How to request a certificate

Version 1.0

PAN-OS 5.0.1

Johan Loos

johan@accessdenied.be

Introduction

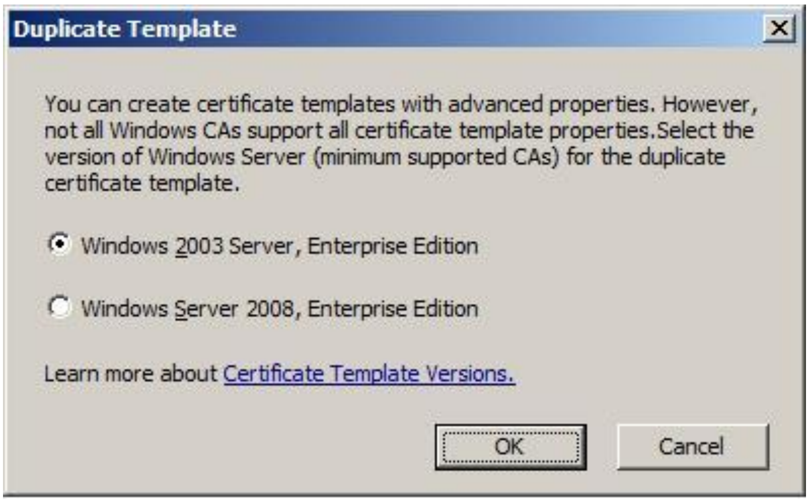
You can use self signed certificates, certificates from your own internal Certification Authority or certificates from a trusted Certification Authority on your firewall. These certificates can be used for GlobalProtect VPN, SSL decryption, etc.

Request a Certificate via a predefined file Task List

- △ Configure a certificate template on the Certification Authority
- △ Modify cert.inf file to use your certificate template
- △ Compile the configuration file into a certificate file
- △ Submit the certificate request file to a CA
- △ Install the certificate
- △ Export the certificate including private key
- △ Import the certificate into your firewall

Configure a certificate template on the Certification Authority

- Open **Certificate Authority** snap-in from **Administrative Tools.**
- Right click on **Certificate Templates** and select **Manage**
- Right click on **Server Authentication Certificate Template** and select **Duplicate Template.**
- On the **Duplicate Template** dialog box, select **Windows 2003 Server** and click **OK**



Duplicate Template

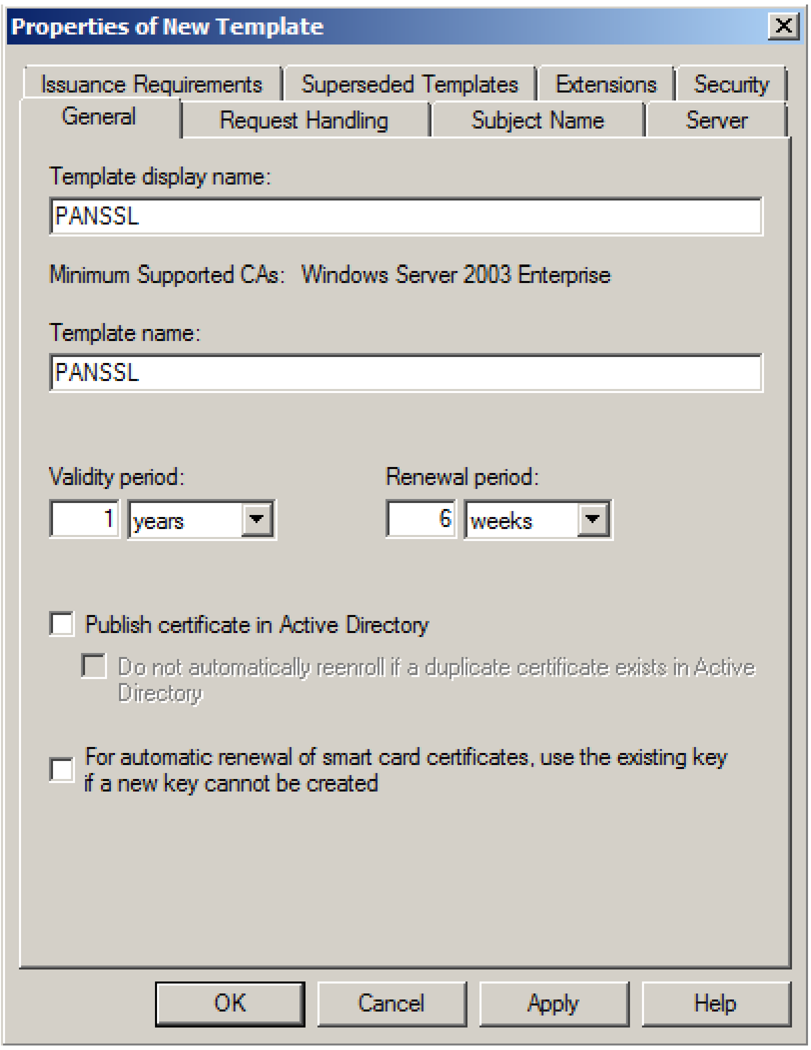
You can create certificate templates with advanced properties. However, not all Windows CAs support all certificate template properties.Select the version of Windows Server (minimum supported CAs) for the duplicate certificate template.

