



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

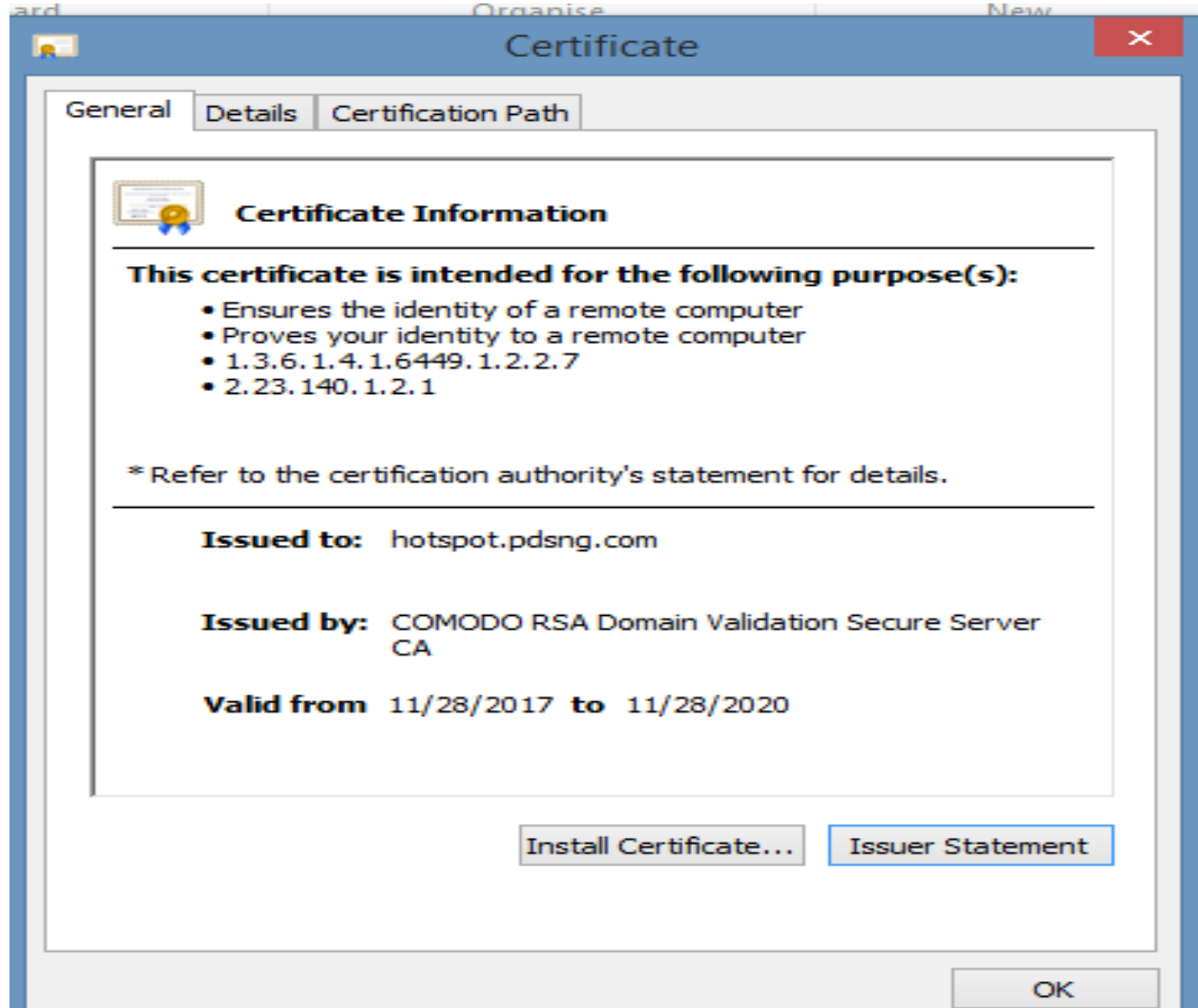
Introduction to Digital Certificate

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

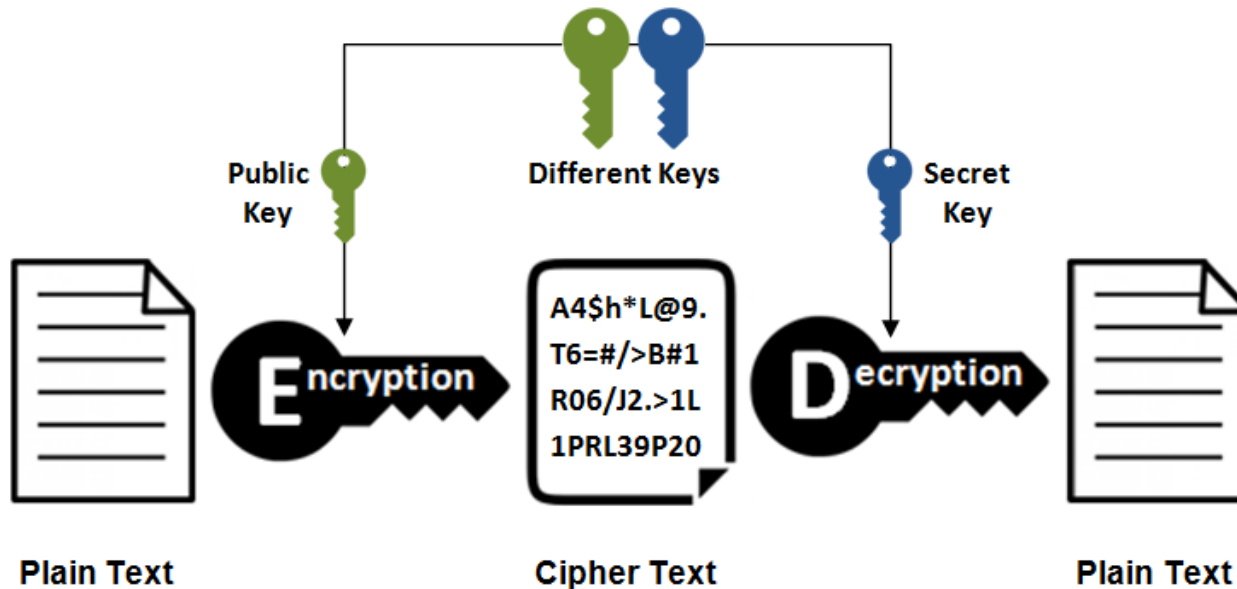
2. Identification & trust

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

Introduction to Digital Certificate

Two types of Encryption:

Asymmetric Encryption



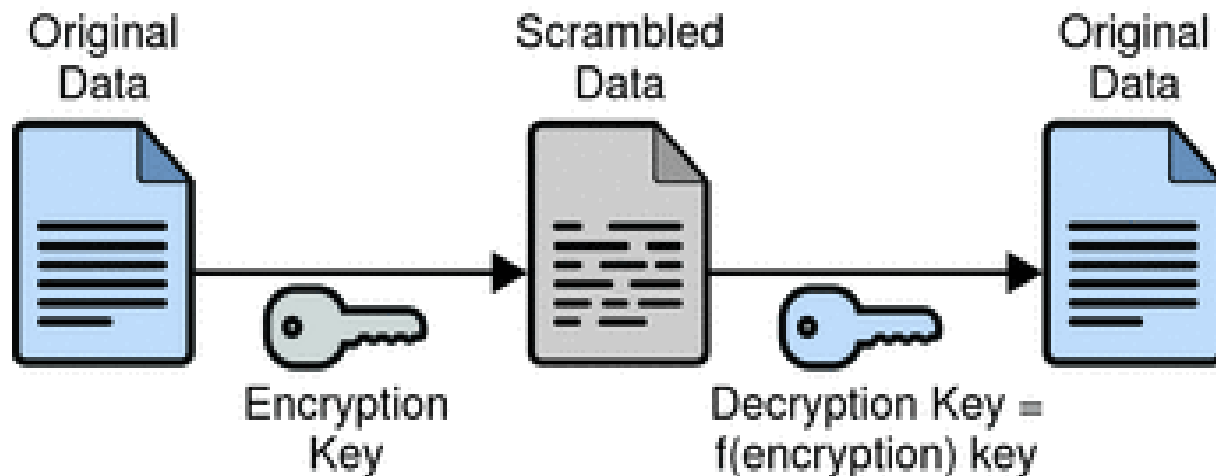
- Larger key size (typically 2048 bits)
- Very slow encoding and decoding process

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

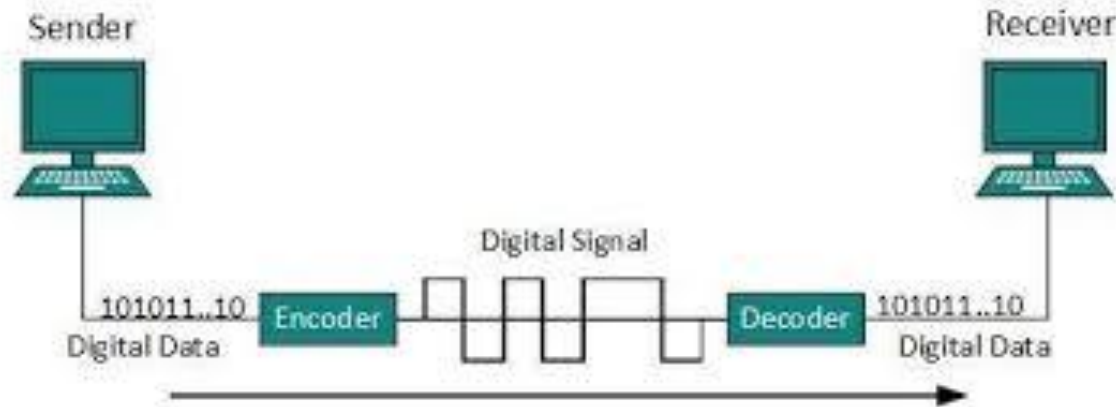
SSL Server Certificate

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.

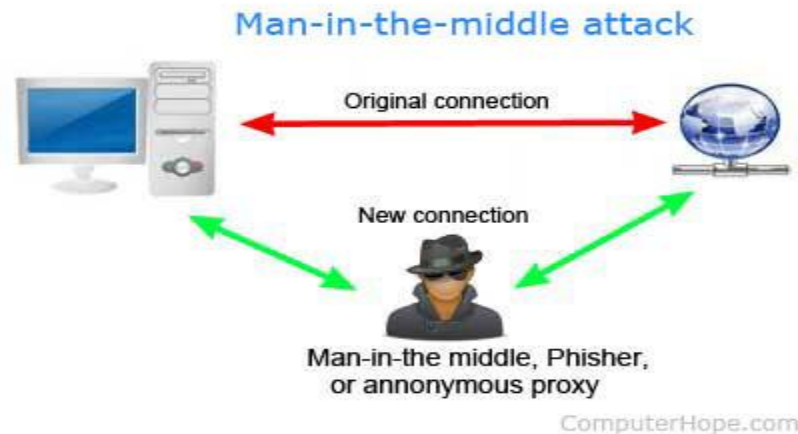


In the absence of SSL or any form of encryption, data is sent as stream of 1s and 0s in a universal encoding format.

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

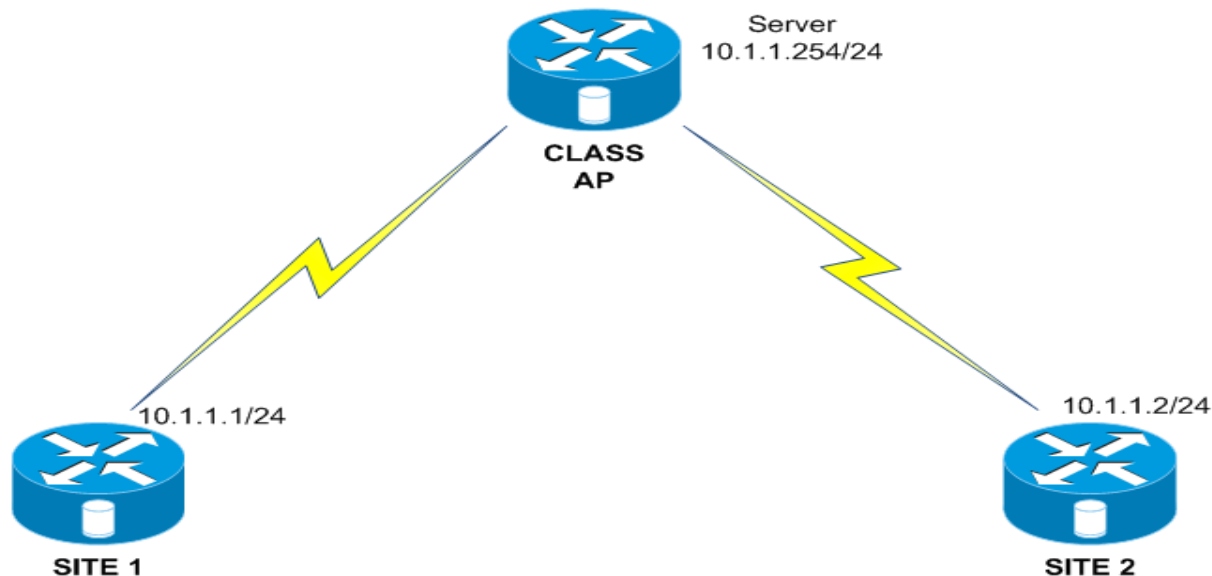
Attack mitigation

- 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 for creating a CA template certificate. The process is annotated with red circles and numbers 1 through 8:

- 1**: The **System** menu item in the left sidebar is highlighted.
- 2**: The **Certificates** menu item in the left sidebar is highlighted.
- 3**: The **+** (Add) button in the Certificates table toolbar is highlighted.
- 4**: The **Name** field in the 'New Certificate' dialog is highlighted with the value **ca-template**.
- 5**: The **Common Name** field in the 'New Certificate' dialog is highlighted with the value **pdsCA**.
- 6**: The **key cert. sign** and **crl sign** checkboxes in the Key Usage section of the 'New Certificate' dialog are highlighted.
- 7**: The **key encipherment** and **data encipherment** checkboxes in the Key Usage section of the 'New Certificate' dialog are highlighted.
- 8**: The **OK** button in the 'New Certificate' dialog is highlighted.

