Keytool and Certificate Management

eMedNy

A guide to utilizing keytool to assist with Certificates for eMedNY SOAP



2/16/2013

TABLE OF CONTENTS

1	Inti	roduction	3
2	Cre	ating a Certificate Signing Request (CSR) and requesting a Certificate	4
	2.1	Create the "KeyStores" Folder & Open the Command Window	4
	2.2	Generate a key pair for your web service client	6
	2.3	Generate a certificate request	7
	2.4	Submit the Certificate Signing Request through ePACES	7
	2.5	Retrieve the Client Certificate from ePACES	8
3	Imp	porting the Certificate	. 10
	3.1	Importing the Client Certificate into the keystore	10
	3.2	Importing the Server Certificate	11
	3.3	Importing certificates using a MMC	12
	3.4	Importing Certifcates Using the IE Certificates Wizard	19
	3.5	Importing the Server Certificate into the Keystore	27
	3.6	Importing private key and certificates from Java to Windows Key Stores	29
4	Ado	ditional Tools and Information	. 34
	4.1	keytool web link	34
	4.2	Requirements for CORE Compliance	34
	4.3	JSSE Reference Guide	34
	4.4	WCF – 2 Way SSL using Certificates	34

1 Introduction

This document is intended to assist providers with the acquisition and use of security certificates when accessing secured eMedNY Web Services (such as the <u>File Transfer Service</u> and the <u>Meds History Service</u>.) It details the processes needed to create a private and public key pair, and an associated Certificate Signing Request (CSR) and how to process the resulting signed certificate delivered in response from eMedNY, as well as how to import any server certificates that may also be required (e.g. MedsHistory Web Service).

The process to enroll as a user of eMedNY-signed certificates, to submit the Certificate Signing Request created as described in this document, and the retrieval of the user's eMedNY-signed certificate are detailed in a separate document <u>eMedNY X509 Certificates Guide</u>.

Please note that the information provided is to be used as a guide only. It will be of greatest interest to developers using Java or Dotnet technologies on Windows platforms. Developers on Linux-variants should be able to adapt the instructions given herein. Developers using key and certificate stores other than those covered in this document will have to adapt the information here to the fit their own situation.

2 Creating a Certificate Signing Request (CSR) and requesting a Certificate

"Keytool" is a key and certificate management utility, which will be used to generate key pairs for your web services client. This utility will need to be installed so that it can be run in any directory. For additional information regarding keytool, see keytool web link in <u>Section 4.1</u>. The following instructions are for Windows-based operating systems. Other operating systems have analogous tools; users should consult the appropriate references or with your IT departments.

eMedNY can provide scripts contained in batch files with these commands. They can be run using instructions contained within these files. Please email <u>emednyproviderservices@gdit.com</u> to request these scripts.

The following instructions are for example purposes only. Words that are in bold are sample text, please use whatever suits the needs of your software in its place.

2.1 Create the "KeyStores" Folder & Open the Command Window

In Windows Explorer you will need to create a new folder for your keytool-related files. In our example, we have called it **KeyStores**:

∞C:\				
File Edit View Favorites To	ools Help			.
🔇 Back 🔹 🜍 🔹 🏂 🍃	🔵 Search 🏾 🌔 F	olders 📴 🍞	X 🍤 💷	
Address 🗢 C:\				🖌 🄁 Go
Name 🔺	Size	Туре	Date Modified	
🚞 app		File Folder	8/7/2007 2:01 AM	
Cocuments and Settings		File Folder	3/5/2009 11:16 PM	
KeyStores		File Folder	5/16/2007 2:47 PM	
Program Files		File Folder	3/18/2009 12:37 PM	~



Next, In Start Menu Click Run:

Type "cmd" and press Enter:

Run	?
	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:	cmd
	OK Cancel Browse

Change directory to the one you created earlier (i.e. Keystores):



2.2 Generate a key pair for your web service client

At the command line, type in the following command, substituting your own data for the text in brackets []. A full explanation of this data appears after the command line:

keytool -genkeypair -v -alias [Client Alias] -keystore [keystore name].jks -keyalg RSA -sigalg SHA1withRSA -storepass [keystore password] -dname "[Client's DN, see below]" -keypass [client password]

Client Alias – An alias set up by the user. It is used to refer to the keystore. A keystore can contain multiple client items, each referenced by its own unique alias.

Keystore Name – The name of the Keystore. A file named [keystore name].jks will be generated.

Keystore Password – A password to access the keystore. We suggest a password should be at least six characters in length and contain at least one number and punctuation mark.

Client's DN – This is information identifying the client. You should populate it with information identifying your organization (using no spaces) as follows: "CN = [Client Name], OU=[Organizational Unit], O=[Organization], L=[City or Locality], S=[State], C=US"

Client Password – The client password to access the private key in this keystore.

This is an example:

keytool -genkeypair -v -alias JDOE -keystore JDOEKeystores.jks -keyalg RSA -sigalg SHA1withRSA -storepass Password1 - dname "CN=JohnDoe,OU=IT,O=JohnDoeInc,L=Anytown,ST=NY,C=US" -keypass Password2

See below for an example:

🐼 C:\WINDOW5\system32\cmd.exe	
C:\>cd keystores C:\>cd keystores alg RSA -sigalg SHA1withRSA -storepass Password1 -dname "CN=JohnDoe,OU=IT,O DoeInc,L=Anytown,ST=NY,C=US" -keypass Password2 Generating 1,024 bit RSA key pair and self-signed certificate (SHA1withRSA) a validity of 90 days for: CN=JohnDoe, OU=IT, O=JohnDoeInc, L=Anytown, ST=NY, C=US [Storing JDOEKeystores.jks]	-key =John with
C:\KeyStores>	
	-

2.3 Generate a certificate request

Type the following command to generate a Certificate Signing Request. Replace the text in brackets with the same data you used to generate the Keystore.

keytool -certreq -alias [Client Alias] -keystore [Keystore Name].jks -file [Client Alias].csr -storepass [Keystore Password] - keypass [Client Password]

See below for an example:

keytool -certreq -alias JDOE -keystore JDOEKeystores.jks -file JDOE.csr -storepass Password1 -keypass Password2

The image follows that example:



This will result in a Certificate Request file (.csr) being placed into the same directory.

