User Manual

Digital Signature Certificate (DSC)

Contents

1. Introduction

SEZ Online system enables users (SEZ units/ Developers/ Co developers) to submit their various applications, customs transactions & compliance reports to DC's office in electronic form. As these applications and transactions consists of critical and confidential information, the system requires all the unit users to submit / DC users to process these applications/transactions after signing them with Digital Signature Certificate (DSC) for security reasons.

These electronic requests are processed and approved by the DC's office online.

A **Digital Signature Certificate**, like hand written signature, establishes the identity of the user filing the documents through internet which user can not revoke or deny. A **Digital Signature Certificate is not only a digital equivalent of a hand written signature** it adds extra data electronically to any message or a document where it is used to make it more authentic and more secured. Digital Signature ensures that no tampering of data is done once the document has been digitally signed. A DSC is normally valid for 1 or 2 years, after which renewal is required.

There are basically 3 types of Digital Signature Certificates Class-1, Class-2 & Class-3 each having different level of security.

Class 1: These certificates do not hold any legal validity as the validation process is based only on a valid e-mail ID and involves no direct verification.

Class 2: Here, the identity of a person is verified against a trusted, pre-verified database.

Class 3: This is the highest level where the person needs to present himself or herself in front of a Registration Authority (RA) and prove his/ her identity.

The DSCs are typically issued with one year validity and two year validity. These are renewable on expiry of the period of initial issue.

2. Procurement of DSC

DSC may be procured from any of the following certifying Authorities (CA).

I. Tata Consultancy Services (www.tcs-ca.tcs.co.in)
II. IDRBT Certifying Authority (www.idrbtca.org.in)
III. MTNL (www.mtnltrustline.com)
IV. Safescript (www.safescrypt.com)
V. Customs and Central Excise [iCERT] (http://icert.gov.in)
VI. (n)code (www.ncodesolutions.com)
VII. eMudhra (www.e-Mudhra.com)
VIII. National Informatics Center [NIC] (http://nicca.nic.in)

The detailed procedure that is required to be followed for procuring a DSC from any of the above mentioned CA can be obtained from their website. For procurement, a duly filled application form needs to be submitted to the CA along with the necessary supporting documents and relevant charges. The CA issues DCS if, after verification of the application form and supporting documents ever thing is found to be in order

SEZ Online system is compatible with **Class 2 and Class 3** levels of Digital Signature Certificates issued by above listed Certifying Authority.

Users like Unit Approver or CHA should have DSC to process the requests.

CHA can have only one DSC for all his registered units

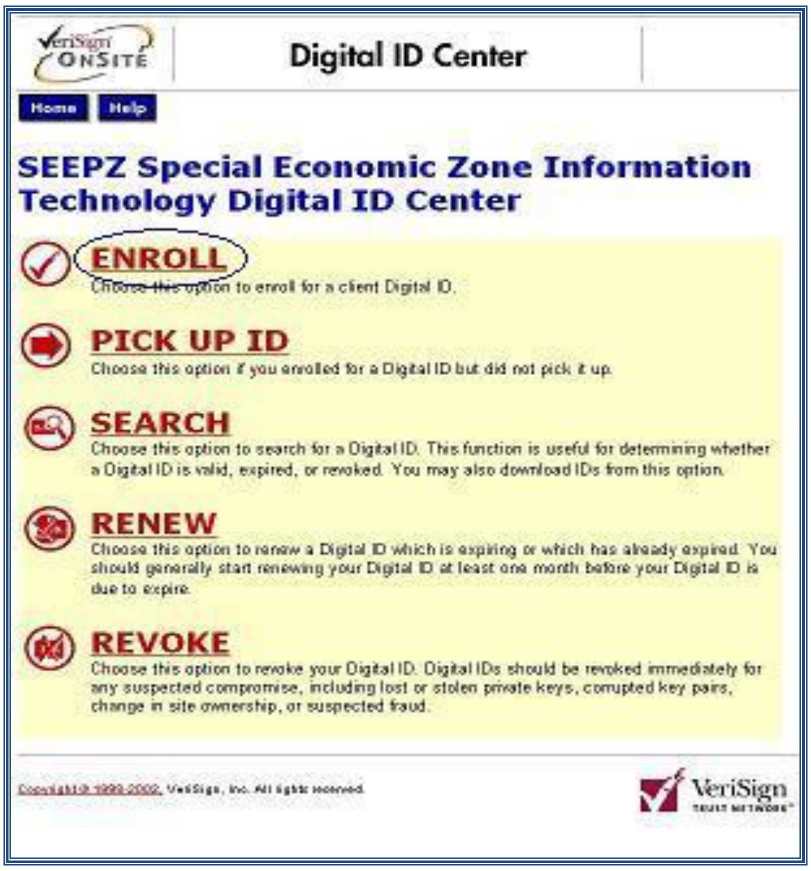
3. Installation of DSC

DSC installation varies according to the Certifying Authority.

Considering one of them i.e **Safescrypt**, as an example to demonstrate the Installation of DSC. After submission of the application, it follows **Enrollment** and **Pick up ID** procedure.

Steps to Enroll for Digital Signature

1. Select the computer to install the digital signature.
2. Ensure that Internet Explorer version 6.0, 128 Bit is installed in the Computer
3. Go to https://onsite.safescrypt.com/services/SEEPZSpecialEconomicZoneInformationTechnology/digitalidCenter.htm
4. The following Menu options are displayed for Digital Signature Enrollment. Click Enroll.



SEEPZ Special Economic Zone Information Technology Digital ID Center

ENROLL
Choose this option to enroll for a client Digital ID.

PICK UP ID
Choose this option if you enrolled for a Digital ID but did not pick it up.

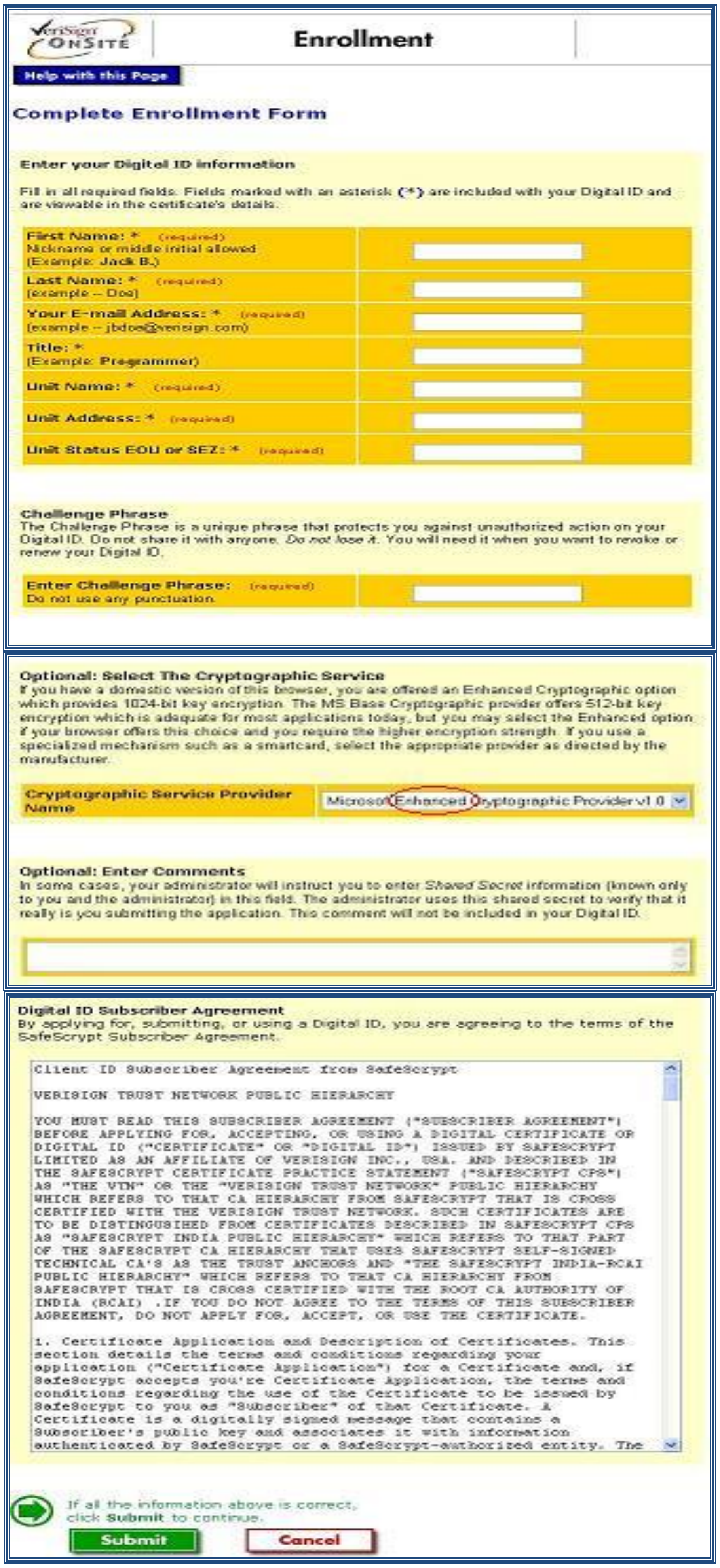
SEARCH
Choose this option to search for a Digital ID. This function is useful for determining whether a Digital ID is valid, expired, or revoked. You may also download IDs from this option.

RENEW
Choose this option to renew a Digital ID which is expiring or which has already expired. You should generally start renewing your Digital ID at least one month before your Digital ID is due to expire.

REVOKE
Choose this option to revoke your Digital ID. Digital IDs should be revoked immediately for any suspected compromise, including lost or stolen private keys, corrupted key pairs, change in site ownership, or suspected fraud.

Copyright © 1998-2002, VeriSign, Inc. All rights reserved.

5. Fill-out the Enrollment form for individual applicant. Select ***“Microsoft Enhanced Cryptographic Provider v1.0”*** in the Service Provide list and click Submit.



Enrollment

Complete Enrollment Form

Enter your Digital ID information

Fill in all required fields. Fields marked with an asterisk (*) are included with your Digital ID and are viewable in the certificate's details.

First Name: * (required) Nickname or middle initial allowed (Example: Jack B.)	
Last Name: * (required) [example -- Doe]	
Your E-mail Address: * (required) (example -- jbdoe@verisign.com)	
Title: * (Example: Programmer)	
Unit Name: * (required)	
Unit Address: * (required)	
Unit Status EOU or SEZ: * (required)	

Challenge Phrase
The Challenge Phrase is a unique phrase that protects you against unauthorized action on your Digital ID. Do not share it with anyone. *Do not lose it.* You will need it when you want to revoke or renew your Digital ID.

