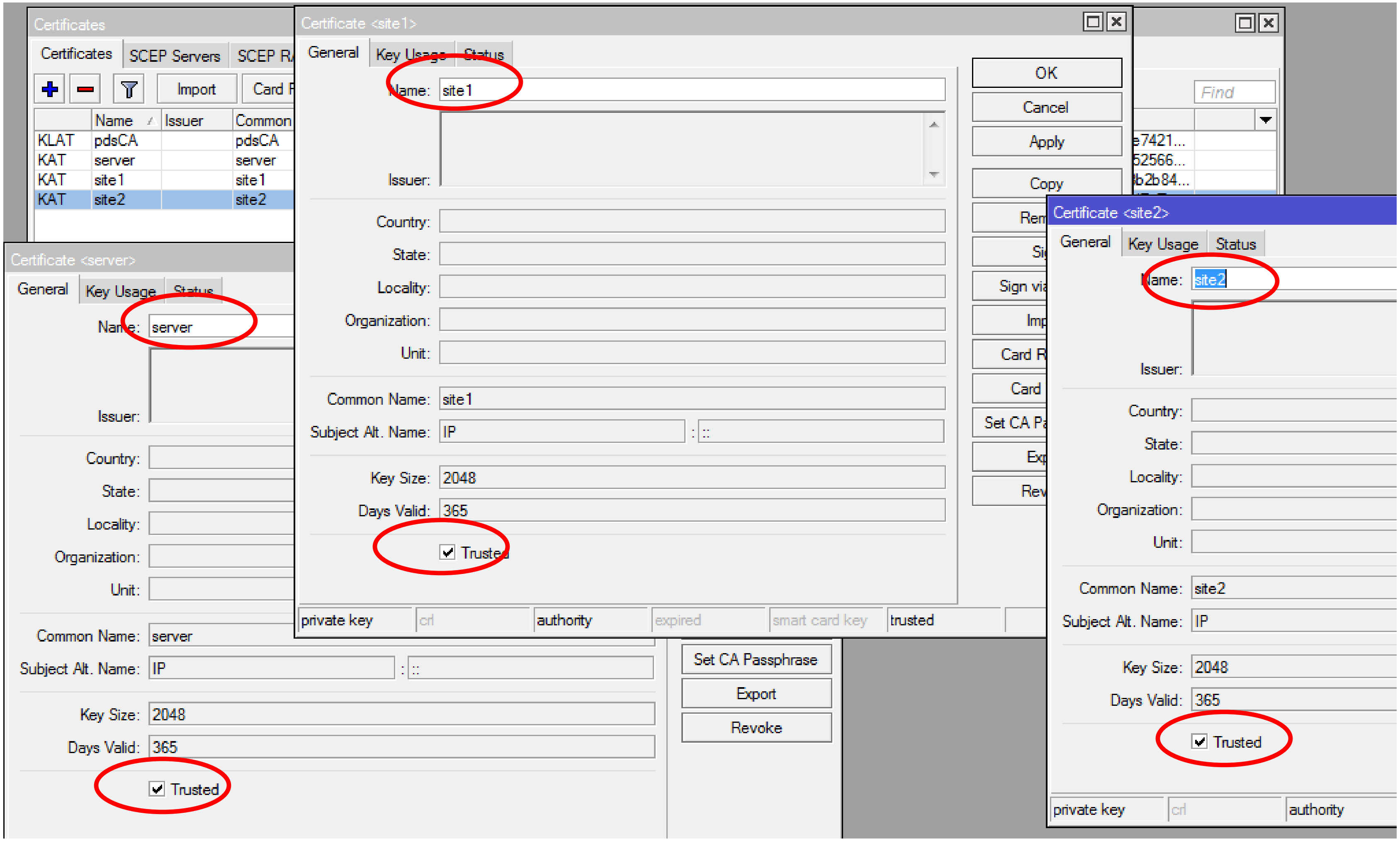


	Name	Issuer	Common Name	Subject Alt. N...	Key Size	Days Valid	Trusted	SCEP URL	CA	Fingerprint	
KLAT	pdsCA		pdsCA	::	2048	365	yes			46abcd3066571b8957511d9ac9f369ae7421...	
KA	server		server	::	2048	365	no		pdsCA	4aea2f7557e57333dab0194c93ba9c852566...	
KA	site1		site1	::	2048	365	no		pdsCA	4d26ab3ab698d0dd76d61e44629be43b2b84...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

4 items

Creating certificates in RouterOs

Set all certificates as Trusted



	Name	Issuer	Common
KLAT	pdsCA		pdsCA
KAT	server		server
KAT	site1		site1
KAT	site2		site2

e7421...
52566...
b2b84...

Certificate <site1>

Name: site1
Issuer:
Country:
State:
Locality:
Organization:
Unit:
Common Name: site1
Subject Alt. Name: IP : ::
Key Size: 2048
Days Valid: 365
☑ Trusted

private key | crl | authority | expired | smart card key | trusted

Certificate <server>

Name: server
Issuer:
Country:
State:
Locality:
Organization:
Unit:
Common Name: server
Subject Alt. Name: IP : ::
Key Size: 2048
Days Valid: 365
☑ Trusted

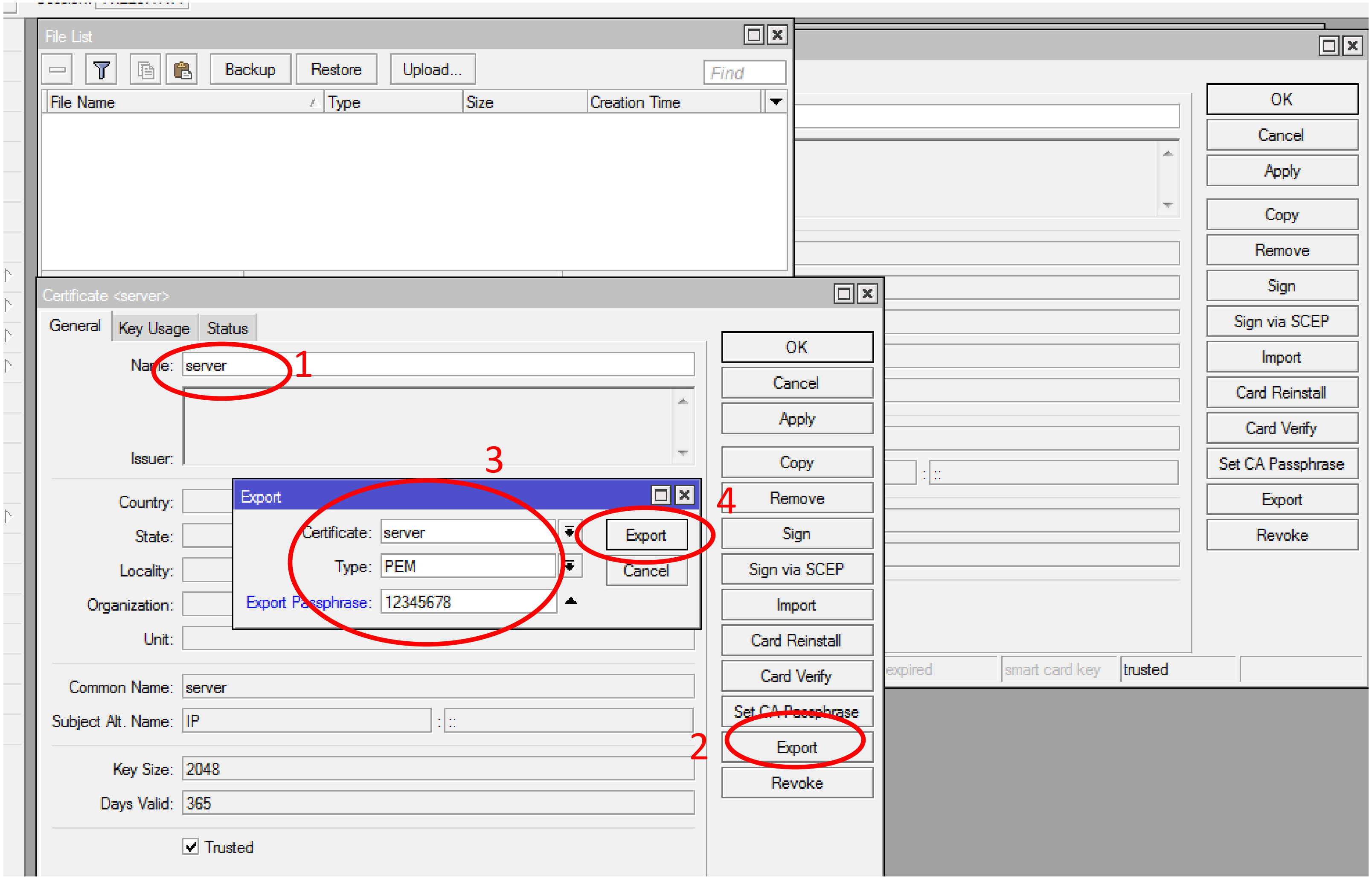
Certificate <site2>

Name: site2
Issuer:
Country:
State:
Locality:
Organization:
Unit:
Common Name: site2
Subject Alt. Name: IP
Key Size: 2048
Days Valid: 365
☑ Trusted

private key | crl | authority

Creating certificates in RouterOs

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



Name: server

Export

Certificate: server

Type: PEM

Export Passphrase: 12345678

Export

Cancel

Common Name: server

Subject Alt. Name: IP : ::

