PKI Authentication For FortiMail Web Mail Access

Version 4.1

Technical Note

PKI Authentication for FortiMail Web Mail Access

Version 4.1

Revision 1

1 September 2010

Trademarks

Dynamic Threat Prevention System (DTPS), APSecure, FortiASIC, FortiBIOS, FortiBridge, FortiClient, FortiGate®, FortiGate Unified Threat Management System, FortiGuard®, FortiGuard-Antispam, FortiGuard-Antivirus, FortiGuard-Intrusion, FortiGuard-Web, FortiLog, FortiAnalyzer, FortiManager, Fortinet®, FortiOS, FortiPartner, FortiProtect, FortiReporter, FortiResponse, FortiShield, FortiVoIP, and FortiWiFi are trademarks of Fortinet, Inc. in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Regulatory compliance

FCC Class A Part 15 CSA/CUS

CAUTION: Risk of explosion if battery is replaced by an incorrect type. Dispose of used batteries according to instructions.

Table of Contents

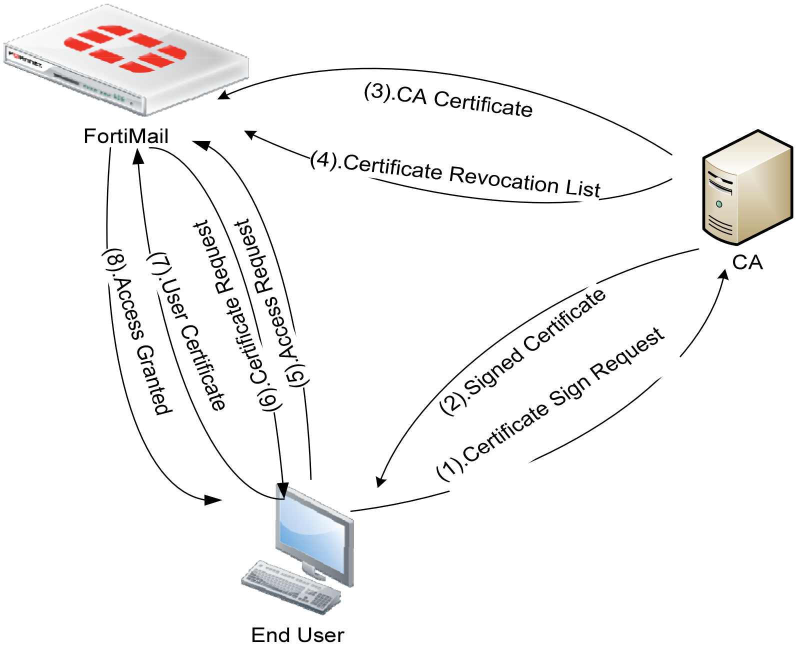
Introduction

PKI authentication is the methodology used to verify the identity of a user by checking the validity of the certificate bound to that user. It is an alternative to traditional password based authentication. The traditional method is based on "what you know" – the password, while PKI authentication is based on "what you have" – the private key related to the certificate. A common weakness of traditional password based authentication is the vulnerability to password guessing or brute force attack. PKI authentication is more resilient to this type of attack hence provides a stronger authentication mechanism in this sense.

In cryptography, a PKI is an arrangement that binds public keys with respective user identities by means of a certificate authority (CA). PKI authentication relies on two factors:

1. The tree of trust. If a CA is trusted, then all the certificates issued by this CA or any intermediate CA trusted by this CA are trusted (Certificate Revocation List (CRL) or Online Certificate Status Protocol (OCSP) is used to handle revoked certificates and not covered in this document)
2. Public key encryption algorithm. The data encrypted by public key can only be decrypted by private key. This is the basis for asymmetric data encryption. Similarly the data encrypted by private key can be decrypted by the public key. This is usually used for digital signature. The private key is only available to a specific individual, while its related public key is embedded in the certificate signed by a CA. Before communication starts, two parties exchange certificates and verify if the certificate is issued by a trusted CA, if the claimed identity matches the one in the certificate, if the certificate has expired and if the certificate type/usage matches the intended usage in the certificate. Since the certificate is freely available, digital signature is used to verify that the request did come from the party who owns the certificate.

The architecture of PKI authentication on FortiMail is described in the diagram below:



Generally speaking, there are six steps to enable PKI authentication on FortiMail as following:

1. **Create user certificates and Import into browser**
2. **Import the CA certificate on FortiMail**
3. **Create domain and local users on FortiMail server**
4. **Create PKI user**
5. **Create incoming policy and enable PKI authentication for webmail access**
6. **Enable PKI authentication on CLI on FortiMail**

Step 1: Generate the required certificates

This step has two objectives:

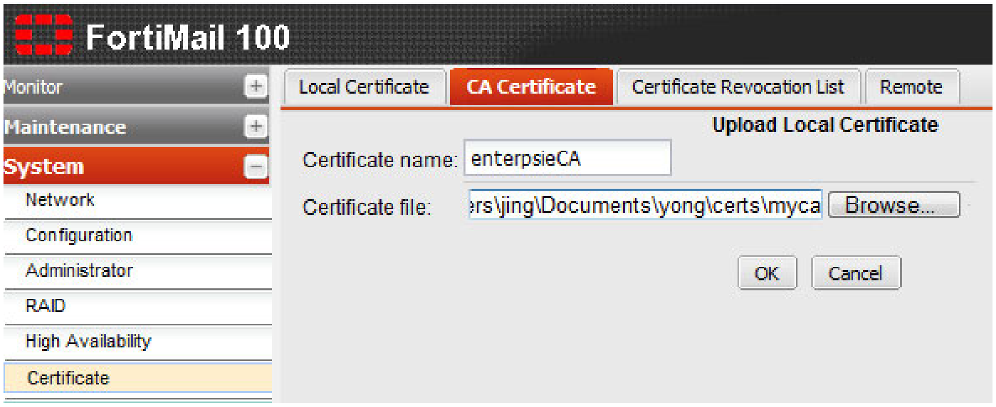
- Obtain the CA certificate in base64 encoding (DER encoding is not supported in FortiMail version 4.0 GA and MR1).
- Generate end user certificates that meet the following two requirement:
  A. Email address in CN field (or Alternative Subject Name) that will be used as the login ID
  B. The type of certificate should be accepted by the browsers for client authentication. Usually TLS or SSL web client certificate or certificate without any type at all will work for most browsers. FortiMail doesn't check the type of certificate, so this check is enforced by the browser on client side.

The certificate can be generated with Microsoft Windows Certificate Service, OpenSSL or any other third-party CA, as long as it meets the requirements set above. Usually the certificate sign request (CSR) is generated on the end user PC so that the private key doesn't have to be exported/imported. Alternatively, a CSR can be generated by administrator on behalf of all end users. Then the private key and the signed certificate have to be exported by administrator and transmitted to end users who then import into their browsers. All the user certificates and related private keys (usually in PKCS12 format) have to be delivered to end users and stored securely. If someone else obtains the private key and certificate, he/she can impersonate that person and gain unauthorized access. If more than one browsers are used, the PKCS12 file needs to be imported into all the browsers separately because different browsers don't share the certificate store.

For instructions on how to generate certificate on Windows Certificate Service 2003, please refer to Appendix A.