The Certificates table shows the following columns: Name, Issuer, Common Name, Subject Alt. N..., Key Size, Days Valid. The 'New Certificate' dialog has tabs for General, Key Usage, and Status. The Key Usage section includes checkboxes for: digital signature, key encipherment, key agreement, key cert. sign, crl sign, decipher only, server gated crypto, timestamp, ipsec tunnel, email protect, tls client, content commitment, data encipherment, encipher only, dvcs, ocsip 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** tab is selected in the top menu bar.
3. The **Name** field in the **New Certificate** dialog is set to **site1-template**.
4. The **Common Name** field is set to **site1**.
5. The **Key Usage** options are checked: digital signature, key encipherment, key cert. sign, crl sign, and decipher only.
6. The **Apply** button is highlighted.

The **New Certificate** dialog also shows the following fields and values:

- Issuer:** (empty)
- Country:** (empty)
- State:** (empty)
- Locality:** (empty)
- Organization:** (empty)
- Unit:** (empty)
- Key Size:** 2048
- Days Valid:** 365

The **Key Usage** options are:

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

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 contains navigation options such as Quick Set, CAPsMAN, Interfaces, Wireless, Bridge, PPP, Switch, Mesh, IP, MPLS, Routing, System, Queues, Files, Log, Radius, Tools, New Terminal, MetaROUTER, Partition, Make Supout.rif, Manual, New WinBox, and Exit.

The main window is titled "Certificates" and contains a table with the following data:

Name	Issuer
ca-template	
site1-template	
site2-template	

Numbered annotations indicate the following steps:

- 1: Selecting the "ca-template" entry in the table.
- 2: The "Name" field in the "Certificate <ca-template>" dialog is set to "ca-template".
- 3: The "Sign" button in the right-hand button panel is highlighted.
- 4: The "Certificate" dropdown in the "Sign" dialog is set to "ca-template".
- 5: The "CA CRL Host" field in the "Sign" dialog is set to "41.223.47.77".
- 6: The "Sign" button in the "Sign" dialog is highlighted.

The "Certificate <ca-template>" dialog shows the following configuration:

- General tab selected.
- Name: ca-template
- Issuer: (empty)
- Country: (empty)
- State: (empty)
- Locality: (empty)
- Organization: (empty)
- Unit: (empty)
- Common Name: pdsCA
- Subject Alt. Name: IP
- Key Size: 2048
- Days Valid: 365

The right-hand button panel includes: OK, Cancel, Apply, Copy, Remove, Sign, Sign via SCEP, Import, Card Reinstall, Card Verify, Set CA Passphrase, Export, and Revoke.

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 following fields and options:

- Name:** server-template (3)
- Common Name:** server (4)
- Subject Alt. Name:** IP
- Key Size:** 2048
- Days Valid:** 365
- Key Usage:** digital signature, key encipherment, key agreement, crl sign, decipher only, server gated crypto, timestamp, ipsec tunnel, email protect, tls client, content commitment, data encipherment, key cert. sign, encipher only, dvcs, ocsip sign, ipsec user, ipsec end system, code sign, tls server (5)
- Buttons:** OK, Cancel, Apply (6)

Creating certificates in RouterOs

Sign certificate templates: Server Template

The screenshot displays the RouterOS Certificates management interface. The main window shows a list of certificates with the following data:

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

The 'server-template' entry is circled in red and labeled with a red '1'. A 'Sign' dialog box is overlaid on the right, showing the following fields:

- Certificate: server-template (circled in red, labeled with a red '4')
- CA: pdsCA (circled in red, labeled with a red '5')
- Buttons: Sign (circled in red), Cancel

The 'Certificate <server-template>' configuration window is also visible, showing the following fields:

- Name: server (circled in red, labeled with a red '2')
- Common Name: server
- Subject Alt. Name: IP
- Key Size: 2048
- Days Valid: 365

A 'Sign' button in the right-hand pane of the configuration window is circled in red and labeled with a red '3'. The 'Sign' dialog box also has a 'Sign' button circled in red and labeled with a red '6'.

Creating certificates in RouterOs

Sign certificate templates: Site1 Template

The screenshot displays the RouterOS Certificates management interface. The main window shows a list of certificates with the following data:

	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	

The 'site1-template' row is highlighted and circled in red, with a red '1' next to it. Below this, the 'Certificate <site1-template>' dialog is open, showing the 'General' tab. The 'Name' field is set to 'site1' and circled in red with a red '2'. The 'Sign' dialog is also open, showing the 'Certificate' dropdown set to 'site1-template' (circled in red with a red '4') and the 'CA' dropdown set to 'pdsCA' (circled in red with a red '5'). The 'Sign' button in the 'Sign' dialog is circled in red with a red '6'. The 'Sign' button in the 'Certificate <site1-template>' dialog is circled in red with a red '3'. The 'Common Name' field is set to 'site1', 'Subject Alt. Name' is 'IP', 'Key Size' is '2048', and 'Days Valid' is '365'.