2.4 Submit the Certificate Signing Request through ePACES

View the **Keystores** directory in Windows explorer.

🚞 KeyStores					<u>_ </u>		
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u>	ools <u>H</u> elp						
😋 Back 🔹 🕥 🖌 🏂 🔎	🕞 Back 🔹 💮 🖌 🏂 Search 📂 Folders 🛛 🎲 🍞 🗙 🍤 💷 🗸						
Address 🛅 C:\KeyStores					💌 🄁 Go		
Name 🔺	Size Ty	уре	Date Modified				
JDOE.csr	1 KB - C	SR File	12/26/2012 11:57 AM				
🖬 JDOEKeystores.jks	2 KB _ JK	KS File	12/26/2012 11:46 AM				
2 objects 1.94 KB 🕄 My Computer							

As you can see above, there are two files in the directory. The .jks is your keystore file. The .csr is your Certificate Signing Request. Open the .csr file in a text editor, such as NotePad. It should look something like this:

Ď JDOE.csr - Notepad	×I
<u>File E</u> dit F <u>o</u> rmat <u>V</u> iew <u>H</u> elp	
BEGIN NEW CERTIFICATE REQUEST MIIBODCCAQkCAQAWYDELMAKGA1UEBhMCVVMxCzAJBgNVBAgTAk5ZMRAWDgYDVQQHEwdBbn10b3du MRMwEQYDVQQKEwpKb2huRG91SW5jMQswCQYELQQVDwJJVDEQMA4GA1UEAxMHSm9obkRvZTCBnzAN BgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAos6mmhfMJQopfDUqjZqs67gQMh7B15kfGiYkU02tLg83 IyoB2cG9QychiYMjiH1VIv+8+pg9f2eBQU90yMQbfOMqIM1s3dbZAmjKEavutJvGS39joqZIRu0e Zg1NzQdleOEwRa1ZJMuQ8p0ySpRxh/KAwT3uvRdkg2SiSjFCyPMCAwEAAaAAMA0GCSqGSIb3DQEB BQUAA4GBAE+02FXys6sAZ4JtaqnC/A7Wv76+bE82JqM1BPyu/pjoCiQa7ZNM3GvDX9N37EcrGqgh cwSCOULgCw8uJo/q79sz30PVouaycU+Y7Ummb+osAmjaNdFohd7QwcsAywfUrAPfeTDN+U61xvp2 01muT5LKp40LkGgjTZR3yDKynXG4 END NEW CERTIFICATE REQUEST	

Copy this information into the "Certificate Signing Request" Field in ePACES as per the instructions in the <u>eMedNY X509</u> <u>Certificates Guide</u>.

2.5 Retrieve the Client Certificate from ePACES

Retrieve the Client Certificate through ePACES as per the instructions in the <u>eMedNY X509 Certificates Guide</u>. Copy the data there into Notepad and save it in the "Keystores" directory under the name [Client Alias].pem

This is a sample of a Client certificate.

📕 JDOE.pem -	- Notepad			
File Edit For	mat <u>V</u> iew	<u>H</u> elp		
BEGIN MIIGJGYJKO jDCCAVWGAW IZAhBGNVBA MDAWMF0XDT ZW50MQWWCO MREWDWYDVQ ggEBAMTMCX hwZzUtJsr7 TBecsUnSCy /ertEhXYdn P120rV2PEI CX0ChmpXi4 EWYDVR01BA BgNVBA0TBm dHkxDTALBO MS9QS01TZX g1hk4ZSDSQ SIb3DQEBBQ MNIbVX02a SIb3DQEBBQ SIb3DQEBBQ SIb3DQEBBQ SIb3DQEBBQ SIb3DQEBQC ZZCCAdCGAW IZAhBGNVBA MDAWMF0XDT EXPTRGV2IE jQAWGYKCGY VJ0242hX/n VVL1M76ha5 hDCBgTA/Bg ZXJ2ZXIG2m BTADAQH/ME AQUFAA0BGQ SThNBKZE69 BS3X0QnHHC END C	I CERTIF I CERTIF I CERTIF I CERTIF I CENT I CENT	IICAT QCCC ITANE CXY gQCC ITANE CXY gQDA2F WNP IODD	E IIGF2CCBhMCAQEXADALBgkqhkiG9w0BBwGgggX7MIID gkqhkiG9w0BAQUFADA2MQ8wDQYDVQQKEw2lTwVkTlkx 2VydGlmawNhdGUgQXV0aG9yaXR5MB4XDTEXMDkxNTA0 ITK10VowXTEbMBkGA1UEChMSZU1l2E5ZU2FtcGXlQ2Xp TMXDDAKBgNVBASTA09VMjEPMA0GA1UECXMGU2FtcGXl EgwMTCCASIwDqYJKoZIhvcNAQEBBQADggEPADCCAQoC JiV+U0siiHolBAYD8MGu/EusiJ6mN6df0QRTAZJZn5e tqbdEb8zD+CZa7XplxKia9NR+/Tpp4NUT8CPasobSvmt VEB/K8kkJKAD/zu/iz4AI+tyRRy/76sIuQ3c0Trvd1+4 SyR8vrtxieb26Nh8mnGBwGuMfLdFqmV78zePB4Q00Fjs M0XlinvhyCV40NoZgi8fe7toe3Fuc5YSMPkKCQNPAw QUHAWIwgZMGA1UdHwSBi2CBiDBNoEugSaRHMEUXDZAN ICEGA1UECXMabURldiBDZXJ0awZpY2F0ZSBBdXRob3Jp DEwN6A1oDOGMwh0dHA6Ly8yMC4yMC4xNTcUNDU60DA4 HMvQ1JMMS5jcmwHQYDVR00BBYEFB1flfTzukL25Eho wQYMBaAFHe2iaN2dUwyEhC6+qUdm3kwc2xSMA0GCSqG DCqd+BTKG0S1QXYSZFk+qvHZsix08bKTpiDY20k99B IfySvaaXYgedigDEIVGzppUEjw8lAyohrvy2ouAL7hnk A0yoR2BYdoJ9BZ1FM6KSwtyYTUGFmK7Li2BQzneMIIC gkqhkiG9w0BAQUFADA2MQ8wDQYDVQQKEw2lTwVkTlkx 2VydGlmaWhhdGUgQXV0aG9yaXR5MB4XDTA5MDIyNZA1 ITK10VowNjEPMA0GA1UEChMGZU11ZE5ZMSMWIQYDVQL XR1IEF1dGhvcm10eTCBnZANBgkqhkiG9w0BAQEFAA0B rvwtK12vp4NhCdEA9jkX4qkS0jd48rub+0/hRU5NErz YewoG6160M/VBvCB0VgS8r/Dw+0ArY09ZFcnrSBbCUJ ifqz1s01wwZceukH1V9j/yDyJHHivdV3nlsCAwEAAa0B Q0EMhWwR2VuZXJhdGVkIGJ5IHR0ZSBTZWN1cm10eSBT FJBQ0YPMA4GA1UdDwEB/wQEAWIBBjAPBgNVHRMBAF8E BR3tomjdnVMMhIQuvq1HZt5FnNSUJANBgkqhkiG9w0B Wtd3JJ]9byfJ0savF3JHp++yHLqHigaHbAhGwi16R8w kVWFC401Cb8TwmHttbUT51/Yncp3XLdmerU1KfQ3T8v iZ/PS5hDowdsI009M3K+wY2/duigwj2gAENT 	
,	Save As		2	
	Save As	ave in:		
		ave in:		
	Recer Deskte My Docur My Comp My Comp	nt pop ments pouter	IDOE.csr IDOEKeystores.jks File name: JDOE.pem Save as type: All Files Encoding: ANSI	