Step 2: Import the CA certificate on FortiMail

To make FortiMail trust a CA, you must import the CA certificate obtained in step 1 into FortiMail by going to **System > Certificate > CA certificate**.



Upload Local Certificate

Certificate name: enterpsieCA

Certificate file: rs\jing\Documents\yong\certs\myca

Step 3: Create local domain and users

If the FortiMail unit is deployed in gateway mode or transparent mode, email users whose email is quarantined on FortiMail are created automatically. And the email users can only access the Bulk folder which contains the quarantined spam in their web mail.

If the FortiMail unit is deployed in server mode, you must manually create local email users. The email users can access all the folders available on the server. Besides, in FortiMail version 4.0.4 and later releases, only local users (server mode) are supported for PKI authentication. External LDAP users are not supported for PKI authentication.

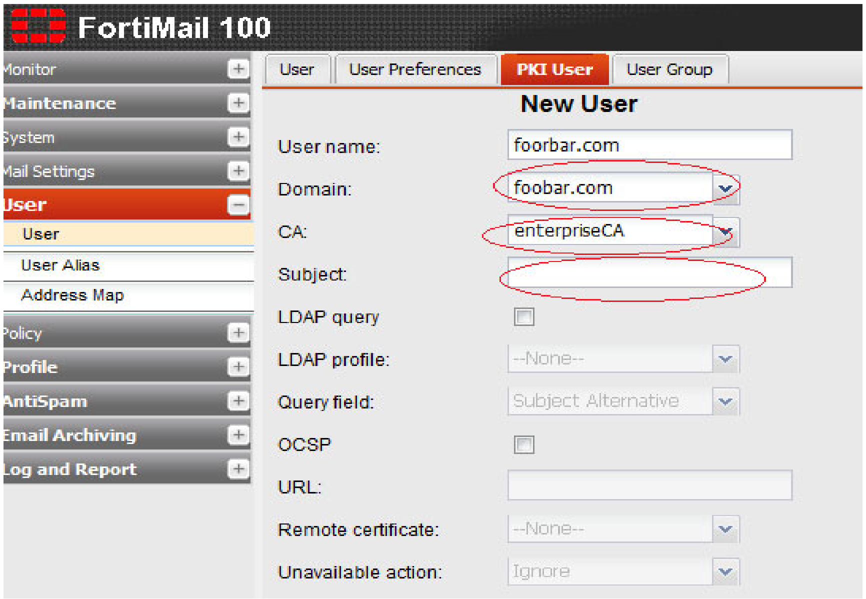
Step 4: Create PKI users

For webmail PKI authentication, PKI user is a template used to specify how FortiMail validates a certificate. The administrator needs to select the CA of which the certificate was imported in step 2. If a field is left empty, it means FortiMail won't check this field. So if the administrator doesn't specify the CA, FortiMail will accept the certificates issued by any CA, which is a security hole. An internal or external attacker could set up a private CA and create a certificate for any email address he/she wants to attack and then gain unauthorized access into the mailbox with the certificate signed by his/her own CA.

To create a PKI user:

1. On the FortiMail web UI, select **User > User > PKI User**, and then click **New**.
2. Give the PKI user a name, say "foobar.com".
3. Select a domain in the drop-down list.
4. Remember to leave the subject field empty. Because the subject field of each individual user is different, we need to leave this field in the PKI user empty to match all the user certificates. Later on, the subject can be configured to restrict access to a subset of users, for example ou=IT.

FortiMail can also retrieve a certificate stored in LDAP directory. For simplicity, this document doesn't cover this.



New User

User name: foorbar.com

Domain: foobar.com

CA: enterpriseCA

Subject:

LDAP query ☐

LDAP profile: --None--

Query field: Subject Alternative

OCSP ☐

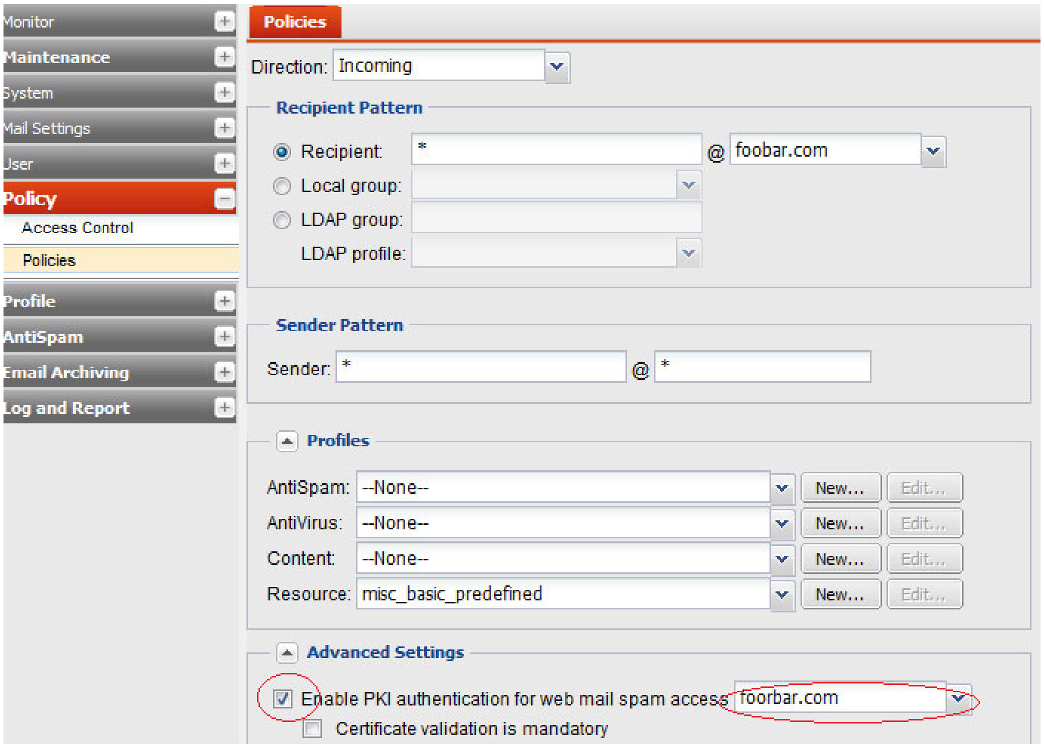
URL:

Remote certificate: --None--

Unavailable action: Ignore

Step 5: Configure policies to enable PKI authentication

Click **Policy > Recipient Policy**, check "Enable PKI authentication for web mail spam access" and select the PKI user template created in step 4. Click "ok" to confirm the change. There is another setting called "Certificate validation is mandatory" that may be enabled based on users' specific requirement. If this setting is not enabled, the system can fall back to traditional password based authentication if certificate-based authentication doesn't succeed. If this setting is enabled, users have to provide a valid certificate to gain access to web mail.



Direction: Incoming

Recipient Pattern

● Recipient: * @ foobar.com
○ Local group:
○ LDAP group:
LDAP profile:

Sender Pattern

Sender: * @ *

Profiles

AntiSpam: --None--
AntiVirus: --None--
Content: --None--
Resource: misc_basic_predefined

Advanced Settings

☑ Enable PKI authentication for web mail spam access foorbar.com
□ Certificate validation is mandatory

Step 6: Enable PKI authentication globally on CLI

The last, but not the least, is to enable PKI authentication globally on CLI. The setting configured in step 5 is domain specific and won't work until PKI authentication is enabled globally.