Creating certificates in RouterOs

Sign certificate templates: Site2 Template

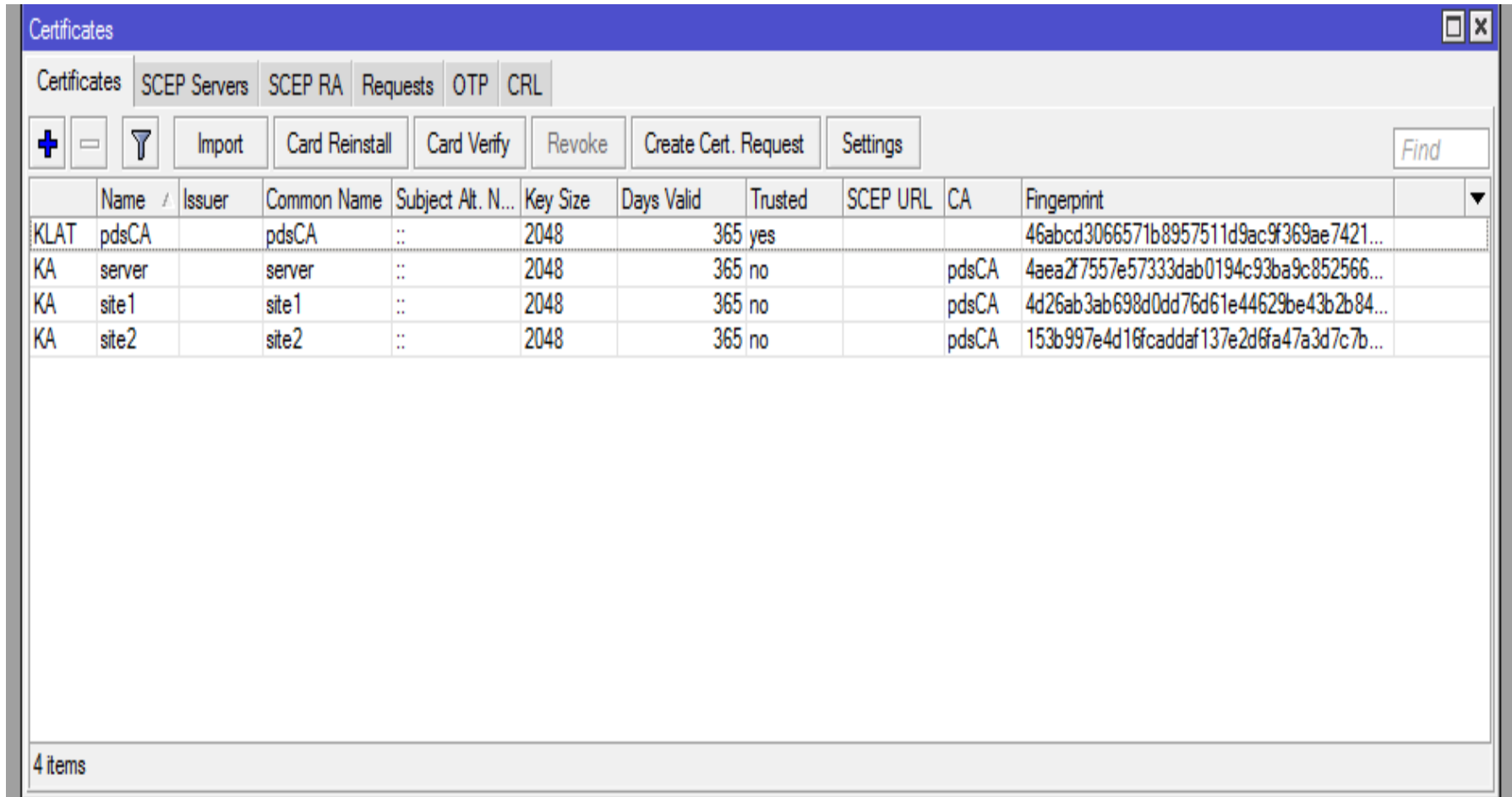
The screenshot displays the RouterOS Certificates management interface. At the top, there are tabs for Certificates, SCEP Servers, SCEP RA, Requests, OTP, and CRL. Below these are various action buttons: Import, Card Reinstall, Card Verify, Revoke, Create Cert. Request, and Settings. A table lists existing certificates:

	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	

The 'site2-template' entry is highlighted and circled with a red '1'. Below the table, the 'Certificate <site2-template>' configuration window is open, showing the 'General' tab. The 'Name' field is set to 'site2' and circled with a red '2'. The 'Common Name' is 'site2', and 'Subject Alt. Name' is 'IP'. The 'Key Size' is '2048' and 'Days Valid' is '365'. To the right, the 'Sign' dialog is open, showing the 'Certificate' dropdown set to 'site2-template' (circled with a red '4') and the 'CA' dropdown set to 'pdsCA' (circled with a red '5'). The 'Sign' button in the dialog is circled with a red '6'. On the right side of the main window, a vertical stack of buttons includes 'Copy', 'Remove', 'Sign' (circled with a red '3'), 'Sign via SCEP', 'Import', 'Card Reinstall', 'Card Verify', 'Set CA Passphrase', 'Export', and 'Revoke'.

Creating certificates in RouterOs

The results after creating and signing certificate



The screenshot shows the RouterOS 'Certificates' management interface. It features a blue title bar, a menu bar with options like 'SCEP Servers', 'SCEP RA', 'Requests', 'OTP', and 'CRL', and a toolbar with various actions such as '+', '-', 'Import', 'Card Reinstall', 'Card Verify', 'Revoke', 'Create Cert. Request', and 'Settings'. A 'Find' search box is also present. The main area contains a table with the following data:

	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

The screenshot displays the RouterOS Certificate Manager interface. On the left, a table lists existing certificates:

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

Three configuration windows are overlaid, each with a red circle around the 'Trusted' checkbox:

- Certificate <server>**: Name: server, Key Size: 2048, Days Valid: 365, Trusted.
- Certificate <site1>**: Name: site1, Common Name: site1, Subject Alt. Name: IP, Key Size: 2048, Days Valid: 365, Trusted.
- Certificate <site2>**: Name: site2, Common Name: site2, Subject Alt. Name: IP, Key Size: 2048, Days Valid: 365, Trusted.

At the bottom of the interface, a row of tabs includes 'private key', 'cert', 'authority', 'expired', 'smart card key', and 'trusted'.

Creating certificates in RouterOs

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

The screenshot displays the RouterOS Certificate Manager interface. The main window is titled "Certificate <server>" and has tabs for "General", "Key Usage", and "Status". The "General" tab is active, showing fields for Name, Issuer, Country, State, Locality, Organization, and Unit. The Name field contains "server" and is circled in red with a red "1" next to it. Below these fields are fields for Common Name (containing "server") and Subject Alt. Name (containing "IP"). The Key Size is set to 2048 and Days Valid to 365. A "Trusted" checkbox is checked. To the right of the main window 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. The "Export" button is circled in red with a red "2" next to it. An "Export" dialog box is open in the foreground, showing the Certificate name as "server", Type as "PEM", and Export Passphrase as "12345678". The "Export" button in this dialog is circled in red with a red "3" next to it. A red "4" is placed between the main window's "Export" button and the dialog's "Export" button. In the background, a "File List" window is visible with columns for File Name, Type, Size, and Creation Time. At the bottom right, there are status indicators for "expired", "smart card key", and "trusted".

Creating certificates in RouterOs

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

The screenshot displays the RouterOS web interface for managing certificates. The main window is titled "Certificates" and has several tabs: "Certificates", "SCEP Servers", "SCEP RA", "Requests", "OTP", and "CRL". The "Import" button is circled in red and labeled with a red "1". Below the tabs is a toolbar with various actions like "Card Reinstall", "Card Verify", "Revoke", "Create Cert. Request", and "Settings". A table below the toolbar shows columns for "Name", "Issuer", "Common Name", "Subject Alt. N...", and "Key Size".

An "Import" dialog box is open in the foreground. It has a blue title bar and contains two input fields: "Only File" with the value "cert_export_site1.crt" and "Passphrase:" with the value "12345678". Both fields are circled in red and labeled with a red "2". To the right of the fields are "Import" and "Cancel" buttons. The "Import" button is circled in red and labeled with a red "3".