Enter Challenge Phrase: (required) Do not use any punctuation.	

Optional: Select The Cryptographic Service
If you have a domestic version of this browser, you are offered an Enhanced Cryptographic option which provides 1024-bit key encryption. The MS Base Cryptographic provider offers 512-bit key encryption which is adequate for most applications today, but you may select the Enhanced option if your browser offers this choice and you require the higher encryption strength. If you use a specialized mechanism such as a smartcard, select the appropriate provider as directed by the manufacturer.

Cryptographic Service Provider Name	Microsoft Enhanced Cryptographic Provider v1.0

Optional: Enter Comments
In some cases, your administrator will instruct you to enter *Shared Secret* information (known only to you and the administrator) in this field. The administrator uses this shared secret to verify that it really is you submitting the application. This comment will not be included in your Digital ID.

Digital ID Subscriber Agreement
By applying for, submitting, or using a Digital ID, you are agreeing to the terms of the SafeScrypt Subscriber Agreement.

```
Client ID Subscriber Agreement from SafeScrypt

VERISIGN TRUST NETWORK PUBLIC HIERARCHY

YOU MUST READ THIS SUBSCRIBER AGREEMENT ("SUBSCRIBER AGREEMENT")
BEFORE APPLYING FOR, ACCEPTING, OR USING A DIGITAL CERTIFICATE OR
DIGITAL ID ("CERTIFICATE" OR "DIGITAL ID") ISSUED BY SAFESCRYPT
LIMITED AS AN AFFILIATE OF VERISIGN INC., USA. AND DESCRIBED IN
THE SAFESCRYPT CERTIFICATE PRACTICE STATEMENT ("SAFESCRYPT CPS")
AS "THE VTN" OR THE "VERISIGN TRUST NETWORK" PUBLIC HIERARCHY
WHICH REFERS TO THAT CA HIERARCHY FROM SAFESCRYPT THAT IS CROSS
CERTIFIED WITH THE VERISIGN TRUST NETWORK. SUCH CERTIFICATES ARE
TO BE DISTINGUSIHED FROM CERTIFICATES DESCRIBED IN SAFESCRYPT CPS
AS "SAFESCRYPT INDIA PUBLIC HIERARCHY" WHICH REFERS TO THAT PART
OF THE SAFESCRYPT CA HIERARCHY THAT USES SAFESCRYPT SELF-SIGNED
TECHNICAL CA'S AS THE TRUST ANCHORS AND "THE SAFESCRYPT INDIA-RCAI
PUBLIC HIERARCHY" WHICH REFERS TO THAT CA HIERARCHY FROM
SAFESCRYPT THAT IS CROSS CERTIFIED WITH THE ROOT CA AUTHORITY OF
INDIA (RCAI) .IF YOU DO NOT AGREE TO THE TERMS OF THIS SUBSCRIBER
AGREEMENT, DO NOT APPLY FOR, ACCEPT, OR USE THE CERTIFICATE.

1. Certificate Application and Description of Certificates. This
section details the terms and conditions regarding your
application ("Certificate Application") for a Certificate and, if
SafeScrypt accepts you're Certificate Application, the terms and
conditions regarding the use of the Certificate to be issued by
SafeScrypt to you as "Subscriber" of that Certificate. A
Certificate is a digitally signed message that contains a
Subscriber's public key and associates it with information
authenticated by SafeScrypt or a SafeScrypt-authorized entity. The
```

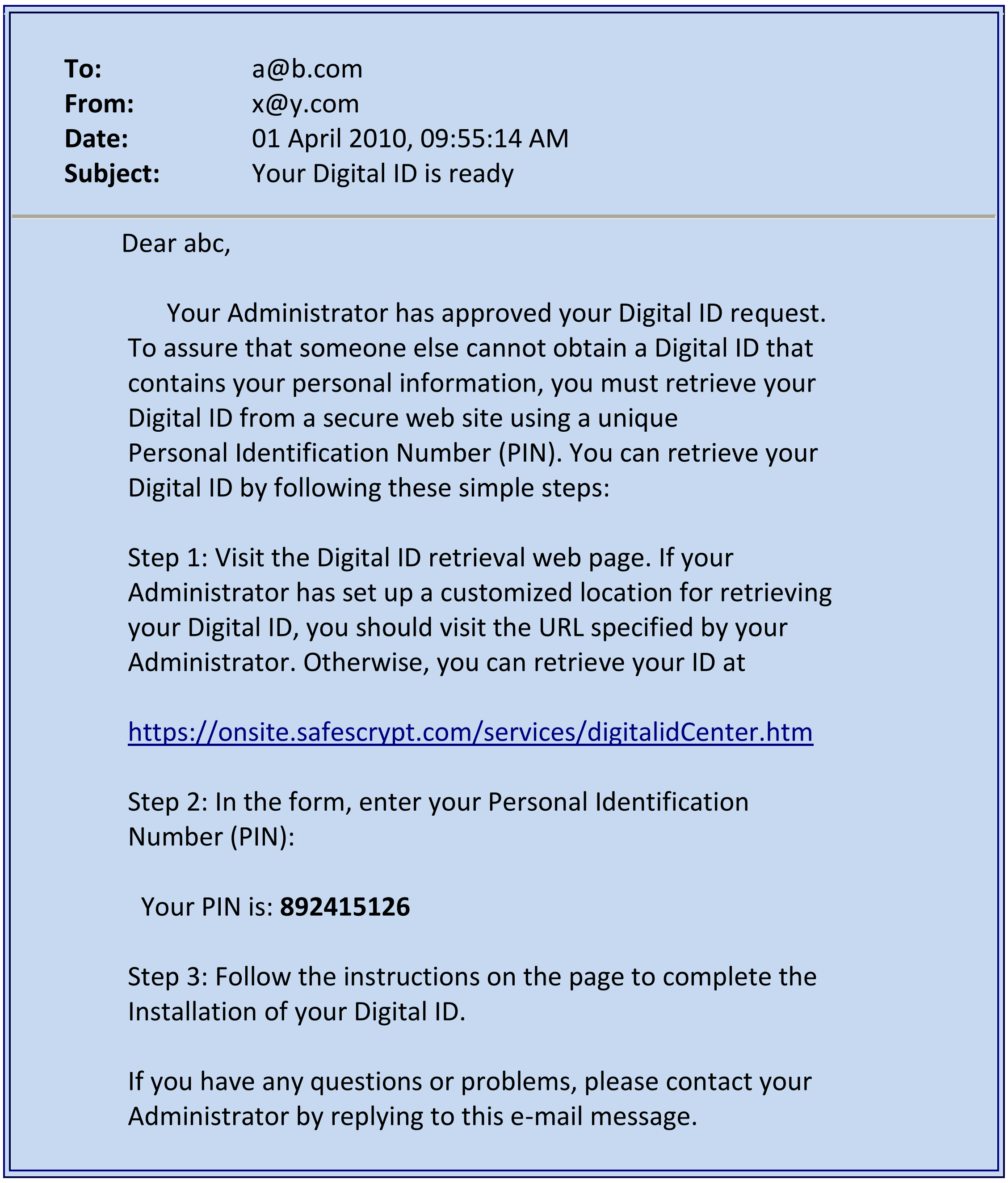
If all the information above is correct, click **Submit** to continue.

- On receiving the enrollment application, the Registering Authority approves your application after verifying it.
- Once approved, you receive an email from the certificate issuing authority containing the PIN for installation along with the installation procedure.

- Do not format the computer until you receive the PIN. The PIN will be installed on the same computer that you used for enrolling for the digital certificate.

Steps to Install for Digital Signature

1. Apply for the digital signature if you have not procured as per the procedure received via email.
2. On completing the Enrollment procedure, you will receive an email in the following format (see Image 1) from the Registration Authority. The email contains a **PIN** number and the URL to download the signature.



To:	a@b.com
From:	x@y.com
Date:	01 April 2010, 09:55:14 AM
Subject:	Your Digital ID is ready

Dear abc,

Your Administrator has approved your Digital ID request. To assure that someone else cannot obtain a Digital ID that contains your personal information, you must retrieve your Digital ID from a secure web site using a unique Personal Identification Number (PIN). You can retrieve your Digital ID by following these simple steps:

Step 1: Visit the Digital ID retrieval web page. If your Administrator has set up a customized location for retrieving your Digital ID, you should visit the URL specified by your Administrator. Otherwise, you can retrieve your ID at

https://onsite.safescrypt.com/services/digitalidCenter.htm

Step 2: In the form, enter your Personal Identification Number (PIN):

Your PIN is: **892415126**

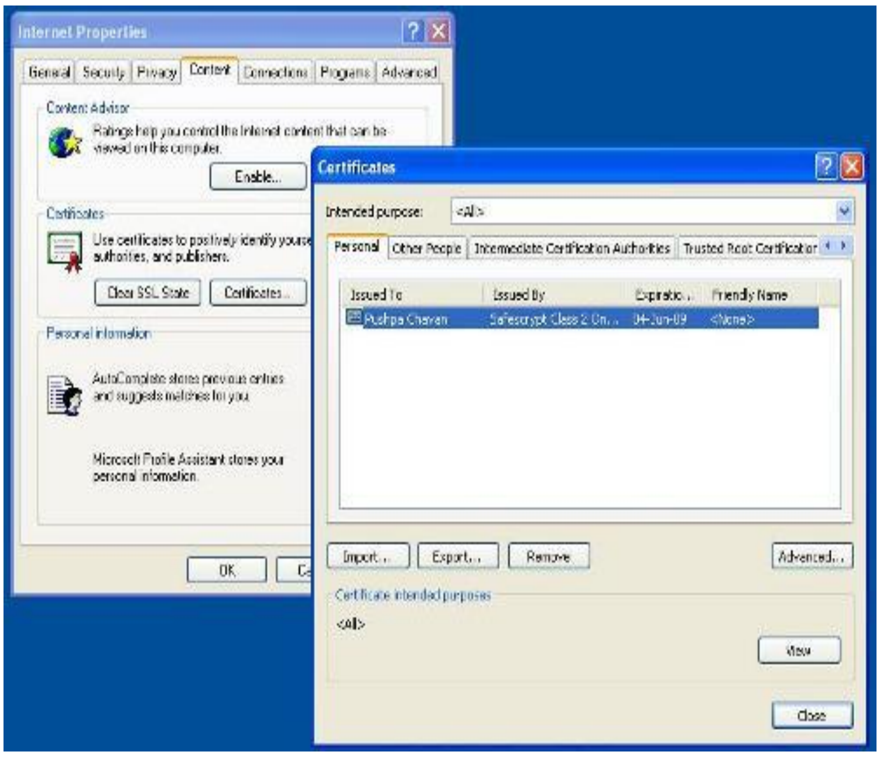
Step 3: Follow the instructions on the page to complete the Installation of your Digital ID.