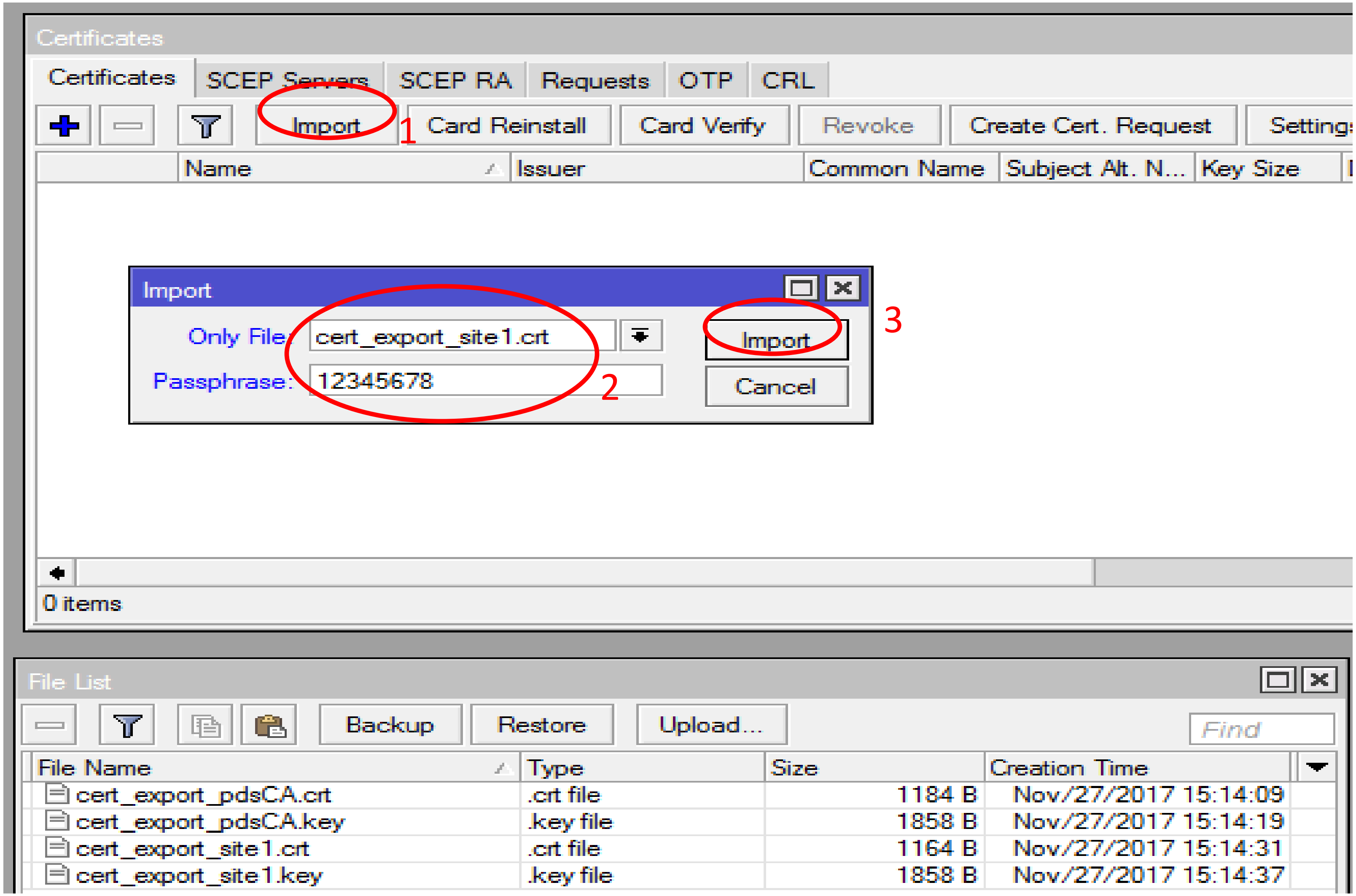
Key Size: 2048

Days Valid: 365

☑ Trusted

Creating certificates in RouterOs

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



1 Import

2

Import

Only File: cert_export_site1.crt

Passphrase: 12345678

3 Import

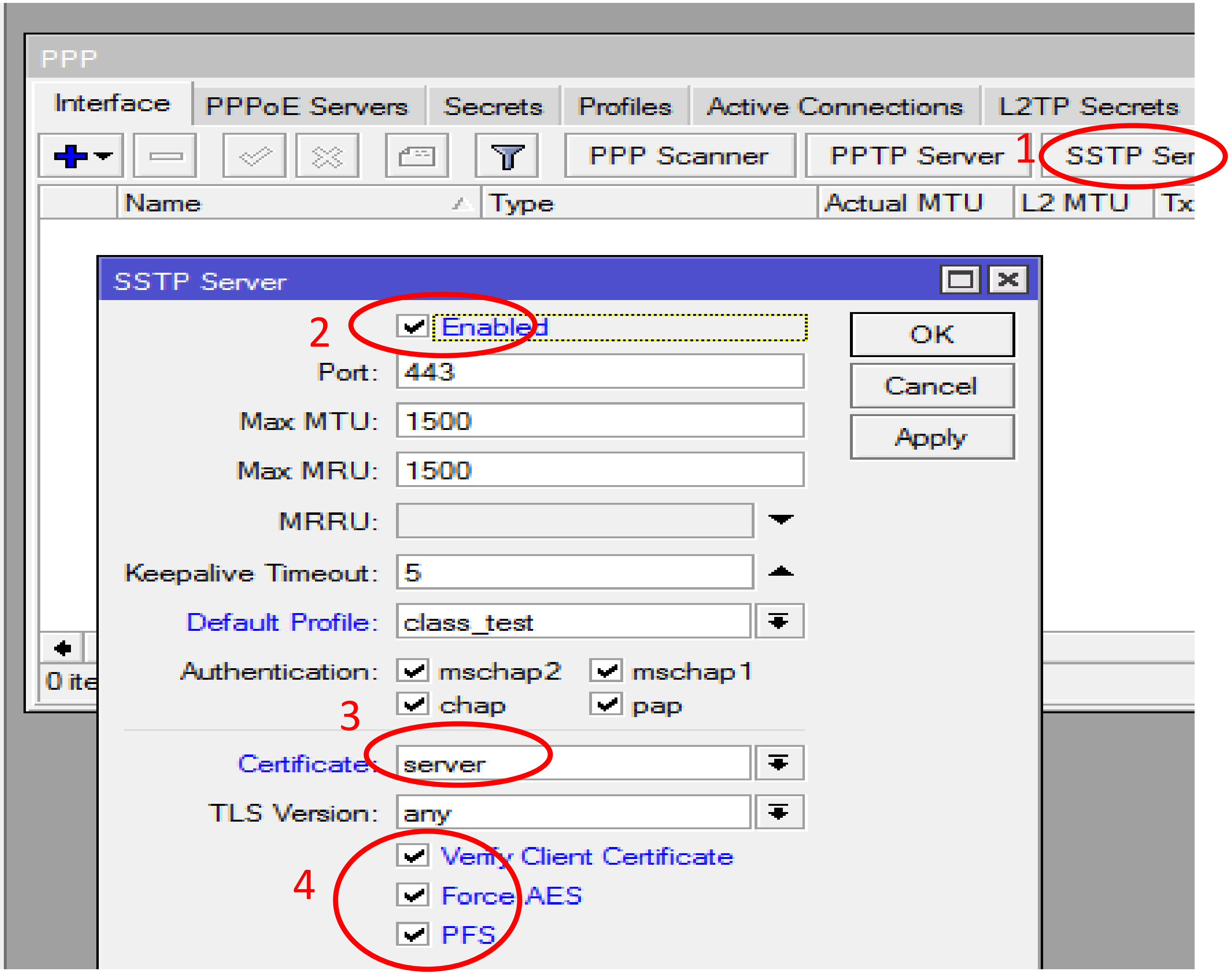
0 items

File Name	Type	Size	Creation Time
cert_export_pdsCA.crt	.crt file	1184 B	Nov/27/2017 15:14:09
cert_export_pdsCA.key	.key file	1858 B	Nov/27/2017 15:14:19
cert_export_site1.crt	.crt file	1164 B	Nov/27/2017 15:14:31
cert_export_site1.key	.key file	1858 B	Nov/27/2017 15:14:37

Deploying digital certificates

Using Digital Certificates on SSTP tunnels

Enable SSTP Server to use Certificate



SSTP Server

☑ Enabled

Port: 443

Max MTU: 1500

Max MRU: 1500

MRRU:

Keepalive Timeout: 5

Default Profile: class_test

Authentication: ☑ mschap2 ☑ mschap1 ☑ chap ☑ pap

Certificate: server

TLS Version: any

☑ Verify Client Certificate

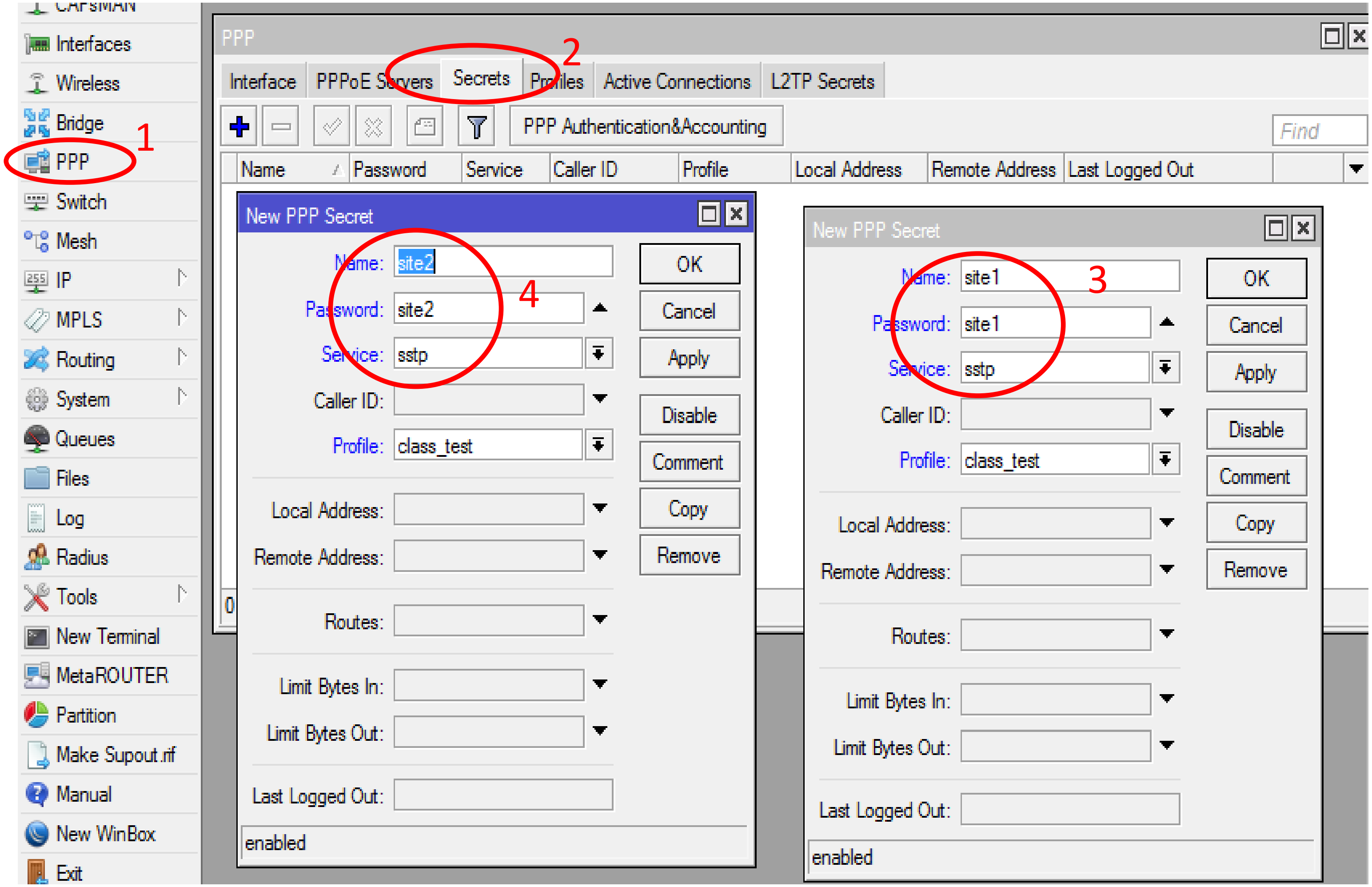
☑ Force AES

☑ PFS

Deploying digital certificates

Using Digital Certificates on SSTP tunnels

Create credentials for site1 and site2 on SSTP Server



New PPP Secret

Name: site2
Password: site2
Service: sstp
Caller ID:
Profile: class_test
Local Address:
Remote Address:
Routes:
Limit Bytes In:
Limit Bytes Out:
Last Logged Out:
enabled

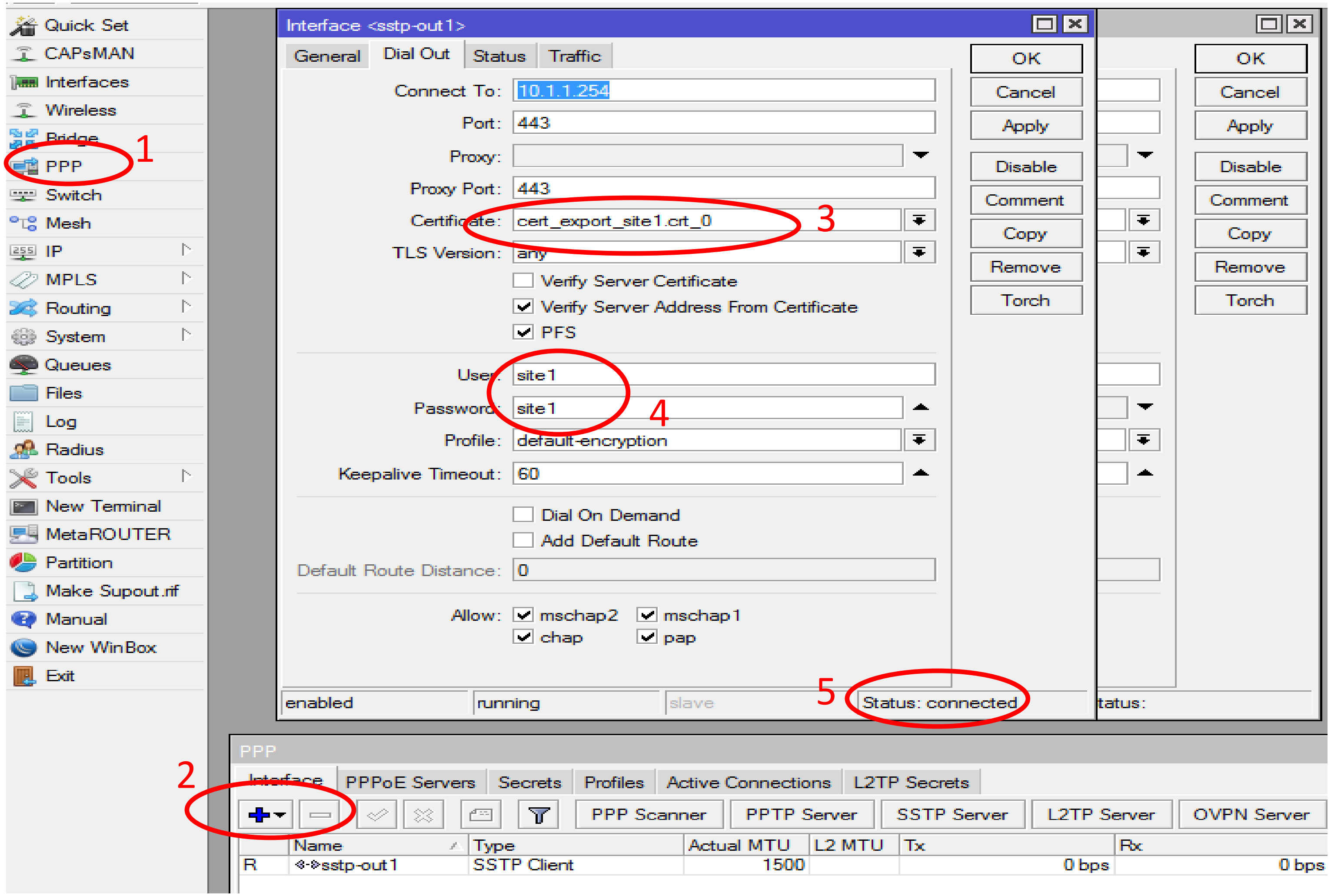
New PPP Secret

Name: site1
Password: site1
Service: sstp
Caller ID:
Profile: class_test
Local Address:
Remote Address:
Routes:
Limit Bytes In:
Limit Bytes Out:
Last Logged Out:
enabled

Deploying digital certificates

Using Digital Certificates on SSTP tunnels

Add SSTP client on site1 as below.



