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:

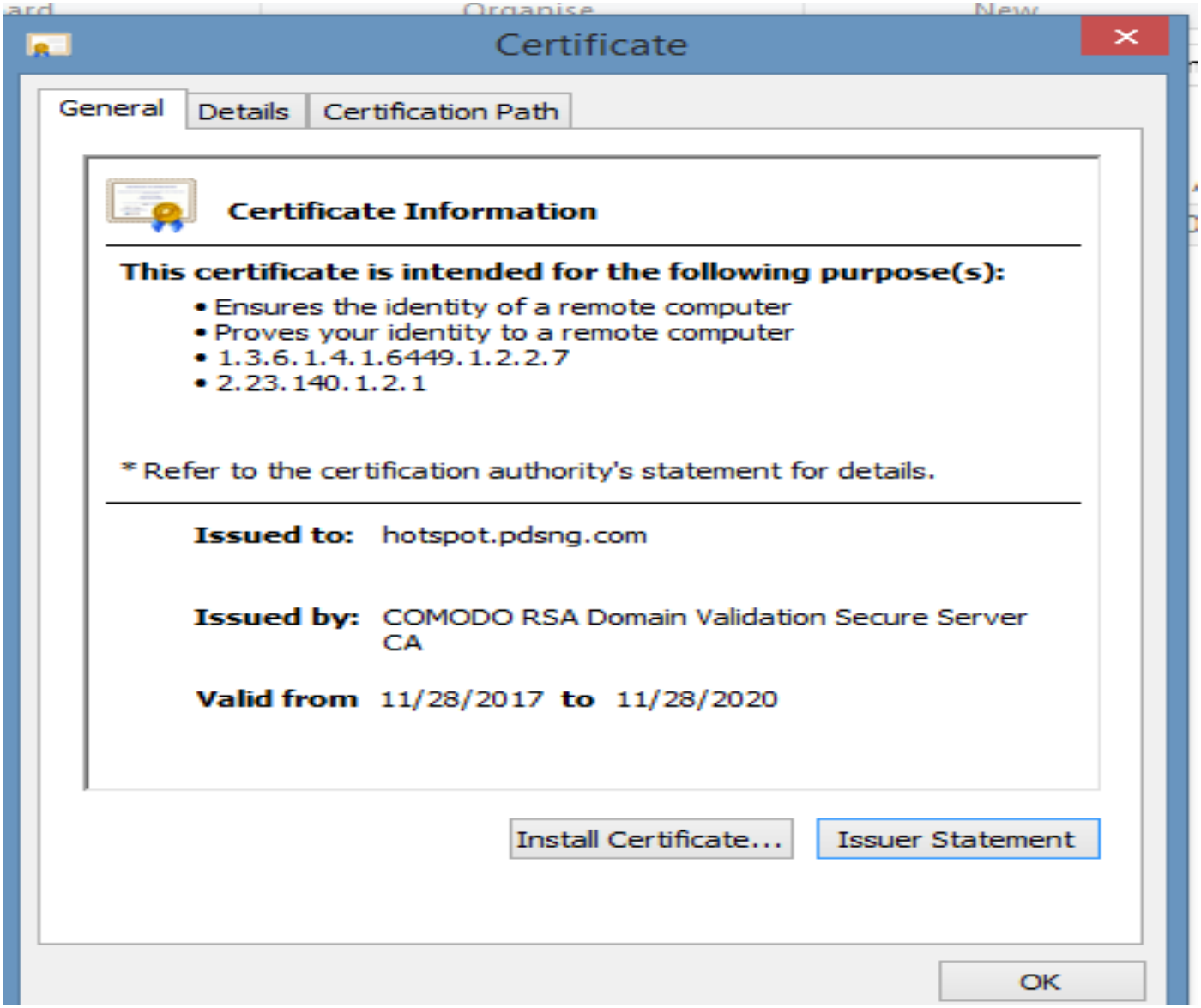
- Name of the certificate holder
- Serial Number
- Expiration date
- Name of the issuer
- Copy of the holders public key
- Digital signature of issuer

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

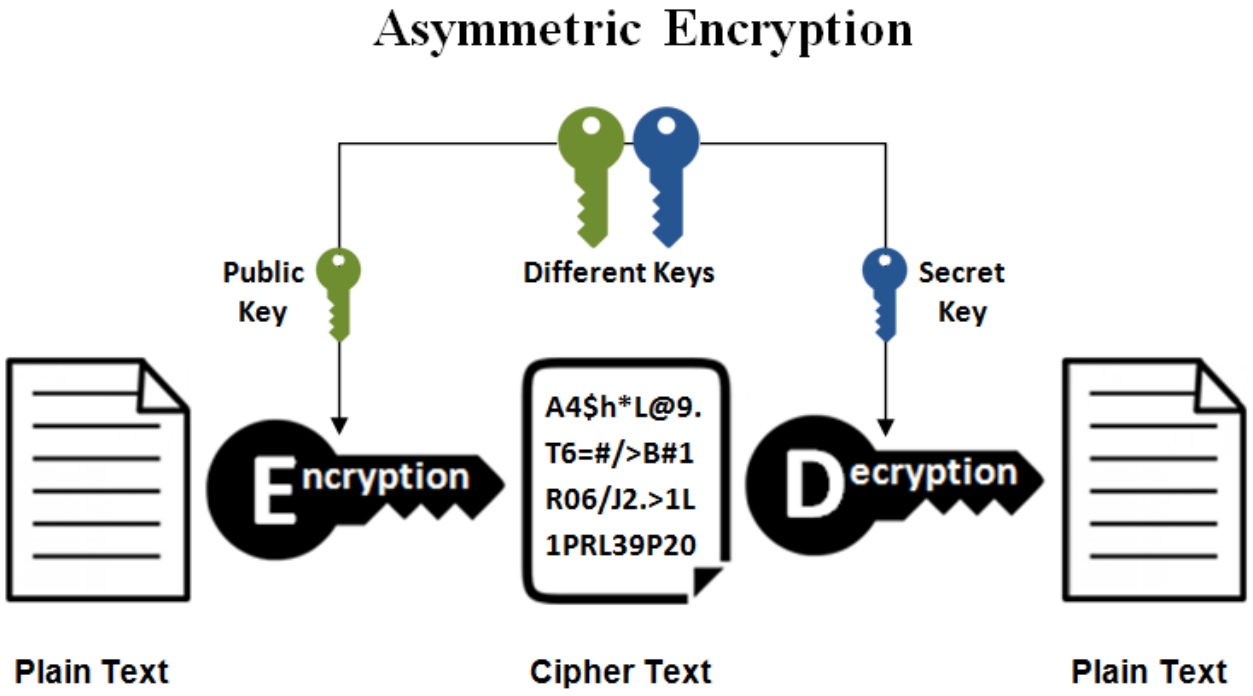
Why do we need certificate:

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:



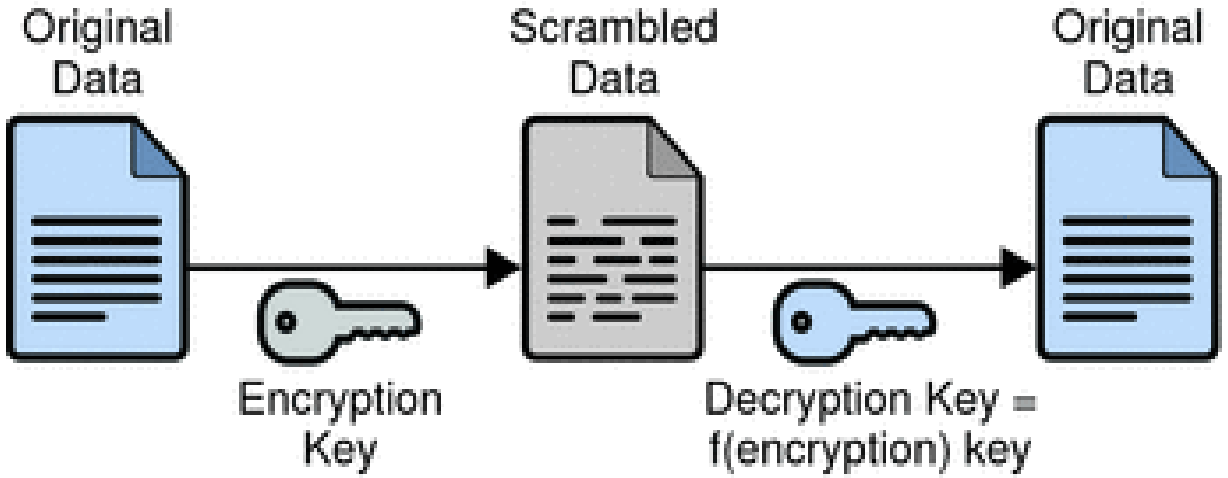
Courtesy ssl2buy.com

- 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

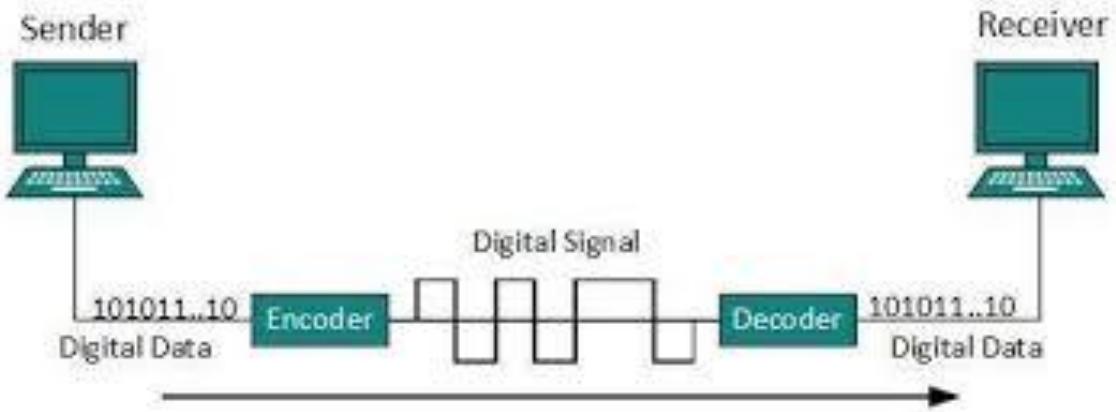
SSL Server Certificate

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.

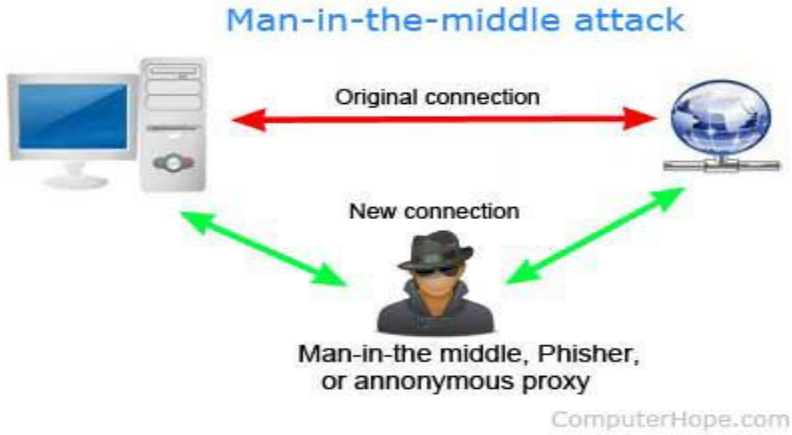


In the absence of SSL or any form of encryption, data is sent as stream of 1s and 0s in a universal encoding format.

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.

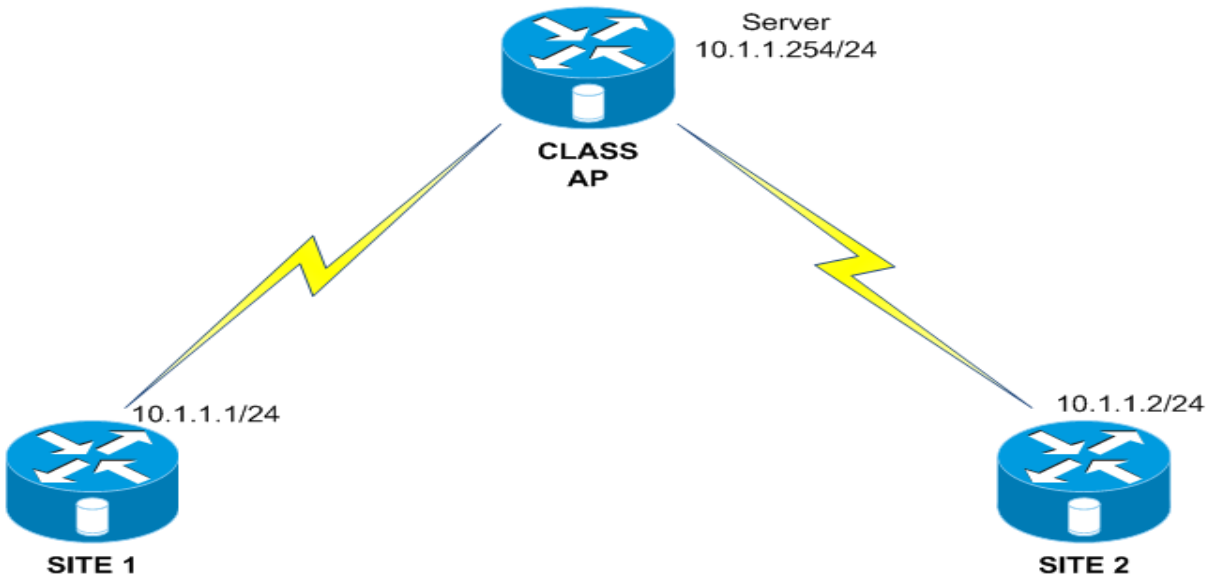
- The use of digital certificates will eliminate the possibility of man in the middle attack as such attackers will have a tough time breaking the connection between a source and the destination devices.