If you have any questions or problems, please contact your Administrator by replying to this e-mail message.

Image 1

3. On submitting the PIN number to the specified URL, the Digital Certificate can be installed on your computer using Internet Explorer.
4. Take a backup of the certificate using the following steps and store the backup in a safe location protected by a password.

a) Open Internet Explorer
b) Select Tools -> Internet Options
c) Select Content Tab -> Certificate
d) The certificate is displayed in the Certificate tab (see Image 2).



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

Use certificates to positively identify yours authorities, and publishers.

AutoComplete stores previous entries and suggests matches for you.

Microsoft Profile Assistant stores your personal information.

Intended purpose: <All>

Issued To	Issued By	Expiratio...	Friendly Name
Pushpa Chavan	Safescrypt Class 2 On...	04-Jun-09	<None>

Certificate intended purposes
<All>

Image 2

e) Click the certificate, and then click the Export button.
f) Click Next, and select Yes, Export with Private Key, and then click next.
g) Enter your Password, and then click Next. (This password is required for installing the certificate again, should the need arise)
h) Select the directory to store the file and assign a name to the file, and then click Next.
i) Click Finish and move the ***.pfx*** file to a safe location.

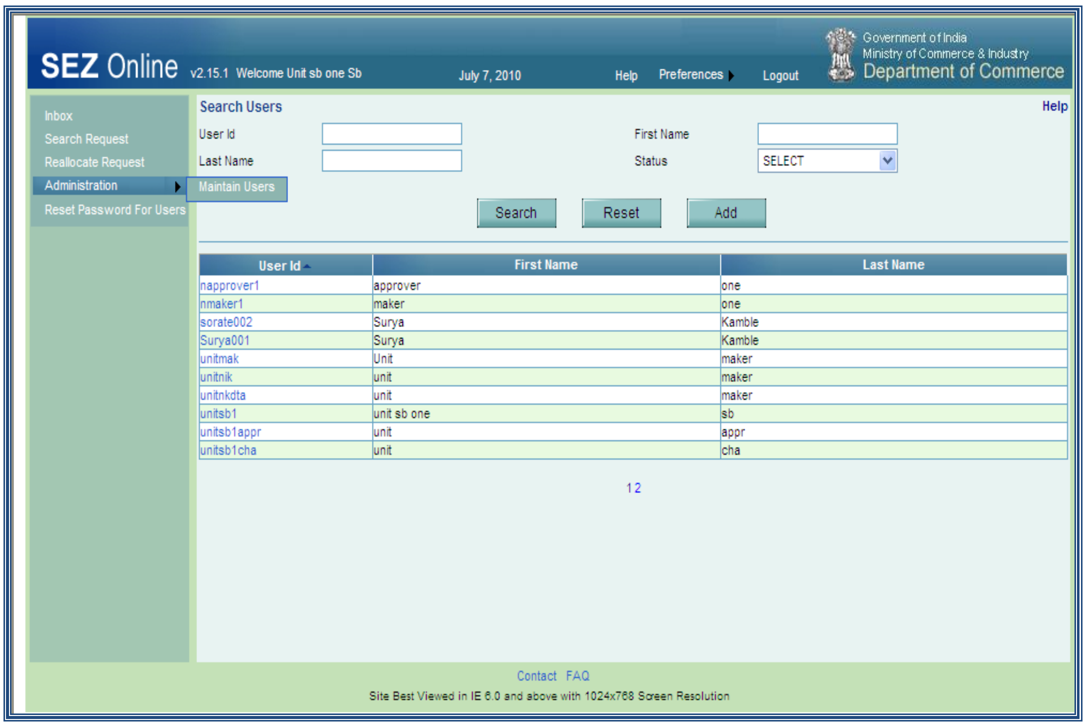
4. Procedure for entering the DSC details of the user in SEZ Online system

3.1. Login as Admin

3.2. Go to Administration -> Maintain Users

3.3. Search for the User

3.4.Click on the link of that user ID



Search Users

User Id		First Name	
Last Name		Status	SELECT

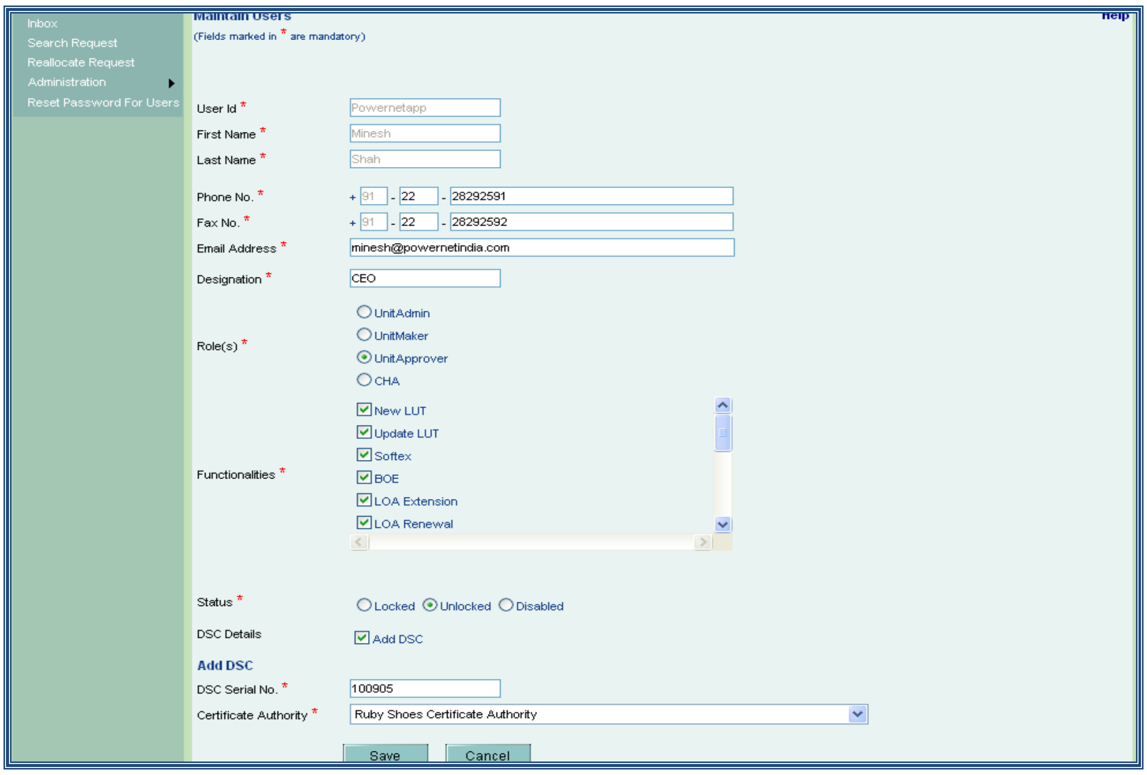
User Id	First Name	Last Name
napprover1	approver	one
nmaker1	maker	one
sorate002	Surya	Kamble
Surya001	Surya	Kamble
unitmak	Unit	maker
unitnik	unit	maker
unitnkdta	unit	maker
unitsb1	unit sb one	sb
unitsb1appr	unit	appr
unitsb1cha	unit	cha

3.5.Then click on "EDIT" button

3.6.Select the "ADD DSC" Checkbox

3.7.Enter the Serial Number of the Certificate

3.8.Select the Appropriate Certificate Authority and Save



Maintain Users

(Fields marked in * are mandatory)

User Id *	Powernetapp
First Name *	Minesh
Last Name *	Shah
Phone No. *	+ 91 - 22 - 28292591
Fax No. *	+ 91 - 22 - 28292592
Email Address *	minesh@powernetindia.com
Designation *	CEO
Role(s) *	○ UnitAdmin ○ UnitMaker ● UnitApprover ○ CHA
Functionalities *	☑ New LUT ☑ Update LUT ☑ Softex ☑ BOE ☑ LOA Extension ☑ LOA Renewal
Status *	○ Locked ● Unlocked ○ Disabled
DSC Details	☑ Add DSC

Add DSC

DSC Serial No. *	100905
Certificate Authority *	Ruby Shoes Certificate Authority

5. Troubleshooting

(i) **"DSC Serial number invalid"**

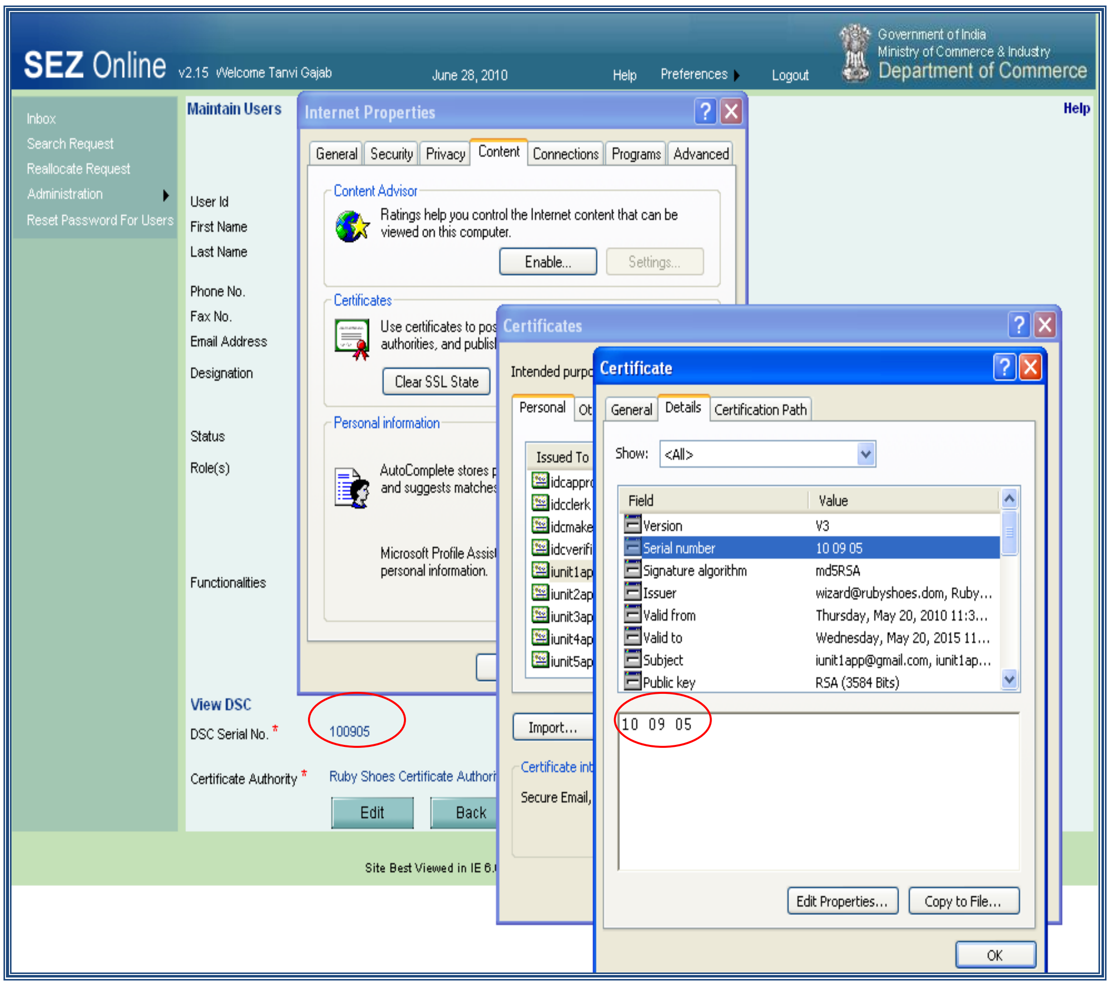
Solution:

- ✓ Login as Admin
- ✓ Search for the User
- ✓ Click on the link
- ✓ Go to Edit User
- ✓ Check whether the serial number entered is same as the DSC serial number

To check Serial Number, Go to

Tools—Internet Options—Content---Certificates---Personal

Select the certificate and click on the view button and go to Details.



DSC Serial No. * 100905

Certificate Authority * Ruby Shoes Certificate Authori

Show: <All>

Field	Value
Version	V3
Serial number	10 09 05
Signature algorithm	md5RSA
Issuer	wizard@rubyshoes.dom, Ruby...
Valid from	Thursday, May 20, 2010 11:3...
Valid to	Wednesday, May 20, 2015 11...
Subject	iunit1app@gmail.com, iunit1ap...
Public key	RSA (3584 Bits)

10 09 05

(ii) "**DSC Signature Failed- Automation Server cannot create object**."

Solution 1:

Check whether the certificate has been expired.

To check:

Go to Tools—Internet Options—Content—Certificates—Personal—select the certificate and click on the view button

Solution 2:

Check whether the user associated the Certificate to the user in the user creation page of SEZ Online System. To Check,

- ✓ Login as Admin
- ✓ Search for the User
- ✓ Click on the link
- ✓ Go to Edit User
- ✓ Check whether the serial number entered is same as the DSC serial number

Solution 3:

Check whether ActiveX enabled on the machine from which the Unit is going to digitally sign data. If No, then do the ActiveX settings (refer Annexure I: ActiveX Settings)

Solution 4:

Check whether Unit user imported the certificate in the browser. If No, then carry out the same by importing the certificate in the browser

(iii) "**Revocation Server offline**" **or** "**Problem is in revocation of certificate**"

Solution:

- ✓ Check if the CRL is imported in the proper CRL folder in CertManager
- ✓ Check if the CRL chain is maintained properly.
- ✓ Check for the expiry dates

For this ask the screen shots of

Trusted Root Certification Authorities

Certificate Information

Certification Path

(iv) "**Certifying Authority not supported**"

Solution:

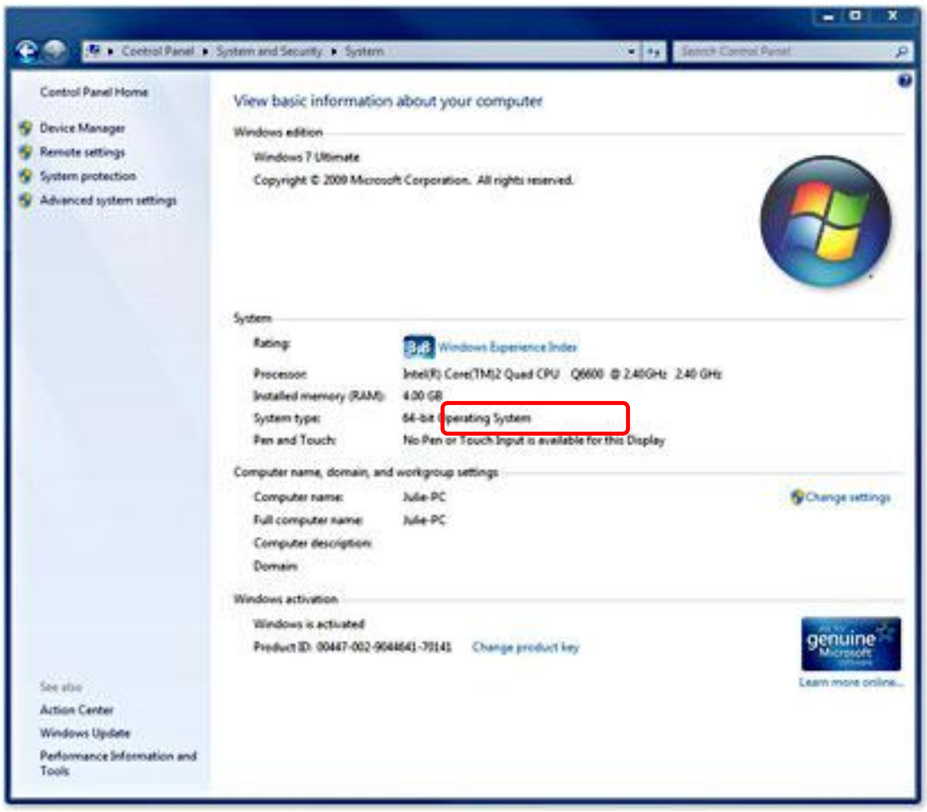
- ✓ Check if the user has selected valid certifying authority while assigning DSC from the drop down box.
- ✓ Check whether the Issued by name is matching with the users DSC name selected by him.

(v) "**Capicom.dll is not available/ register on local machine**"

If ’Capicom.dll’ is not registered or installed on user’s machine, this error message appears. Capicom.dll is required for functioning of DSC.

Solution: Installation of Capicom.dll. The method of installation is as mentioned below:

Installation or registration of CAPICOM.dll varies according to the windows bit versions viz. **32 bit** or **64 bit**. To identify the bit version of the Operating system, go to *Control panel→ System*



View basic information about your computer

Windows edition

Windows 7 Ultimate

Copyright © 2009 Microsoft Corporation. All rights reserved.

System

Rating: 3.8

Processor: Intel(R) Core(TM)2 Quad CPU Q6600 @ 2.40GHz 2.40 GHz

Installed memory (RAM): 4.00 GB

System type: 64-bit Operating System

Pen and Touch: No Pen or Touch Input is available for this Display

Computer name, domain, and workgroup settings

Computer name: Julie-PC

Full computer name: Julie-PC

Computer description:

Domain:

Windows activation

Windows is activated

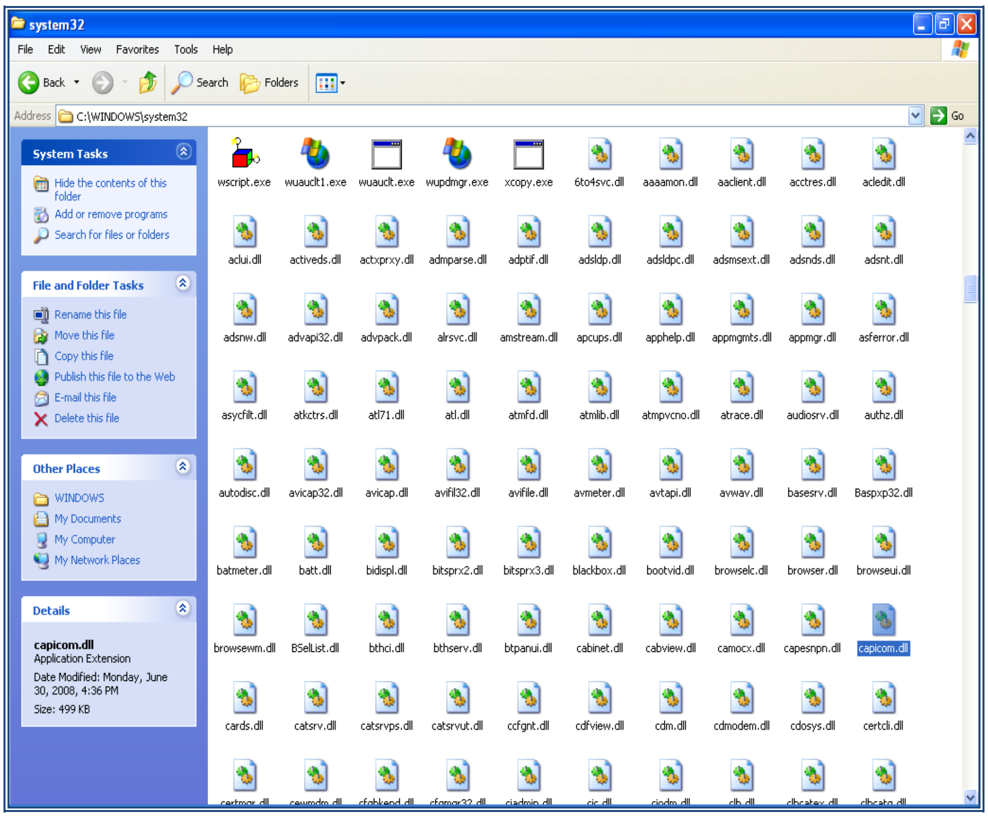
Product ID: 00447-002-9044641-70141

Based on the bit version of operation system, capicom.dll has to be selected. The capicom.dll files of the 32 & 64 bit versions are enclosed below. The enclosed zip files may used for installation of Capicom.dll

Capicom.dll file for 32 bit version of OS:	capicom.zip
Capicom.dll file for 64 bit version of OS:	capicom.zip