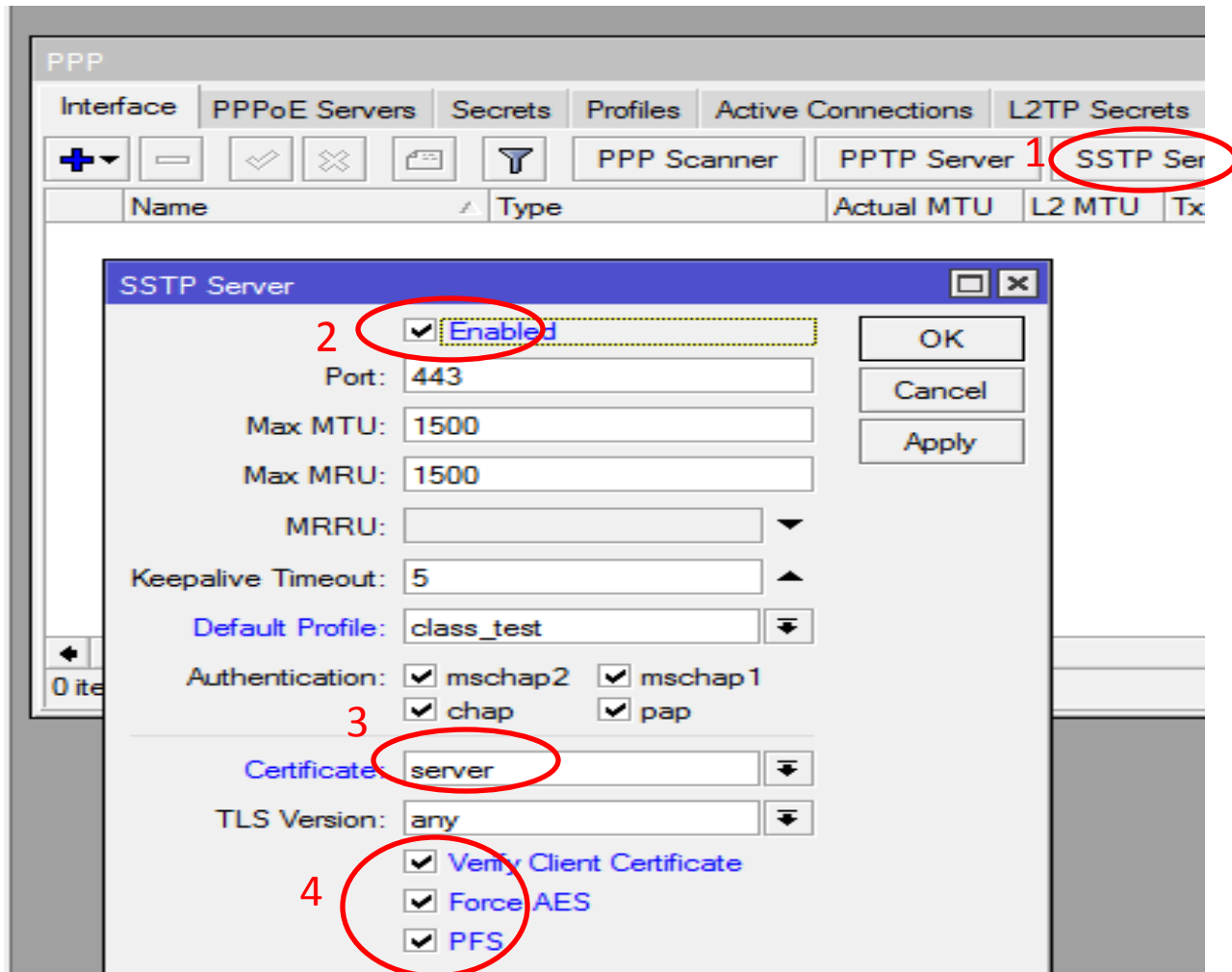
At the bottom of the interface is a "File List" window. It has a toolbar with "Backup", "Restore", and "Upload..." buttons, and a "Find" search box. Below the toolbar is a table with the following data:

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



Deploying digital certificates

Using Digital Certificates on SSTP tunnels

Create credentials for site1 and site2 on SSTP Server

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 'PPP' configuration page with the 'Secrets' tab selected, also circled in red and labeled with a red '2'. Below this, a table lists PPP secrets with columns for Name, Password, Service, Caller ID, Profile, Local Address, Remote Address, and Last Logged Out. Two 'New PPP Secret' dialog boxes are open. The first dialog, labeled with a red '4', shows the 'Name' field set to 'site2' and the 'Password' field set to 'site2'. The second dialog, labeled with a red '3', shows the 'Name' field set to 'site1' and the 'Password' field set to 'site1'. Both dialogs have 'Service' set to 'sstp' and 'Profile' set to 'class_test'. The 'Last Logged Out' field in both dialogs is set to 'enabled'.

Deploying digital certificates

Using Digital Certificates on SSTP tunnels

Add SSTP client on site1 as below.

The screenshot displays the Mikrotik WinBox interface for configuring an SSTP client. The left sidebar shows the 'PPP' option circled in red with a '1'. The main window shows the configuration for interface '<sstp-out1>'. The 'Certificate' field is circled in red with a '3', containing 'cert_export_site1.crt_0'. The 'Password' field is circled in red with a '4', containing 'site1'. The 'Status' field at the bottom right is circled in red with a '5', showing 'Status: connected'. Below the main configuration window, the 'PPP' interface list is visible, with the '+' button circled in red with a '2'. The table below shows the configuration for the SSTP client.

Interface	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.

The screenshot displays the Mikrotik WinBox interface for configuring a PPP interface. The left sidebar shows the 'PPP' option selected (1). The main window shows the 'Interface' configuration for 'sstp-out1' (2). The 'Certificate' field is set to 'cert_export_site2.crt_0' (3). The 'User' field is set to 'site2' (4). The status at the bottom is 'Status: connected' (5).

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

Interface <sstp-out1> configuration details:

- Connect To: 10.1.1.254
- Port: 443
- Proxy: (empty)
- 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

Status: connected

Deploying digital certificates

Using Digital Certificates on OpenVPN tunnels

Enable OpenVPN Server to use Certificate

The image shows a screenshot of the Mikrotik WinBox interface. On the left is a sidebar menu with various configuration categories. The 'PPP' option is circled in red and labeled with a red '1'. The main window displays the 'PPP' configuration page, with the 'Secrets' tab selected. A table lists two secrets: 'site1' and 'site2', both with passwords 'site1' and 'site2' respectively, and service 'ovpn'. Below this, the 'OVPN Server' configuration window is open. The 'Enabled' checkbox is checked and circled in red, labeled with a red '2'. The 'Certificate' dropdown menu is set to 'server' and is also circled in red, labeled with a red '3'. The 'Require Client Certificate' checkbox is checked. Under 'Auth.', 'sha1' and 'md5' are checked, while 'null' is unchecked. Under 'Cipher', 'blowfish 128' and 'aes 128' are checked, while 'aes 192', 'aes 256', and 'null' are unchecked. A red '4' is placed near the cipher options. The 'OK', 'Cancel', and 'Apply' buttons are visible on the right side of the OVPN Server window.

Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Switch
Mesh
IP
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
MetaROUTER
Partition
Make Supout.rif
Manual
New WinBox

PPP

Name	Password	Service	Caller ID	Profile	Local
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

OK
Cancel
Apply

Deploying digital certificates

Using Digital Certificates on OpenVPN tunnels

Add OpenVPN client on site1 and site2 as below.

The screenshot shows the Mikrotik WinBox interface for configuring an OpenVPN client. The background window displays the 'Interface' configuration for 'ovpn-out1', showing it is an 'OVPN Client' with an 'Actual MTU' of 1500. The foreground window is the 'Interface <ovpn-out1>' configuration dialog, with the 'General' tab selected. The configuration includes:

- 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

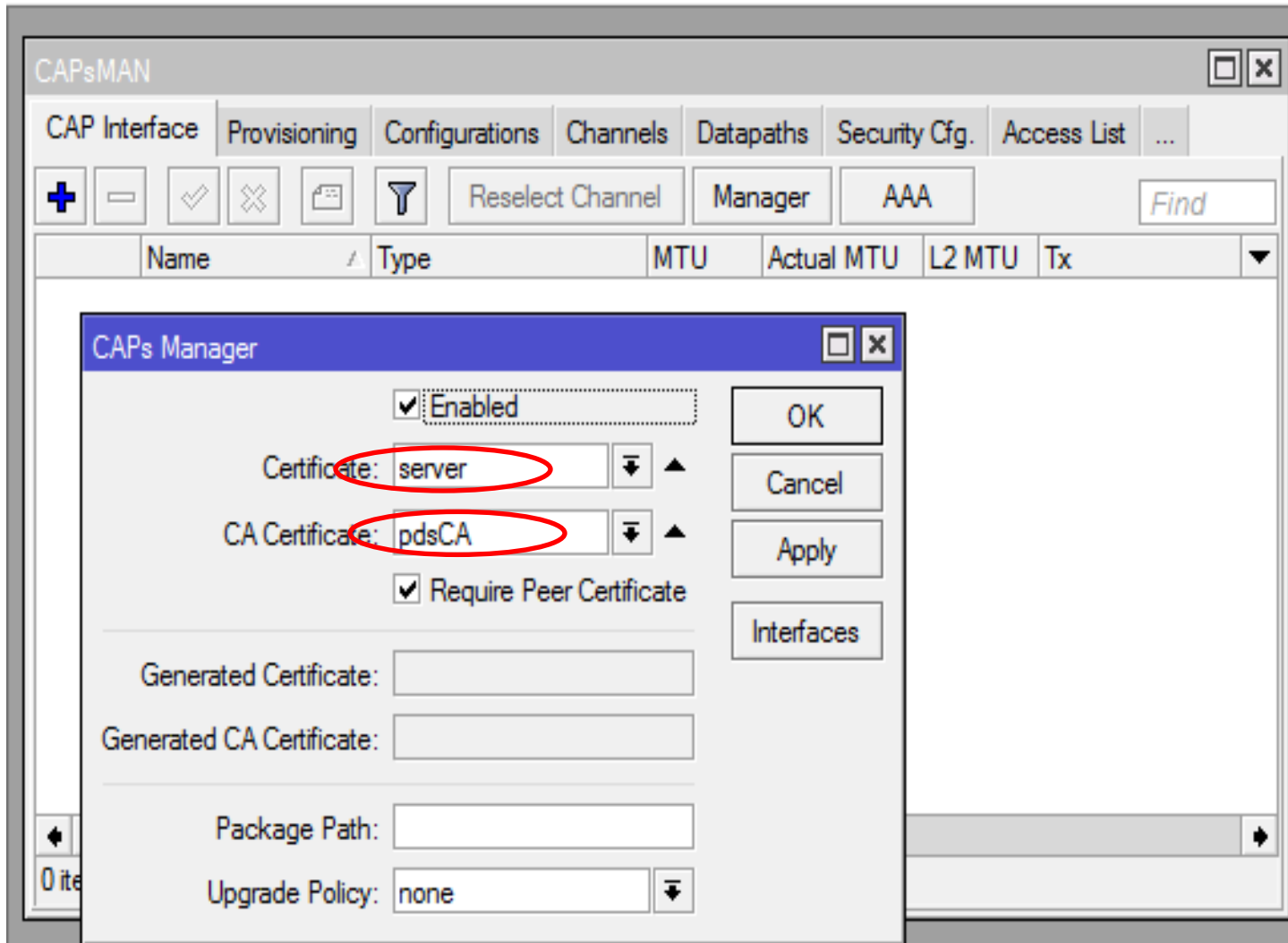
At the bottom of the dialog, the status is shown as 'enabled', 'running', 'slave', and 'Status: connected'. Red circles and numbers 1-4 highlight the following elements:

1. The '+' button in the interface list.
2. The 'User' field containing 'site1'.
3. The 'Certificate' field containing 'cert_export_site1.crt_0'.
4. The 'Status: connected' field at the bottom right.

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:

The screenshot displays the Mikrotik WinBox interface. On the left is a sidebar menu with various system configuration options. The main window is titled 'Wireless Tables' and shows a table of wireless interfaces. A 'CAP' configuration dialog box is open over the 'wlan1' interface row. In this dialog, the 'Enabled' checkbox is checked and circled in red. The 'Certificate' dropdown menu is also circled in red and shows 'cert_export_site1.crt_0'. Other fields include 'Interfaces' set to 'wlan1', 'Discovery Interfaces' set to 'ether1', 'CAPsMAN Addresses' set to '10.1.1.254', and 'Bridge' set to 'none'.

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

CAP Configuration:

- 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 for CAP to CapsMan connections
Enable CAP with certificate

The screenshot displays the Mikrotik WinBox interface. On the left is a sidebar with various system configuration options. The main window is titled 'Wireless Tables' and shows a table of wireless interfaces. A 'CAP' configuration dialog box is open over the 'wlan1' interface row.

Wireless Tables Table:

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:

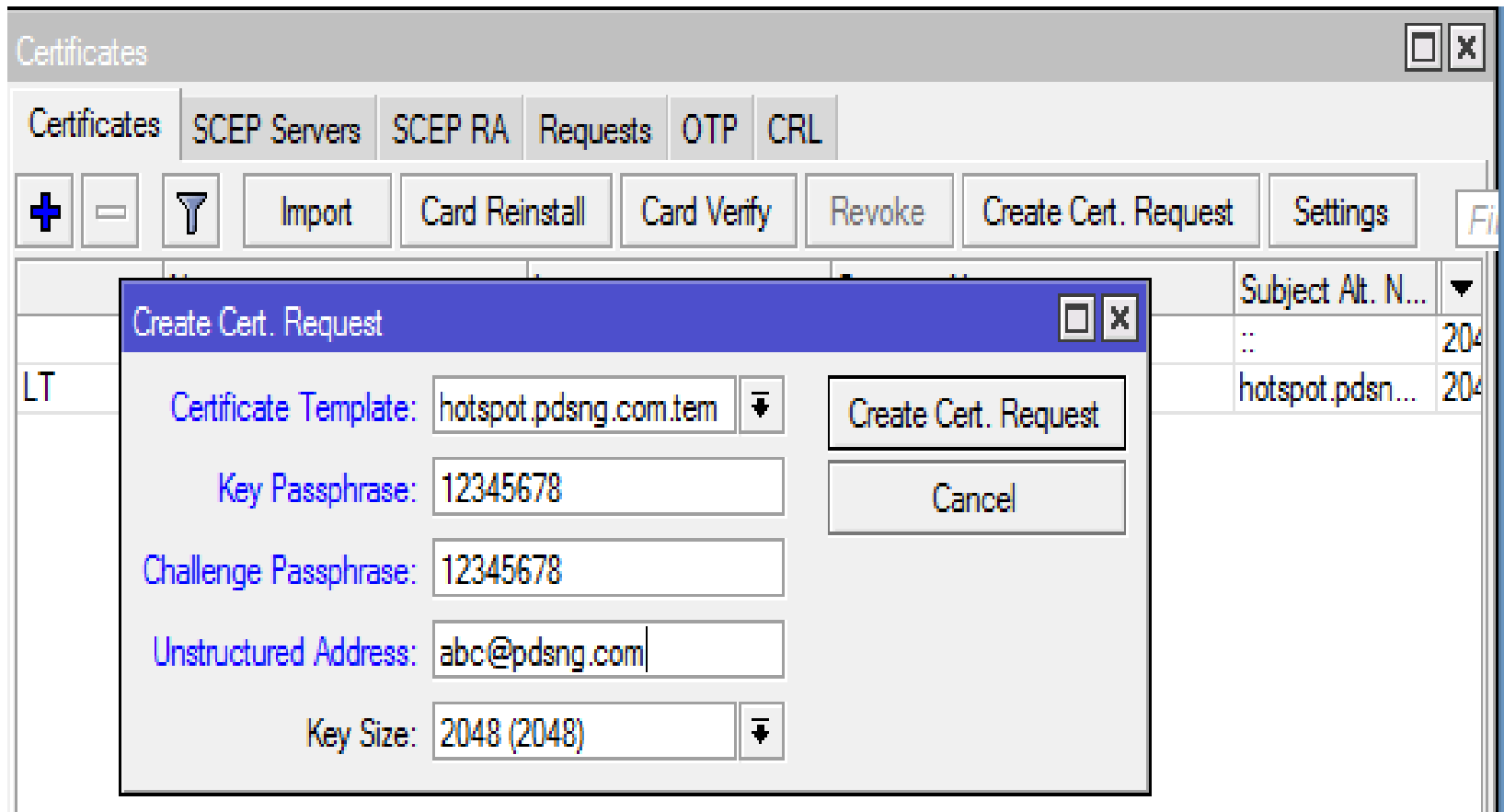
The image shows a screenshot of the 'Certificate' dialog box in a Windows operating system. The dialog box has a title bar that reads 'Certificates' and a subtitle 'Certificate <hotspot.pdsng.com.tem>'. It features three tabs: 'General', 'Key Usage', and 'Status', with 'General' currently selected. The 'General' tab contains several input fields for certificate information: '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), and 'Days Valid' (365). On the right side of the dialog box, 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.

Field	Value
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:



Deploying digital certificates

Deploying digital certificates on Hotspots

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

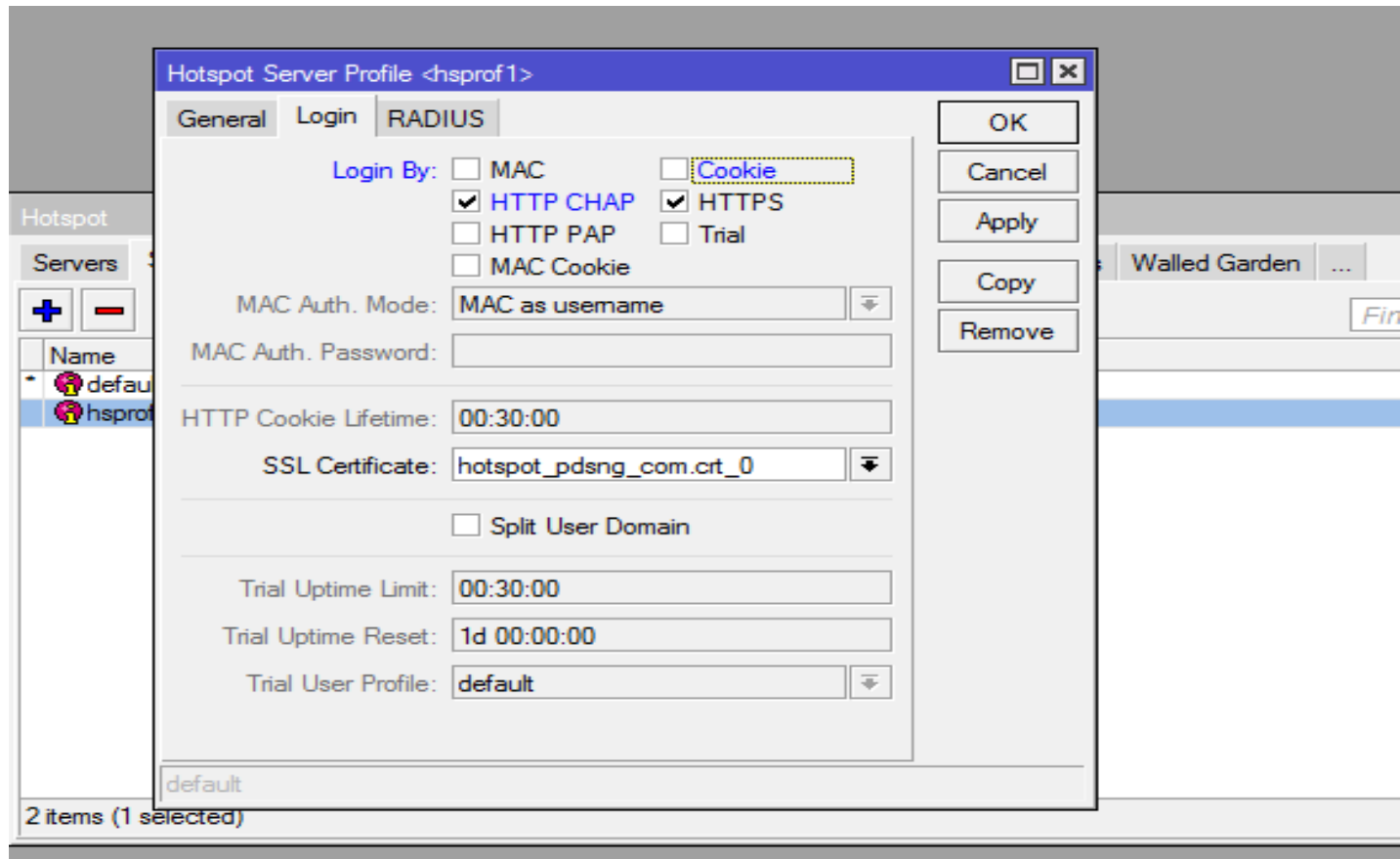
```
-----BEGIN CERTIFICATE REQUEST-----  
MIIDKDCCAhACAQIwgYcxCzAJBgNVBAYTAk5HMQ4wDAYDVQQIDAVMYWdvczEYMBYG  
A1UEBwwPVmljdG9yaWEgSXNsYW5kMSQwlgYDVQQKBtQYW5vcnFtYSBEYXRhIFNv  
bHV0aW9ucyBmdGQxDDAKBgNVBAsMA05PQzEaMBGGA1UEAwwRaG90c3BvdC5wZHNu  
Zy5jb20wgGaiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCsMiohfqTfCnqR  
lW2WUJfN60ikkAIBFZaYxFKjVNn51YDY3F+l2JMqBaVlibnjpPpWMtoXVgZN4tZ1  
NHbPYWR32aMrVkjpmzVNjOhWoFfQ81FInvucr3Ug7sSAcoeAwCfWY7WAwdjJCY/w  
kF6p648SCK8wja9IDT+mNMPla56kp7ccmzj316QKBOoYGg/l4xf0qH4hAqHJHnuR  
xFG4LyfMLrC10Qx/bAHM2dtRs12bohQHeunRgTuf59do5ofuw3S5hhQOZYHGw+s  
rC/qxV+seRvl16xK/HdvaFBje0m1mulsasW7Gcnlc+ZCoIC9eoLACgNBFDl6o67z  
8itHKdgrAgMBAAGgWzAXBgkqhkiG9w0BCQcxGwIcGRzbnMxMjMwHwYJKoZIhvcN  
AQkCMRIMEG1hZ251c0BwZHNuZy5jb20wHwYJKoZIhvcNAQkOMRIwEDA0BgNVHQ8B  
Af8EBAMCAbYwDQYJKoZIhvcNAQELBQADggEBAKB8R6aVFBBfZMJz8frB+YUGyxmI  
gQUw5LgcnjblqeJUMsZqkOzuNfk3Kdh5jrBfqTNNzied8kKTzE82+kcw4trc8P8  
1H7FU8pdRIUHFTxFe/hH5zYkWAjRb4UtCiryjoK1mq62wvK9QJ7fPceWtj46GY7  
n/vkR2BbHrqMVdMhNX0f5V3f/pvwn4C5KvZEUPo80vLDGBX/jXb/k7LaU5NOS4Ro  
l/6O8ep03Ry246VSuc+g64tbGYaB6jzSLy5Mlt31kg8n/18Wv6uBQlApvwQl6xbb  
hS/B01g8elwseatsCRmWxyH6THtcwZmejlgp2F7GuY/IFaMYbAm1F3SAzWs=  
-----END CERTIFICATE REQUEST-----
```