- 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

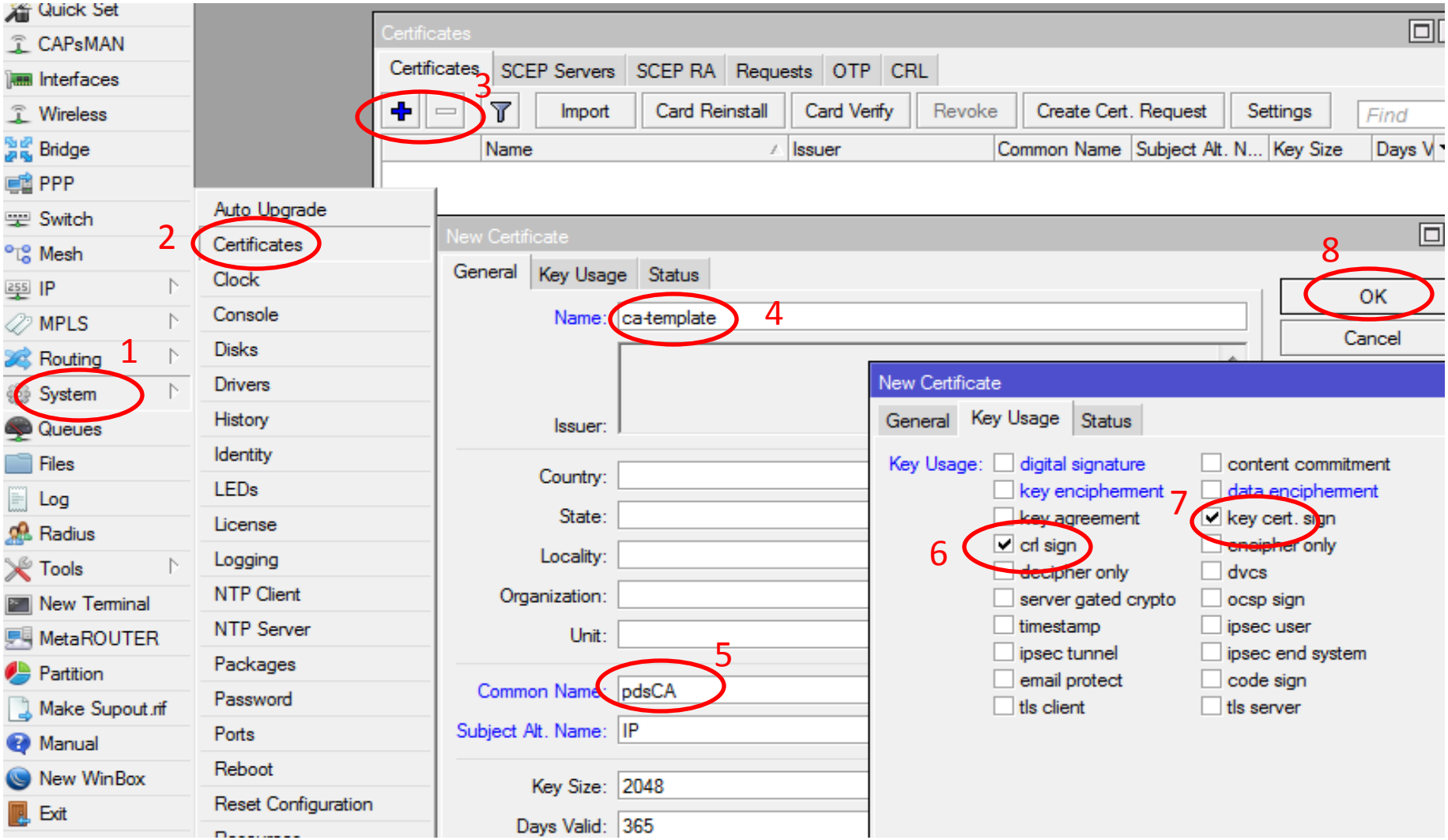
1. Make certificate templates
2. Sign the certificates and add CRL url
3. Export client certificates with keys and CA certificates and import to client routers

Network Topology:



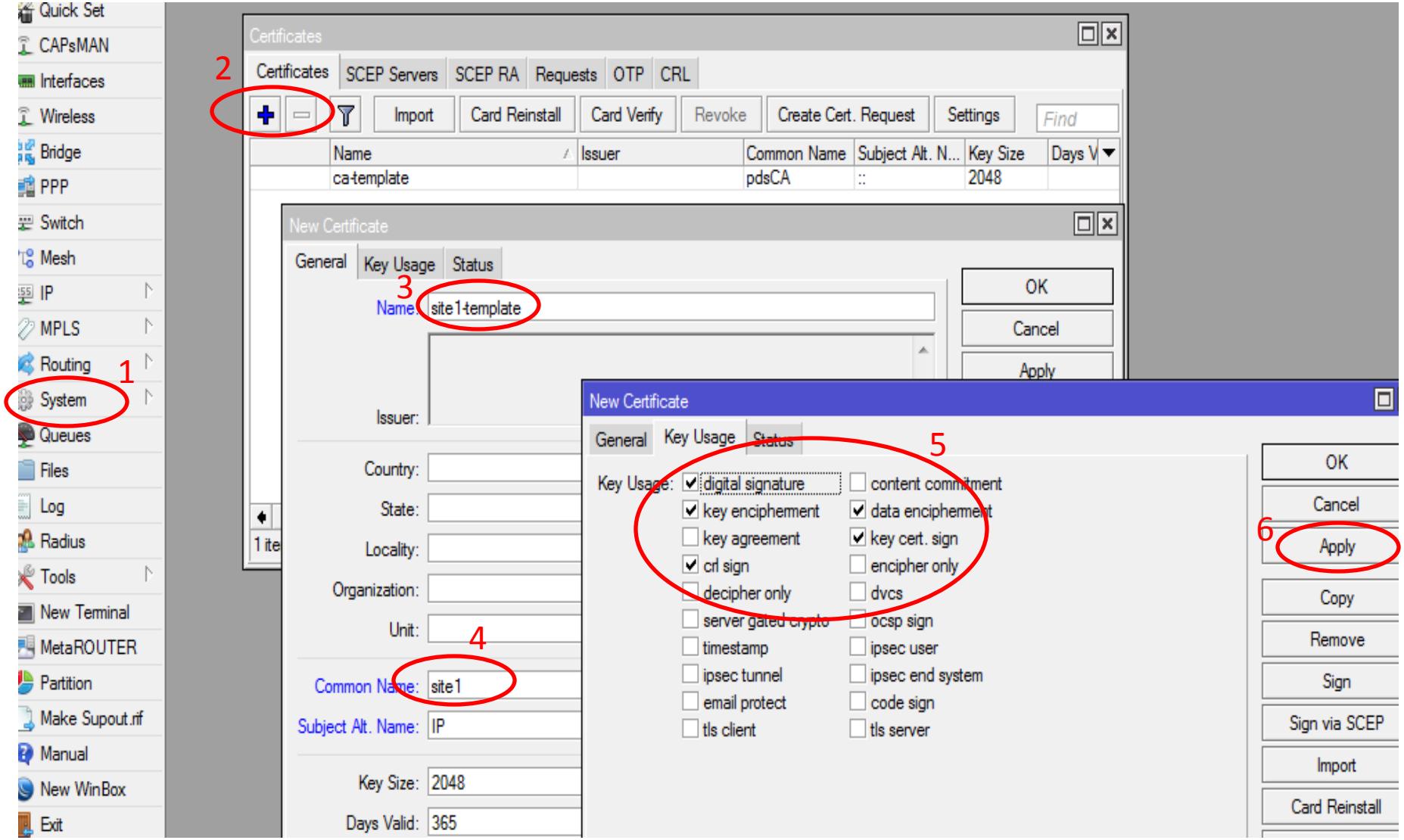
Creating certificates in RouterOs

Make certificate templates: CA Template



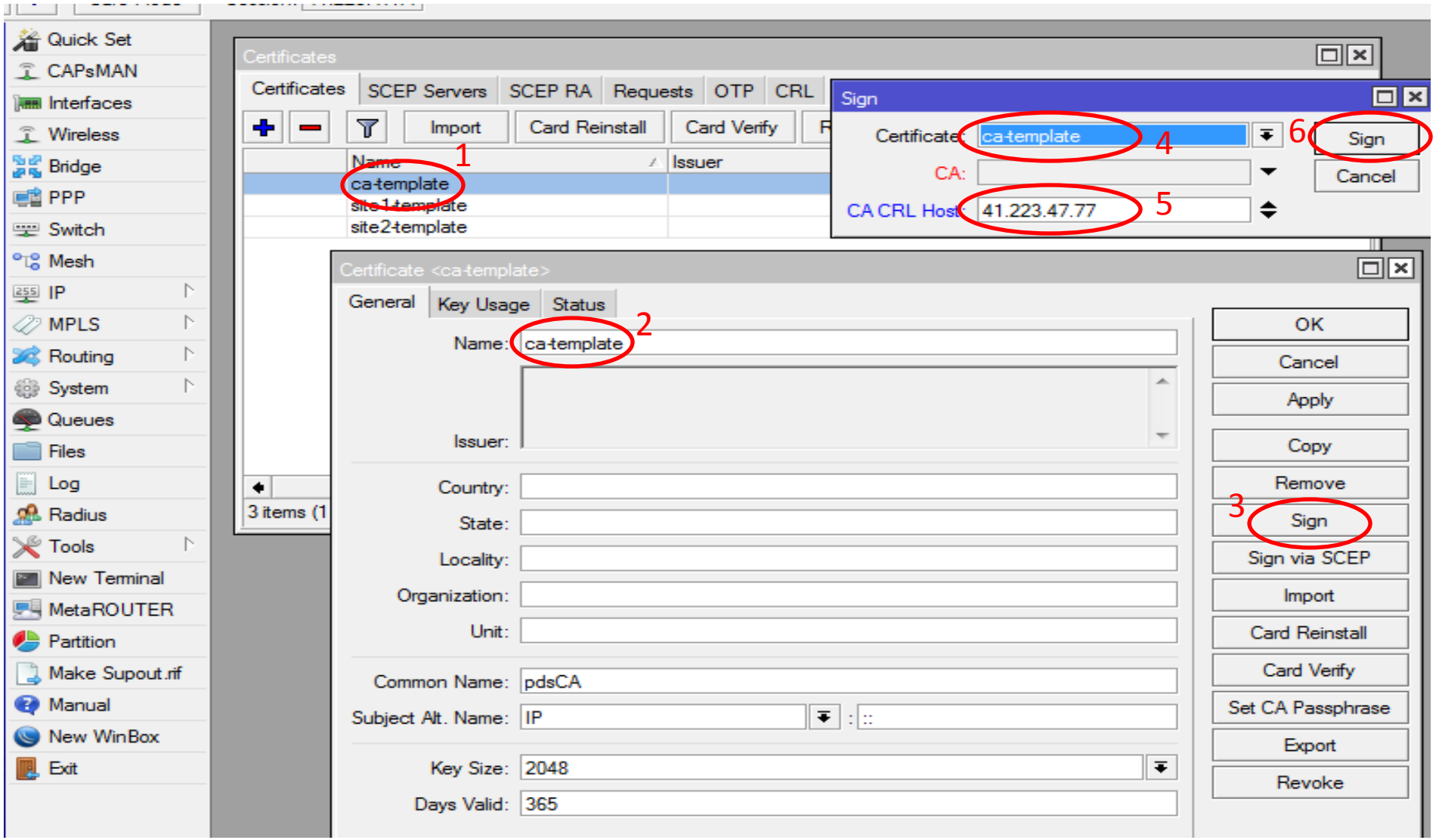
Creating certificates in RouterOs

Make certificate templates: Site1 Template



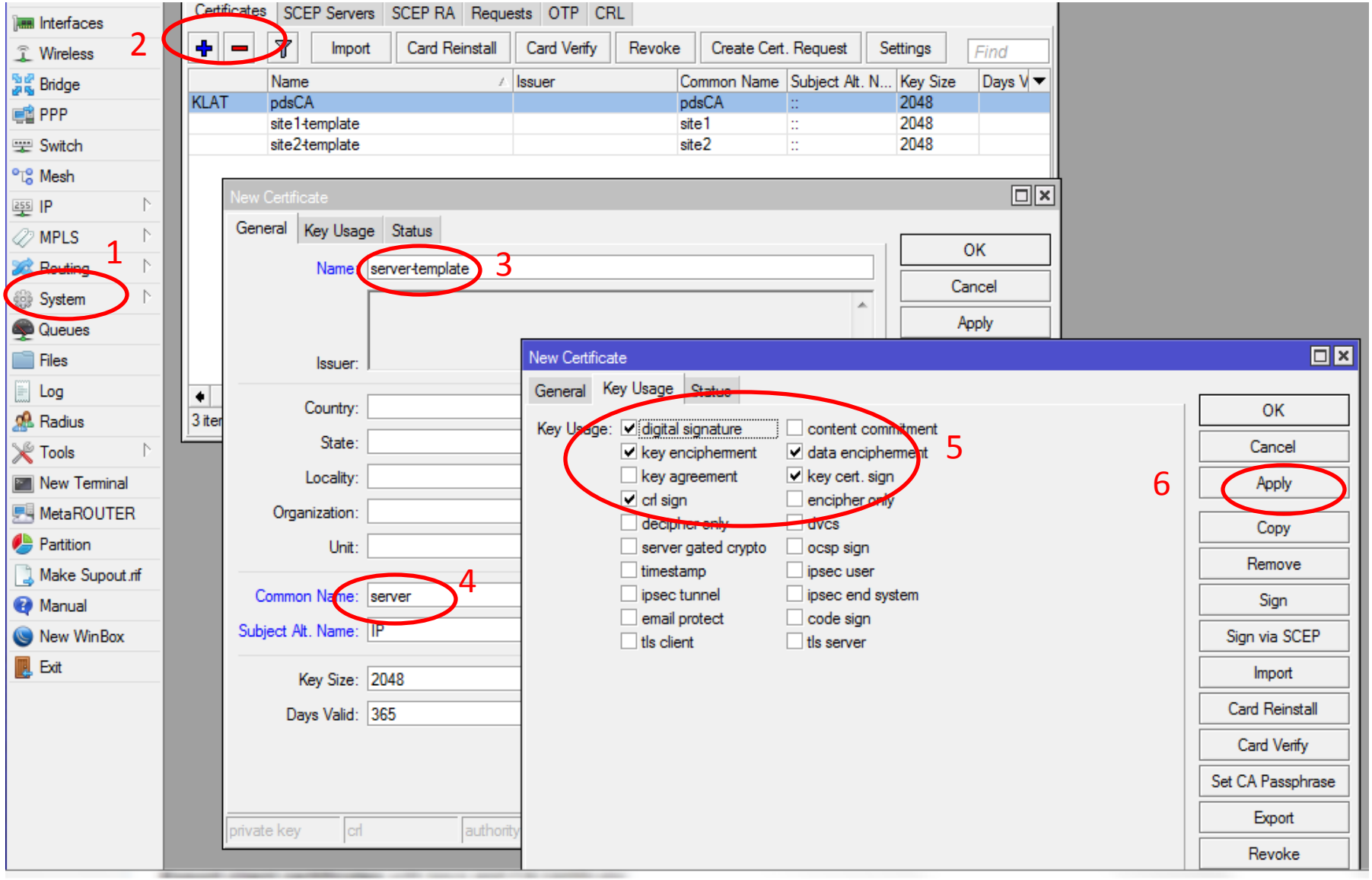
Creating certificates in RouterOs

Sign the CA certificate and add CRL url



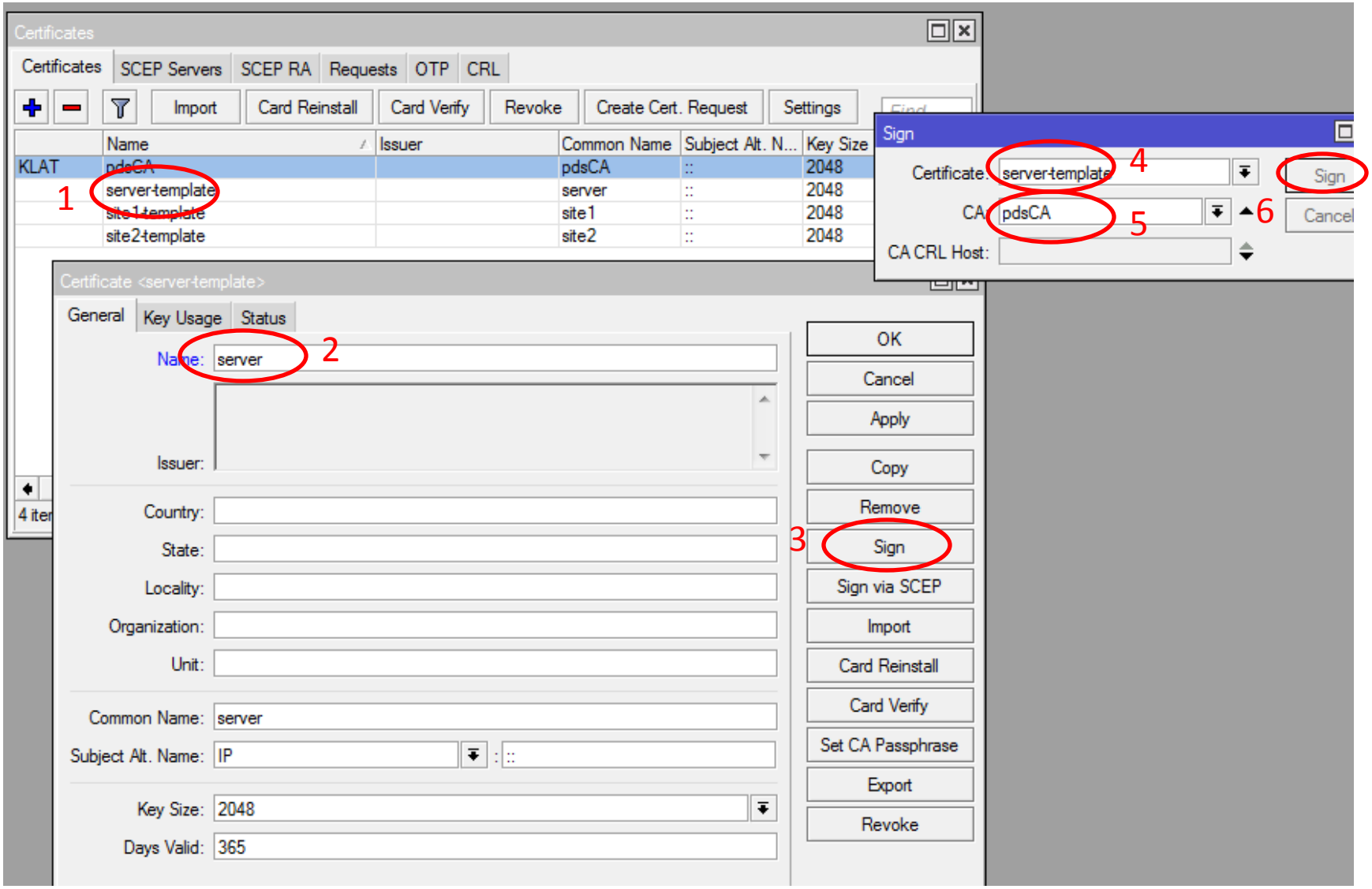
Creating certificates in RouterOs

Make certificate templates: Server Template



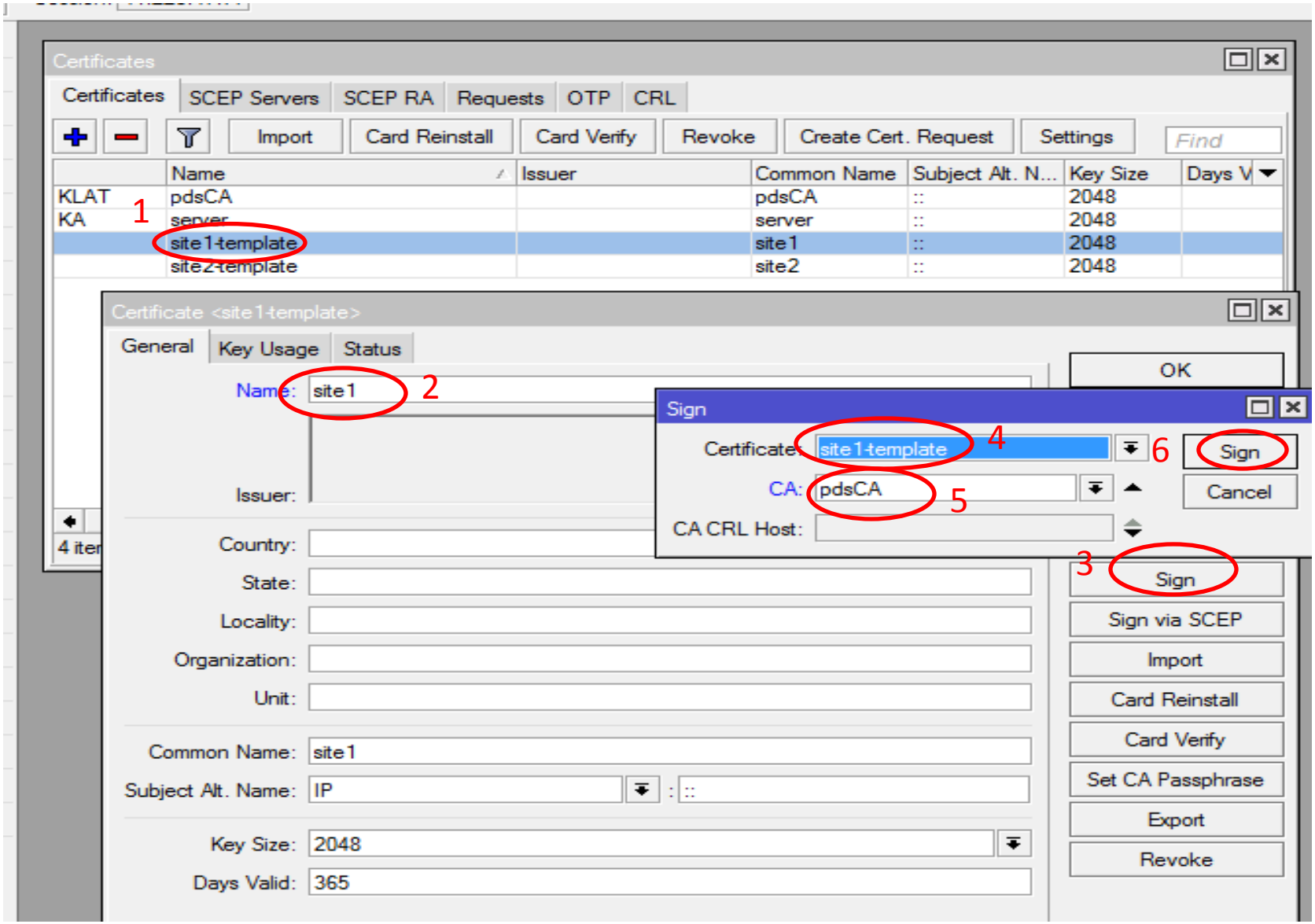
Creating certificates in RouterOs