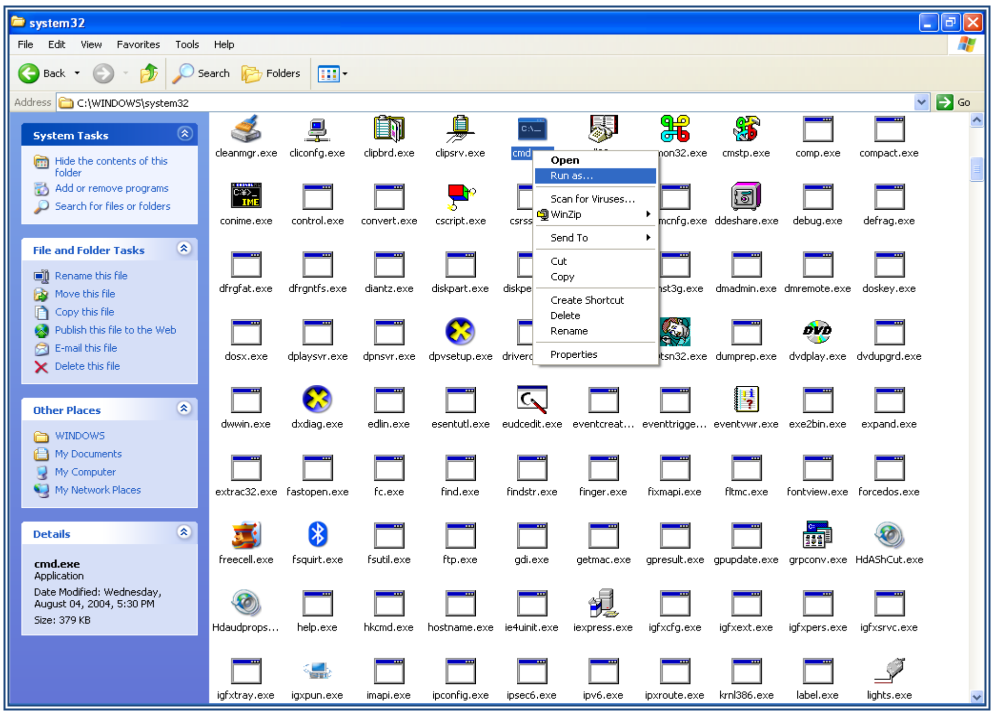
Procedure of Installation of capicom.dll for Windows XP, Windows Vista, Windows 7 (32bit)

- Go to My Computer/ Local Disk ***(C:) / Windows/ System32***

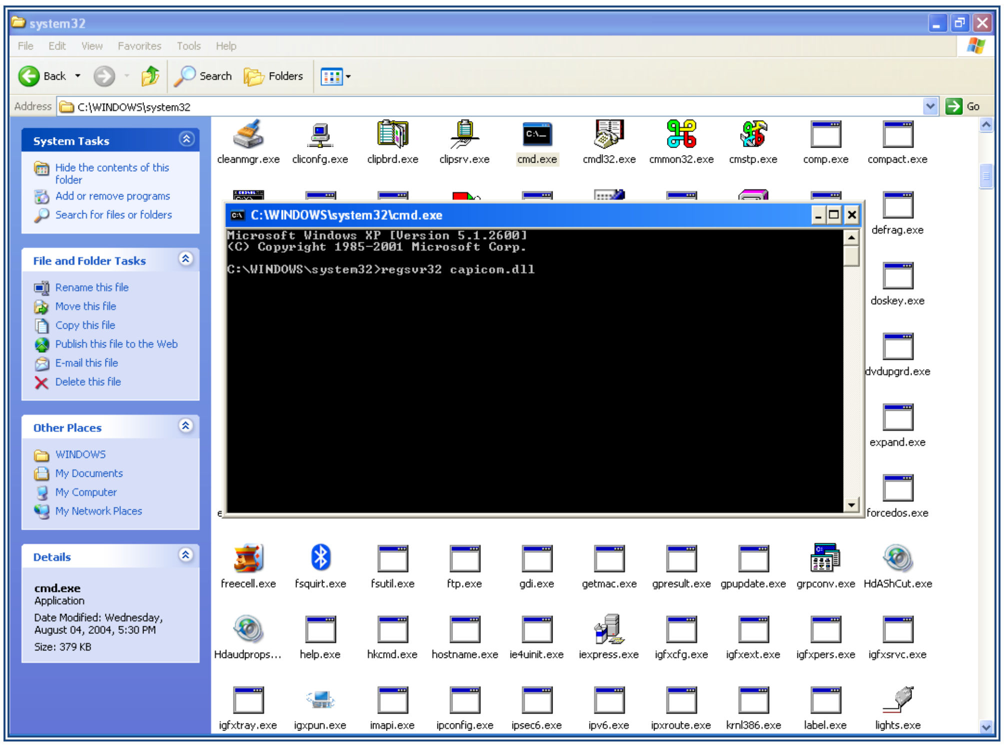


capicom.dll
Application Extension
Date Modified: Monday, June 30, 2008, 4:36 PM
Size: 499 KB

- Copy capicom.dll file for 32bit version to system32 folder.
- Search “**CMD”** file from the System32 folder.
- Right Click on “**CMD”** file and select **Run** option. User should have **administration** rights to run “**CMD”**



- Type command ‘**regsvr32 Capicom.dll’** in the command screen & press **Enter** to install Capicom.dll. On successful installation, message is displayed.