● Windows 2003 Server, Enterprise Edition

○ Windows Server 2008, Enterprise Edition

Learn more about Certificate Template Versions.

- On the **General** tab, in the **Template** display name field, type PANSSL



Template display name: PANSSL

Minimum Supported CAs: Windows Server 2003 Enterprise

Template name: PANSSL

Validity period: 1 years

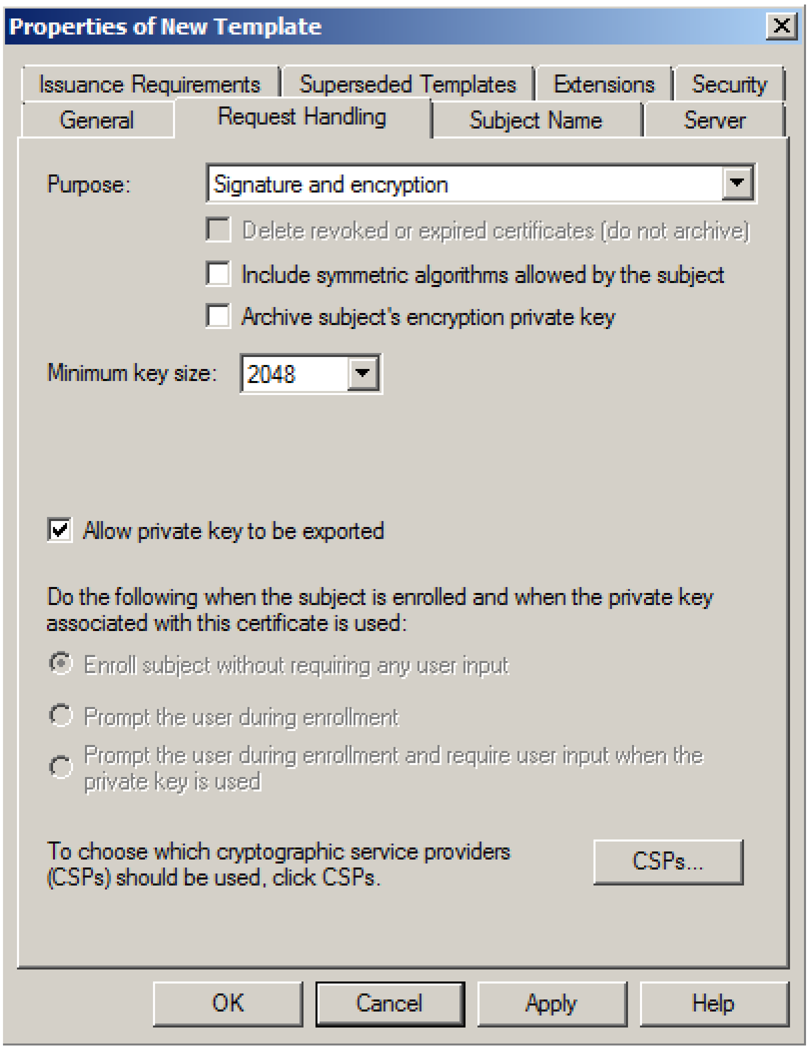
Renewal period: 6 weeks

□ Publish certificate in Active Directory

□ Do not automatically reenroll if a duplicate certificate exists in Active Directory