3 Importing the Certificate

3.1 Importing the Client Certificate into the keystore

Type the following command to import the Client Certificate into your keystore. Replace the text in brackets with the appropriate data – [Cert file name] is the name of the file where you saved the certificate from ePACES. An explanation of the data elements follows the command:

keytool -importcert -v -alias [Client Alias] -file [Cert file Name].pem -keystore [Keystore name].jks -storepass [keystore password] -keypass [client password]

Client Alias – The same Client Alias as above.

Cert File Name – the Name of the desired certificate file. We recommend the same as the Client Alias for tracking purposes.

Keystore Password – A password to access the keystore. We suggest a password should be at least six characters in length and contain at least one number and punctuation mark. This is the same as used for creating the keystore and generating the CSR.

Client Password – The client password to access the private key in this keystore.

This is an example command:

keytool -importcert -v -alias JDOE -file JDOE.pem -keystore JDOEKeystores.jks -storepass Password1 -keypass Password2

The following image follows our example:

```
- 0 ×
Select C:\WINDOWS\system32\cmd.exe
C:\KeyStores>keytool -certreq -alias JDOE -keystore JDOEKeystores.jks -file JDOE
.csr -storepass Password1 -keypass Password2
Top-level certificate in reply:
Owner: OU=rPrd Certificate Authority, O=eMedNY
Issuer: OU=rPrd_Certificate Authority, O=eMedNY
 Serial number: 0
Valid from: Mon May 11 00:00:00 EDT 2009 until: Tue Feb 09 22:59:59 EST 2021
Certificate fingerprints:
MD5: B6:75:E4:87:48:05:7D:19:C8:9C:72:91:51:BA:0B:77
SHA1: 7B:FB:D2:AA:6F:A0:52:E3:76:92:4B:2C:EF:0C:86:CE:A9:81:5E:E1
               Signature algorithm name: SHA1withRSA
               Version: 3
Extensions:
#1: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
Key_CertSign
Cr1_Sign
#2: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
   CA:true
   PathLen:2147483647
#3: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: C1 BA 37 B5 74 45 72 4D 30 37 98 3
0010: EC 55 1E 74
                                                                                              ..7.tErM07.6....
                                                    30 37 98 36 0C F4 BE FF
#4: ObjectId: 2.16.840.1.113730.1.13 Criticality=false
... is not trusted. Install reply anyway? [no]:
Certificate reply was installed in keystore
[Storing JDOE.jks]
                                                                                 yes
```

The reason the certificate is indicated as "not trusted" as the certificate returned by eMedNY is a chain consisting of the user's cert as well as the Certificate Administrator Signer Cert (rPrd Certificate Authority.) It is the latter certificate that is "not trusted." You can also import only the eMedNY client cert without the CA signer cert if you first import the returned chain into Internet Explorer and then re-export just the eMedNY client cert from the browser. If you need to do this for your software, see the instructions under Importing Certificates using the IE Certificates Wizard.

3.2 Importing the Server Certificate

For Java based web service clients, doing message level security (e.g. Meds History Service - MHS,) the Server certificate needs to be imported into this keystore or in a separate keystore. We will do it in this keystore.

The Server certificate can be obtained from eMedNY – please email <u>emednyproviderservices@gdit.com</u> if you need this certificate. For this demo, it will be downloaded to:

C:\Keystores\dev_server.pem

And imported using KeyToolIUI via Import > Keystore's entry > Trusted Certificate > Regular Certificate

However, this will fail. This is because the eMedNY cert contains a certificate chain (server cert + CA cert) and a jks keystore will not allow one to import a cert as a trusted cert if it contains a chain. We will need the server certificate without a chain (i.e remove the CA cert.) Note we could import the client cert **jsmith.cer** because the keystore contains its private key and we imported into an existing entry and replaced the self-signed cert in it with the **jsmith** cert + CA cert. However as we do not have the server's private key we cannot do the same. (Other alternatives are also possible such as creating a pkcs12 keystore, or obtain the signer certificate and importing it as a trusted cert. However the process given in this document will be applicable to both Java and Dotnet developers on Windows platforms.)