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>regsvr32 capicom.dll
```

<u>Procedure of Installation of capicom.dll for Windows Vista, Windows 7 (64bit)</u>

- Click on Windows **Start** button
- Type **‘%systemroot%\SysWoW64\’** in the search text box to open system folder

- Copy the capicom.dll file for 64 bit version to following folder **“%systemroot%\SysWoW64\”**
- Open the **CMD** prompt in administrator mode
- Go to folder **“%systemroot%\SysWoW64”** from **CMD** prompt
- Run command **“regsvr32 capicom.dll”**
- On clicking the **‘Enter’** button, the successful installation message displays.

(vi) "**Cannot sign the Data. No certificate information registered with the System**"

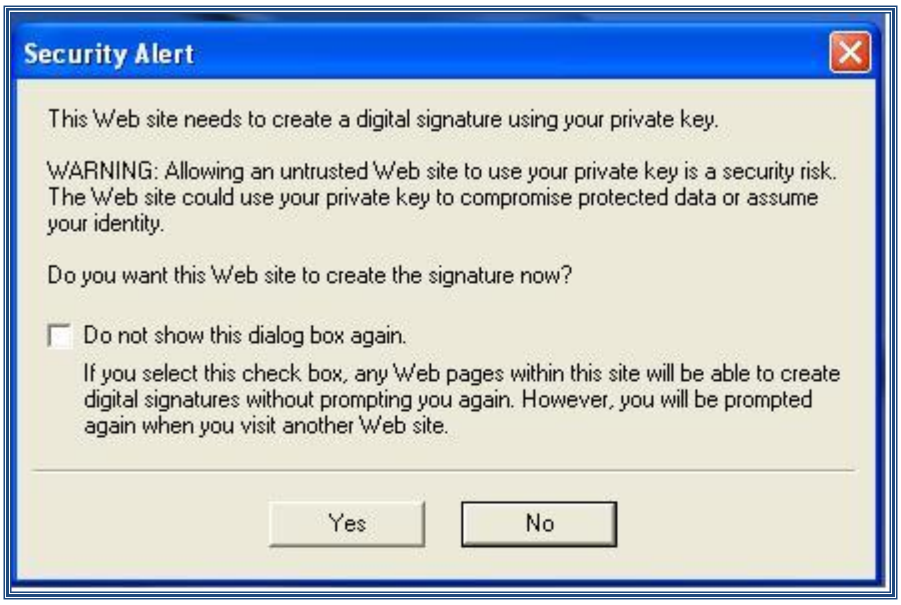
Solution:

- ✓ Login as Admin
- ✓ Search for the User
- ✓ Click on the link for that user
- ✓ Go to Edit User
- ✓ Check the Add DSC radio button
- ✓ Add the Serial Number of DSC
- ✓ Select the appropriate provider and Save

(vii) "**No Data to Sign**"

Solution:

While submitting the application, when you select the Certificate, the security alert pop up, Select "Yes"



Security Alert

This Web site needs to create a digital signature using your private key.

WARNING: Allowing an untrusted Web site to use your private key is a security risk. The Web site could use your private key to compromise protected data or assume your identity.

Do you want this Web site to create the signature now?

□ Do not show this dialog box again.

If you select this check box, any Web pages within this site will be able to create digital signatures without prompting you again. However, you will be prompted again when you visit another Web site.

6. Digital Signature Glossary of Terms

- **Certificate Authority** (CA) :

  An authority that creates and signs Digital Certificates for one or more users. Usually CA's form a hierarchy. The top of this hierarchy is called the root CA.

- **CRL** :

  Certificate Revocation List - the place where a CA stores the IDs of all the Digital Certificates that have been revoked.

- **RA** :

  Registration Authority – An RA does the required identification for certain certificate data, which is then passed to the CA for issuing the Digital Certificate.

- **PKI** :

  Public Key Infrastructure – The combination of standards, protocols and policies that support Digital Signatures and Encryption

- **Private Key** :

The secret key in a PKI system, used to decrypt incoming messages and sign outgoing ones. A Private Key is always paired with its Public Key during key generation.

7. Annexure I

ActiveX Settings of Internet Explorer:

Active X Settings varies for different versions of Internet Explorer

IE 6.0 Settings:-

ActiveX Controls and Plug ins			
ActiveX Control	Enable	Disable	Prompt
Automatic prompting for ActiveX controls	-	Y	-
Binary and script behaviors	Y	-	-
Download signed ActiveX controls	-	-	Y
Download unsigned ActiveX controls	-	Y	-
Initialize and script ActiveX controls not marked as safe for scripting	-	Y	-
Run ActiveX controls and plug-ins	Y	-	-
Script ActiveX controls marked safe for scripting	Y	-	-

IE 7.0 Settings:-

ActiveX Controls and Plug ins			
ActiveX Control	Enable	Disable	Prompt
Allow previously unused ActiveX controls to run without prompt	Y	-	-
Allow Scriptlets	-	Y	-
Automatic prompting of ActiveX controls	Y	-	-
Binary and script behaviors	-	Y	-
Display video and animation on a webpage that does not use external media player	-	Y	-
Download signed ActiveX controls	-	Y	-
Download unsigned ActiveX controls	-	Y	-
Initialize and script ActiveX controls not marked as safe for scripting	-	Y	-
Run ActiveX controls and plug-ins	Y	-	-
Script ActiveX controls marked safe for scripting	Y	-	-

IE 8.0 Settings:-

ActiveX Controls and Plug ins			
ActiveX Control	Enable	Disable	Prompt
Allow previously unused ActiveX controls to run without prompt	Y	-	-
Allow Scriptlets	Y	-	-
Automatic prompting of ActiveX controls	Y	-	-