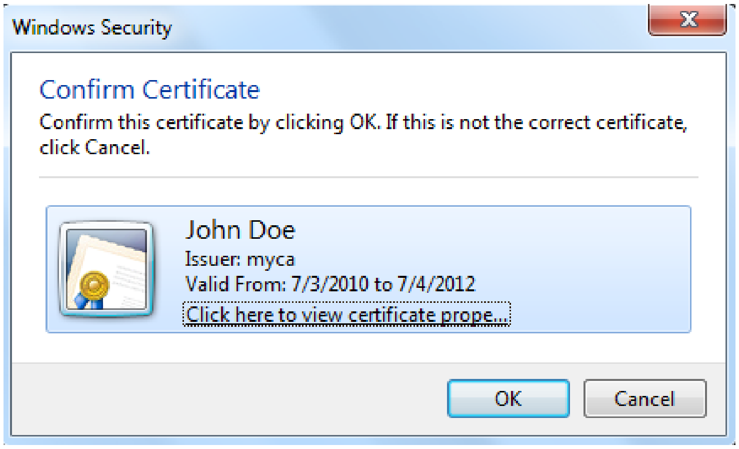
In the FortiMail CLI console, type the following command:

```
config system global

          set pki-mode enable

end
```

After this, when end users try to access the web mail, they should be prompted for certificates. If users are not prompted, it may be because the FortiMail HHTP server has not loaded the new settings yet. You can use the CLI command "exec reload" to manually enforce reload of the configuration.

Step 7: Test PKI authentication

To test whether PKI authentication works, end users type the URL of the webmail on their browsers. The end users should be prompted for certificate confirmation like below:



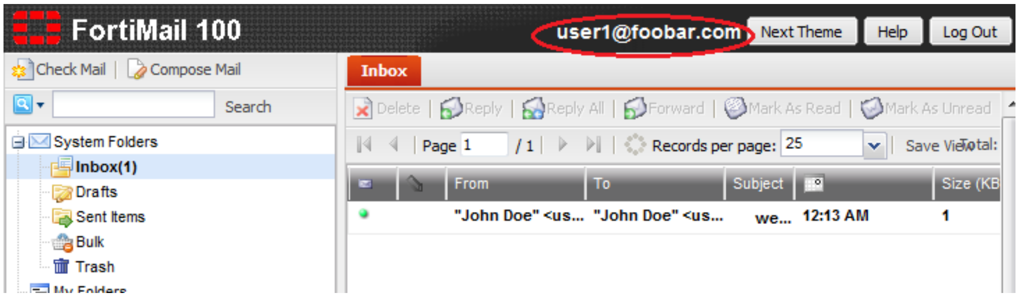
Windows Security

Confirm Certificate

Confirm this certificate by clicking OK. If this is not the correct certificate, click Cancel.

John Doe
Issuer: myca
Valid From: 7/3/2010 to 7/4/2012
Click here to view certificate prope...

If the end user clicks OK, the user will be able to log on to the web mail as below:

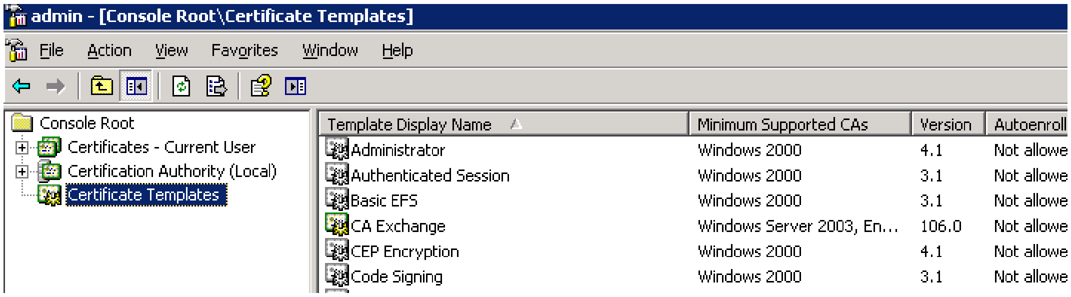


		From	To	Subject		Size (KB
		"John Doe" <us...	"John Doe" <us...	we...	12:13 AM	1

Appendix: Generate User Certificates with MS CA

This section describes how to use MS Certificate Service 2003 to generate user certificates that can be used for PKI authentication on FortiMail. The default certificate template coming with MS 2003 CA doesn’t work. A customized template has to be created. Because Windows 2003 server standard doesn’t support the customization of certificate template, so Windows Server 2003 Enterprise edition is required.

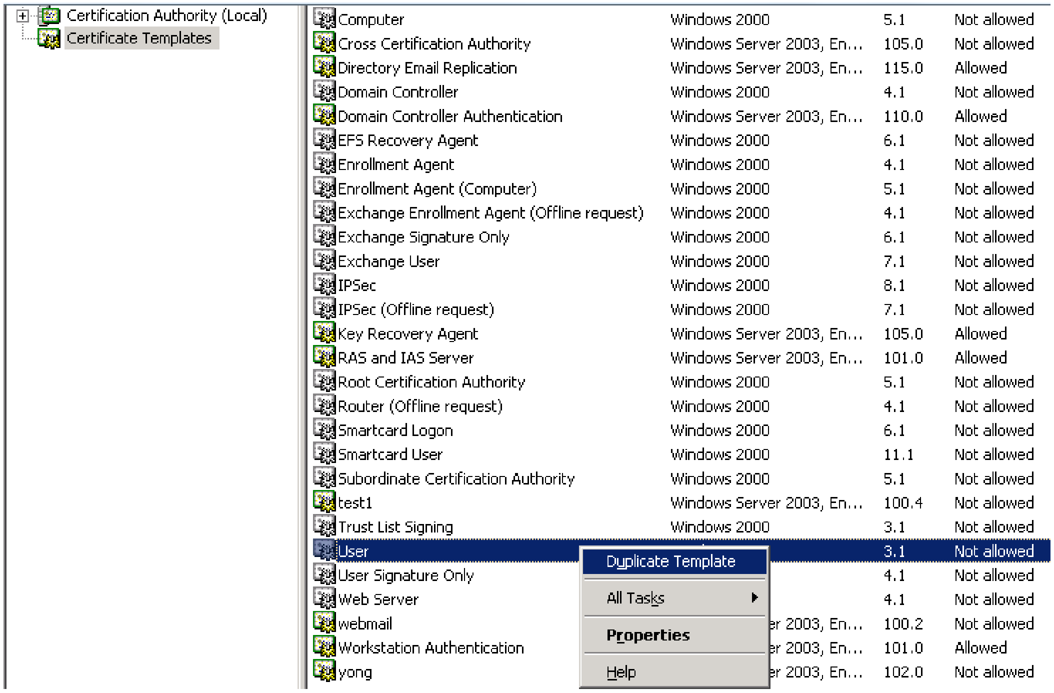
1. Install MS CA with web enrollment on Windows 2003 Enterprise Server.
2. On Windows 2003 server, run MMC and add “Certificate Template” and “Certificate Authority” snap-ins.



admin - [Console Root\Certificate Templates]