The way around this is to first import the eMedNY Server certificates (servercert + cacert) into the Windows Certificate Store. Then export only the servercert from the Windows Certificate Store and then import the servercert into the keystore as a trusted cert.

There are two ways of doing this, the first giving a more detailed view into the Windows Certificate Store, while the second is less granular but simpler to use.

- Using a Microsoft Mangement Console (mmc) for the Windows Certificate Stores
- Using the Internet Explorer Certificates Wizard.

3.3 Importing certificates using a MMC.

First create a Microsoft Management Console (mmc) for the Certificate Store by doing the following:

3.3.1 From the Windows task bar, Start > Run > mmc



3.3.2 File > Add/Remove Snap-in

🚡 Console 1 📃 📃					
File Action View Favorites Window	Help				
New Ctrl+	N				
Open Ctrl+	0				
Save Ctrl+					
Save As					
Add/Remove Snap-in Ctrl+	Mere are no items to show in this view.				
Options					
1 C:\WINDOWS\\compmgmt.msc					
2 C:\WINDOW5\System32\gpedit.msc					
Exit					
Enables you to add snap-ins to or remove them	from the sr				

3.3.3 Click "Add ... "

Add/Remove Snap-in	? X
Standalone Extensions	
Use this page to add or remove a stand-alone snap-in from the console	
Snap-ins added to:	
Description	
Add Remove About	
OK Ca	ncel

3.3.4 In the "Add Standalone Snap-in", select "Certificates" and Click "Add"

Add Standalone Snap-in		? ×
Available standalone snap-ins:		
Snap-in	Vendor	
and the second s	Microsoft Corporation	
Active Directory Domains and Trusts	Microsoft Corporation	
Contractive Directory Schema	Microsoft Corporation	
Active Directory Sites and Services	Microsoft Corporation	_
Active Directory Users and Compu	Microsoft Corporation	
al ActiveX Control	Microsoft Corporation	
Certificates	Microsoft Corporation	
Component Services	Microsoft Corporation	
Computer Management	Microsoft Corporation	
Bevice Manager	Microsoft Corporation	-
Description The Certificates snap-in allows you to bro certificate stores for yourself, a service,	owse the contents of the or a computer.	
[Add Clos	e

3.3.5 Select "Computer account", then click "Next"

ertificates snap-in	
This map in will always manage certificates for	
O My user account	
O Service account	
Computer account	
	(lack Next) Cancel
	Carce

3.3.6 Select "Local computer (the computer this console is running on)", and click Finish

* *1-4		
Add/Remove Snap-in	? 🗙	
Standalone Extensions		
Use this page to add or remove a stand-alone snap-in from the conso	e.	
Shap-ins added to:	Add Standalone Soon in 2 V	
	Select Computer	
	Calast the encounter you want this many in to many and	
	This even in will always and this shappin to manage.	
	(ris snaphr will always manage.	
	Cocal computer: (the computer this console is running on)	is to show in this view.
	Another computer: Browse	
	Allow the selected computer to be changed when launching from the command line. This	
Description	only applies if you save the console.	
Add Remove About		
ОК С	a	
	1	
	< Back Finish Cance	

3.3.7 Note that the "Certificates (Local Computer)" has been added to the "Add/Remove Snap-in"

* ^!-+			
Add/Remove Snap-in	2×		
Standalone Extensions			
Use this page to add or remove a stand-alone snap-in from the console			
Snap-ins added to: 🚔 Console Root 🗸 🗸	Add Standalone Snan-in	20	า
	Had Standarone Shap in		
Certificates (Local Computer)	Available standalone snap-ins:		
	Snap-in	Vendor	
	INET Framework 1.1 Configuration Month Stramework 2.0 Configuration	Microsoft Corporation	
	ActiveX Control	Microsoft Corporation	There are as Barry to show in this size.
	Certificates	Microsoft Corporation	There are no items to show in this view.
	Component Services	Microsoft Corporation	
	Computer Management	Microsoft Corporation Microsoft Corporation	
Description	Bisk Defragmenter	Microsoft Corp, Execut	
	🛱 Disk Management	Microsoft and VERITAS	
	Event Viewer	Microsoft Corporation	
	Description		
Add Remove About	The Certificates snap-in allows you to b certificate stores for yourself, a service	owse the contents of the	
		for a compatorr	
		Add Close	

Close the "Add Standalone Snap in".

3.3.8 In the "Add/Remove Snap-in" click on the "Add.." again and repeat steps 3.3.4 and 3.3.5, but this time for step 3.3.5 select the "My user account".

Mentere Seap In	2 🔀					
ndalone Elibanaiona						
se this page to add or remove a stand-alone snap-in fro	to the console.					
and any other than 100 million of the				-		
Console Root	Add Standalone Snap-in		R	8		
Certificates (Local Computer)	Available standalone snap-ins:					
Certificates - Current User	Snap-in	Vendor		^		
	IS NET Pranetwork 1.1. Configuration	Microsoft Cor Microsoft Cor	poration			
	Computer Management	Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor	poration poration poration poration		There are no terms to show in this view.	
Description	Club, Defragtienter	Microsoft Cor	p, Execut			
	BCkk Management	Nicrosoft and	VERITAS			
	ESCARK Newer	Micresoft Cor	poration	M		
Add	The Certificates snap-in allows you to b certificate stores for yourself, a service	owse the contre , or a computer	nts of the			
		Add	Oter			_
	1			_		

Then Close the "Add Standalone Snap-in"

* Cl-4				
Add/Remove Snap-in 🛛 ? 🔀				
Standalone Extensions				
Use this page to add or remove a stand-alone span-ip from the console				
ose dils page to ada di remove a scand-adone snap-in nom die console.				
Snap-ins added to: 🔄 Console Root				
Certificates (Local Computer)				
Certificates - Current User	The Console Root			
	Console Root	Name		
		Manic		
			There are no items to show in this view.	
Description				
Add Remove About				