Sign certificate templates: Server Template



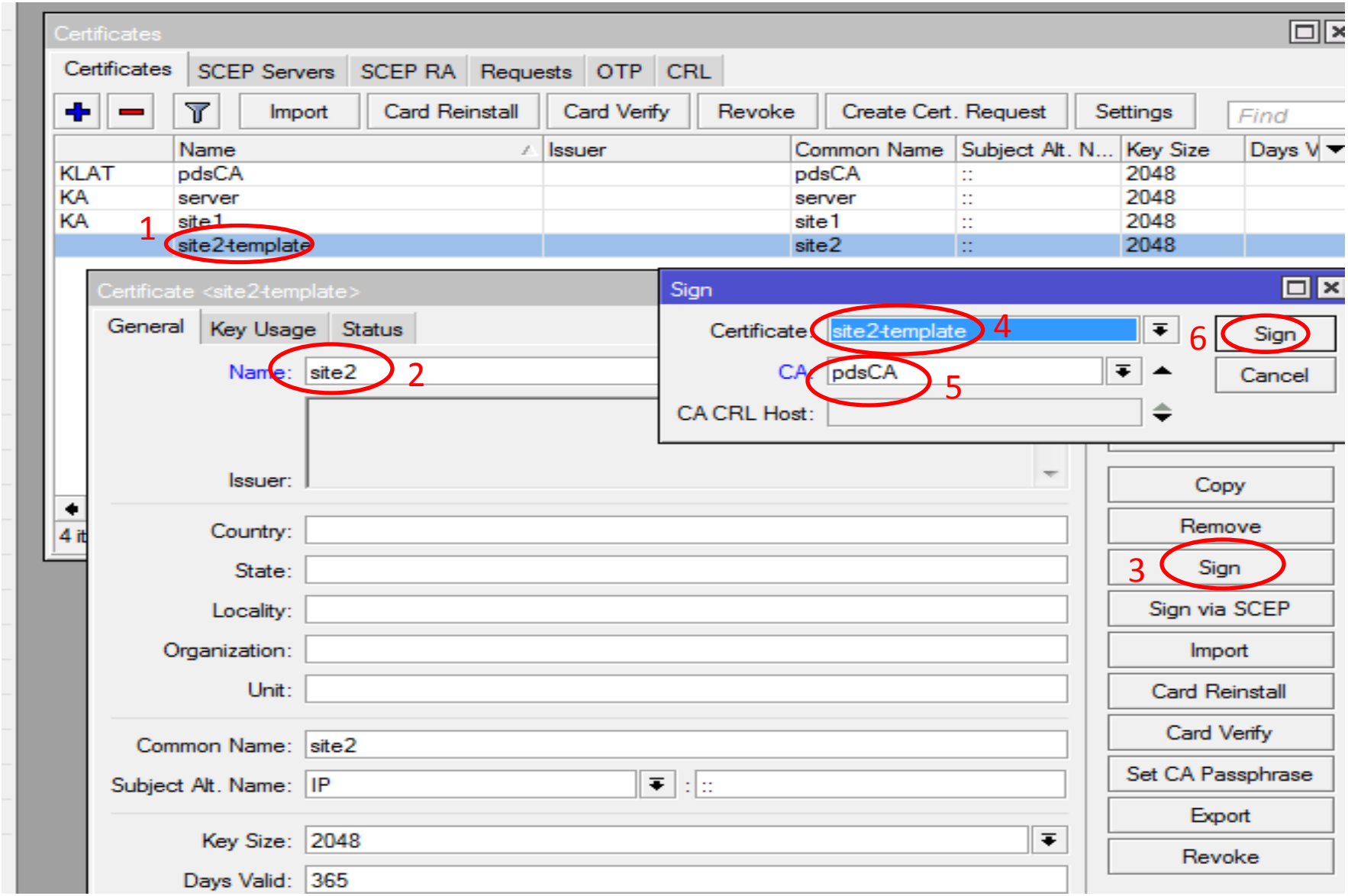
Creating certificates in RouterOs

Sign certificate templates: Site1 Template



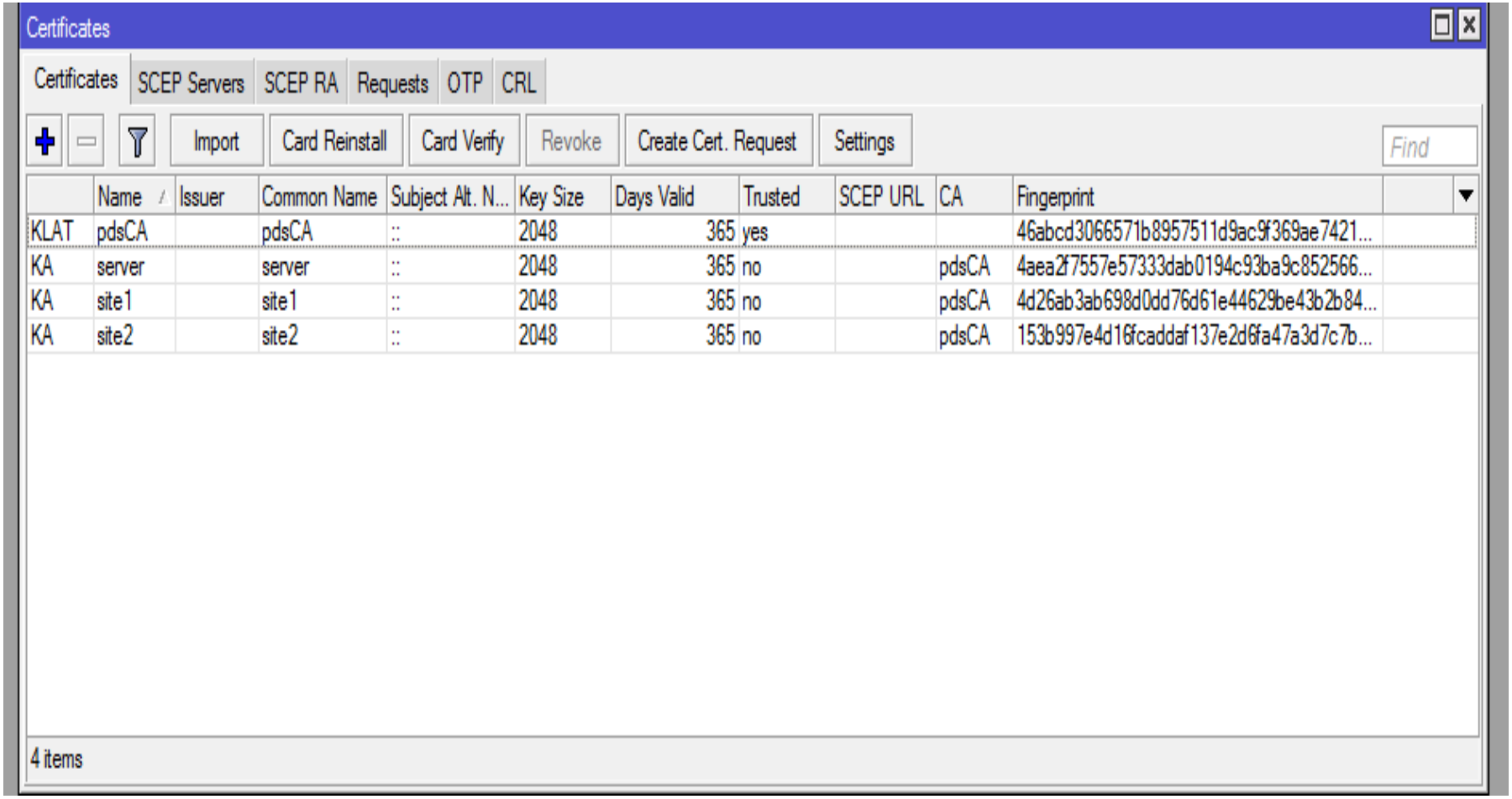
Creating certificates in RouterOs

Sign certificate templates: Site2 Template



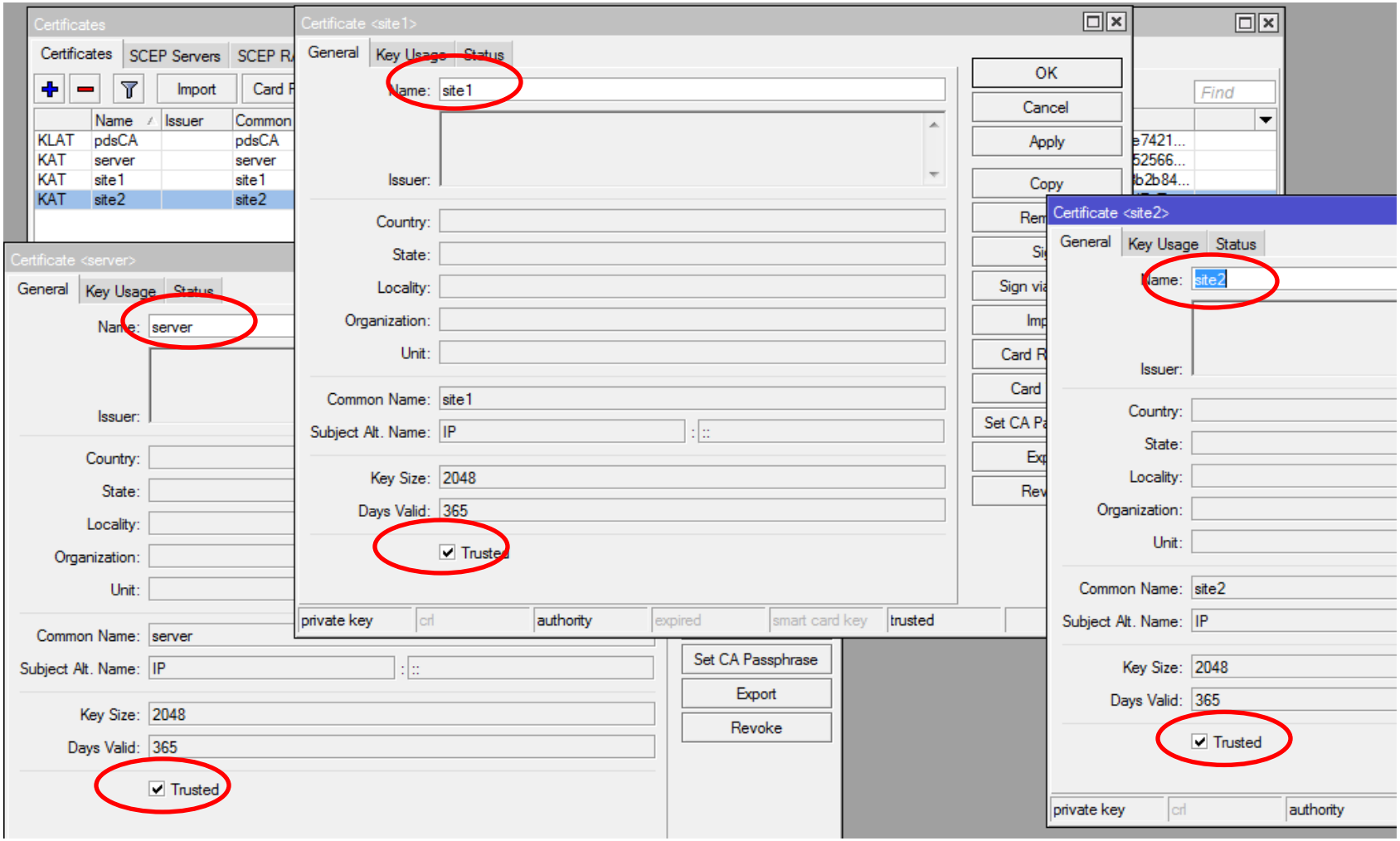
Creating certificates in RouterOs

The results after creating and signing certificate



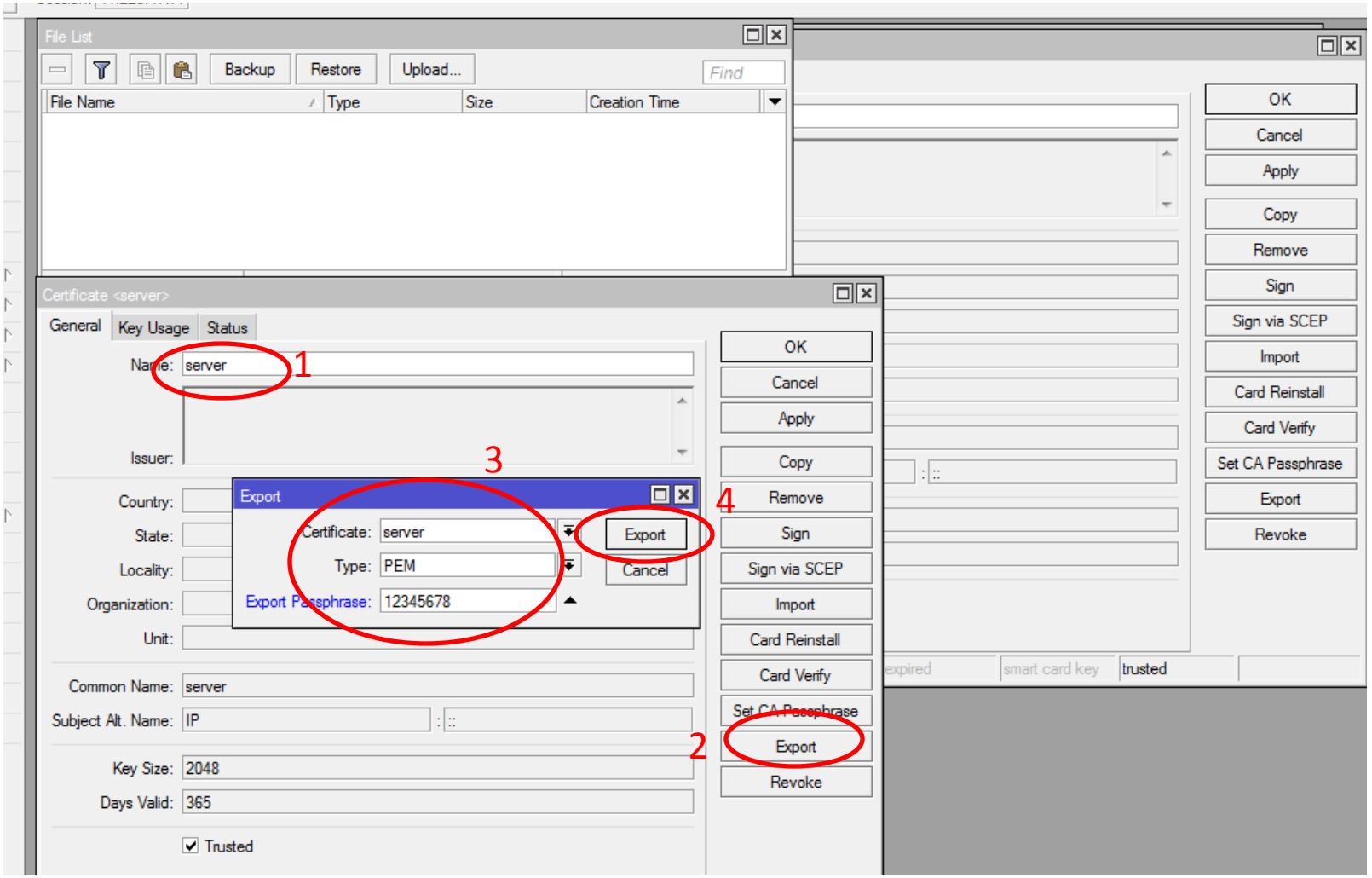
Creating certificates in RouterOs

Set all certificates as Trusted



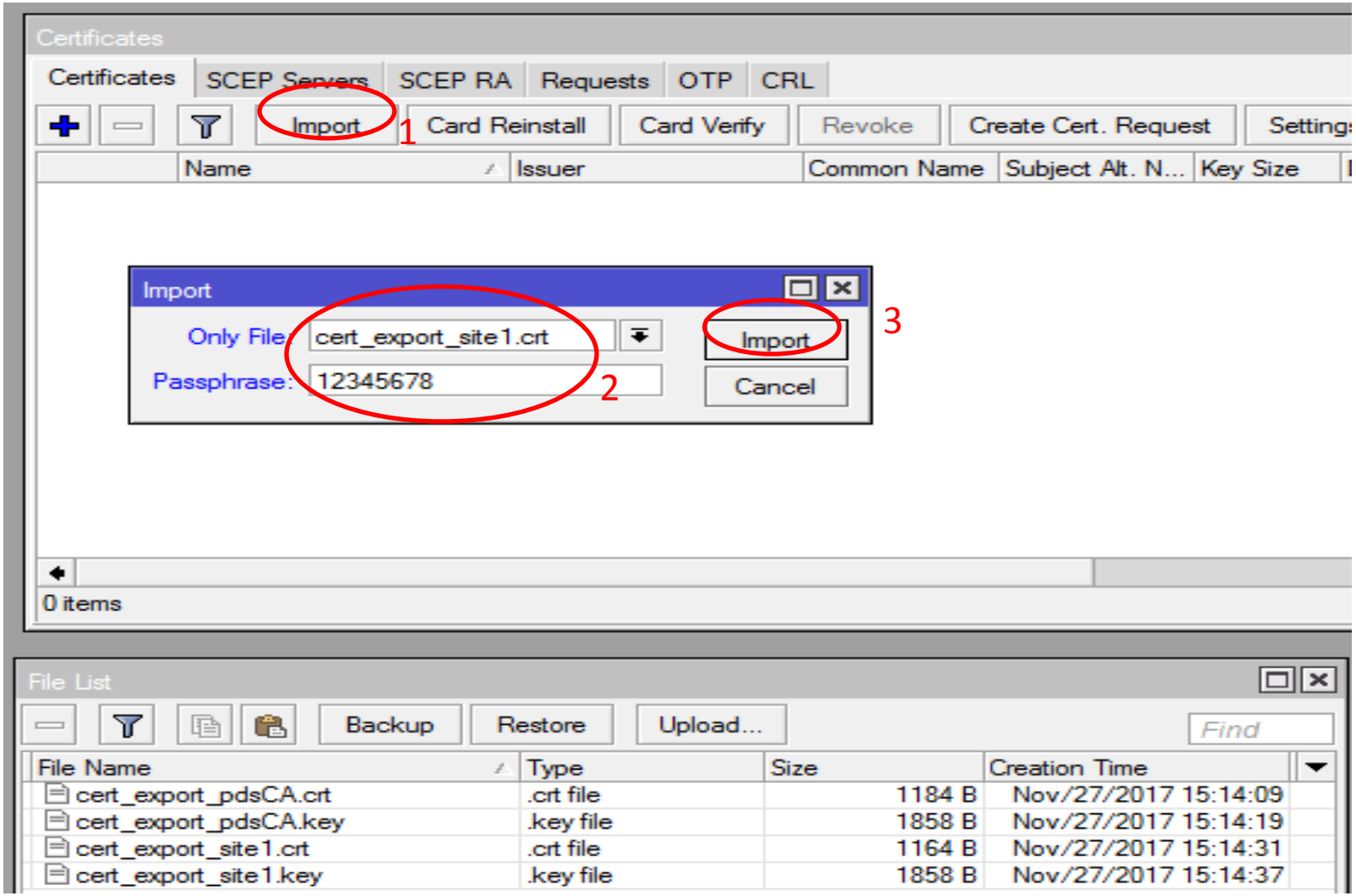