Interface <sstp-out1>

Connect To: 10.1.1.254

Port: 443

Proxy:

Proxy Port: 443

Certificate: cert_export_site1.crt_0

TLS Version: any

□ Verify Server Certificate

☑ Verify Server Address From Certificate

☑ PFS

User: site1

Password: site1

Profile: default-encryption

Keepalive Timeout: 60

□ Dial On Demand

□ Add Default Route

Default Route Distance: 0

Allow: ☑ mschap2 ☑ mschap1 ☑ chap ☑ pap

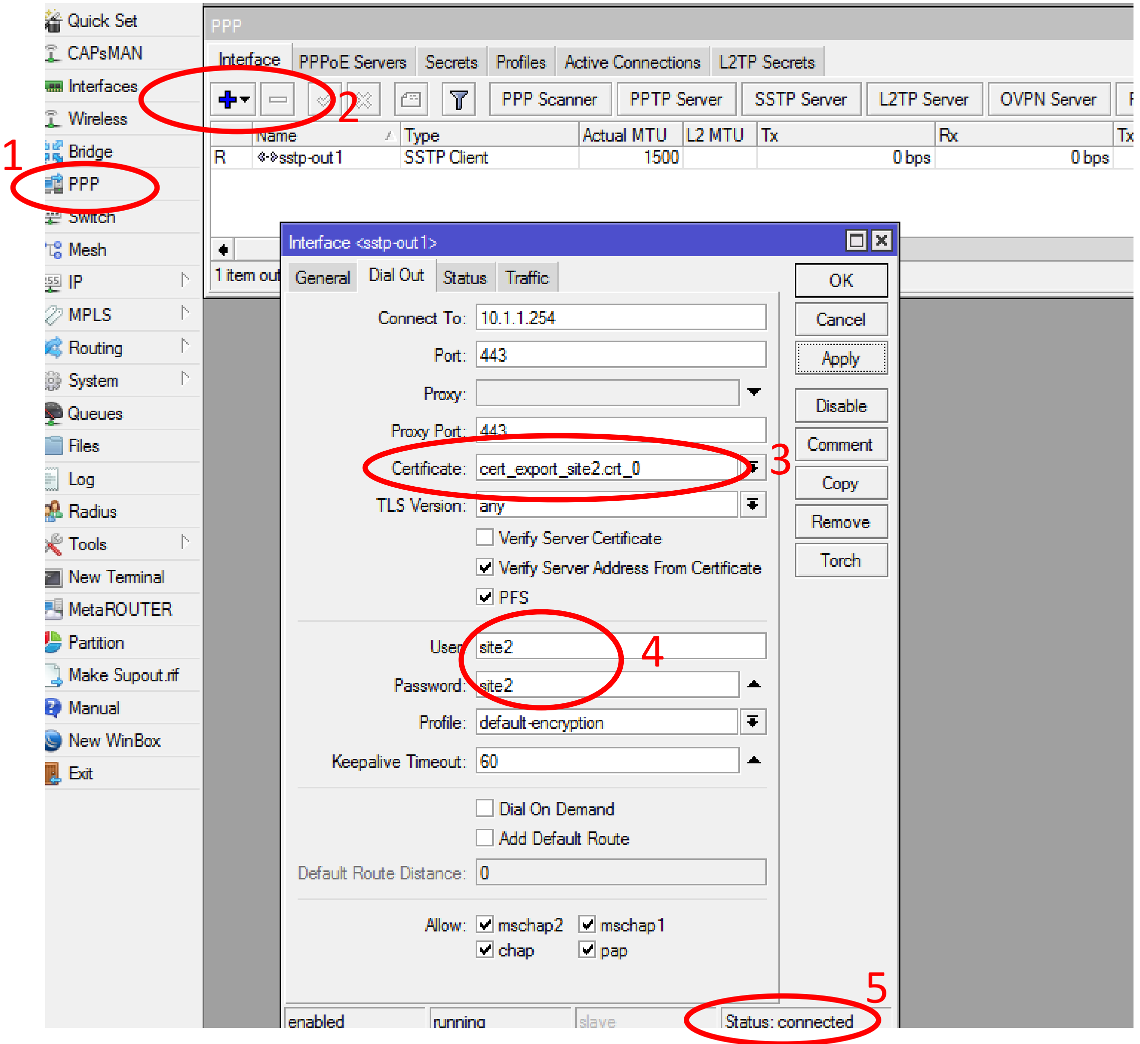
enabled | running | slave | Status: connected

	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.



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

1 item out

Interface <sstp-out1>

Connect To: 10.1.1.254

Port: 443

Proxy:

Proxy Port: 443

Certificate: cert_export_site2.crt_0

TLS Version: any

□ Verify Server Certificate

☑ Verify Server Address From Certificate

☑ PFS

User: site2

Password: site2

Profile: default-encryption

Keepalive Timeout: 60

□ Dial On Demand

□ Add Default Route

Default Route Distance: 0

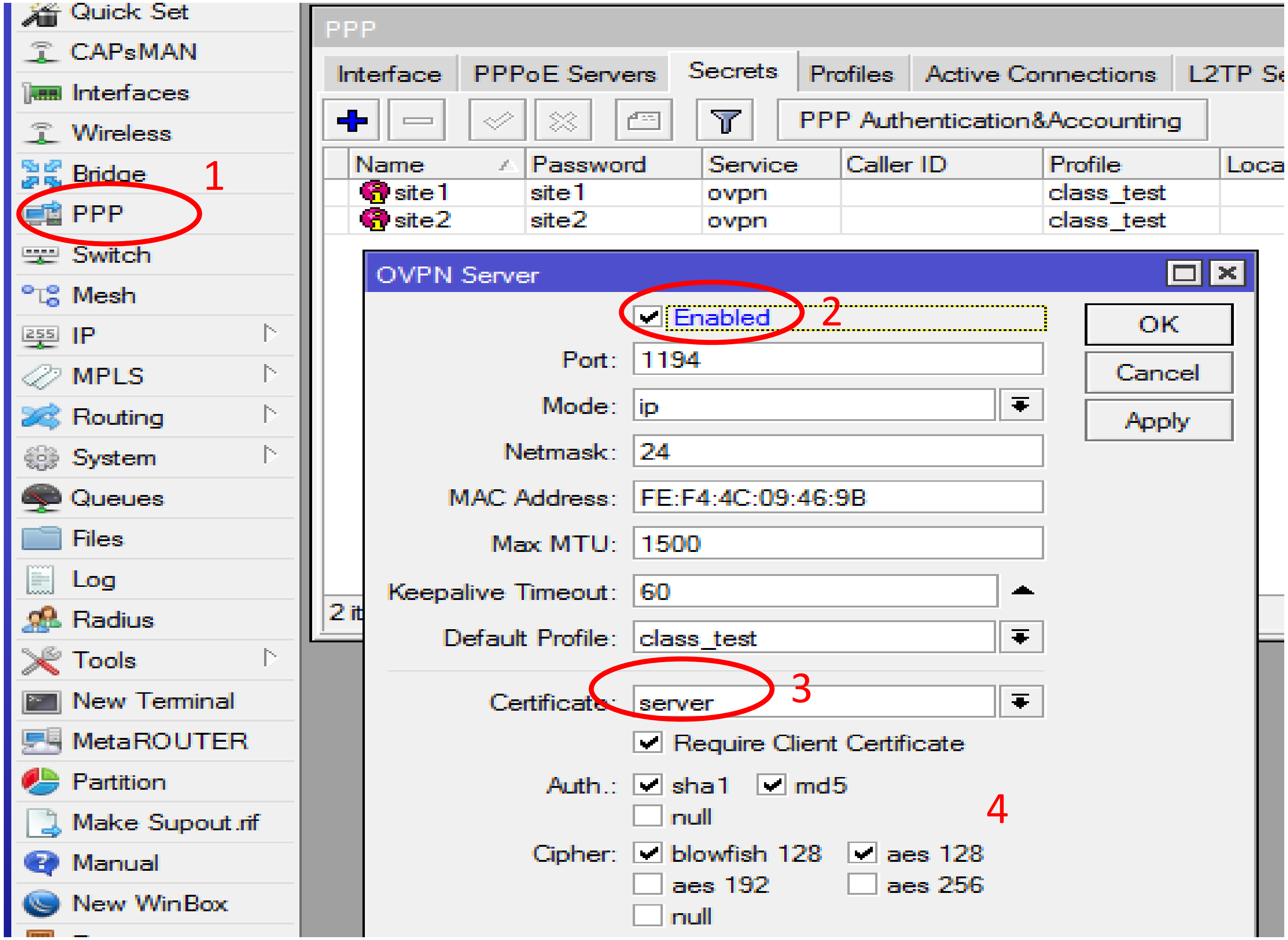
Allow: ☑ mschap2 ☑ mschap1 ☑ chap ☑ pap

enabled | running | slave | Status: connected

Deploying digital certificates

Using Digital Certificates on OpenVPN tunnels

Enable OpenVPN Server to use Certificate



Name	Password	Service	Caller ID	Profile	Loca
site1	site1	ovpn		class_test	
site2	site2	ovpn		class_test	