Your Certificate Issuer will require this code

Deploying digital certificates

Deploying digital certificates on Hotspots

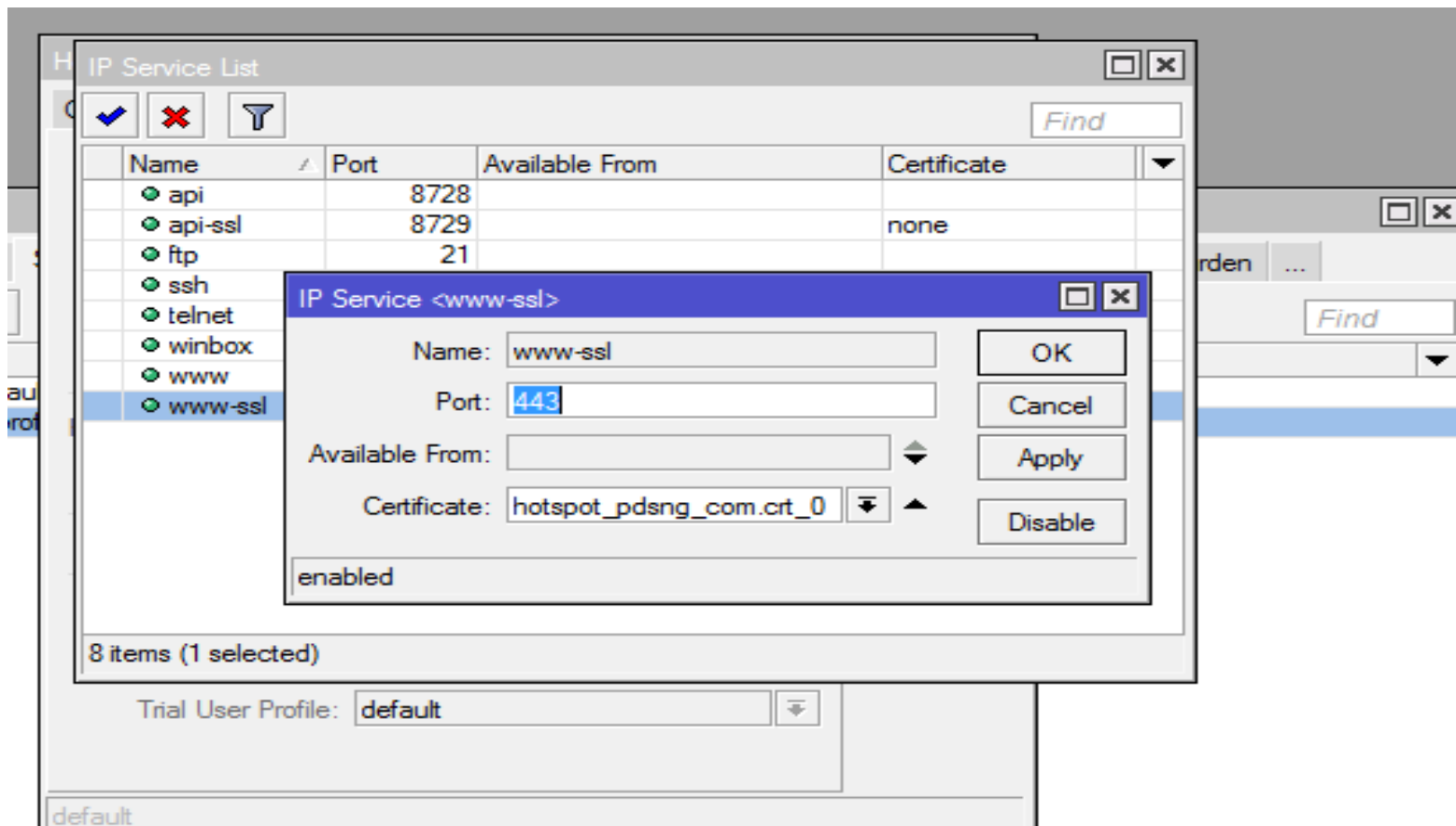
Setup hotspot to use the certificate:



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?