Creating certificates in RouterOs

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



Creating certificates in RouterOs

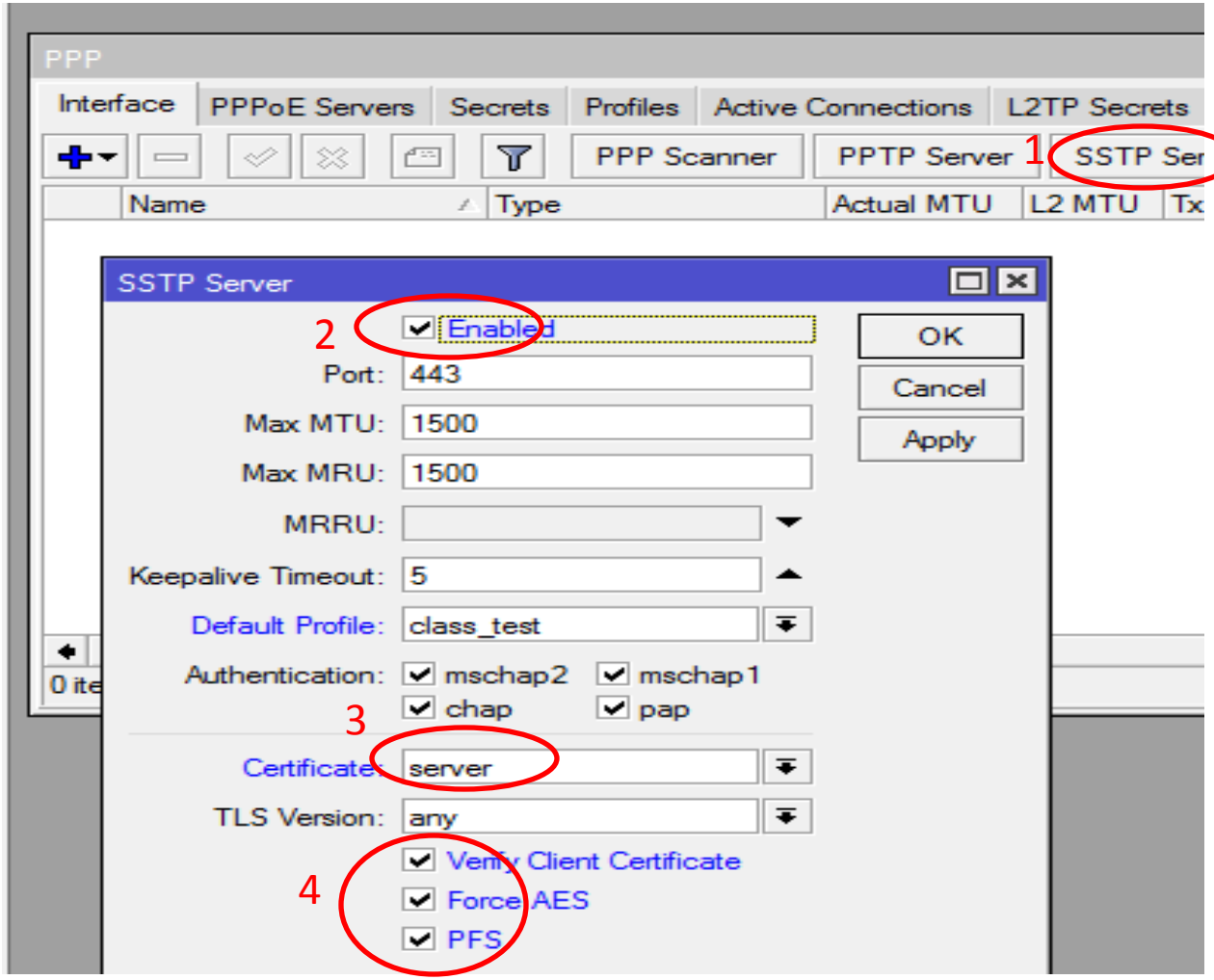
Import client certificates with keys and CA certificates on site1 and site2.



Deploying digital certificates

Using Digital Certificates on SSTP tunnels

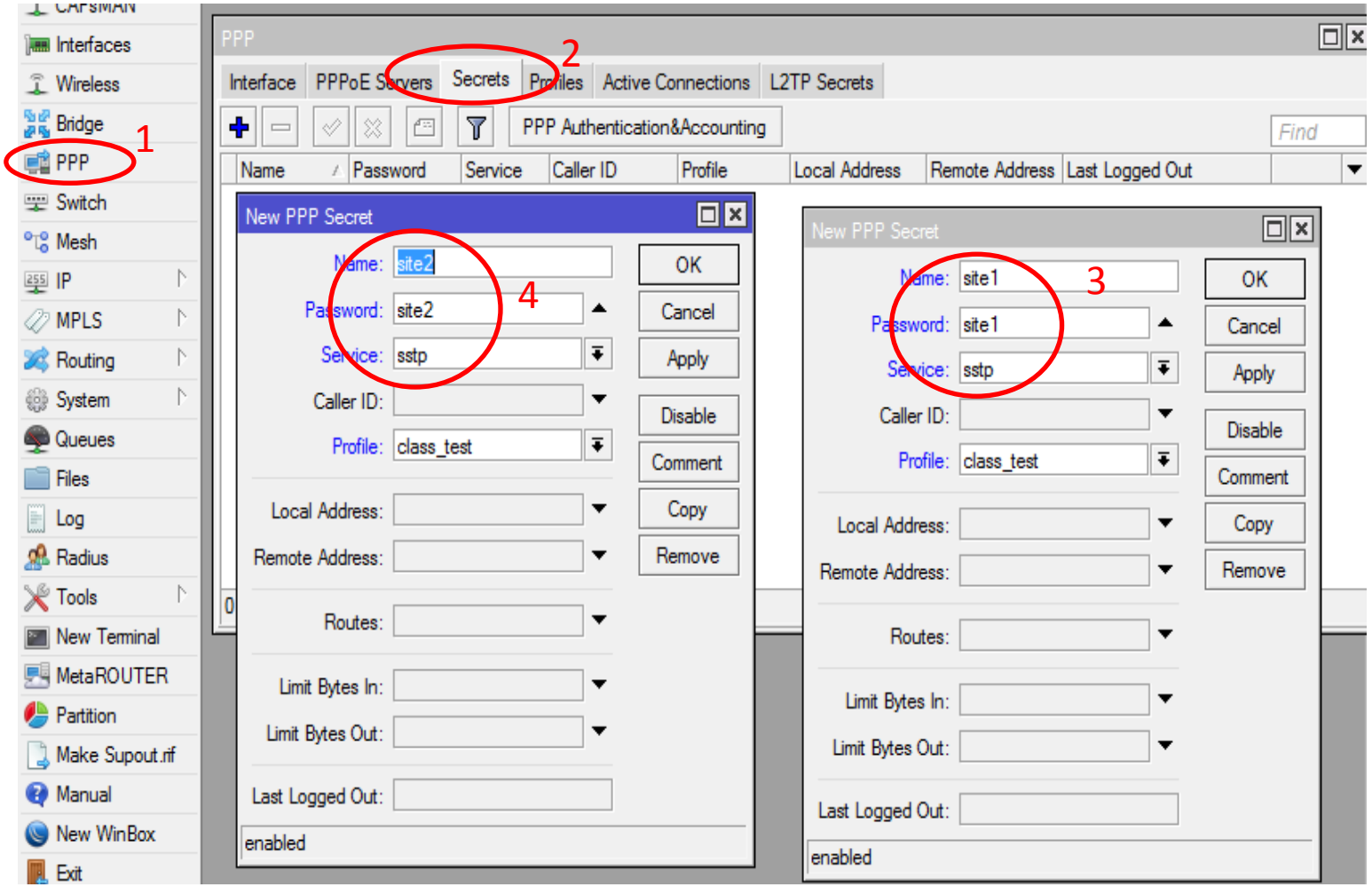
Enable SSTP Server to use Certificate



Deploying digital certificates

Using Digital Certificates on SSTP tunnels

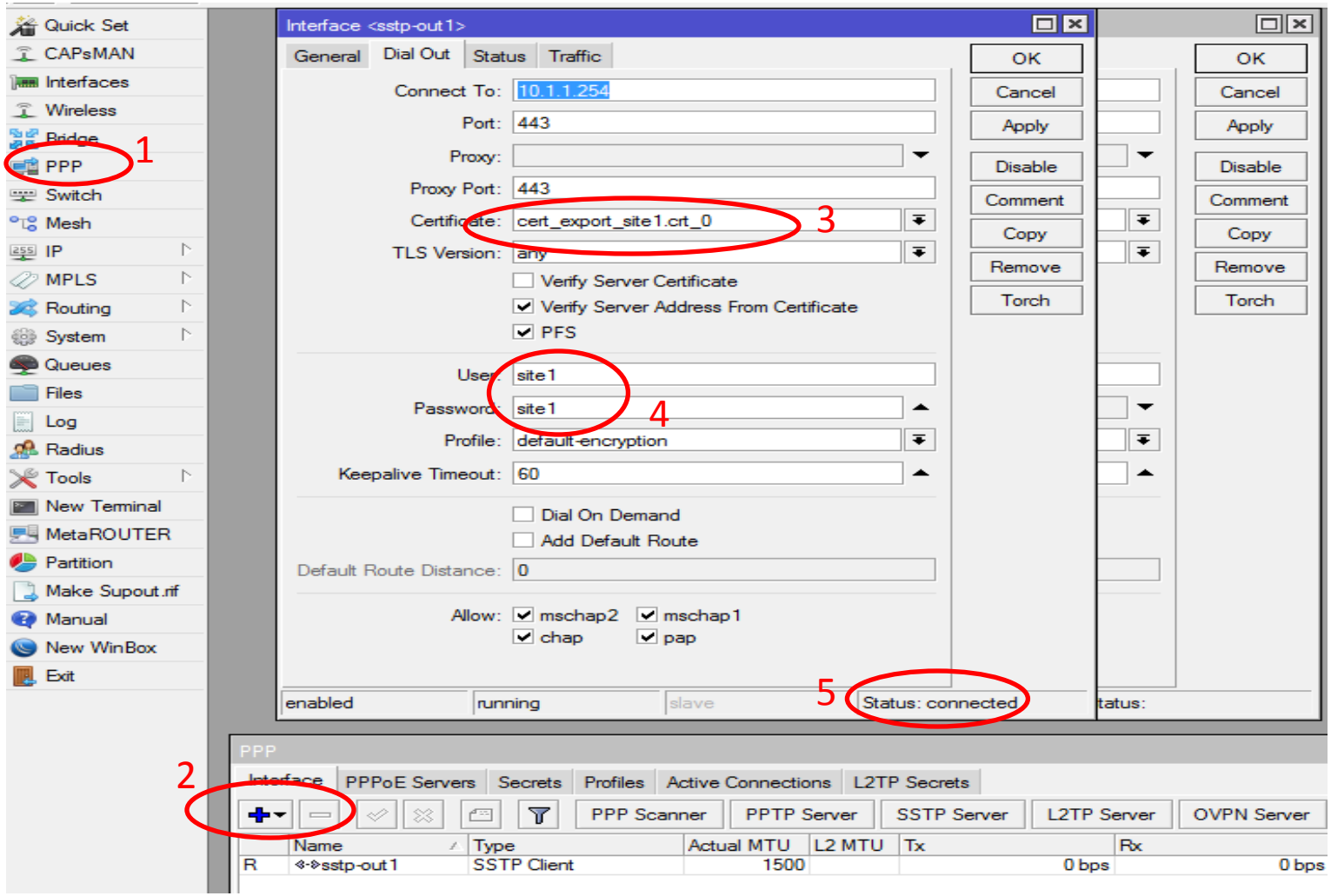
Create credentials for site1 and site2 on SSTP Server