Note that "Certificates - Current User" has also been added to the "Add/Remove Snap-in"

Click on the OK button

3.3.8 Save the mmc console



For example, in the Keystores folder as "MyWindowsCertStore"



3.4 Importing Certificates Using the IE Certificates Wizard

Open Internet Explorer go to the Tools > Internet Options menu



Go to the Contents tab and click on the Certificates button

nternet Optio	ns				? ×
General Sec	urity Privacy	Content	Connections	Programs	Advanced
Content Adv	isor atings help you iewed on this co	i control the omputer.	Internet cor	ntent that ca Settin	n be gs
Certificates					
, L	lse certificates f	for encrypte	d connectior	ns and identif	ication.
Clear	<u>S</u> SL state	⊆ertifi	ates	Pu <u>b</u> lish	ers
AutoComplet	e utoComplete st n webpages an or you,	ores previou d suggests r	us entries natches	Settin	gs
Feeds Fe	eeds provide up vebsites that ca xplorer and oth	odated conto n be read in er programs	ent from Internet	Setti <u>n</u>	gs
				'apresi 1	česku
		OK			Anna.

Certificates				? ×
Intended purpose:				•
Personal Other People In	termediate Certification Au	ithorities 🗍 Tru:	sted Root Certification	Þ
Issued To	Issued By	Expiratio	Friendly Name	-
Import Export	<u>R</u> emove		<u>A</u> dvanced	i
Certificate intended purpose	s			
			⊻jew	
			⊆lose	

Click on Import...

Certificate Import Wizard		x
	Welcome to the Certificate Import Wizard	
	This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.	
	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.	
	< Back Cancel	

Click the Next button

Navigate to the **dev_server.pem** file which you downloaded from eMedNY

Certificate Import Wizard	×
File to Import	
Specify the file you want to import.	
	-
<u>F</u> ile name:	
C:\KeyStores\dev_server.pem	
The second se	
Note: More than one certificate can be stored in a single file in the following formats:	
Personal Information Exchange- PKCS #12 (.PFX).P12)	
Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)	
Microsoft Serialized Certificate Store (.SST)	
	-
< <u>B</u> ack <u>N</u> ext > Cancel	

Click Next

Notice it says Personal store. Click on Browse, select the "Other People" store. (Note: you can also put it in the "Personal" store, but as it is a server certificate, it might be more appropriate to put it in the "Other People" store and leave the "Personal" store for your own certificates. Also note that these are put into what is known as the "Certificates – Current User" stores. There is also a "Certificates (Local Computer)" stores which can also be used.)

And click OK

Certificate Import Wizard Certificate Store Certificate stores are system	m areas where certificates are kept.	×
Windows can automatically	Select Certificate Store ? X Select the certificate store you want to use.	
 Place all certificates i Certificate store: Personal 	Untrusted Certificates Third-Party Root Certification Authorities Trusted People Other People McAfee Trust Show physical stores	
	OKCancel	

Ce	rtificate Import Wizard	×
	Certificate Store	
	Certificate stores are system areas where certificates are kept.	
	Windows can automatically select a certificate store, or you can specify a location for	
	$\mathbb C$ Automatically select the certificate store based on the type of certificate	
	Place all certificates in the following store	
	Certificate store:	
	Other People Browse	
	< <u>B</u> ack <u>N</u> ext > Cancel	

Click Next

Certificate Import Wizard		×
	Completing the Certificate Import Wizard You have successfully completed the Certificate Import wizard.	
	You have specified the following settings: Certificate Store Selected by User Other People Content PKCS #7 Certificates File Name U:\KeyToolDemo\dev	
	< Back Finish Cancel	

Click Finish. Note the import was successful and click OK.

Click on "Other People" tab. The **DPMedsHistory** (which is the name of servercert) issued by "**rPrd Certificate Authority**" (the eMedNY CA) is now in the Windows Certificate Store. Note also that the CA cert in the chain, **rPrd Certificate Authority** is also imported. Click on the **DPMedsHistory** entry to select it. The Export button is now enabled.

Certificates				? ×
Intended purpose: <a>	,			•
Personal Other People Ir	ntermediate Certification Au	ithorities Tru	sted Root Certifica	tior 🔸 🕨
Issued To	Issued By	Expiratio	Friendly Name	
DPMedsHistory	rPrd Certificate Autho	8/19/2013	<none></none>	
Prd Certificate Aut	rPrd Certificate Autho	2/9/2021	<none></none>	
Import Export	Remove		Adv	anced
Server Authentication, Clien	es Authentication		<u>V</u> ie	8W
			9	Close

Click on the Export... button, and then Next

Certificate Export Wizard		×
	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.	
		_
	< <u>B</u> ack <u>Next</u> > Cancel	

And select the base-64 encoded X.509 radio button,

Certificate Export Wizard	×
Export File Format Certificates can be exported in a variety of file formats.	
Select the format you want to use:	
C DER encoded binary X.509 (.CER)	
Base-64 encoded X.509 (.CER)	
C gryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B) Include all certificates in the certification path if possible	
 Personal Information Exchange - PKC5 #12 (.PFX) Indude all certificates in the certification path if possible 	
Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)	
\square Delete the private <u>key</u> if the export is successful	
< <u>B</u> ack <u>N</u> ext > Cancel	

Click Next

Navigate to the folder you created for your keystores (in our example "Kestores") folder and give the exported file a name (for example "**server**" here) with extension ".cer" and Save it.

Save As					<u>?</u> ×
Save jn:	C KeyStores		•	G 🦻 🖻	 •
) Recent					
Desktop					
My Documents					
My Computer					
i					
My Network Places	File <u>n</u> ame:	Sever			<u>s</u> ave
	Save as <u>type</u> :	Base64 Encoded X.50	09 (*.cer)	•	Cancel

Ce	ertificate Export Wizard	x
	File to Export Specify the name of the file you want to export	
-	File name:	
	< <u>B</u> ack <u>N</u> ext > Cancel	

Click Next

Cast Casta Francis III and		Y
Certificate Export Wizard	Completing the Certificate E Wizard You have successfully completed the Certificate wizard. You have specified the following settings: File Name Export Keys Include all certificates in the certification path File Format	Export U:\Key No Base64
	< Back Finish	Cancel

Note that the Keys (i.e private keys if any) are not exported and that all certificates in the certification path are not included (i.e. the CA cert is not included,) which is what we wanted from this digression using the Windows Certificate Store tool.