Binary and script behaviors	Y	-	-
Display video and animation on a webpage that does not use external media player	-	Y	-
Download signed ActiveX controls	-	-	Y
Download unsigned ActiveX controls	-	Y	-
Initialize and script ActiveX controls not marked as safe for scripting	-	Y	-
Run ActiveX controls and plug-ins	Y	-	-

Script ActiveX controls marked safe for scripting	Y	-	-
Only allowed approved domains to use ActiveX without prompt	-	Y	-

IE 9.0 Settings:-

ActiveX Controls and Plug ins			
ActiveX Control	Enable	Disable	Prompt
Allow previously unused ActiveX controls to run without prompt	Y	-	-
Allow Scriptlets	Y	-	-
Automatic prompting of ActiveX controls	Y	-	-
Binary and script behaviors	Y	-	-
Display video and animation on a webpage that does not use external media player	-	Y	-
Download signed ActiveX controls	-	-	Y
Download unsigned ActiveX controls	-	Y	-
Initialize and script ActiveX controls not marked as safe for scripting	-	Y	-
Only allowed approved domains to use ActiveX without prompt	-	Y	-
Run ActiveX controls and plug-ins	Y	-	-
Script ActiveX controls marked safe for scripting	Y	-	-

- Custom Level ->miscellaneous Option of security setting -> enable ‘Use Pop-up blocker’

8. Annexure II

Installation of Root Certificate:

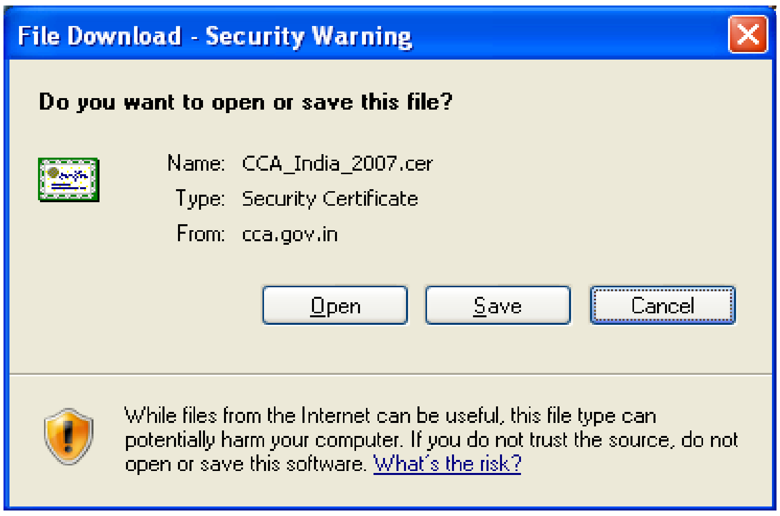
A root certificate is a self-signed certificate. A root certificate, the top-most certificate of the tree, is based on the ITU-T X.509 standard. All certificates below the root certificate inherit the trustworthiness of the root certificate.

Below is one of the examples of the procedure for installation of root certificate:

Visit the website of the Controller of Certifying Authorities (CCA) at *www.cca.gov.in* to obtain the digital signature certificate of the CCA. This certificate must be installed on our computer before we begin the process to obtain our personal digital signature certificate. The detailed procedure for the same is outlined below:

i. Click on “Download 2007 Root Certificate” image.

ii. The following screen will open up. Click on “Open”

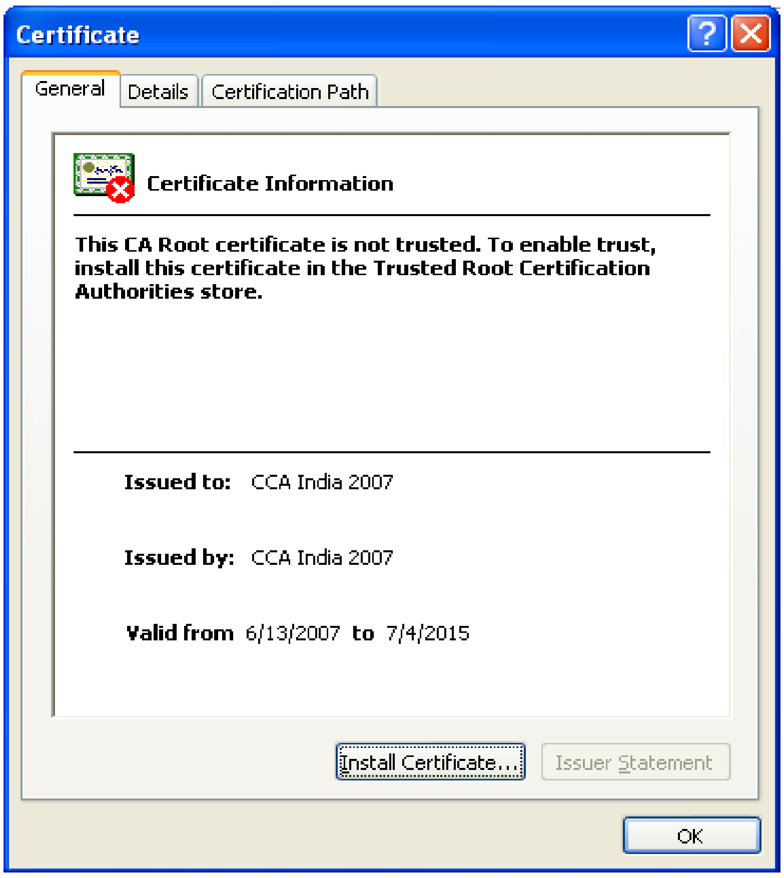


Do you want to open or save this file?

Name: CCA_India_2007.cer
Type: Security Certificate
From: cca.gov.in

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open or save this software. What's the risk?

iii. The following digital signature certificate will open up on your screen:



Certificate

Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: CCA India 2007

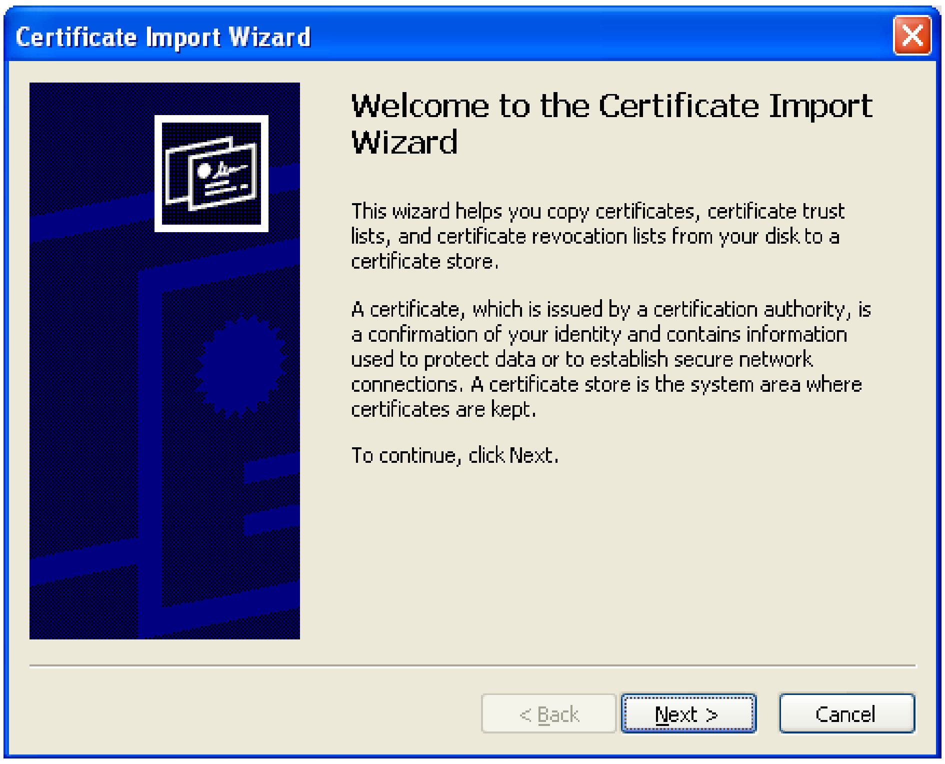
Issued by: CCA India 2007

Valid from 6/13/2007 to 7/4/2015

iv. The certificate displays the message that:

"This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store".

The reason for this is that this certificate is not installed in the Microsoft Internet Explorer browser by default. We will manually need to do so. Click on "**Install Certificate**" The following screen opens up:



Certificate Import Wizard

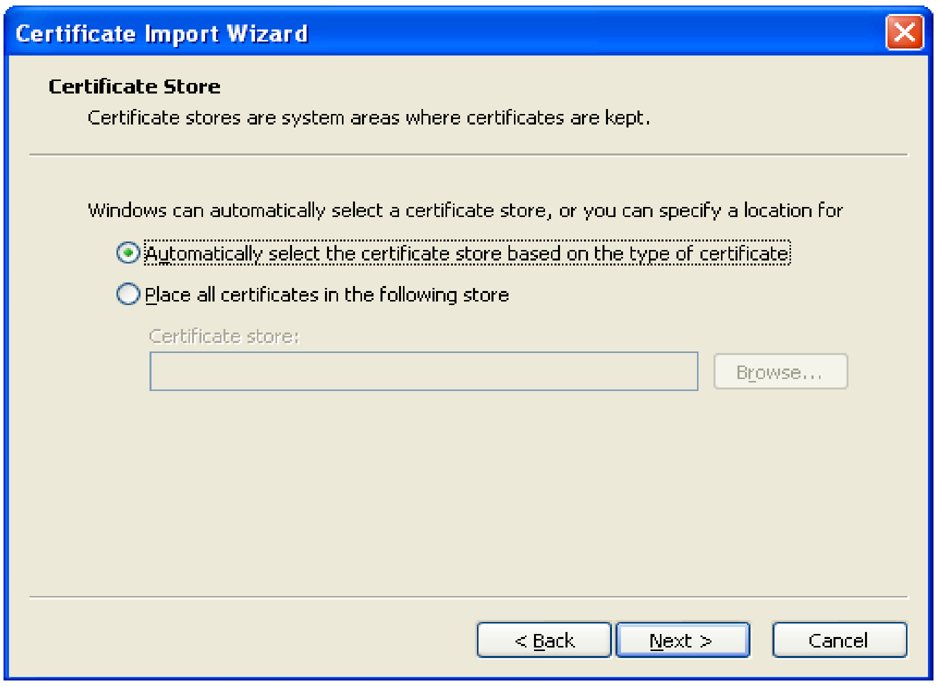
Welcome to the Certificate Import Wizard

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.

Click on "**Next**" The following screen will open up. Again click on "**Next**".



Certificate Store

Certificate stores are system areas where certificates are kept.

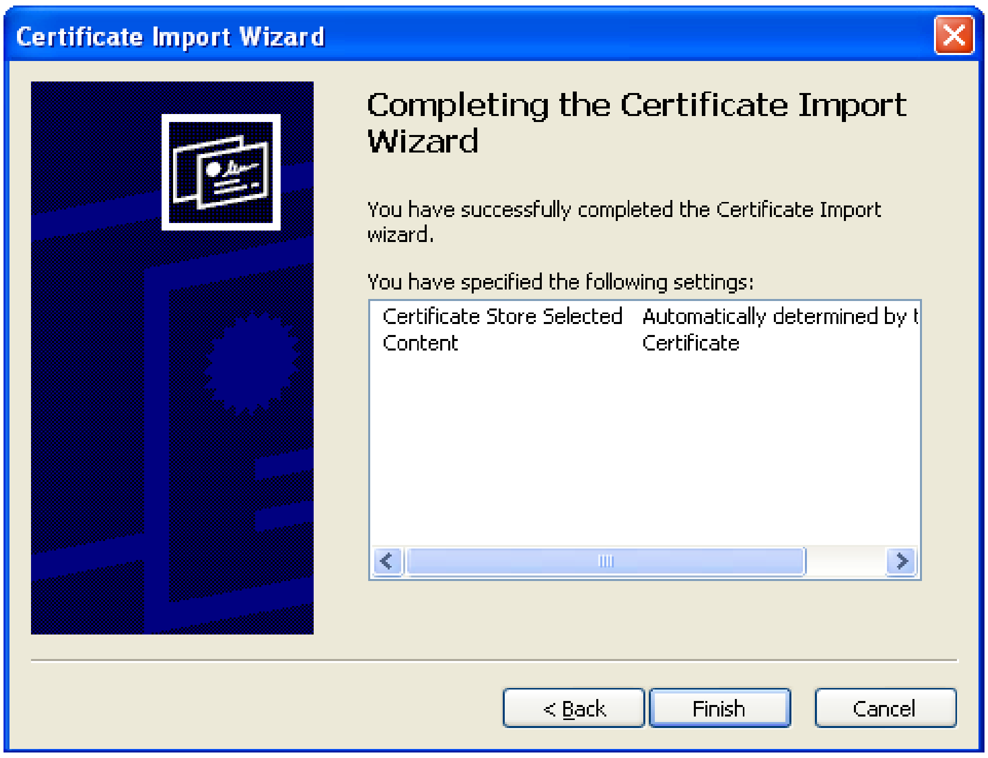
Windows can automatically select a certificate store, or you can specify a location for

● Automatically select the certificate store based on the type of certificate

○ Place all certificates in the following store

Certificate store:

v. The following screen will open up. Click on "**Finish**".



Completing the Certificate Import Wizard

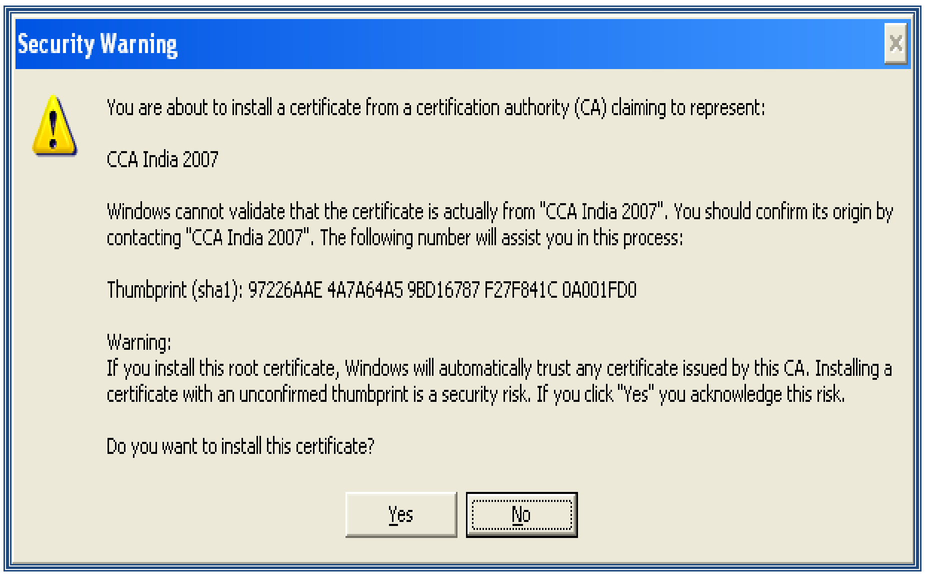
You have successfully completed the Certificate Import wizard.

You have specified the following settings:

Certificate Store Selected	Automatically determined by t
Content	Certificate