OVPN Server

☑ Enabled

Port: 1194

Mode: ip

Netmask: 24

MAC Address: FE:F4:4C:09:46:9B

Max MTU: 1500

Keepalive Timeout: 60

Default Profile: class_test

Certificate: server

☑ Require Client Certificate

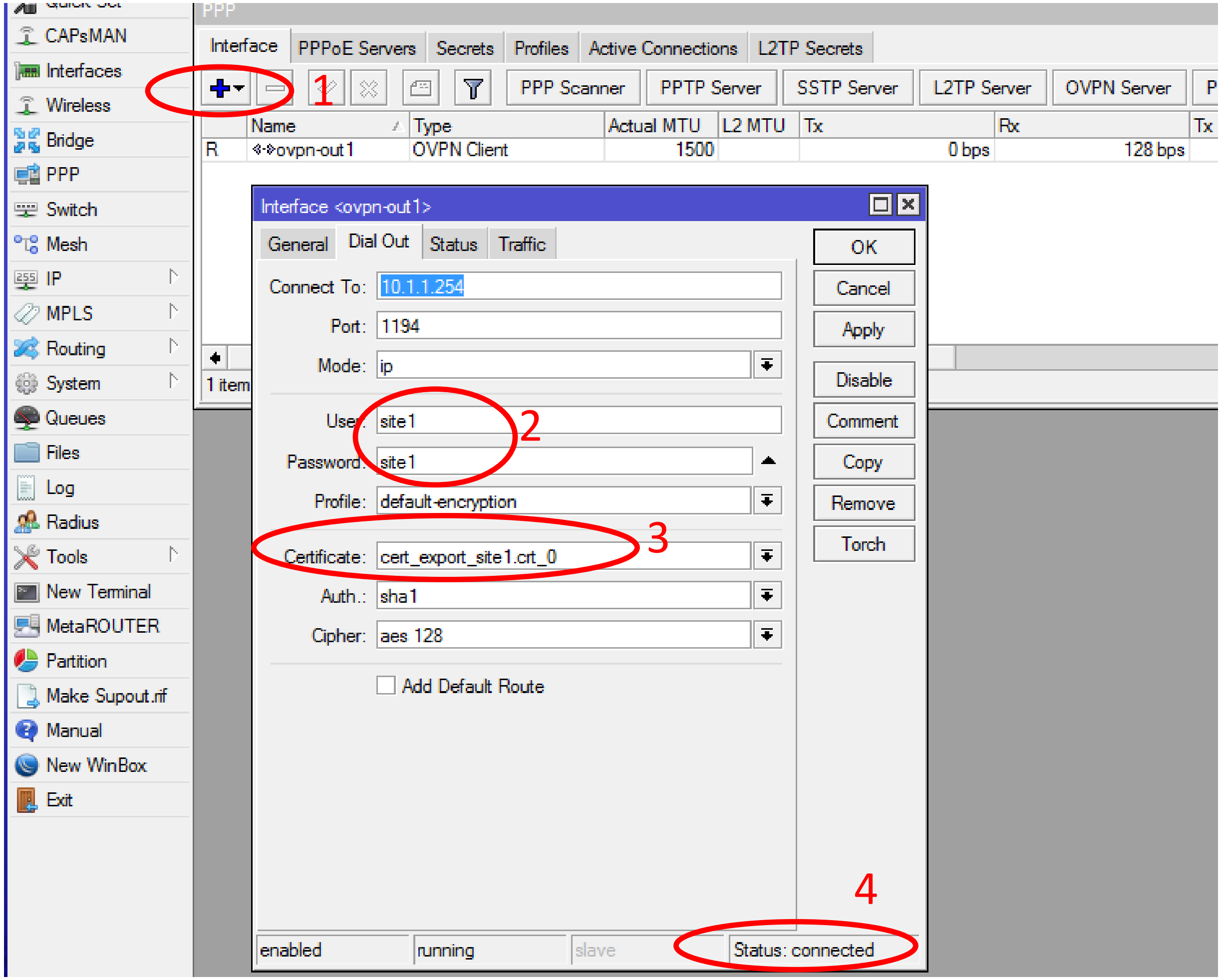
Auth.: ☑ sha1 ☑ md5
☐ null

Cipher: ☑ blowfish 128 ☑ aes 128
☐ aes 192 ☐ aes 256
☐ null

Deploying digital certificates

Using Digital Certificates on OpenVPN tunnels

Add OpenVPN client on site1 and site2 as below.



	Name	Type	Actual MTU	L2 MTU	Tx	Rx
R	ovpn-out1	OVPN Client	1500		0 bps	128 bps

Interface <ovpn-out1>

Connect To: 10.1.1.254

Port: 1194

Mode: ip

User: site1

Password: site1

Profile: default-encryption

Certificate: cert_export_site1.crt_0

Auth.: sha1

Cipher: aes 128

□ Add Default Route

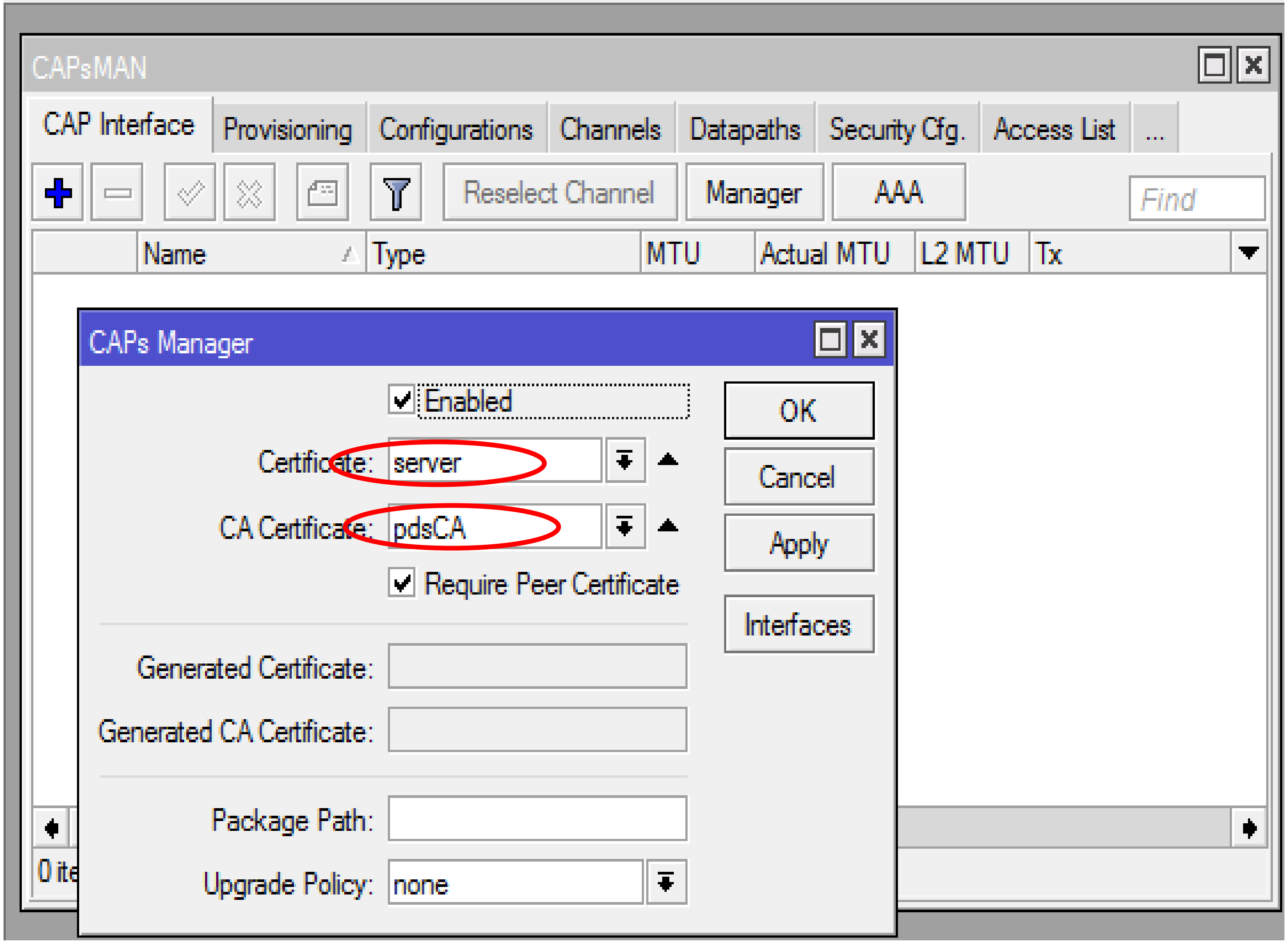
enabled | running | slave | Status: connected

Repeat the setup for site2

Deploying digital certificates

Deploying digital certificates for CAP to CapsMan connections

Enable CapsManager with certificate



☑ Enabled

Certificate: server

CA Certificate: pdsCA

☑ Require Peer Certificate

Generated Certificate:

Generated CA Certificate:

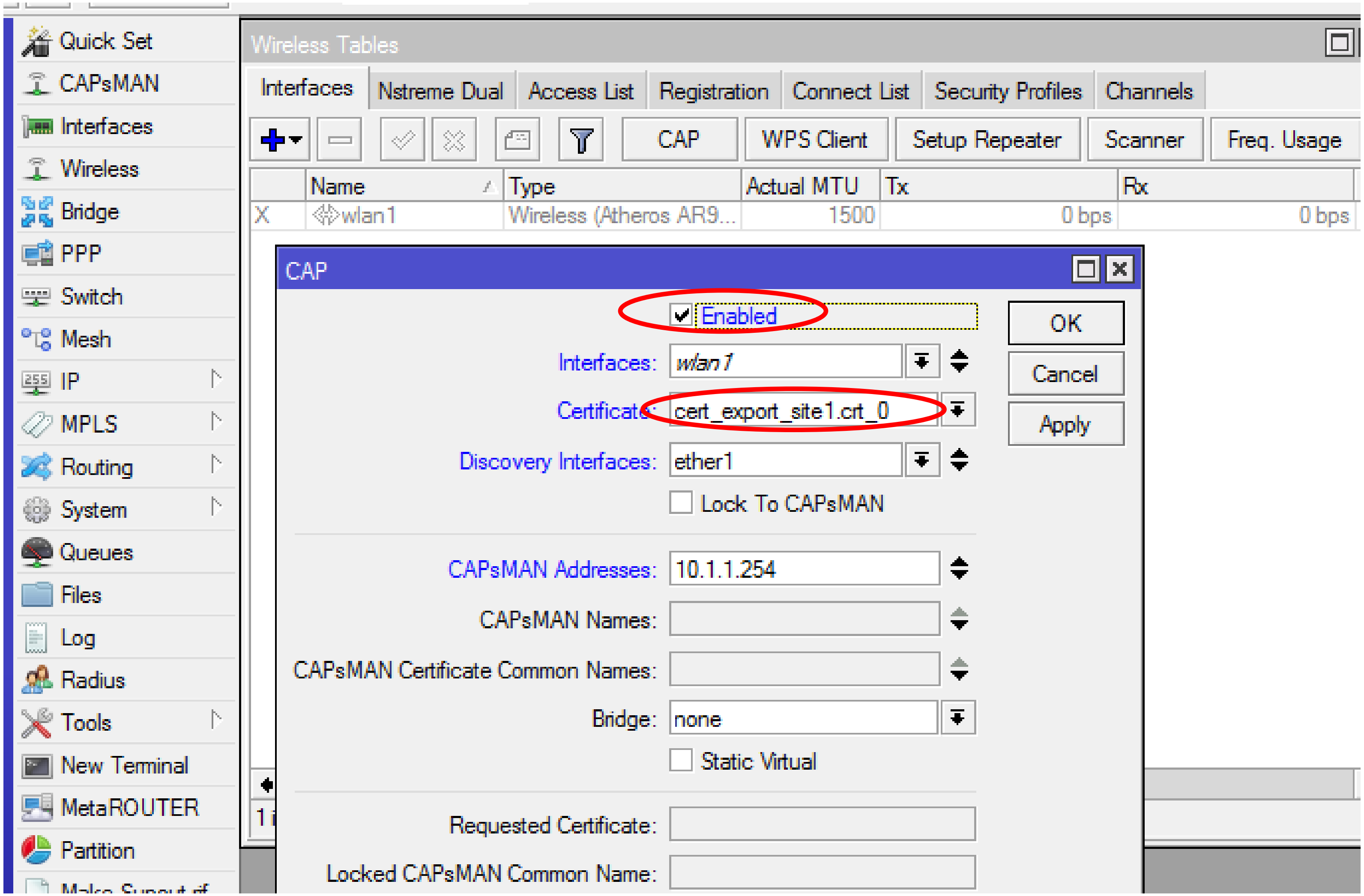
Package Path:

Upgrade Policy: none

Deploying digital certificates

Deploying digital certificates for CAP to CapsMan connections

Enable CAP with certificate:



	Name	Type	Actual MTU	Tx	Rx
X	wlan1	Wireless (Atheros AR9...	1500	0 bps	0 bps

CAP

☑ Enabled

Interfaces: wlan1

Certificate: cert_export_site1.crt_0

Discovery Interfaces: ether1

□ Lock To CAPsMAN

CAPsMAN Addresses: 10.1.1.254

CAPsMAN Names:

CAPsMAN Certificate Common Names:

Bridge: none

□ Static Virtual

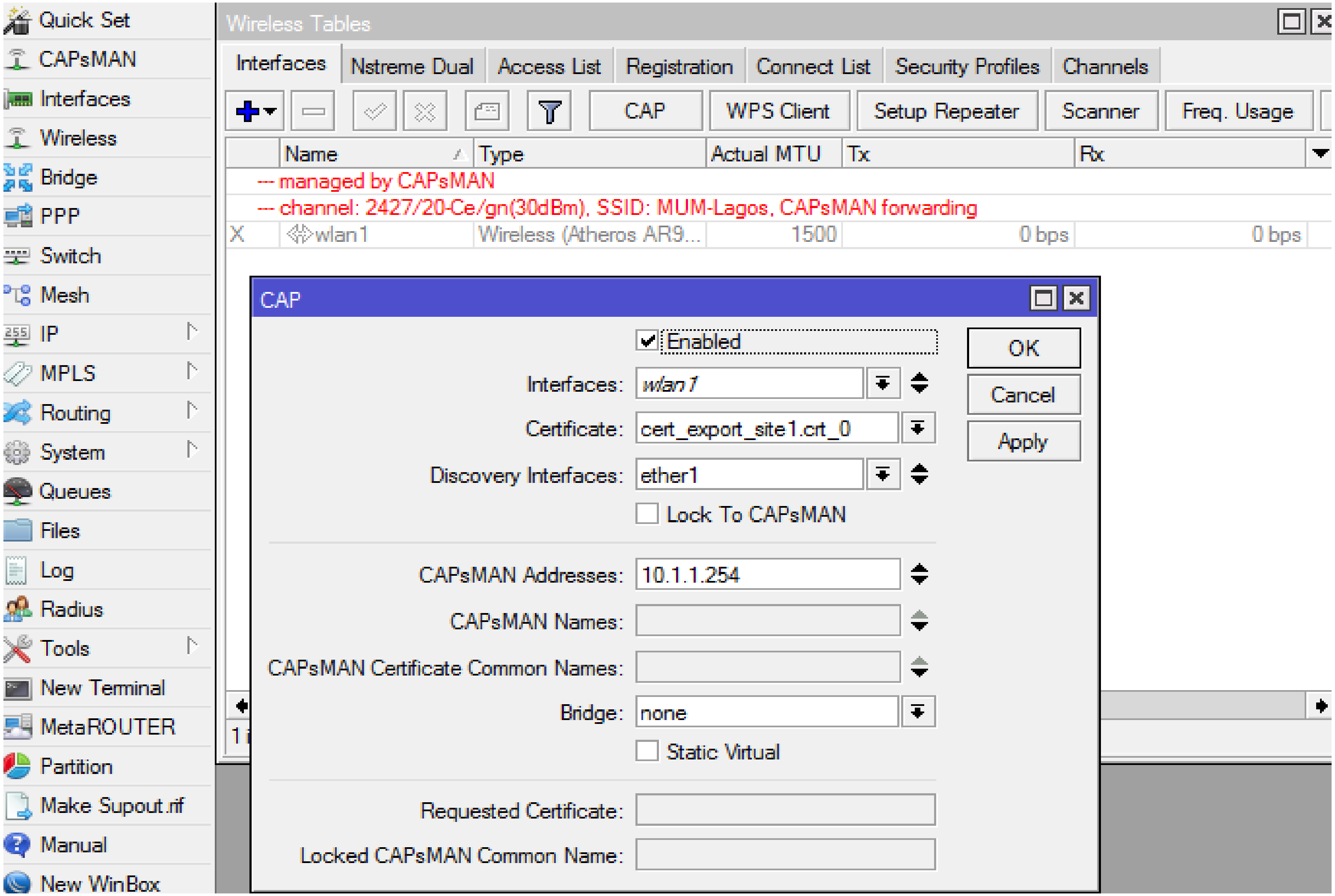
Requested Certificate:

Locked CAPsMAN Common Name:

Deploying digital certificates

Deploying digital certificates for CAP to CapsMan connections

Enable CAP with certificate



```
-- 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

☑ Enabled

Interfaces: wlan1

Certificate: cert_export_site1.crt_0

Discovery Interfaces: ether1

☐ Lock To CAPsMAN

CAPsMAN Addresses: 10.1.1.254

CAPsMAN Names:

CAPsMAN Certificate Common Names:

Bridge: none

☐ Static Virtual

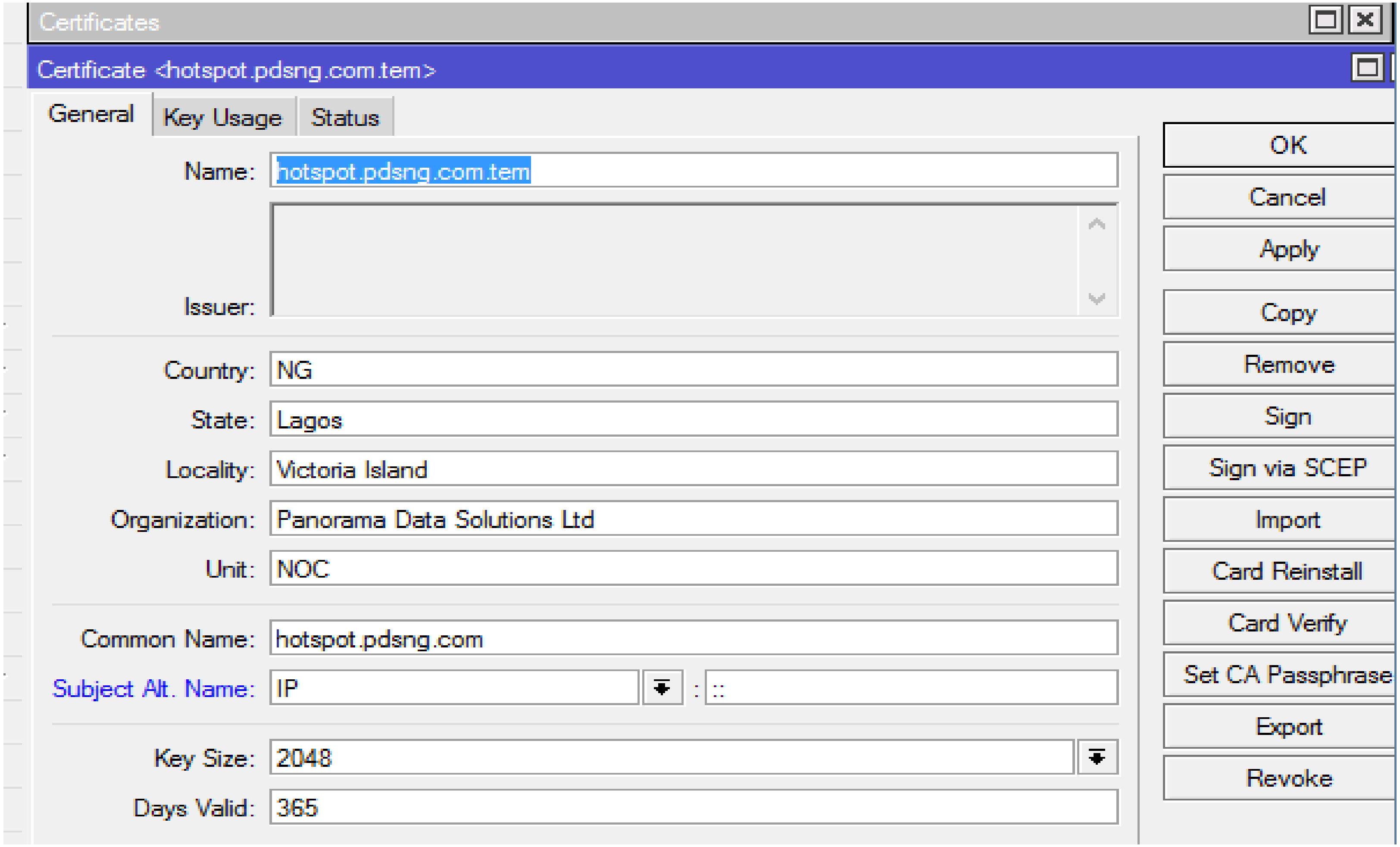
Requested Certificate:

Locked CAPsMAN Common Name:

Deploying digital certificates

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

Create a certificate template:

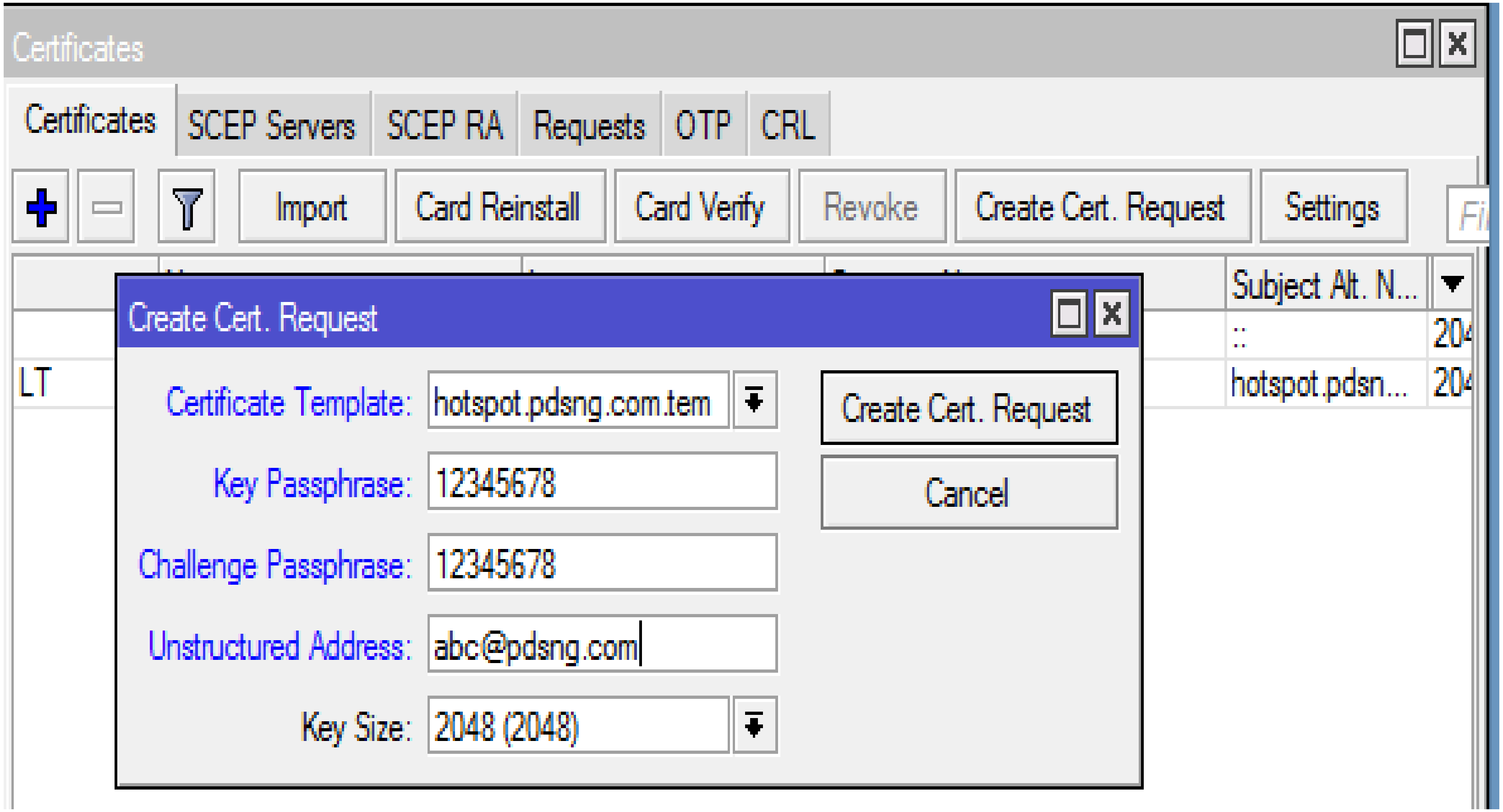


Name:	hotspot.pdsng.com.tem
Issuer:	
Country:	NG
State:	Lagos
Locality:	Victoria Island
Organization:	Panorama Data Solutions Ltd
Unit:	NOC
Common Name:	hotspot.pdsng.com
Subject Alt. Name:	IP : ::
Key Size:	2048
Days Valid:	365

Deploying digital certificates

Deploying digital certificates on Hotspots

Create a certificate Signing request:



Certificate Template: hotspot.pdsng.com.tem

Key Passphrase: 12345678

Challenge Passphrase: 12345678

Unstructured Address: abc@pdsng.com

Key Size: 2048 (2048)

Deploying digital certificates

Deploying digital certificates on Hotspots

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

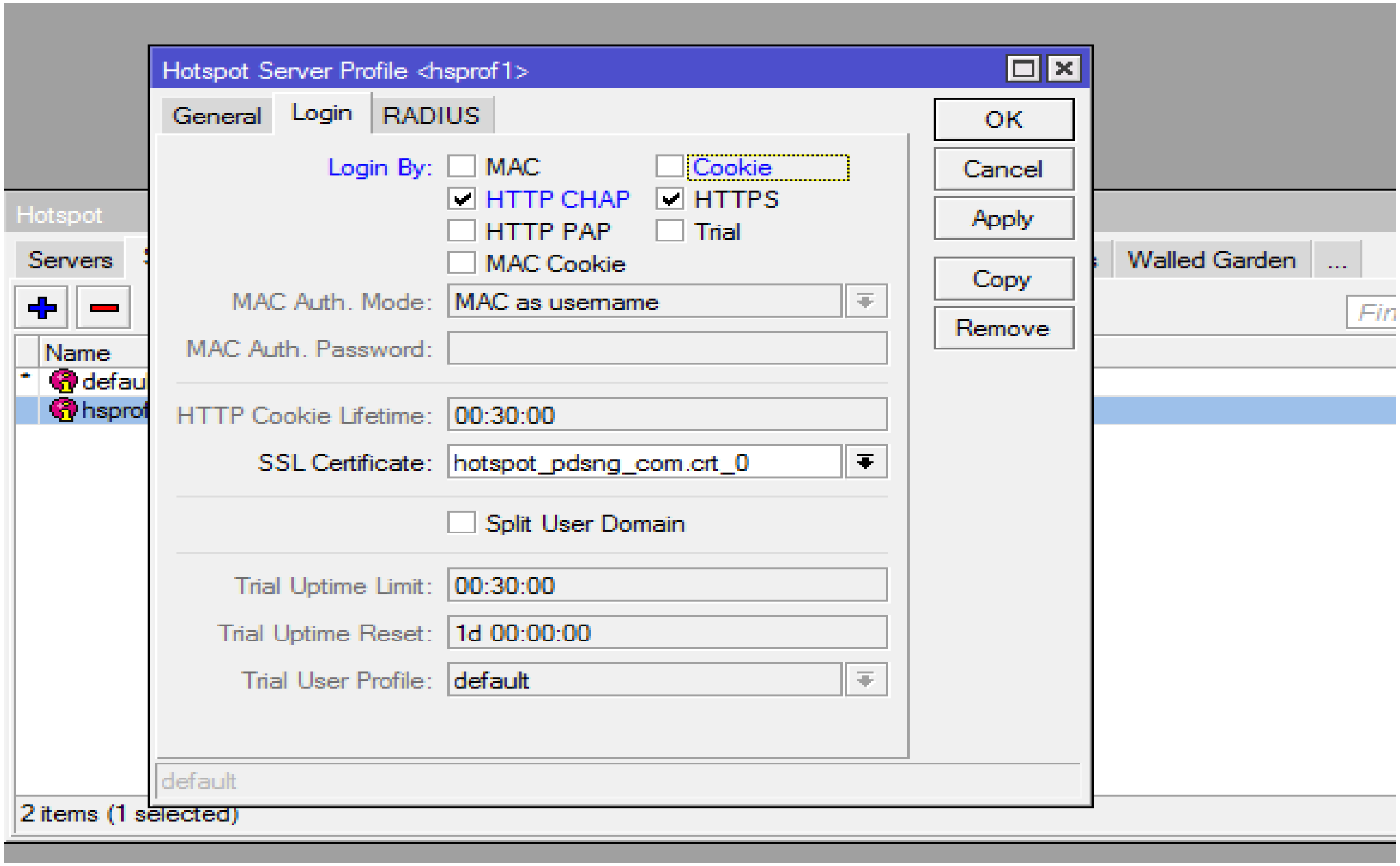
```
-----BEGIN CERTIFICATE REQUEST-----
MIIDKDCCAhACAQIwgYcxCzAJBgNVBAYTAk5HMQ4wDAYDVQQIDAVMYWdvczEYMBYG
A1UEBwwPVmljdG9yaWEgSXNsYW5kMSQwIgYDVQQKDBtQYW5vcmFtYSBEYXRhIFNv
bHV0aW9ucyBMdGQxDDAKBgNVBAsMA05PQzEaMBgGA1UEAwwRaG90c3BvdC5wZHNu
Zy5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCsMiohfqTfCNqR
lW2WUJfN60ikkAlBFZaYxFKjVNn51YDY3F+l2JMqBaVIibnjpPpWMtoXVgZN4tZ1
NHbPYWR32aMrVkjpmzVNjOhWoFfQ81FJnvucr3Ug7sSAcoeAwCfWY7WAwDjJCY/w
kF6p648SCK8wja9lDT+mNMPla56kp7ccmzj316QKBOoYGg/l4xf0qH4hAqHJHnuR
xFG4LyfMLrC10Qx/bAHM2dtRs12bohbQHeunRgTuf59do5ofuw3S5hhQOZYHGw+s
rC/qxV+seRvI16xK/HdvaFBje0m1mulsasW7GcnIc+ZCoIC9eoLACgNBFdl6o67z
8itHKdgRAgMBAAGgWzAXBgkqhkiG9w0BCQcxCgwIcGRzbmcxMjMwHwYJKoZIhvcN
AQkCMRIMEG1hZ251c0BwZHNuZy5jb20wHwYJKoZIhvcNAQkOMRIwEDAOBgNVHQ8B
Af8EBAMCAbYwDQYJKoZIhvcNAQELBQADggEBAKB8R6aVFBBfZMJz8frB+YUGyxmI
gQUw5LgcnjblqeJYUMsZqkOzuNfk3Kdh5jrBfqTNnZied8kKTzE82+kcw4trc8P8
1H7FU8pdRlUHFThxFe/hH5zYKwAjRb4UtCiryjoK1mq62wvK9QJ7fPceWtj46GY7
n/vkR2BbHrqMVdMhNX0f5V3f/pvwn4C5KvZEUPo80vLDGBX/jXb/k7LaU5NOS4Ro
I/6O8ep03Ry246VSuc+g64tbGYaB6jzSLy5MIt31kg8n/18Wv6uBQIApvwQI6xbb
hS/B01g8eIwseatsCRmWxyH6THtcwZmejlgp2F7GuY/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:



Login By: ☐ MAC ☐ Cookie

☑ HTTP CHAP ☑ HTTPS

☐ HTTP PAP ☐ Trial

☐ MAC Cookie

MAC Auth. Mode: MAC as username

MAC Auth. Password:

HTTP Cookie Lifetime: 00:30:00

SSL Certificate: hotspot_pdsng_com.crt_0

☐ Split User Domain

Trial Uptime Limit: 00:30:00

Trial Uptime Reset: 1d 00:00:00

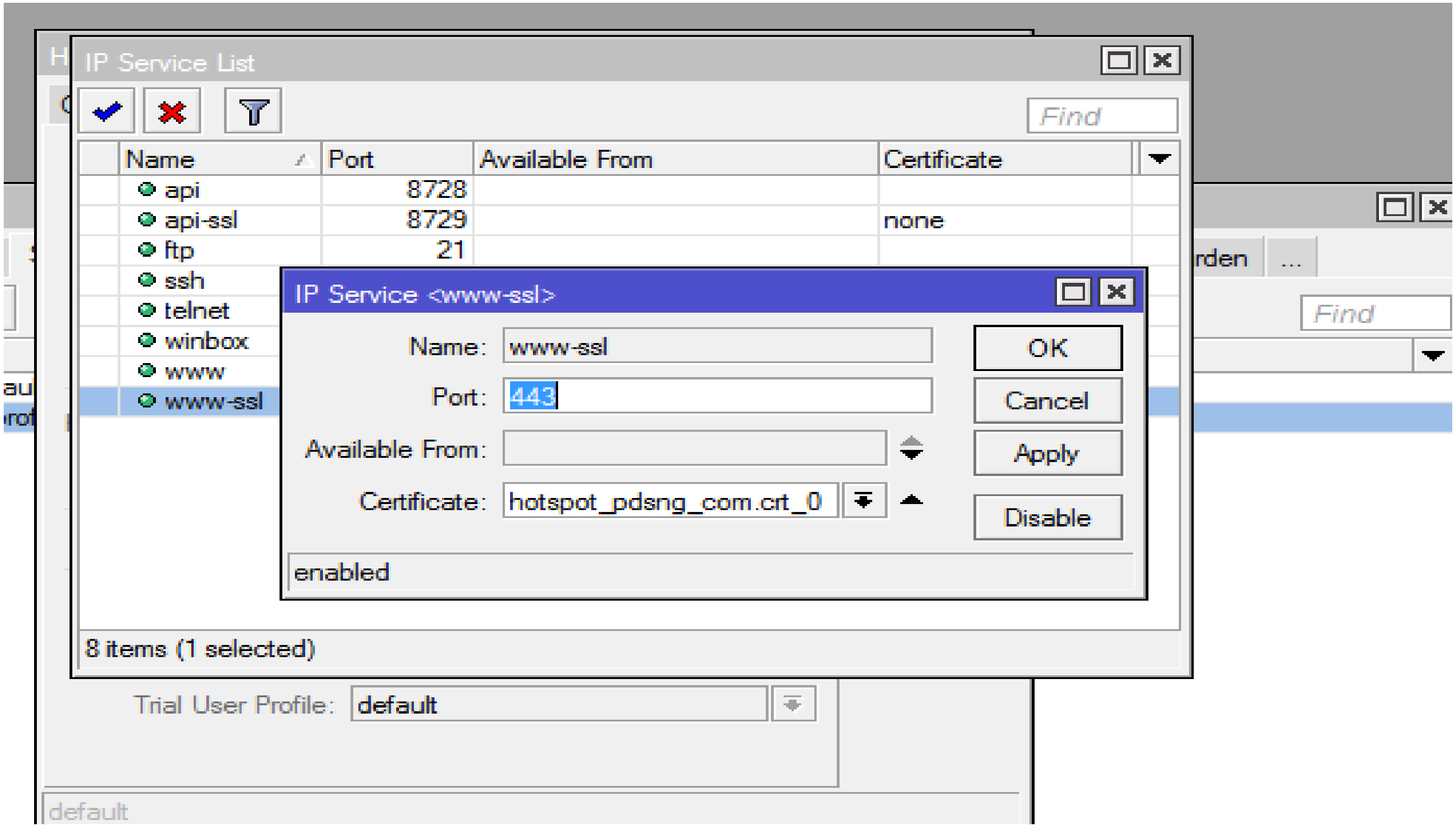
Trial User Profile: default

default

Deploying digital certificates

Deploying digital certificates on Hotspots

Setup www-ssl on IP services with the certificate:



IP Service List

Name	Port	Available From	Certificate
api	8728		
api-ssl	8729		none
ftp	21		
ssh			
telnet			
winbox			
www			
www-ssl			

8 items (1 selected)

IP Service <www-ssl>

Name: www-ssl

Port: 443

Available From:

Certificate: hotspot_pdsng_com.crt_0

enabled

Trial User Profile: default

default

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?