Click Finish and note that the export was successful

CSC: BUSINESS SOLUTIONS, TECHNOLOGY AND OUTSOURCING - Windows Internet Explorer	
() ▼ ■ http://www.csc.com/	S ← × P Web Search
File Edit View Favorites Tools Help	
X Google Vig Search + V More >>	🔵 ykeenlee 🛪 🔧 🔻
\$ \$	
CSC: BUSINESS SOLUTIONS, TECHNOLOGY AND OUT	🏠 • 🖻 - 🖃 🖶 • 🕞• 📎• 🎽
Internet Options RAL LEADER IN PROVIDING TECHNOLOGY Search csc.com	SEARCH ADVANCED
Contification	
Certificate Export Wizard About Us Services Case Studies Insights Cont	tact Us Careers
Completing the Certificate Export Wizard You have successfully completed the Certificate Export wizard. You have specified the following settings:	rev 1 2 3 4 5 next- LET'S GET STARTED
Cancel Ith the public and private sectors, for the benefit of every clipter of the sector is the benefit of every clipter of the sector is	ient.
OK Cancel Apply Natural Resources Oil & Gas P&C - General Insurance Travel & Tr Tr Travel & Tr Tr Tr<th>& Consumer </th>	& Consumer
Google News CSC Acquires IT testing firm Web CSC Acquires IT testing firm (5) A CSC Acquires IT testing firm (5) A Communications Supply Corporation	× Options

Click OK



Click Close and then OK.

So now we have the "server.cer" exported into the KeyToolDemo folder

3.5 Importing the Server Certificate into the Keystore

We can now proceed to import the server certificate into the keystore.

Open the command prompt and navigate to the folder you created for your Keystore. In our example, we named it "Keystores."

Type the following command line:

keytool -importcert -v -alias [Server Cert Alias] -file [Cert file Name].pem -keystore [Keystore name].jks -storepass [keystore password] -keypass [client password]

The following is a sample command:

keytool -importcert -v -alias Server -file Server.cer -keystore JDOEKeystores.jks -storepass Password1 -keypass Password2

This image follows the sample:

_ 🗆 × 🔤 C:\WINDOWS\system32\cmd.exe C:\KeyStores>keytool -importcert -v -alias JDOE -file JDOE.pem -keystore JDOEKey stores.jks -storepass Password1 -keypass Password2 keytool error: java.lang.Exception: Certificate reply does not contain public ke y for <JDOE> java.lang.Exception: Certificate reply does not contain public key for 〈JDOE〉 at sun.security.tools.KeyTool.validateReply(Unknown Source〉 at sun.security.tools.KeyTool.installReply(Unknown Source〉 at sun.security.tools.KeyTool.doCommands(Unknown Source〉 at sun.security.tools.KeyTool.run(Unknown Source〉 at sun.security.tools.KeyTool.run(Unknown Source〉 at sun.security.tools.KeyTool.main(Unknown Source〉 C:\KeyStores>keytool -importcert -v -alias Server -file Server.cer -keystore JDO EKeystores.jks -storepass Password1 -keypass Password2 Owner: CN=DPMedsHistory, OU=eServers, OU=ePaces, OU=eMedNY-PROD, O=eMedNY Issuer: OU=rPrd Certificate Authority, O=eMedNY Issuer: OU=rPrd Certificate Huthority, U=eMedNY Serial number: f Valid from: Tue Feb 16 00:00:00 EST 2010 until: Mon Aug 19 23:59:59 EDT 2013 Certificate fingerprints: MD5: 05:52:94:C1:75:3C:A1:68:BB:48:D8:BD:08:F1:AF:E2 SHA1: C7:B7:ED:92:61:AB:63:31:D2:AC:71:2F:A8:55:D3:60:F4:A9:BD:6D Signature algorithm name: SHA1withRSA Version: 3 Extensions: #1: ObjectId: 2.5.29.15 Criticality=true KeyUsage [DigitalSignature Non_repudiation Key_Encipherment Data_Encipherment #2: ObjectId: 2.5.29.14 Criticality=false SubjectKeyIdentifier [KeyIdentifier [0000: B3 AD 22 1E 93 1C FC 9C F6 17 89 0 0010: 5B 59 72 8D F6 17 89 6D FE 51 E7 2D "....m.Q.-[Ÿr #3: ObjectId: 2.5.29.31 Criticality=false CRLDistributionPoints [[DistributionPoint: [CN=CRL1, OU=rPrd Certificate Authority, O=eMedNY] , DistributionPoint: [URIName: http://www.emedny.org/ePaces/cacerts/CRL1.crl]]] #4: ObjectId: 2.5.29.37 Criticality=false ExtendedKeyUsages [serverAuth clientAuth 1 #5: ObjectId: 2.5.29.35 Criticality=false AuthorityKeyIdentifier [KeyIdentifier [0000: C1 BA 37 B5 74 45 72 4D 30 37 98 36 0C F4 BE FF 0010: EC 55 1E 74 ..7.tErM07.6.... Trust this certificate? [no]: yes Gertificate was added to keystore [Storing JDOEKeystores.jks] C:\KeyStores>_

3.6 Importing private key and certificates from Java to Windows Key Stores

If you have a Dotnet application, you will not be able to use the java **JDOEKeystores**.jks so you will have to export the private key and cert of **JDOE** into the Windows Certificate Store. You have already imported the server certificate into that store.

The procedure for doing the **JDOE.pem** is similar.

Open your IE browser, From the menu, go to Tools > Internet options > Content tab and click on Certificates button.