□ For automatic renewal of smart card certificates, use the existing key if a new key cannot be created

- Click on the **Subject Name** tab, select **Supply in the request**
- Click on the **Request Handling** tab, select **Allow private key to be exported**



Purpose: Signature and encryption

☐ Delete revoked or expired certificates (do not archive)

☐ Include symmetric algorithms allowed by the subject

☐ Archive subject's encryption private key

Minimum key size: 2048

☑ Allow private key to be exported

Do the following when the subject is enrolled and when the private key associated with this certificate is used:

● Enroll subject without requiring any user input

○ Prompt the user during enrollment

○ Prompt the user during enrollment and require user input when the private key is used

To choose which cryptographic service providers (CSPs) should be used, click CSPs.

- Click **OK**

Add Certificate Template to Certification Authority

- Right click on **Certificate Templates**, select **New Certificate Template to Issue**
- On the **Enable Certificate Template** dialog box, select PANSSL certificate template and click **OK**

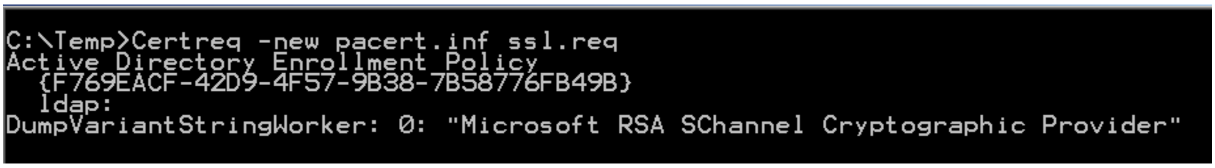
Modify cert.ini file to use your certificate template

```
 [Version]

Signature="$Windows NT$"



[NewRequest]

Subject = "CN=PA-VM.addev.local"
```

```
Exportable = TRUE ; Private key is exportable!
KeyLength = 2048
KeySpec = 1 ; AT_KEYEXCHANGE
KeyUsage = 0xA0 ; Digital Signature, Key Encipherment
MachineKeySet = True
ProviderName = "Microsoft RSA SChannel Cryptographic Provider"
ProviderType = 12
SMIME = FALSE
RequestType = CMC

[Strings]
szOID_SUBJECT_ALT_NAME2 = "2.5.29.17"
szOID_ENHANCED_KEY_USAGE = "2.5.29.37"
szOID_PKIX_KP_SERVER_AUTH = "1.3.6.1.5.5.7.3.1"
szOID_PKIX_KP_CLIENT_AUTH = "1.3.6.1.5.5.7.3.2"

[Extensions]
%szOID_SUBJECT_ALT_NAME2% = "{text}dns=PA-VM.addev.local&dns=sslvpn.addev.local"
%szOID_ENHANCED_KEY_USAGE%
="{text}%szOID_PKIX_KP_SERVER_AUTH%,%szOID_PKIX_KP_CLIENT_AUTH%"

[RequestAttributes]
CertificateTemplate= PANSSL
```