Deploying digital certificates

Using Digital Certificates on SSTP tunnels

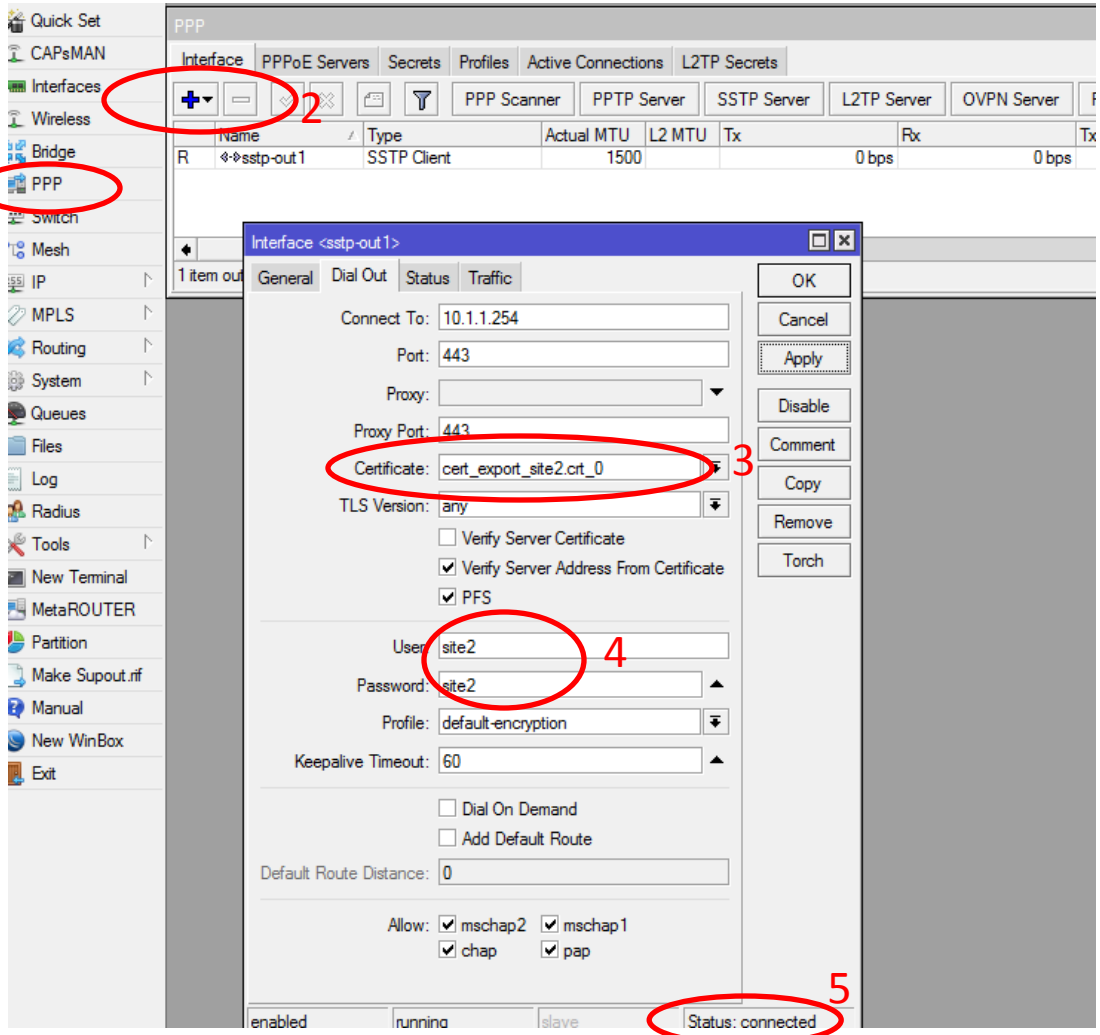
Add SSTP client on site1 as below.



Deploying digital certificates

Using Digital Certificates on SSTP tunnels

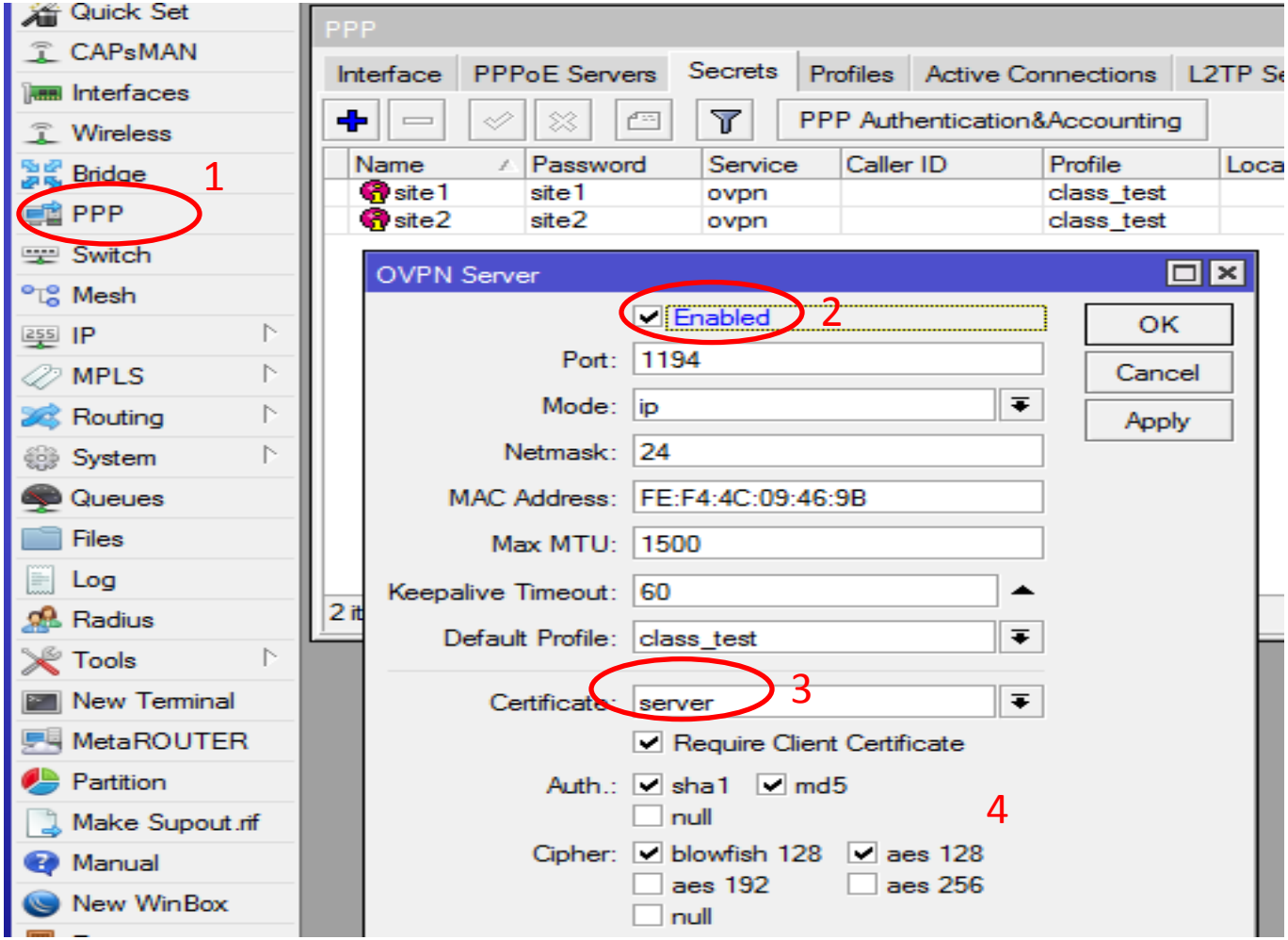
Add SSTP client on site2 as below.



Deploying digital certificates

Using Digital Certificates on OpenVPN tunnels

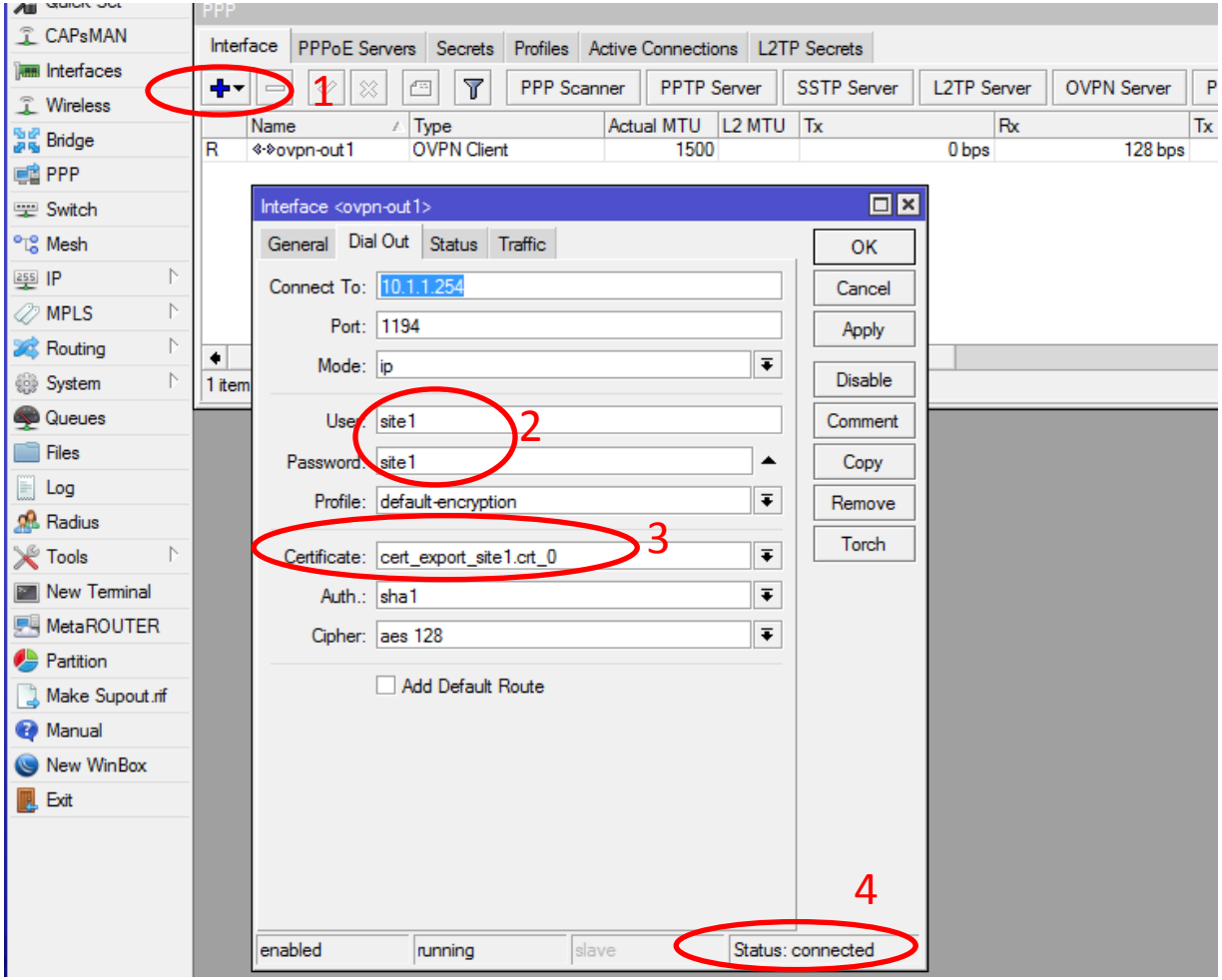
Enable OpenVPN Server to use Certificate



Deploying digital certificates

Using Digital Certificates on OpenVPN tunnels

Add OpenVPN client on site1 and site2 as below.