Images Videos Maps News Shopping Grail more + Web Intrages Videos Maps News Shopping Grail more +	
File Edit. View Favorites Toda Help X Coogle Image: Videos	
x Coogle viewenee vieweenee viewenee v	
 ★ ★ ★ Societ 	enlee • 🔌 •
S Google S Videos Maps News Shopping Gmail more - ykeenlee@gmail.com - 4	
Web Images Videos Maps News Shopping Gmail more - ykeenlee@gmail.com -	• 🔊 • »
	m- 🗱 🖄
General Security Privacy Content Connections Programs Advanced Content Advisor Ratings hely you control the Internet content that can be viewed on this computer. Enable Settings Certificates Certificates for encrypted connections and identification. Clear SSL state Certificates Publishers AutoComplete AutoComplete	
an webpages matches or webpages matches or webpages and web Sites Feeds and Web Sites for decided and web Sites	10
🚱 Internet 🌾 👻 🕄 100%	100% •

🕖 Google - Windows Internet Explorer			
Solo v State://www.google.com/		• ا	🕨 🗶 Web Search
File Edit View Favorites Tools Help			
× Google	Search 🔹 🖉 M 🔹	More >>	🔵 ykeenlee 🔻 🔧 🔻
🚖 🚖			
Google			🏠 • 🔝 - 🖃 🖶 • 🗗 • 🖉 • 🏾
Web Images Videos Maps News Shopp	ping Gmail more -		ykeenlee@gmail.com - 🔅 🎴
2	ſ	nternet Options	
	1	Certificates ?X	
		Personal Other Dende Intermediate Cartification Authorities Tructed Doct Cartification	
		Other People Internediate Certification Automities Indiced Root Certification	
		Issued To Issued By Expiratio Friendly Name	
		20.20.159.144 20.20.159.144 7/14/2023 default	
		20.20.159.148 20.20.159.148 7/13/2023 default	
		alice myca 9/20/2008 alice	
		Chuck Dennis Chuck Dennis 4/27/2021 LIPIX	
		DO_NOT_TRUST_Fi DO_NOT_TRUST_Fidd 12/31/2039 <none></none>	
		extended-validatio DO_NOT_TRUST_Fidd 7/26/2021 <none></none>	
		Import Export Remove Advanced	
		Certificate intended purposes	
		View	
		Close	
	Ļ		
		OK Cancel Apply	
Advertising Programs Business Solu	itions About Google	Privacy	Change background image
			😜 Internet 🦓 👻 🔍 100% 💌 🚲

Click Import..., Next and select your JDOE.pem file that was returned with your csr request.

🟉 Google - Windows Internet Explorer		
Core I http://www.google.com/	v (47	X P Web Search
File Edit View Favorites Tools Help		
× Google v Search • · · ⊘ M •	More >>	🔵 ykeenlee 🔹 🔧 🔹
🚖 🍰		
Google		
Web Images Videos Maps News Shopping Gmail more -		ykeenlee@gmail.com - 🗱 🤗
	nternet Options	
Advertising Programs Business Solutions About Google	Certificate Import Wizard File to Import Specify the file you want to import. File name: Cit/KeyTooDDemoljsmith_cer.pem Note: More than one certificate can be stored in a single file in the following formats: Personal Information Exchange - PKCS #12 (.PFX, P12) Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P78) Microsoft Serialized Certificate Store (.SST) Close Ck Cancel Apply Privacy	Change background image
		🍚 Internet 🛛 🦓 🕶 🍕 100% 💌 🔬

Click Next

🔗 Google - Windows Internet Explorer		
🕞 😔 🗸 http://www.google.com/	V (+)	× P Web Search
File Edit View Favorites Tools Help		
x Google v 🔮 Search * · · Ø M	r More »	🔵 ykeenlee 🔹 🔧 🔹
* 🚖		
Google		🏠 • 🔊 - 🗆 🖶 • 📴 • 🔗 • 🏾 👋
Web Images Videos Maps News Shopping Gmail more -		ykeenlee@gmail.com - 🔅 🗠
	Internet Options	
	Certificate Import Wizard Certificate Import Wizard Certificate Store Certificate stores are system areas where certificates are kept. Windows can automatically select the certificate store, or you can specify a location for Automatically select the certificate store based on the type of certificate Place all certificates in the following store Certificate store: Personal Rowse Close OK Cancel OK Cancel	
Advertising Programs Business Solutions About Google	e Privacy	Change background image
		Internet 4 + € 100% +



And place the certifcate in the "Personal" store. Click Next

And Finish

C	Google - Windows Internet Explorer		- a 🛛
0	💽 🗢 🔀 http://www.google.com/		P web Search
Fi	e Edit View Favorites Tools Help		
×	Google Search • • Ø M •	More >>	🔵 ykeenlee 🔹 🔧 🔹
*	h		
	Google		🏠 • 🔊 · 🖃 🖶 • 📴 • 🔗 • 🏾 *
	Web Images Videos Maps News Shopping Gmail more -		ykeenlee@gmail.com 🗸 🔅 ≙
»		Internet Options	
Ģ		Certificates ?X	
		Rescond Other Decks Telementicle Contribution Authorities Transfer Deck Contribution (
		rosonal Other People Internetiate Certification Authonoles Trusted Root Certification	
		Issued To Issued By Expiratio Friendly Name	
		2020.20.159.144 Certificate Import Wizard 2023 default	
		20.20.159.148 1023 default 2024 2028 202 20 202 20	
		Malice 2008 alice	
		Coci Lipin Coci Coci Lipin Coci Coci Coci Coci Coci Coci Coci Coci	
		Content Co	
		Import Export Remove Advanced	
		Certificate intended purposes	
		View	
		Liose	
		OK Cancel Apply	
1111	Advertising Programs Business Solutions About Google	Privacy	Change background image
_			🕒 Internet 🌇 🔹 🔍 100% 🔹 🚲

You will need to create a mmc certificates to view cert for **JDOE** imported into CurrentUser/Personal/Certificates. The Windows Cert Store only shows CurrentComputer stores.