Compile the configuration file into a certificate file

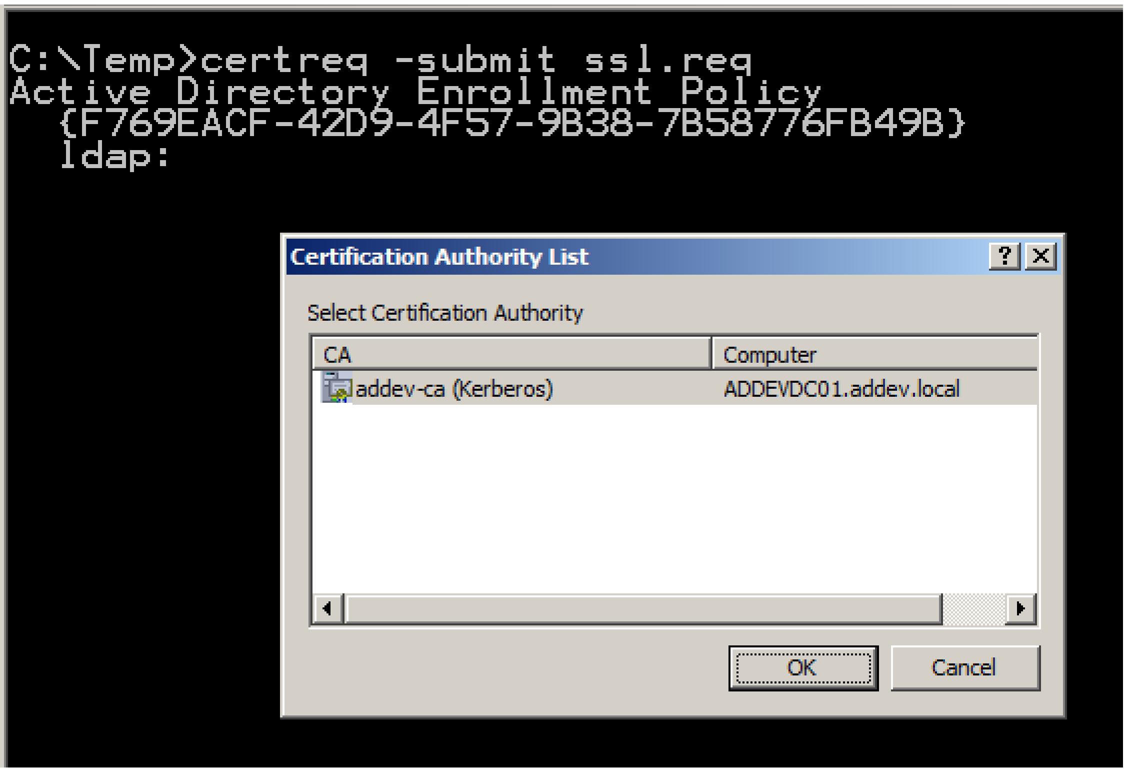
Certreq –new ssl.inf ssl.req



```
C:\Temp>Certreq -new pacert.inf ssl.req
Active Directory Enrollment Policy
  {F769EACF-42D9-4F57-9B38-7B58776FB49B}
  ldap:
DumpVariantStringWorker: 0: "Microsoft RSA SChannel Cryptographic Provider"
```

Submit the certificate request file to a CA

Certreq –submit ssl.req



```
C:\Temp>certreq -submit ssl.req
Active Directory Enrollment Policy
  {F769EACF-42D9-4F57-9B38-7B58776FB49B}
  ldap:
```