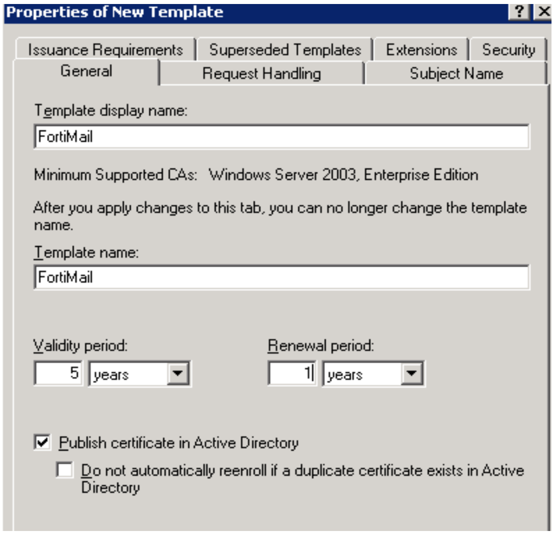
Template Display Name	Minimum Supported CAs	Version	Autoenroll
Administrator	Windows 2000	4.1	Not allowe
Authenticated Session	Windows 2000	3.1	Not allowe
Basic EFS	Windows 2000	3.1	Not allowe
CA Exchange	Windows Server 2003, En...	106.0	Not allowe
CEP Encryption	Windows 2000	4.1	Not allowe
Code Signing	Windows 2000	3.1	Not allowe

3. Select “Certificate Templates” and right click “User” in the right pane. Then select “Duplicate Template”.



Computer	Windows 2000	5.1	Not allowed
Cross Certification Authority	Windows Server 2003, En...	105.0	Not allowed
Directory Email Replication	Windows Server 2003, En...	115.0	Allowed
Domain Controller	Windows 2000	4.1	Not allowed
Domain Controller Authentication	Windows Server 2003, En...	110.0	Allowed
EFS Recovery Agent	Windows 2000	6.1	Not allowed
Enrollment Agent	Windows 2000	4.1	Not allowed
Enrollment Agent (Computer)	Windows 2000	5.1	Not allowed
Exchange Enrollment Agent (Offline request)	Windows 2000	4.1	Not allowed
Exchange Signature Only	Windows 2000	6.1	Not allowed
Exchange User	Windows 2000	7.1	Not allowed
IPSec	Windows 2000	8.1	Not allowed
IPSec (Offline request)	Windows 2000	7.1	Not allowed
Key Recovery Agent	Windows Server 2003, En...	105.0	Allowed
RAS and IAS Server	Windows Server 2003, En...	101.0	Allowed
Root Certification Authority	Windows 2000	5.1	Not allowed
Router (Offline request)	Windows 2000	4.1	Not allowed
Smartcard Logon	Windows 2000	6.1	Not allowed
Smartcard User	Windows 2000	11.1	Not allowed
Subordinate Certification Authority	Windows 2000	5.1	Not allowed
test1	Windows Server 2003, En...	100.4	Not allowed
Trust List Signing	Windows 2000	3.1	Not allowed
User		3.1	Not allowed
User Signature Only		4.1	Not allowed
Web Server		4.1	Not allowed
webmail	r 2003, En...	100.2	Not allowed
Workstation Authentication	r 2003, En...	101.0	Allowed
yong	r 2003, En...	102.0	Not allowed

4. Fill in the template name, validity period and renewal period according to your specific requirement on the "General" tab.



Template display name: FortiMail

Minimum Supported CAs: Windows Server 2003, Enterprise Edition

After you apply changes to this tab, you can no longer change the template name.

Template name: FortiMail

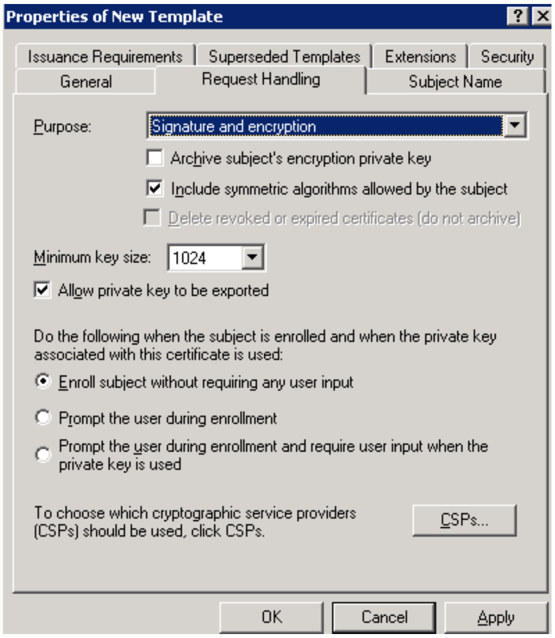
Validity period: 5 years

Renewal period: 1 years

☑ Publish certificate in Active Directory

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

5. On "Request handling" tab, select "signature and encryption" for Purpose.



Purpose: Signature and encryption

☐ Archive subject's encryption private key

☑ Include symmetric algorithms allowed by the subject

☐ Delete revoked or expired certificates (do not archive)

Minimum key size: 1024

☑ 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:

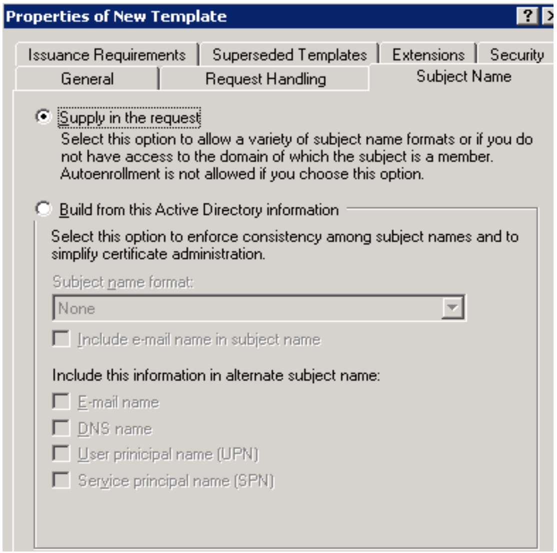
● Enroll subject without requiring any user input

○ 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.

6. Select “Supply in the request” on the “Subject Name” tab because the default subject name doesn’t work with FortiMail.



● Supply in the request

Select this option to allow a variety of subject name formats or if you do not have access to the domain of which the subject is a member. Autoenrollment is not allowed if you choose this option.

○ Build from this Active Directory information

Select this option to enforce consistency among subject names and to simplify certificate administration.