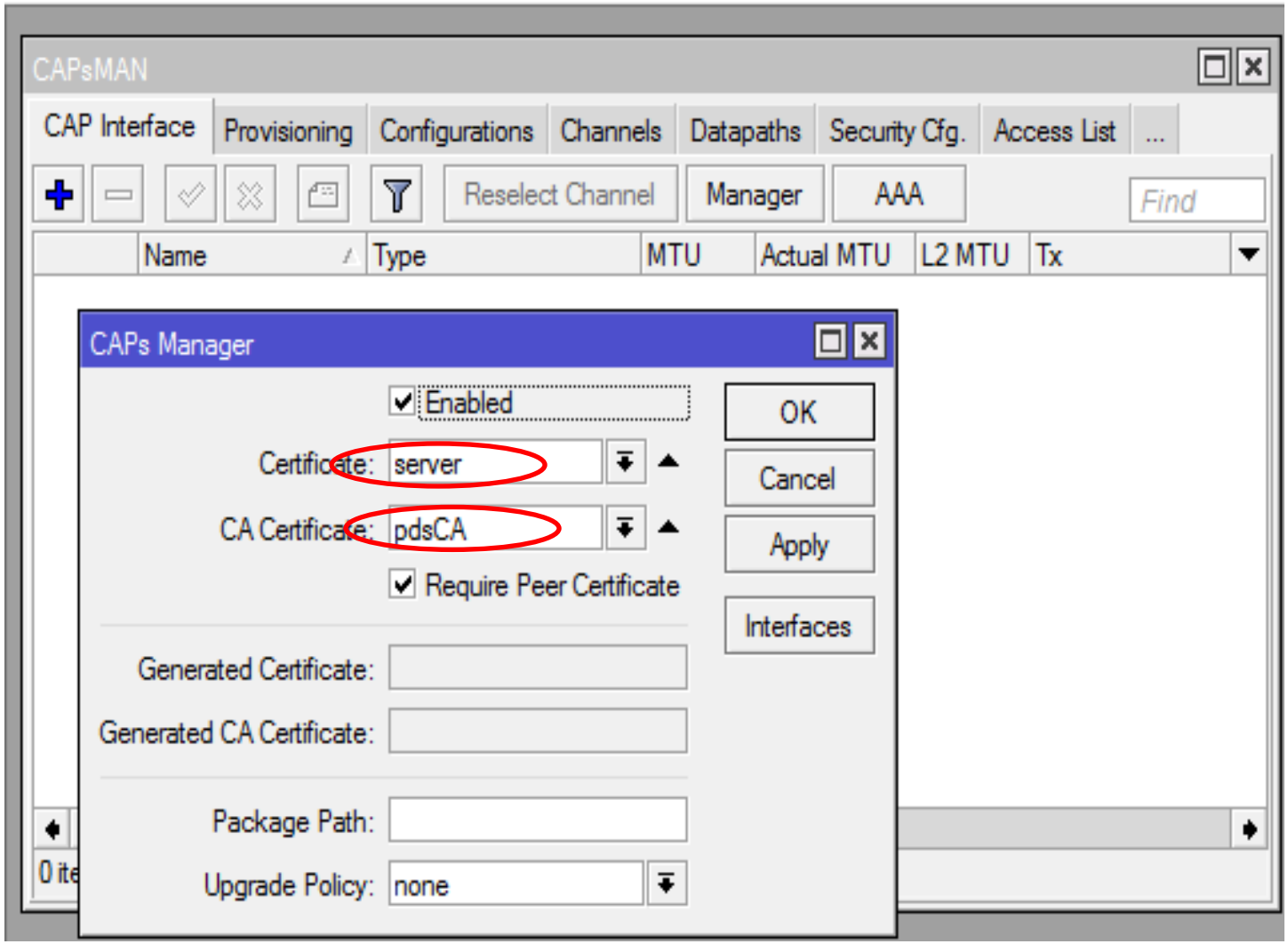


Repeat the setup for site2

Deploying digital certificates

Deploying digital certificates for CAP to CapsMan connections

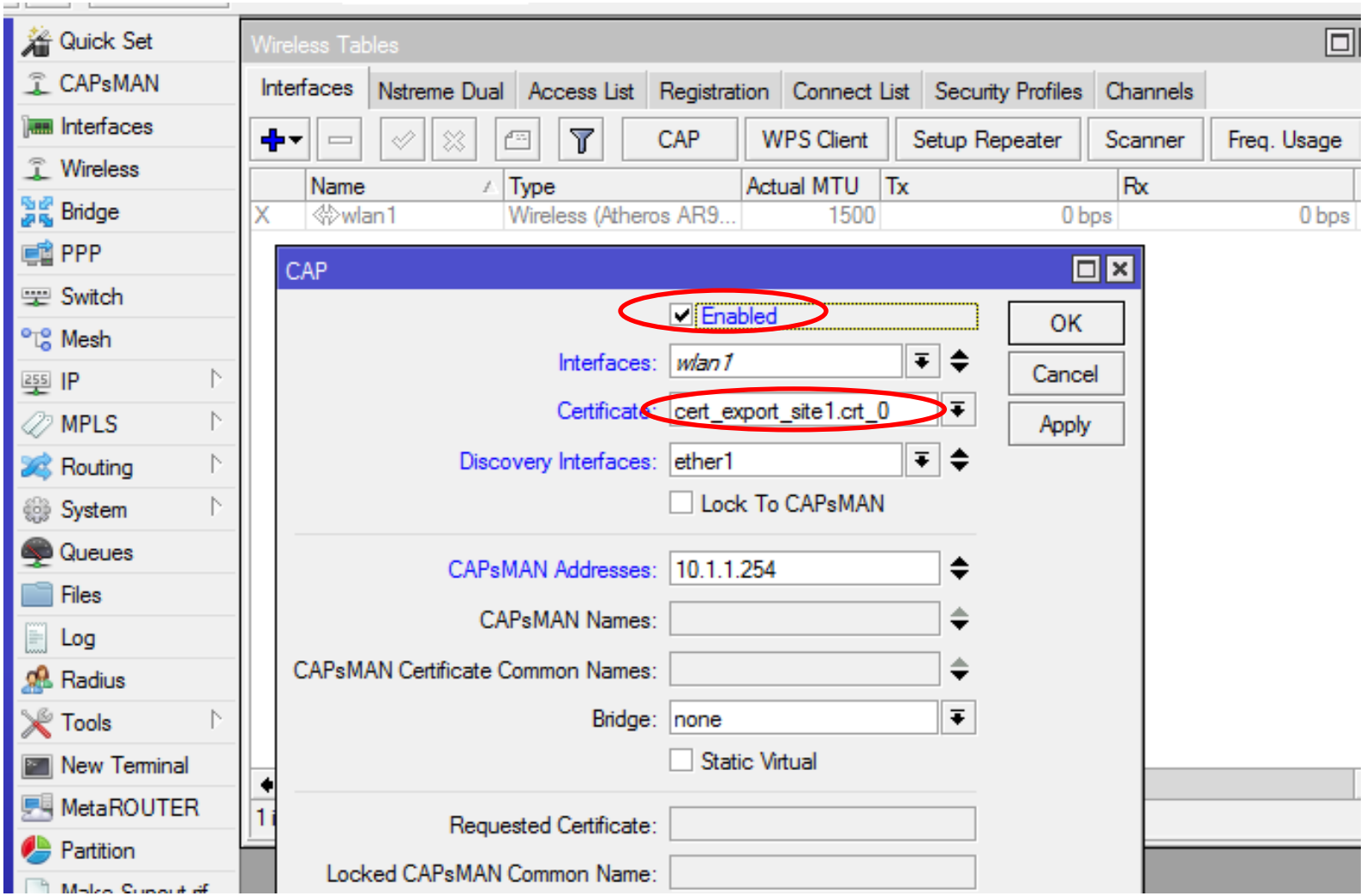
Enable CapsManager with certificate



Deploying digital certificates

Deploying digital certificates for CAP to CapsMan connections

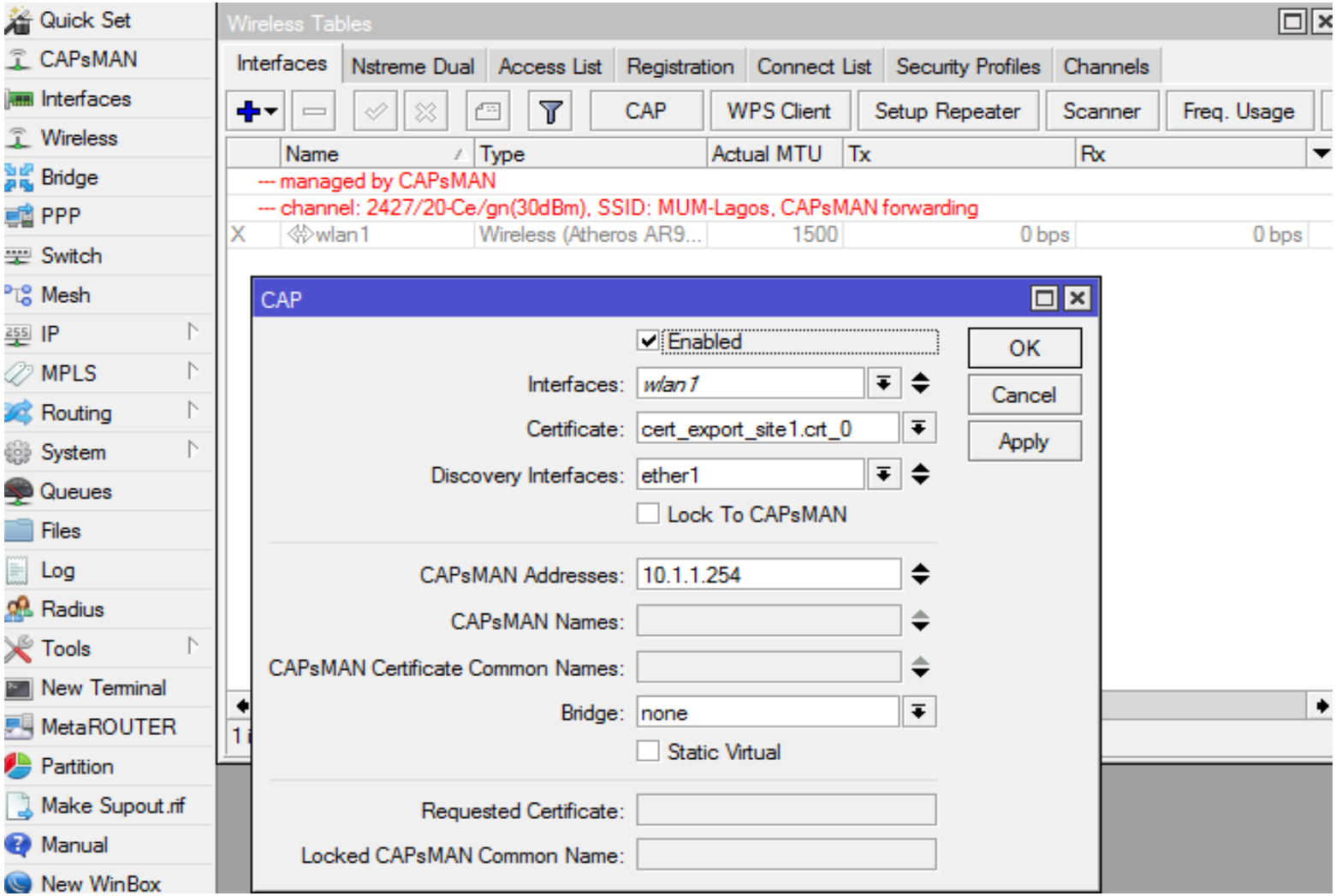
Enable CAP with certificate:



Deploying digital certificates

Deploying digital certificates for CAP to CapsMan connections

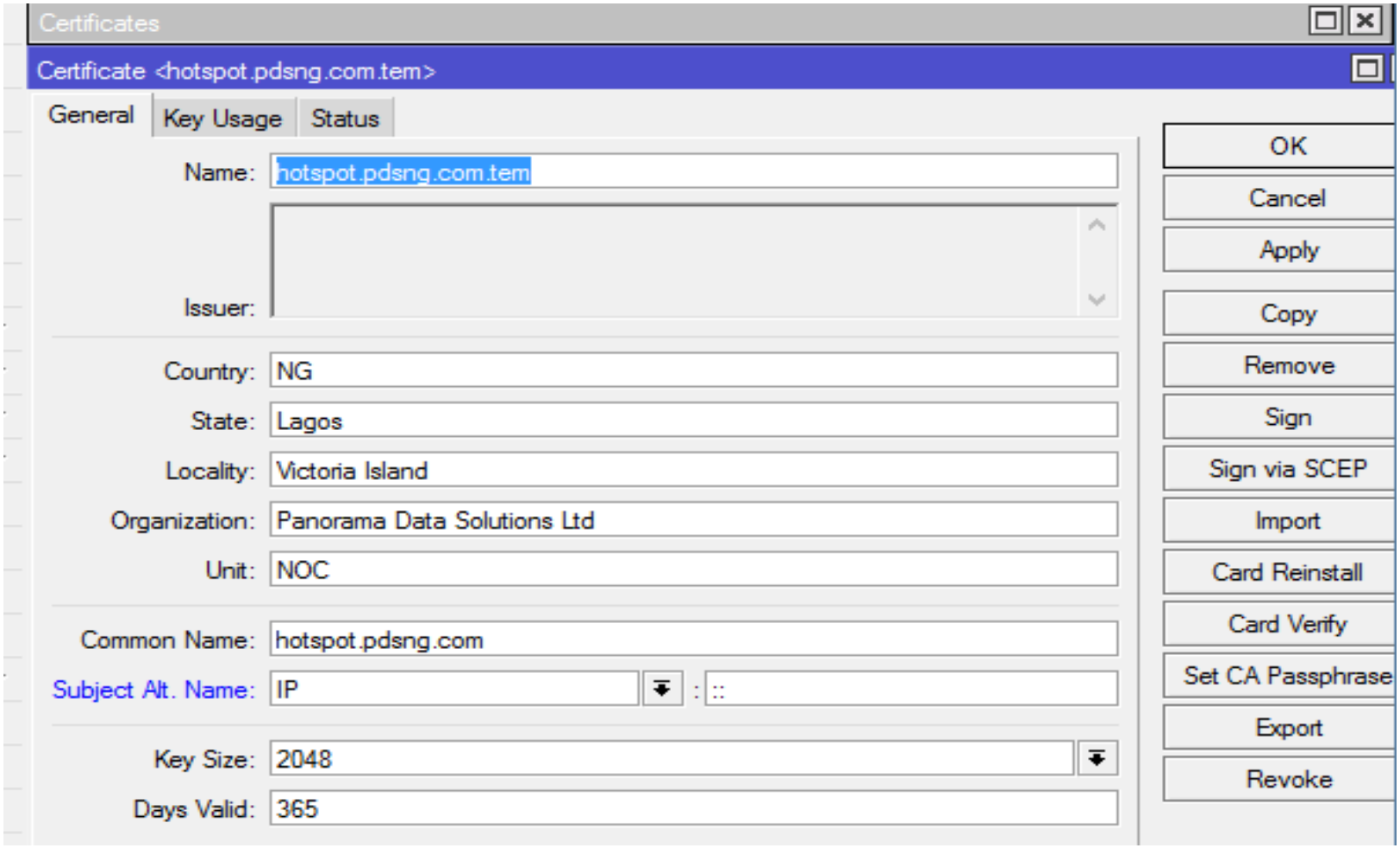
Enable CAP with certificate



Deploying digital certificates

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

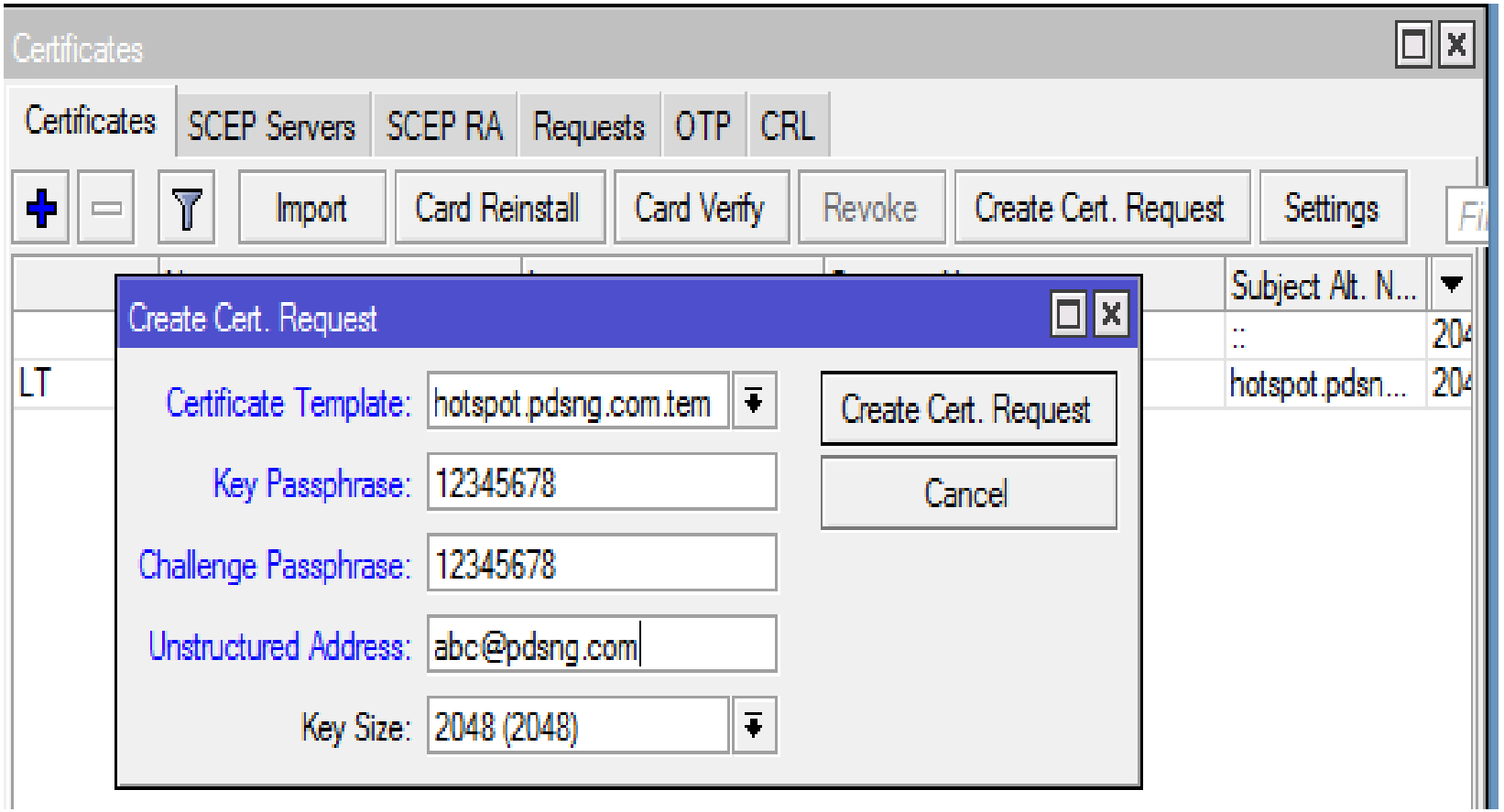
Create a certificate template:



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:

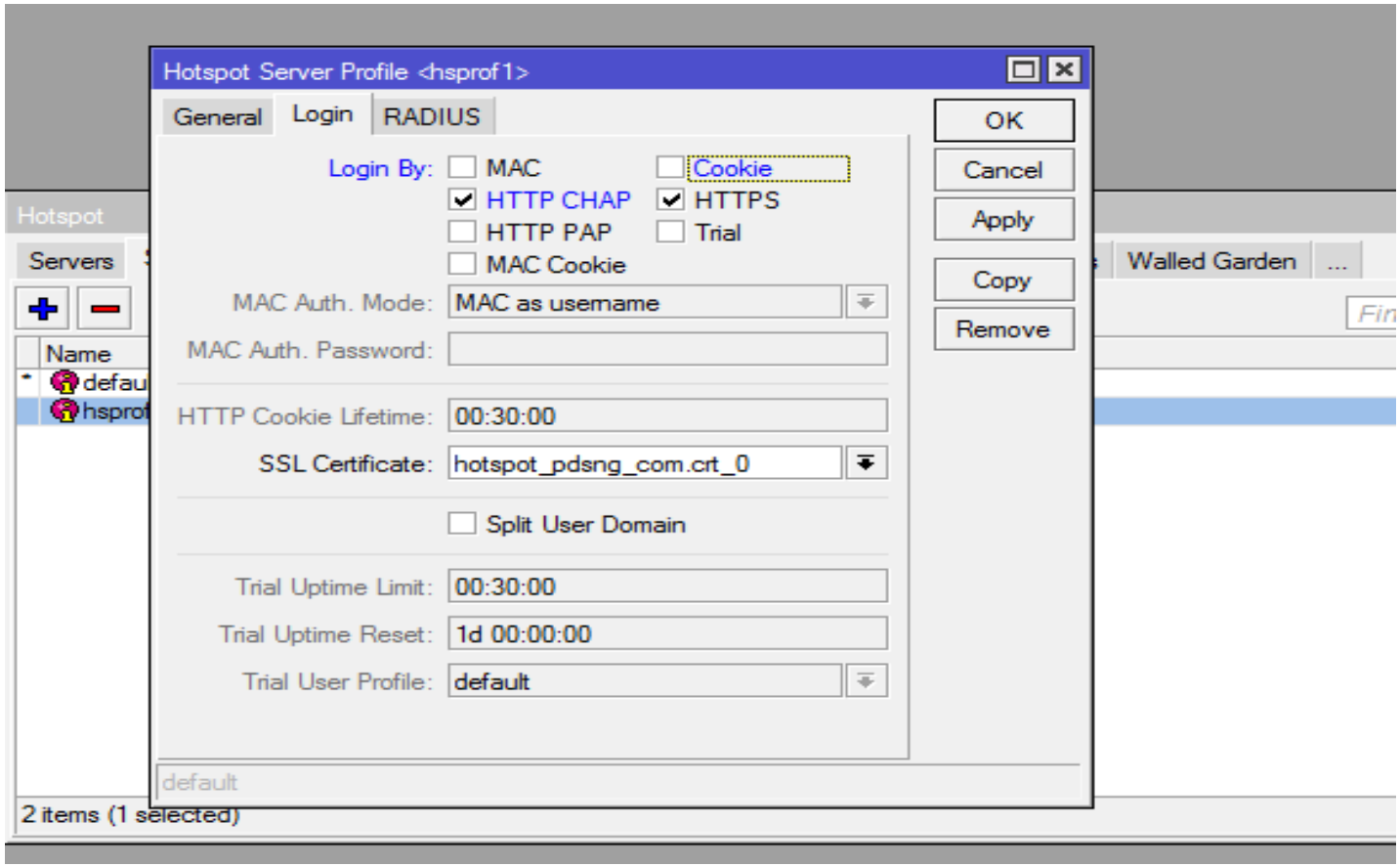
```
-----BEGIN CERTIFICATE REQUEST-----
MIIDKDCCAhACAQIwgYcxCzAJBgNVBAYTAk5HMQ4wDAYDVQQIDAVMYWdvczEYMBYG
A1UEBwwPVmljdG9yaWEgSXNsYW5kMSQwIgYDVQQKDBtQYW5vcmFtYSBEYXRhIFNv
bHV0aW9ucyBMdGQxDDAKBgNVBAsMA05PQzEaMBgGA1UEAwwRaG90c3BvdC5wZHNu
Zy5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCsMiohfqTfCNqR
lW2WUJfN60ikkAlBFZaYxFKjVNn51YDY3F+l2JMqBaVIibnjpPpWMtoXVgZN4tZ1
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

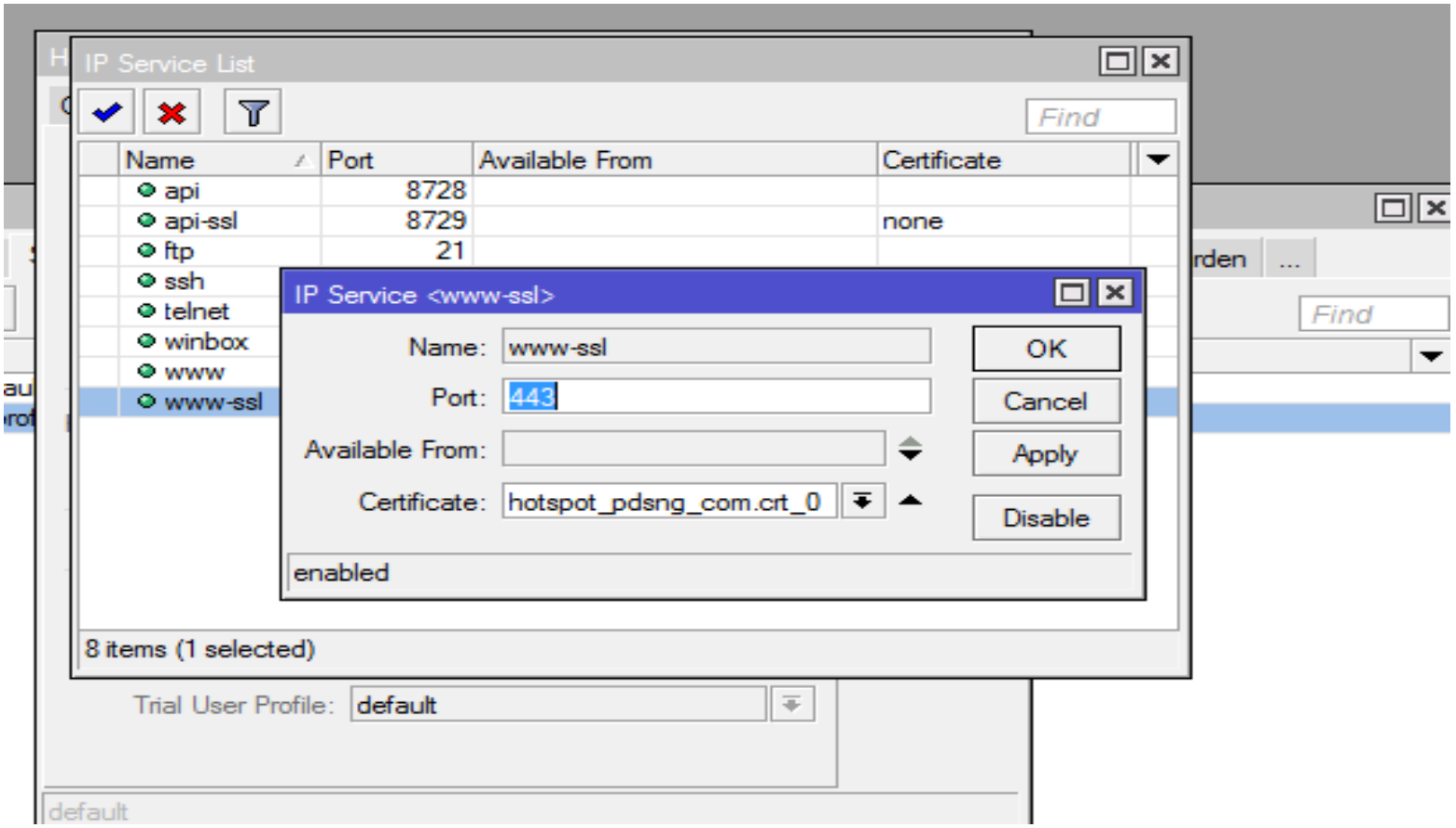
Setup hotspot to use the certificate:



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?