CA	Computer
addev-ca (Kerberos)	ADDEVDC01.addev.local

Select your certification authority and click **OK**

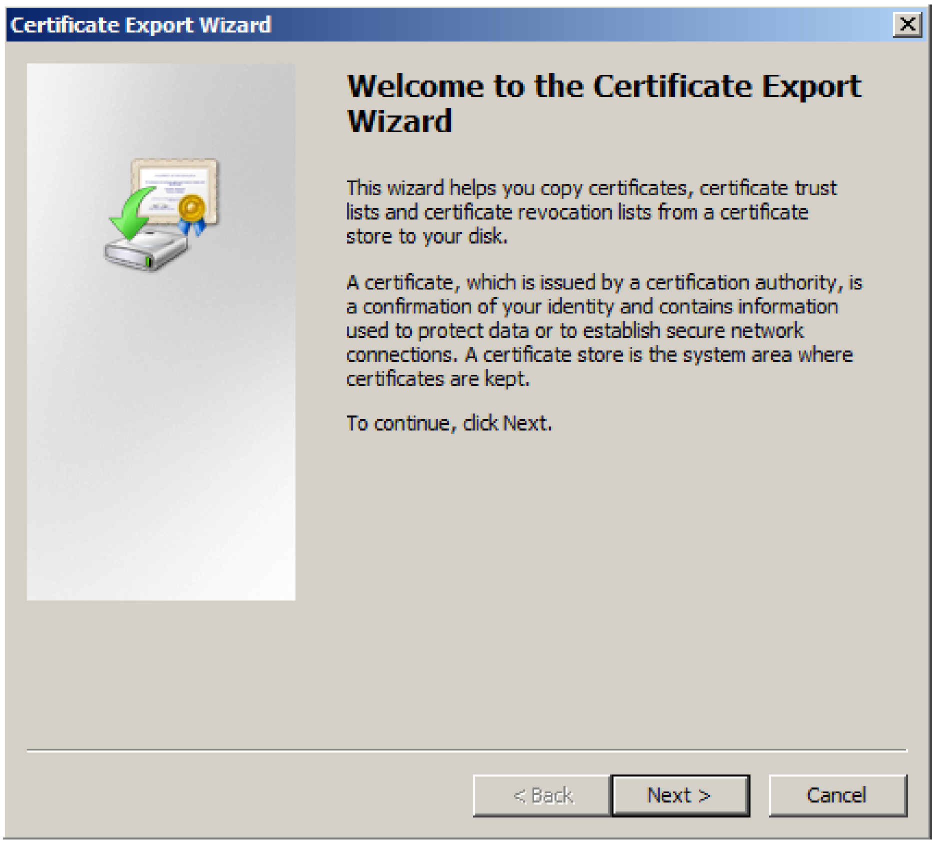
Install the certificate

Certreq –accept ssl.cer

This command places the certificate into the certificate store on the local computer

Export the certificate including private key

- Open MMC, add/remove snap-in certificates, and select **Computer**
- Locate your certificate in Certificates (Local Computer) | Personal | Certificates. Browse for your certificate, right click and select **Export**
- On the **Welcome to Certificate Export Wizard** page, click **Next**



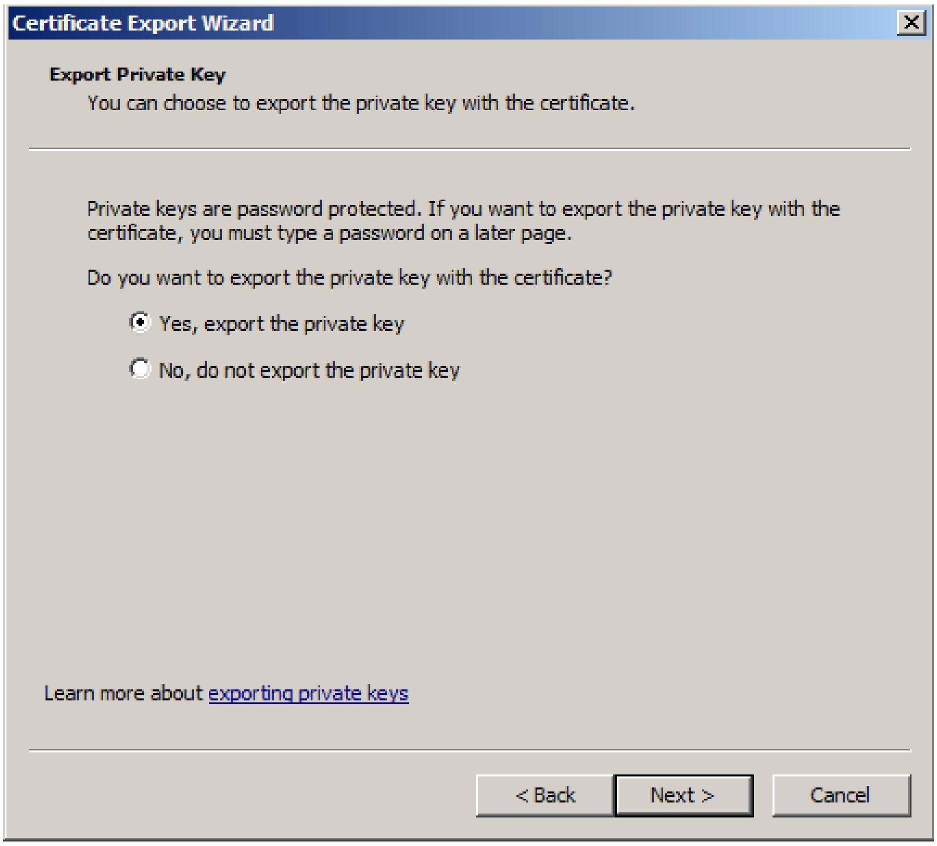
Welcome to the Certificate Export Wizard