Subject name format: None

☐ Include e-mail name in subject name

Include this information in alternate subject name:

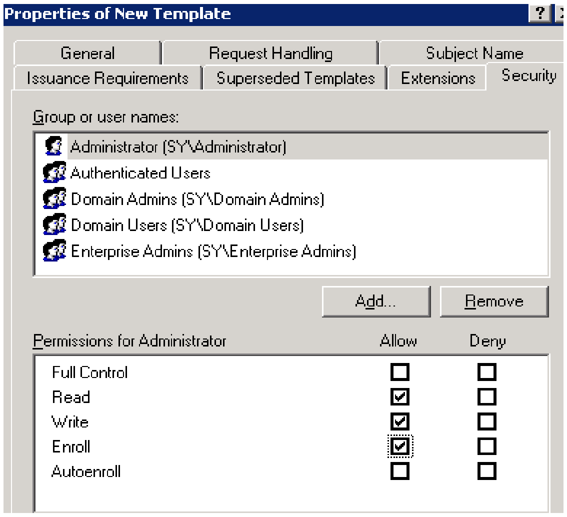
☐ E-mail name

☐ DNS name

☐ User pricipal name (UPN)

☐ Service principal name (SPN)

7. Enable “Enroll” permission for administrator on the “Security” tab

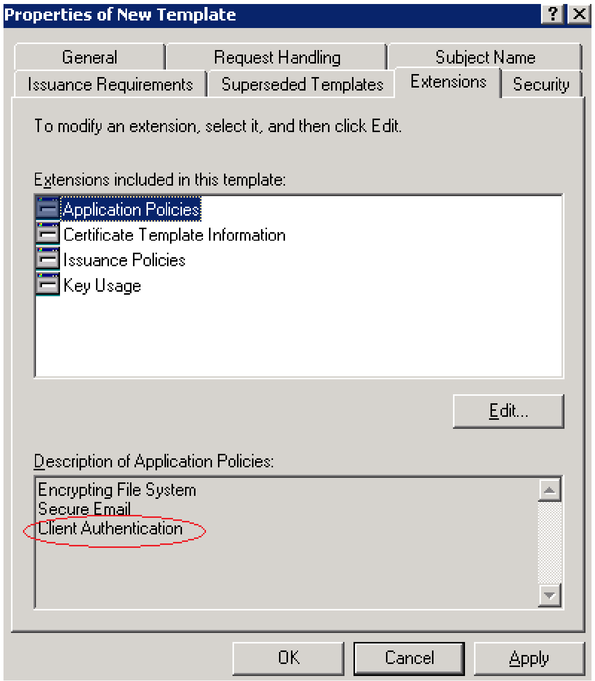


Group or user names:

- Administrator (SY\Administrator)
- Authenticated Users
- Domain Admins (SY\Domain Admins)
- Domain Users (SY\Domain Users)
- Enterprise Admins (SY\Enterprise Admins)

Permissions for Administrator	Allow	Deny
Full Control	□	□
Read	☑	□
Write	☑	□
Enroll	☑	□
Autoenroll	□	□

8. On the “Extensions” tab, make sure “Client Authentication” is enabled for “Application Policies” (client authentication is enabled by default).



To modify an extension, select it, and then click Edit.

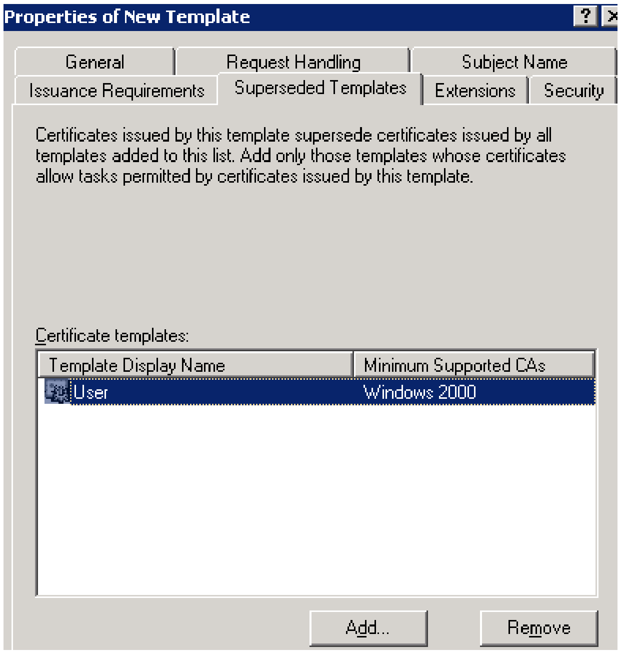
Extensions included in this template:

- Application Policies
- Certificate Template Information
- Issuance Policies
- Key Usage

Description of Application Policies:

Encrypting File System
Secure Email
Client Authentication

9. On the “Superseded Templates” tab, select “User” template on which this new template is based.



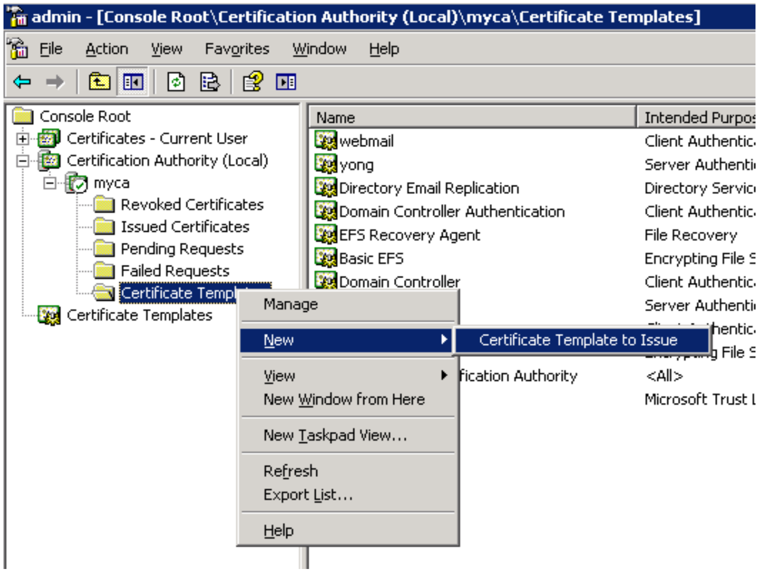
Certificates issued by this template supersede certificates issued by all templates added to this list. Add only those templates whose certificates allow tasks permitted by certificates issued by this template.

Certificate templates:

Template Display Name	Minimum Supported CAs
User	Windows 2000

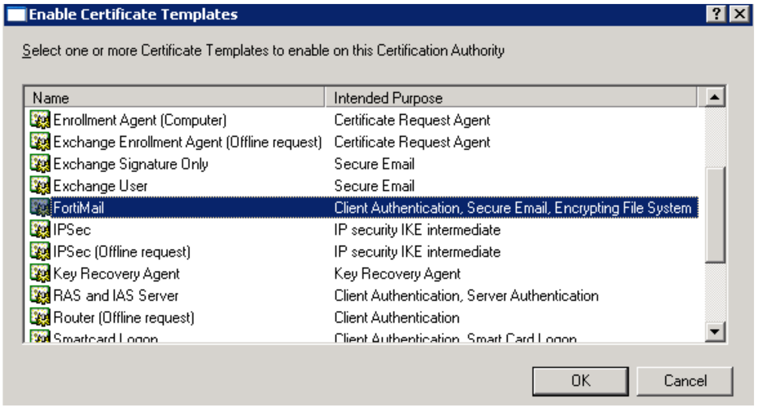
10. Leave other settings as default, and click "OK" to create the new template.
    Then the Certificate Authority needs to be configured to issue certificate with the new template just created.

11. Select "Certificate Authority" on MMC. Right click "Certificate Templates" under the root CA and select "New > Certificate Template to Issue".