n WS-SecurityTutorialCertificates - [Console Root\Certificates - Current UserPersonal\Certificates]							
🚡 File Action View Favorites Window He	lp.						_ 8 ×
← → 🗈 🖬 🐰 🖿 🔀 🔗 🛙	N I						
Console Root	Issued To 🛛	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Tem.
😑 🗐 Certificates - Current User	172.27.155.83	DO_NOT_TRUST_FiddlerRoot	8/12/2021	Server Authentication	<none></none>		
😑 🔜 Personal	20.20.159.144	20.20.159.144	7/14/2023	<all></all>	default		
Certificates	20.20.159.148	20.20.159.148	7/13/2023	<all></all>	default		
Trusted Root Certification Authorities	ACOKE	mSit Certificate Authority	1/27/2011	Client Authentication	CN=ACOKE,OU=ePa		
Enterprise Trust	🔛 alice	myca	9/20/2008	<all></all>	alice		
Active Directory Lloss Object	🖼 Chuck Dennis	Chuck Dennis	4/27/2021	<all></all>	LIPIX		
Active Directory Oser Object	🔤 clients4.google.com	DO_NOT_TRUST_FiddlerRoot	7/26/2021	Server Authentication	<none></none>		
Induced Publishers	BO_NOT_TRUST_FiddlerRoot	DO_NOT_TRUST_FiddlerRoot	12/31/2039	Server Authentication	<none></none>		
Dird-Party Root Certification Authorities	DP101deva	mDev Certificate Authority	1/10/2013	Server Authenticatio	<none></none>		
Trusted People	extended-validation-ssl.verisign.com	DO_NOT_TRUST_FiddlerRoot	7/26/2021	Server Authentication	<none></none>		
🗉 🧰 Other People	🔛 jclient	jclient	10/13/2021	<all></all>	dummyclientsigner		
🛓 🧰 McAfee Trust	iserver 1	jserver	10/13/2021	<all></all>	dummyserversigner		
😨 🧰 Certificate Enrollment Requests	ISMITH01	mDev Certificate Authority	3/17/2012	Client Authentication	<none></none>		
😠 🧰 SPC	Keen Lee	rPrd Certificate Authority	12/7/2009	Client Authentication	CN=Keen Lee,OU=e		
🖮 🐻 Certificates (Local Computer)	🔤 login.live.com	DO_NOT_TRUST_FiddlerRoot	7/26/2021	Server Authentication	<none></none>		
😑 🧰 Personal	MADAMS	mSit Certificate Authority	7/22/2010	Client Authentication	CN=MADAMS,OU=e		
Certificates	🔤 mail.google.com	DO_NOT_TRUST_FiddlerRoot	12/31/2039	Server Authentication	<none></none>		
Trusted Root Certification Authorities	mDev Certificate Authority	mDev Certificate Authority	2/10/2021	<all></all>	OU=mDev Certificat		
Enterprise Trust	Sit Certificate Authority	mSit Certificate Authority	2/10/2021	<all></all>	OU=mSit Certificate		
Intermediate Certification Authorities	🔤 msit1a05	mSit Certificate Authority	10/22/2009	Client Authentication	<none></none>		
Invisted Publishers	prodClient1	rPrd Certificate Authority	2/27/2013	Client Authentication	prodClient1		
Third-Party Post Certification Authorities	2 RFINELLI	mSit Certificate Authority	7/23/2010	Client Authentication	CN=RFINELLI,OU=e		
Tructed People	ROSENTHA	mDev Certificate Authority	7/16/2013	Client Authentication	<none></none>		
Other People	rPrd Certificate Authority	rPrd Certificate Authority	2/9/2021	<all></all>	<none></none>		
Certificates	secure.shared.live.com	DO_NOT_TRUST_FiddlerRoot	7/26/2021	Server Authentication	<none></none>		
H McAfee Trust	WSE2QuickStartClient	Root Agency	12/31/2039	<all></all>	<none></none>		
Certificate Enrollment Requests	www.emedny.org	DO_NOT_TRUST_FiddlerRoot	8/12/2021	Server Authentication	<none></none>		
🗄 🧰 SPC	www.emedny.org	VeriSign Class 3 International Server CA - G3	5/3/2012	2.16.840.1.113730	<none></none>		
	www.google.com	DO_NOT_TRUST_FiddlerRoot	12/31/2039	Server Authentication	<none></none>		
	zinx1p01.emedlvp1.csc.com	zin×1p01.emedivp1.csc.com	7/17/2008	<all></all>	<none></none>		
	zinx1p01.emedlvp1.csc.com	zlnx1p01.emedlvp1.csc.com	6/14/2009	<a >	<none></none>		
	zinx1p02.emedlvp1.csc.com	zin×1p02.emedlvp1.csc.com	7/24/2008	<all></all>	cdx_zlnx1p02_cert		
			100			_	>
Personal store contains 32 certificates.							

4 Additional Tools and Information

4.1 keytool web link

http://java.sun.com/j2se/1.3/docs/tooldocs/win32/keytool.html

4.2 Requirements for CORE Compliance

http://www.caqh.org/benefits.php

4.3 JSSE Reference Guide

http://docs.oracle.com/javase/6/docs/technotes/guides/security/jsse/JSSERefGuide.html#SSLOverview

4.4 WCF – 2 Way SSL using Certificates

http://blogs.msdn.com/b/imayak/archive/2008/09/12/wcf-2-way-ssl-security-using-certificates.aspx

eMedNY neither endorses nor recommends any of the tools linked or referenced in this document. The intent here is strictly informational.



eMedNY is the name of the electronic New York State Medicaid system. The eMedNY system allows New York Medicaid providers to submit claims and receive payments for Medicaid-covered services provided to eligible clients.

eMedNY offers several innovative technical and architectural features, facilitating the adjudication and payment of claims and providing extensive support and convenience for its users.

The information contained within this document was created in concert by eMedNY and DOH. More information about eMedNY can be found at <u>www.emedny.org</u>.