This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

- On the **Export Private Key** page, select **Yes, export the private key** and click **Next**



Export Private Key

You can choose to export the private key with the certificate.

Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

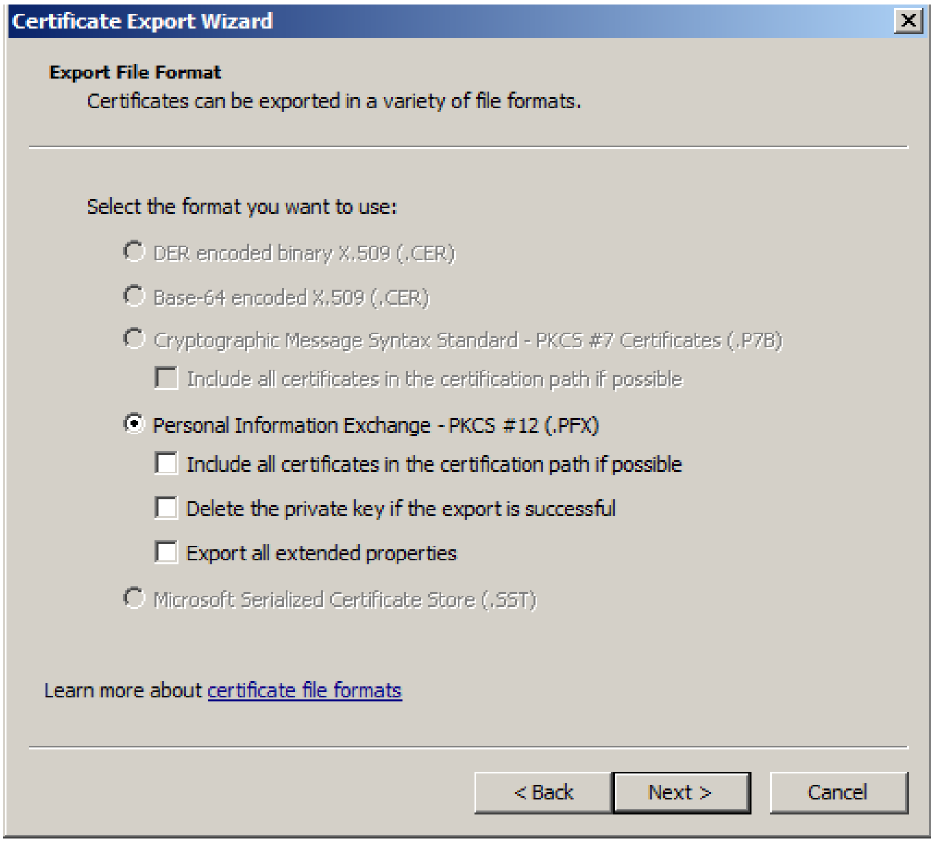
Do you want to export the private key with the certificate?