Name	Intended Purpos
webmail	Client Authentic
yong	Server Authenti
Directory Email Replication	Directory Servic
Domain Controller Authentication	Client Authentic
EFS Recovery Agent	File Recovery
Basic EFS	Encrypting File S
Domain Controller	Client Authentic
	Server Authenti
	hentic
	g File S
fication Authority	<All>
	Microsoft Trust L

12. Select the new template just created from the list and click OK.

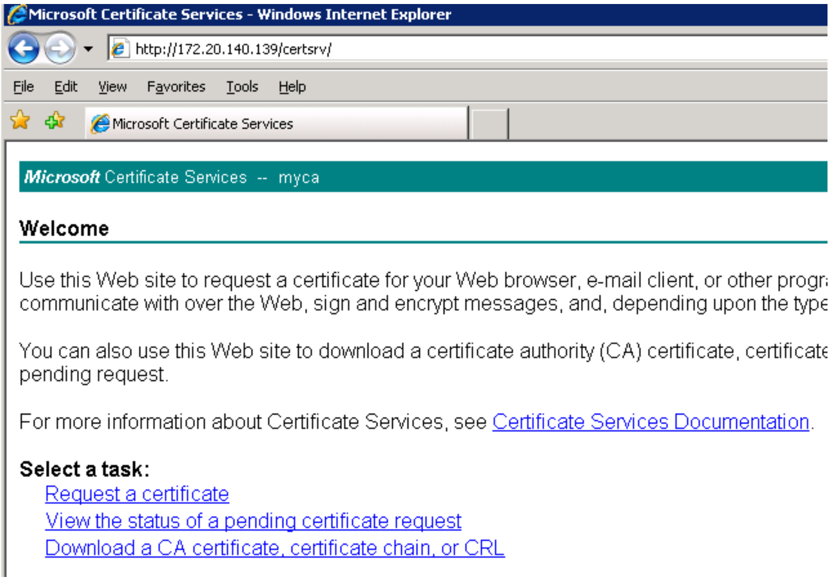


Select one or more Certificate Templates to enable on this Certification Authority

Name	Intended Purpose
Enrollment Agent (Computer)	Certificate Request Agent
Exchange Enrollment Agent (Offline request)	Certificate Request Agent
Exchange Signature Only	Secure Email
Exchange User	Secure Email
FortiMail	Client Authentication, Secure Email, Encrypting File System
IPSec	IP security IKE intermediate
IPSec (Offline request)	IP security IKE intermediate
Key Recovery Agent	Key Recovery Agent
RAS and IAS Server	Client Authentication, Server Authentication
Router (Offline request)	Client Authentication
Smartcard Logon	Client Authentication, Smart Card Logon

Now the administrator need to use web enroll to create certificates for all the users as following:

13. Type http://your_ip_of_ms_ca_server/certsrv/ and login in as **administrator**
This document assumes all certificates are requested by administrator on behalf of end users.



Microsoft Certificate Services - Windows Internet Explorer
http://172.20.140.139/certsrv/
File
Edit
View
Favorites
Tools
Help
Microsoft Certificate Services

Microsoft Certificate Services -- myca

Welcome

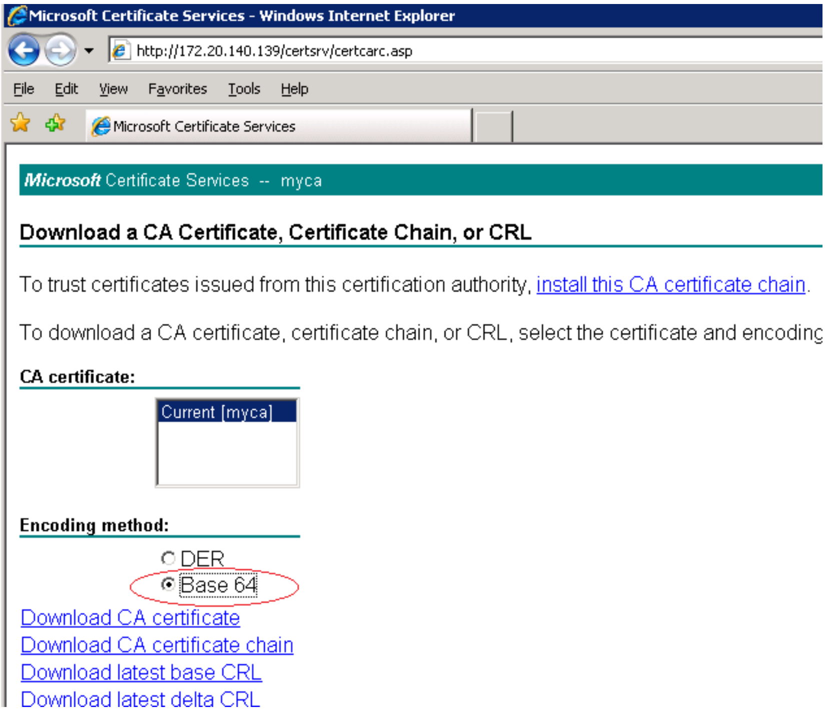
Use this Web site to request a certificate for your Web browser, e-mail client, or other progr
communicate with over the Web, sign and encrypt messages, and, depending upon the type

You can also use this Web site to download a certificate authority (CA) certificate, certificate
pending request.

For more information about Certificate Services, see Certificate Services Documentation.

Select a task:
Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL

14. Click the last option “Download CA certificate”, and then select “Base64” for CA certificate encoding. Click “Download CA certificate” and save the CA certificate.


Microsoft Certificate Services - Windows Internet Explorer
http://172.20.140.139/certsrv/certcarc.asp
File Edit View Favorites Tools Help
Microsoft Certificate Services

Microsoft Certificate Services -- myca

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, install this CA certificate chain.

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding

CA certificate:

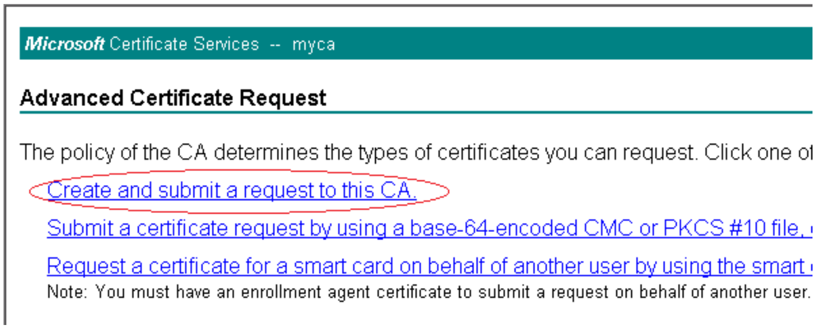
Current [myca]

Encoding method:

○ DER
● Base 64

Download CA certificate
Download CA certificate chain
Download latest base CRL
Download latest delta CRL

15. Click Back button of the browser to return to the welcome page of certsrv as shown in step 13. Click “Request a certificate”, click “Advanced certificate request”, then click “Create and Submit a request to this CA”.



Microsoft Certificate Services -- myca

Advanced Certificate Request

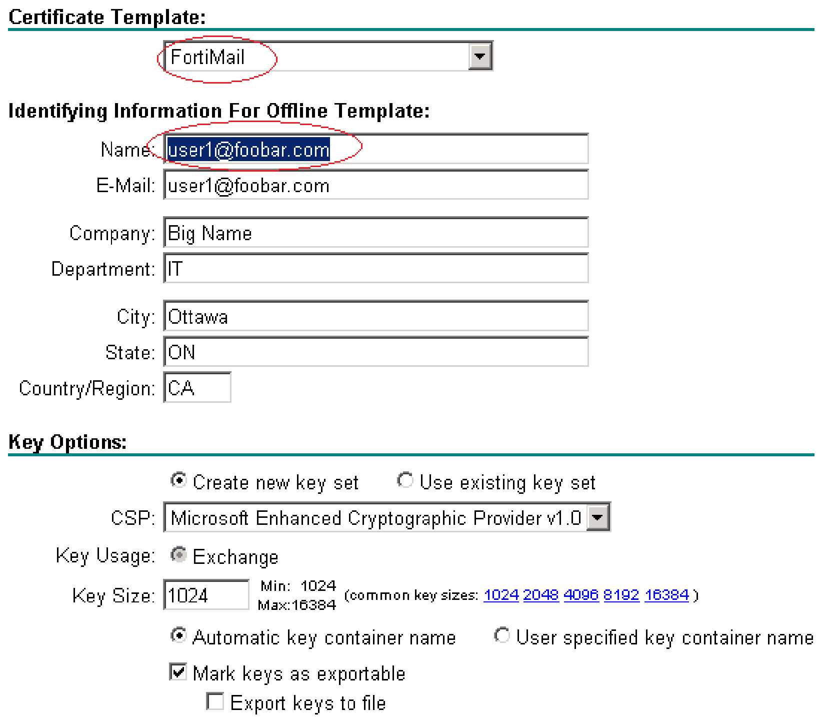
The policy of the CA determines the types of certificates you can request. Click one of

Create and submit a request to this CA.

Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file,

Request a certificate for a smart card on behalf of another user by using the smart
Note: You must have an enrollment agent certificate to submit a request on behalf of another user.

16. Select the new template created previously and fill in the information for subject. Please note that only the name field is required and it needs to match the email account set up on FortiMail. FortiMail will use the email address either in Name (Common Name) or Alternative Subject Name field as the login ID. Alternative Subject Name is not supported by default in MS CA 2003. For simplicity, we used Name field in this document. The full name of this user can be added as the optional “friendly name”.



Certificate Template:

FortiMail ▾

Identifying Information For Offline Template:

Name: user1@foobar.com

E-Mail: user1@foobar.com

Company: Big Name

Department: IT

City: Ottawa

State: ON

Country/Region: CA

Key Options:

● Create new key set ○ Use existing key set

CSP: Microsoft Enhanced Cryptographic Provider v1.0 ▾

Key Usage: ● Exchange

Key Size: 1024 Min: 1024 Max:16384 (common key sizes: 1024 2048 4096 8192 16384)

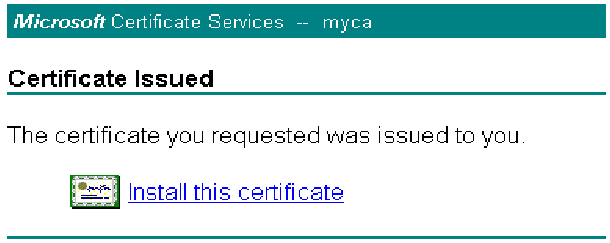
● Automatic key container name ○ User specified key container name

☑ Mark keys as exportable

□ Export keys to file

17. Then click "Submit" to submit the certificate request.

18. If CA is configured to issue the certificate automatically, you will see "Install the certificate" link on the web page soon after the certificate request submission. Click this link to load your certificate into your certificate store.

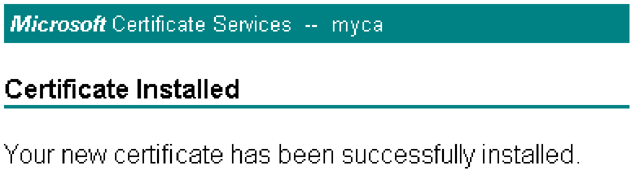


Microsoft Certificate Services -- myca

Certificate Issued

The certificate you requested was issued to you.

Install this certificate

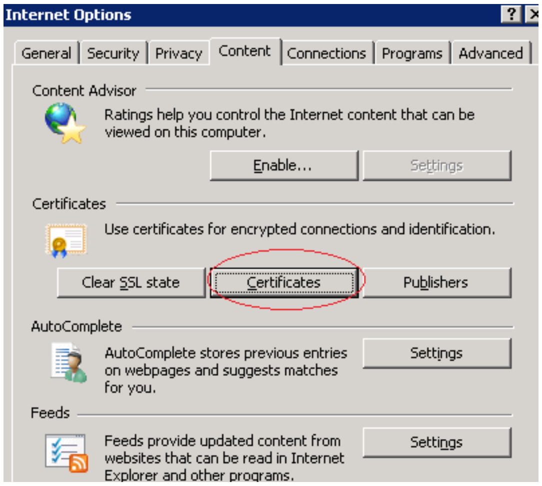


Microsoft Certificate Services -- myca

Certificate Installed

Your new certificate has been successfully installed.

19. On your browser (IE 7 in this document), select Tools > Internet Options > Content > Certificates.



Content Advisor

Ratings help you control the Internet content that can be viewed on this computer.

Certificates

Use certificates for encrypted connections and identification.

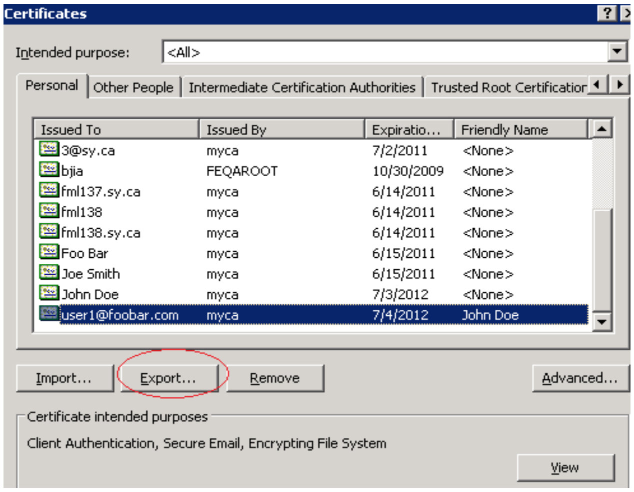
AutoComplete

AutoComplete stores previous entries on webpages and suggests matches for you.

Feeds

Feeds provide updated content from websites that can be read in Internet Explorer and other programs.

20. Select the certificate we just created in the list and click “Export” to export it to a file so that end user can import into their browser.