● Yes, export the private key

○ No, do not export the private key

Learn more about exporting private keys

- On the **Export File Format** page, select **Personal Information Exchange** and click **Next**



Certificate Export Wizard

Export File Format

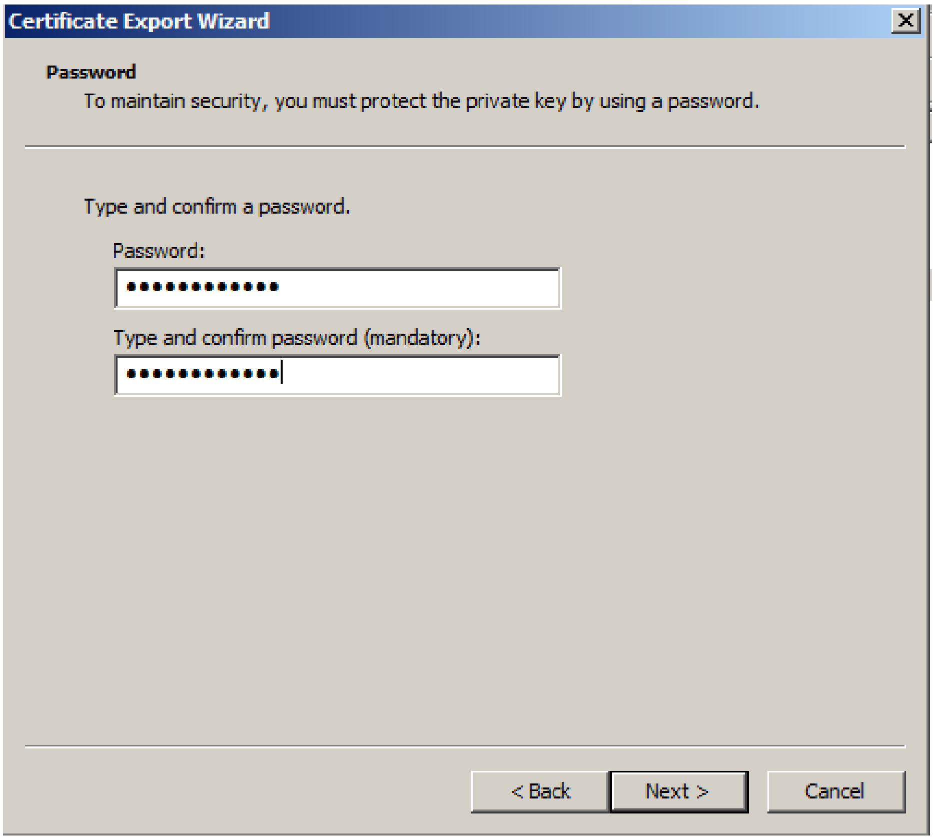
Certificates can be exported in a variety of file formats.

Select the format you want to use:

- ○ DER encoded binary X.509 (.CER)
- ○ Base-64 encoded X.509 (.CER)
- ○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
  - □ Include all certificates in the certification path if possible
- ● Personal Information Exchange - PKCS #12 (.PFX)
  - □ Include all certificates in the certification path if possible
  - □ Delete the private key if the export is successful
  - □ Export all extended properties
- ○ Microsoft Serialized Certificate Store (.SST)

Learn more about certificate file formats

- On the **Password** page, type a password and click **Next**



Certificate Export Wizard

Password

To maintain security, you must protect the private key by using a password.

Type and confirm a password.