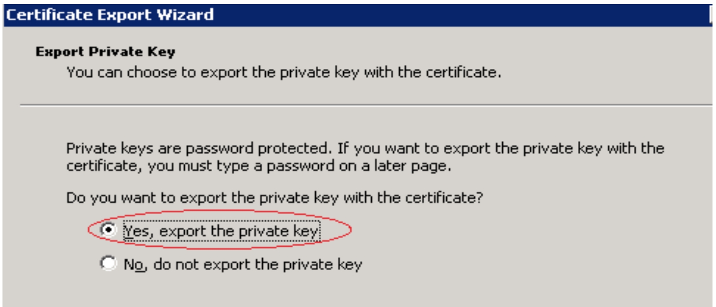
Intended purpose: <All>

Issued To	Issued By	Expiratio...	Friendly Name
3@sy.ca	myca	7/2/2011	<None>
bjia	FEQAROOT	10/30/2009	<None>
fml137.sy.ca	myca	6/14/2011	<None>
fml138	myca	6/14/2011	<None>
fml138.sy.ca	myca	6/14/2011	<None>
Foo Bar	myca	6/15/2011	<None>
Joe Smith	myca	6/15/2011	<None>
John Doe	myca	7/3/2012	<None>
user1@foobar.com	myca	7/4/2012	John Doe

Certificate intended purposes

Client Authentication, Secure Email, Encrypting File System

21. On the certificate export wizard, please remember to export the private key together with the certificate:



Export Private Key

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

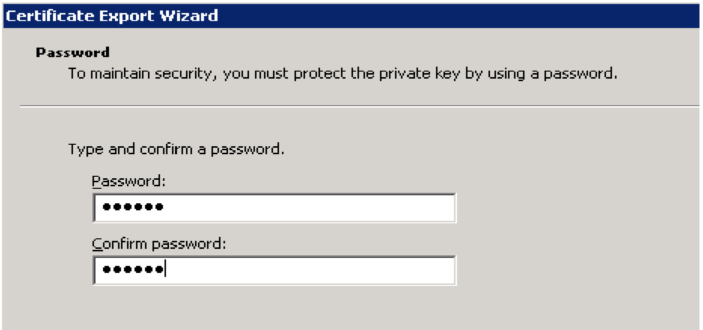
Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

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

● Yes, export the private key

○ No, do not export the private key

22. Configure password to protect the private key and certificate.



Certificate Export Wizard

Password

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

Type and confirm a password.

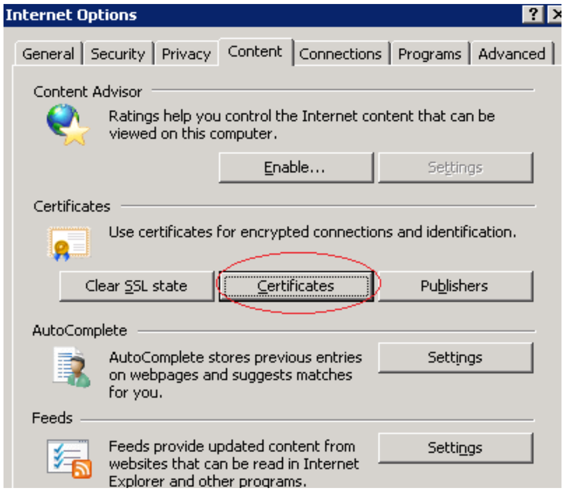
Password: ••••••

Confirm password: ••••••

23. Name the PPCS file, say user1@foobar.com in this document, and click “Finish” to export the certificate and private key.

    Now the user certificate should be transported to end user securely. End user needs to import the certificate/private key into their browser.

24. End user open their browser (IE 8 in this example), select Tools > Internet Options > Content Certificates.



Content Advisor

Ratings help you control the Internet content that can be viewed on this computer.

Certificates

Use certificates for encrypted connections and identification.

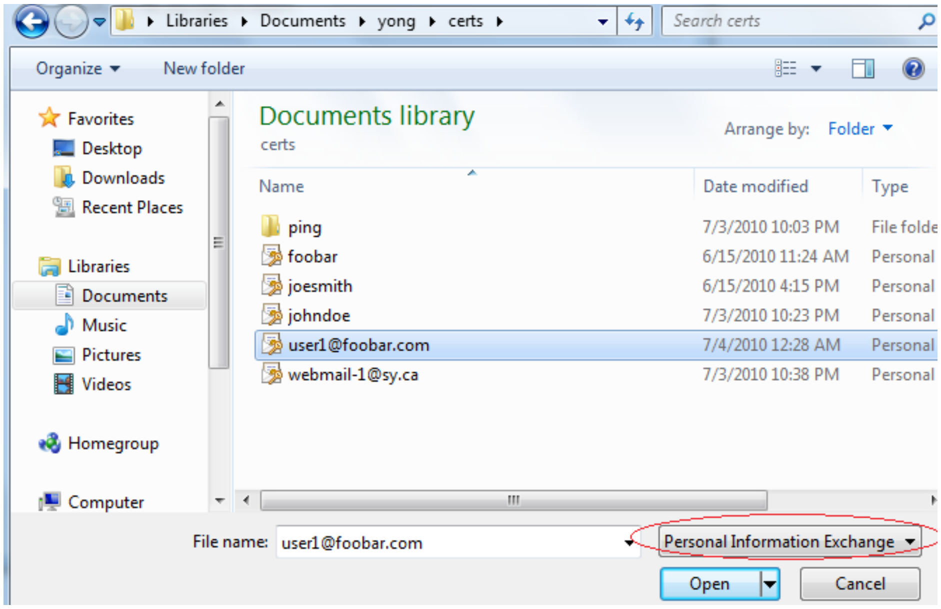
AutoComplete

AutoComplete stores previous entries on webpages and suggests matches for you.

Feeds

Feeds provide updated content from websites that can be read in Internet Explorer and other programs.

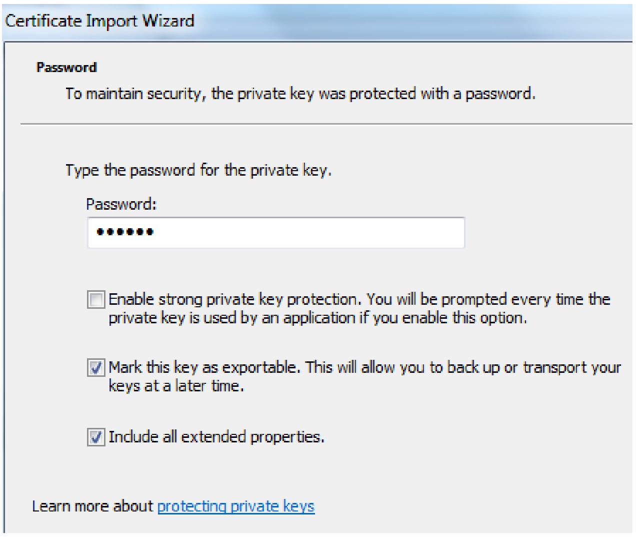
25. Click “Import” on “Personal” tab. Then select user1@foorbar.com.pfx , supply the same password as configured by administrator when exporting this certificate/private key and import the certificate into “Personal” certificate store.



Name	Date modified	Type
ping	7/3/2010 10:03 PM	File folde
foobar	6/15/2010 11:24 AM	Personal
joesmith	6/15/2010 4:15 PM	Personal
johndoe	7/3/2010 10:23 PM	Personal
user1@foobar.com	7/4/2010 12:28 AM	Personal
webmail-1@sy.ca	7/3/2010 10:38 PM	Personal

File name: user1@foobar.com

Personal Information Exchange



Certificate Import Wizard

Password

To maintain security, the private key was protected with a password.

Type the password for the private key.

Password:
••••••

□ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

☑ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

☑ Include all extended properties.

Learn more about protecting private keys

Now the certificate preparation is done. Next step is to configure FortiMail to enable PKI authentication for web mail access. See detailed instructions in the early section of this document.