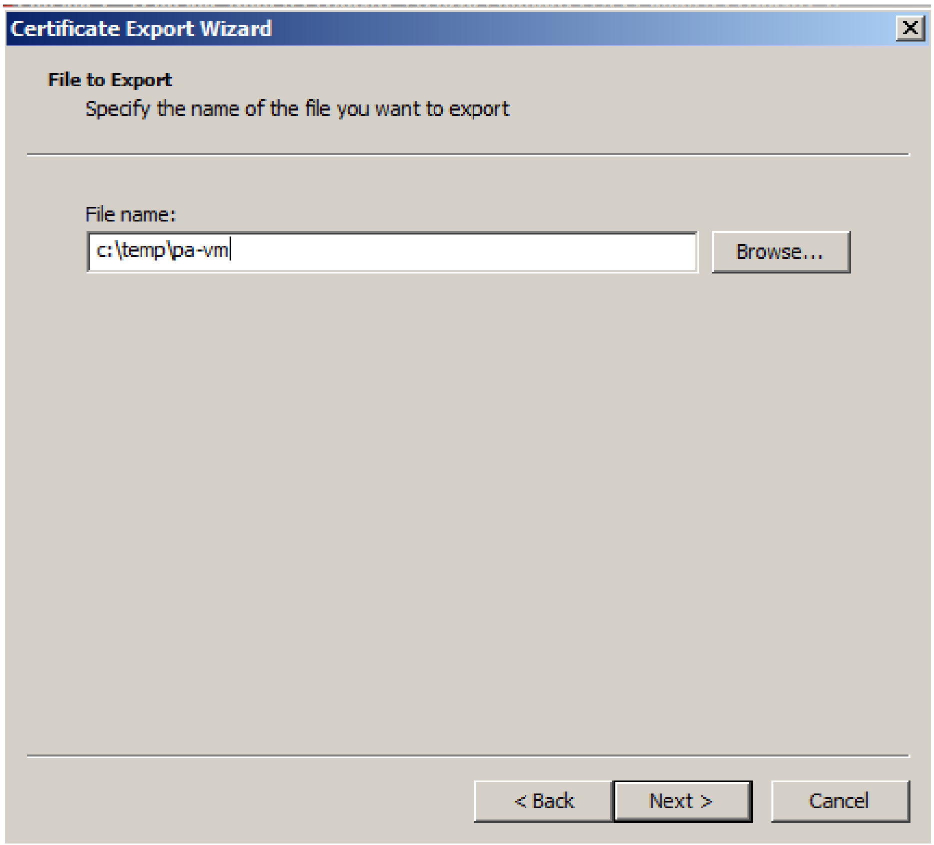
Password:

●●●●●●●●●●●●

Type and confirm password (mandatory):

●●●●●●●●●●●●

- On the **File to Export** page, type the filename for your certificate and click **Next**



Certificate Export Wizard

File to Export

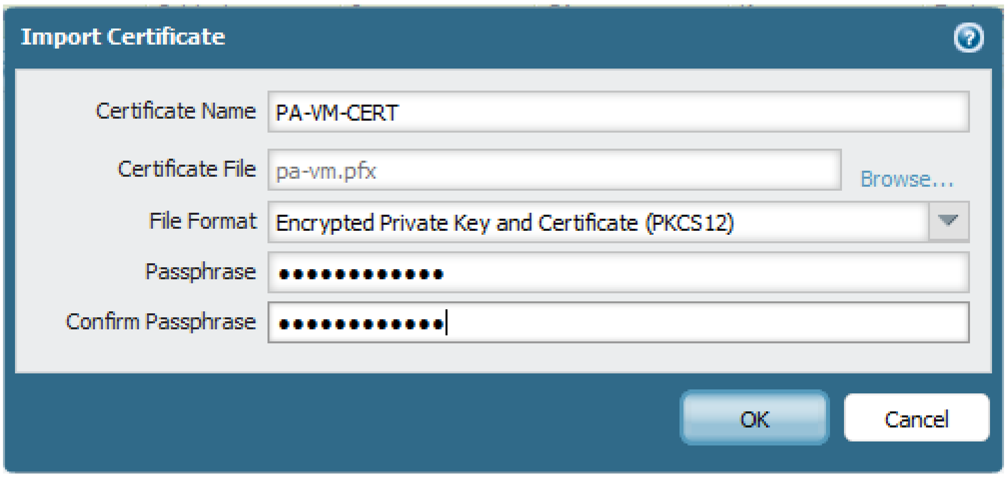
Specify the name of the file you want to export

File name: c:\temp\pa-vm

- On the **Completing** page, click **Next**

Import the certificate into your firewall

- Navigate to **Device | Certificate Management | Certificates | Device Certificates** and click **Import**
- On the **Import Certificate** page, for Certificate File click **Browse**
- Select the certificate for your firewall, type a name for your certificate, **select Encrypted Private Key and Certificate,** type the passphrase you have specified in the previous step



Import Certificate

Certificate Name: PA-VM-CERT

Certificate File: pa-vm.pfx

File Format: Encrypted Private Key and Certificate (PKCS12)

Passphrase: ••••••••••••

Confirm Passphrase: ••••••••••••

- Click **OK**