This is the final stage for installing the CCA certificate on our computer. It must be clearly understood that once this root certificate is installed in our browser, it becomes a trusted root certificate. All Certifying Authorities who are issued certificates by the CCA will automatically be trusted by our computer.

vi. The following screen will open up. Click on “Yes”



Security Warning

You are about to install a certificate from a certification authority (CA) claiming to represent:

CCA India 2007

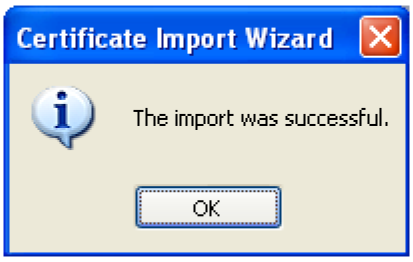
Windows cannot validate that the certificate is actually from "CCA India 2007". You should confirm its origin by contacting "CCA India 2007". The following number will assist you in this process:

Thumbprint (sha1): 97226AAE 4A7A64A5 9BD16787 F27F841C 0A001FD0

Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

vii. The screen below will open up. Click “OK”.

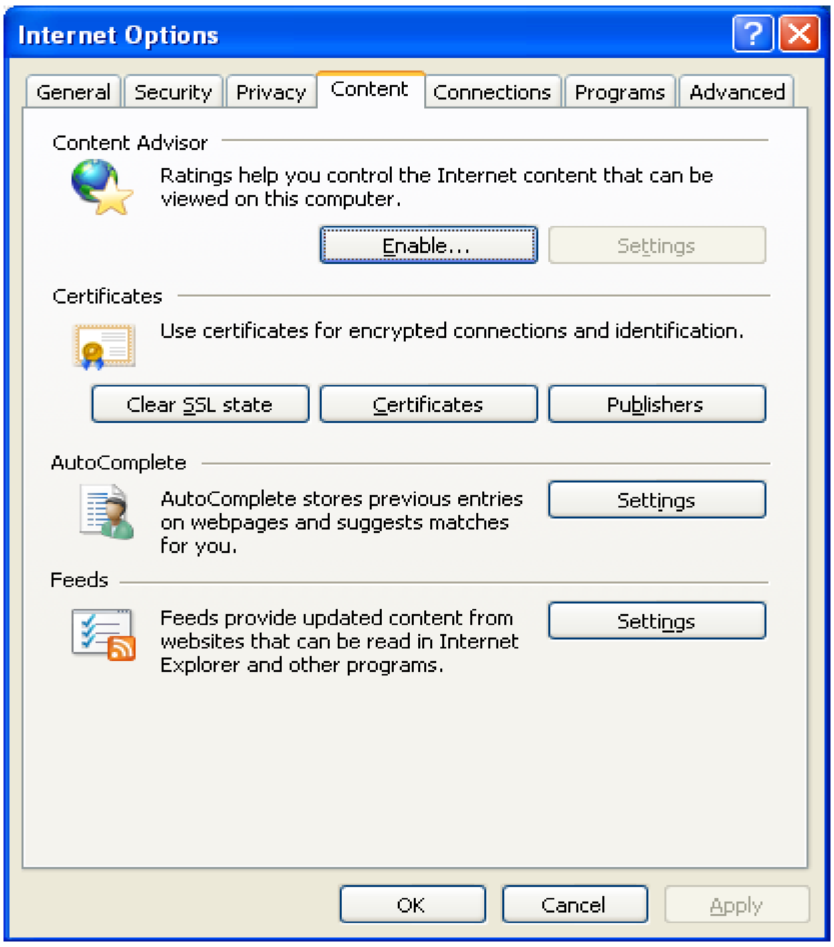


Certificate Import Wizard

The import was successful.

viii. To view the installed CCA certificate, open up a window of Microsoft Internet Explorer and then click on

Tools-Internet Options-Content



Internet Options

Content Advisor

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

Certificates

Use certificates for encrypted connections and identification.

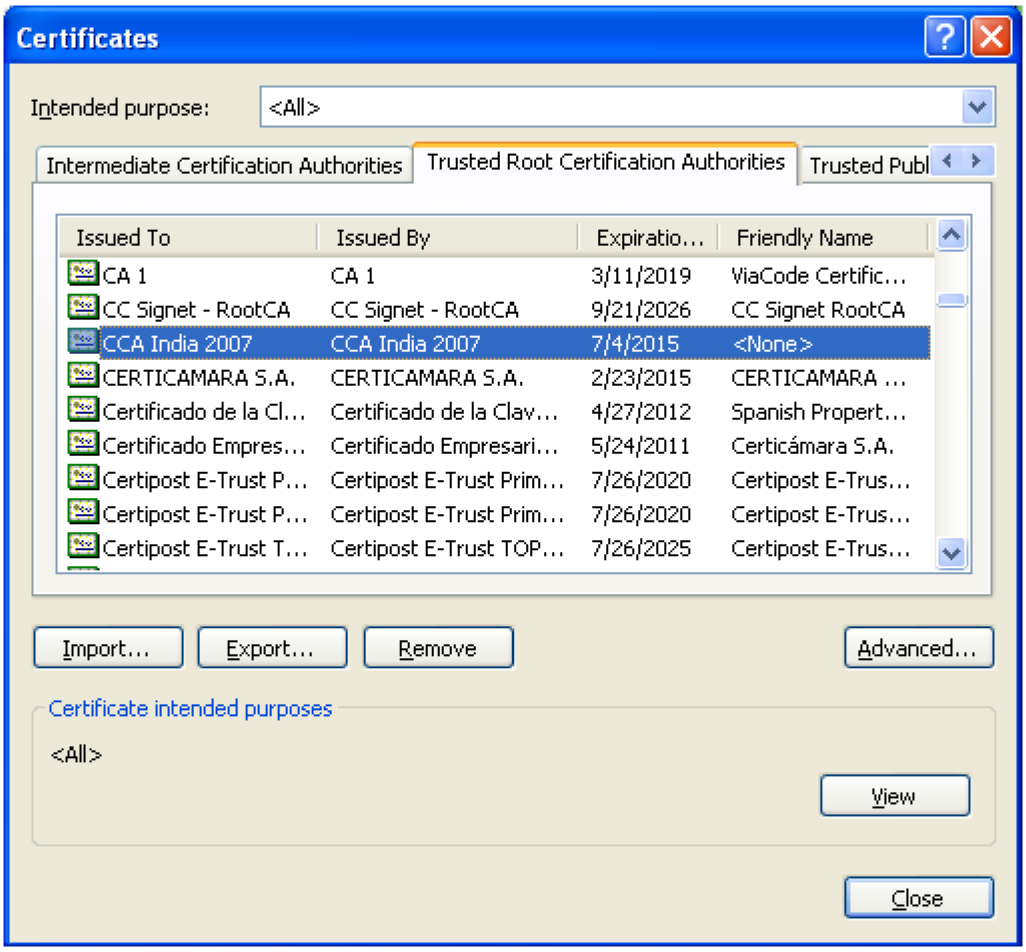
AutoComplete

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.

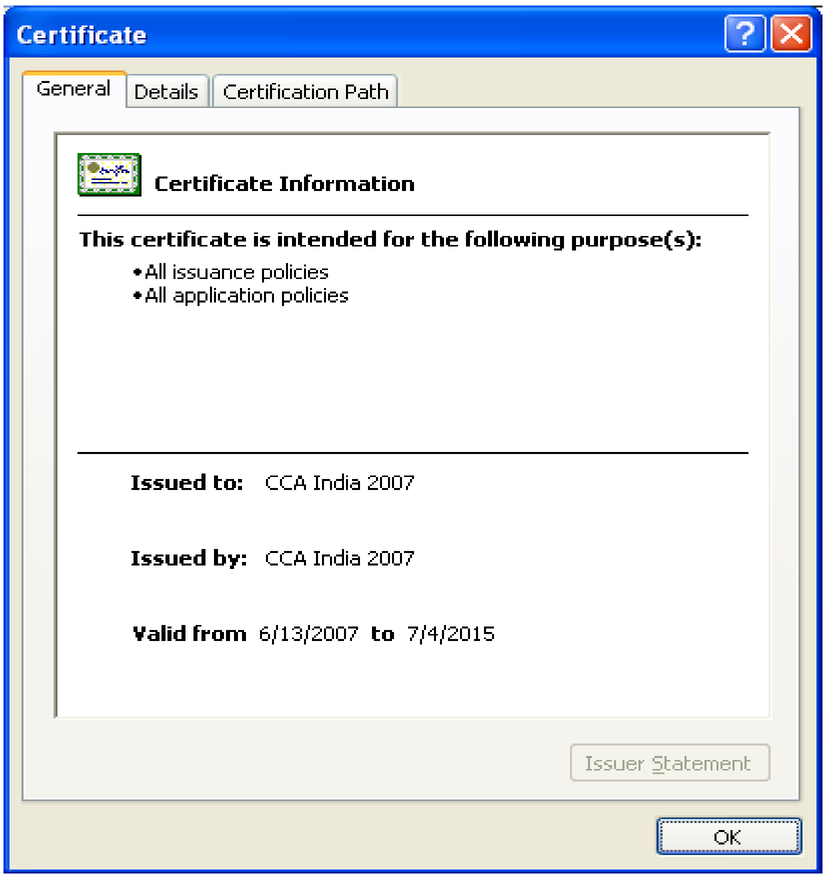
When the above window opens up, click on "**Certificates**" and then click on the "Trusted Root Certification Authorities" tab. The following screen will open up. Click on "CCA India 2007" and then click on "**View**".



Certificates
Intended purpose:
<All>
Intermediate Certification Authorities
Trusted Root Certification Authorities
Trusted Publ
Import...
Export...
Remove
Advanced...
Certificate intended purposes
<All>
View
Close

Issued To	Issued By	Expiratio...	Friendly Name
CA 1	CA 1	3/11/2019	ViaCode Certific...
CC Signet - RootCA	CC Signet - RootCA	9/21/2026	CC Signet RootCA
CCA India 2007	CCA India 2007	7/4/2015	<None>
CERTICAMARA S.A.	CERTICAMARA S.A.	2/23/2015	CERTICAMARA ...
Certificado de la Cl...	Certificado de la Clav...	4/27/2012	Spanish Propert...
Certificado Empres...	Certificado Empresari...	5/24/2011	Certicámara S.A.
Certipost E-Trust P...	Certipost E-Trust Prim...	7/26/2020	Certipost E-Trus...
Certipost E-Trust P...	Certipost E-Trust Prim...	7/26/2020	Certipost E-Trus...
Certipost E-Trust T...	Certipost E-Trust TOP...	7/26/2025	Certipost E-Trus...

The certificate illustrated in the next page will now open up on your screen.



Certificate Information

This certificate is intended for the following purpose(s):

- All issuance policies
- All application policies

Issued to: CCA India 2007

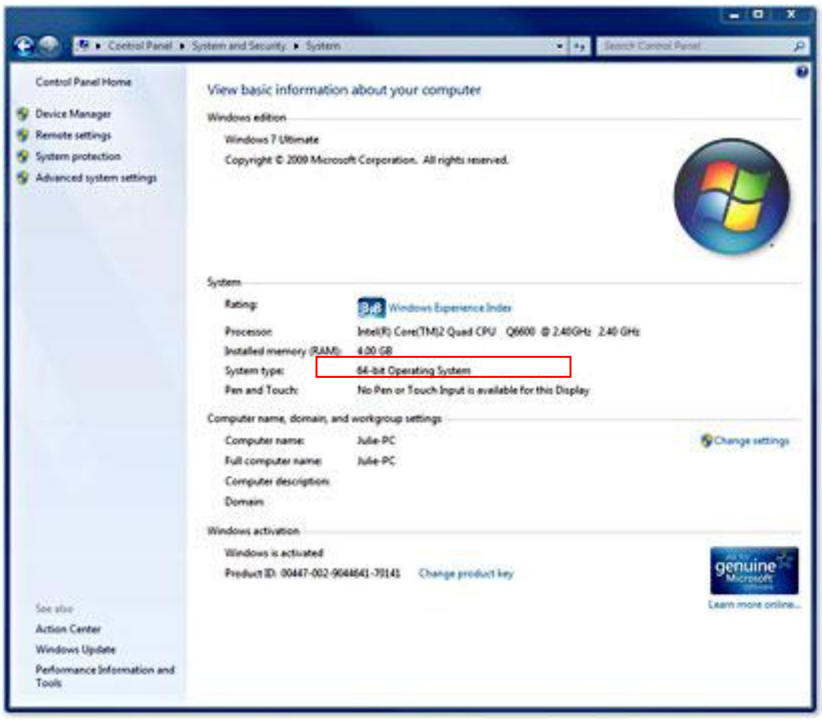
Issued by: CCA India 2007

Valid from 6/13/2007 to 7/4/2015

9. STEPS TO INSTALL CAPICOM.DLL:

The pre-requisites required for the installation of Capicom.dll as already explained above in the point no.5 (v). The installation or registration of CAPICOM.dll varies according to the windows bit versions like 32 bit version or 64 bit version.

- ✓ **For Windows XP, Windows Vista, Windows 7 (32 bit)**
- ✓ **For Windows Vista, Windows 7 (64 bit)**



View basic information about your computer

Windows edition

Windows 7 Ultimate
Copyright © 2009 Microsoft Corporation. All rights reserved.

System

Rating: 3.8 Windows Experience Index
Processor: Intel(R) Core(TM)2 Quad CPU Q6600 @ 2.40GHz 2.40 GHz
Installed memory (RAM): 4.00 GB
System type: 64-bit Operating System
Pen and Touch: No Pen or Touch Input is available for this Display

Computer name, domain, and workgroup settings

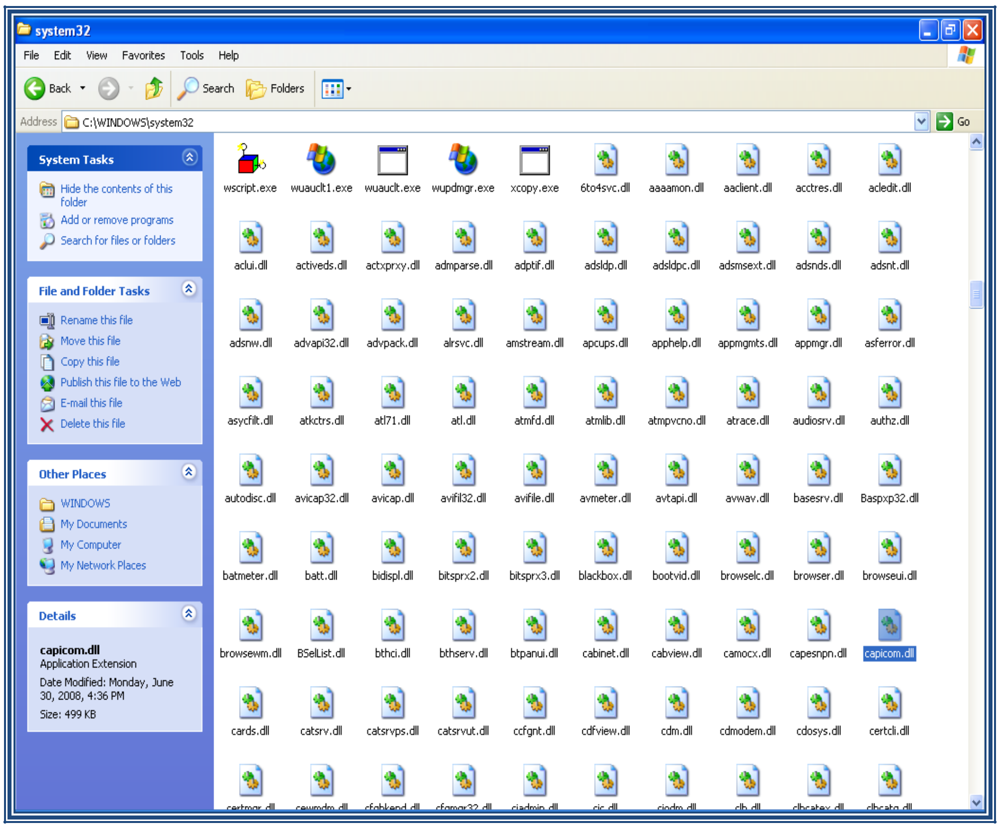
Computer name: Julie-PC
Full computer name: Julie-PC
Computer description:
Domain:

Windows activation

Windows is activated
Product ID: 00447-002-9044641-70141

➢ For Windows XP, Windows Vista, Windows 7 (32 bit)

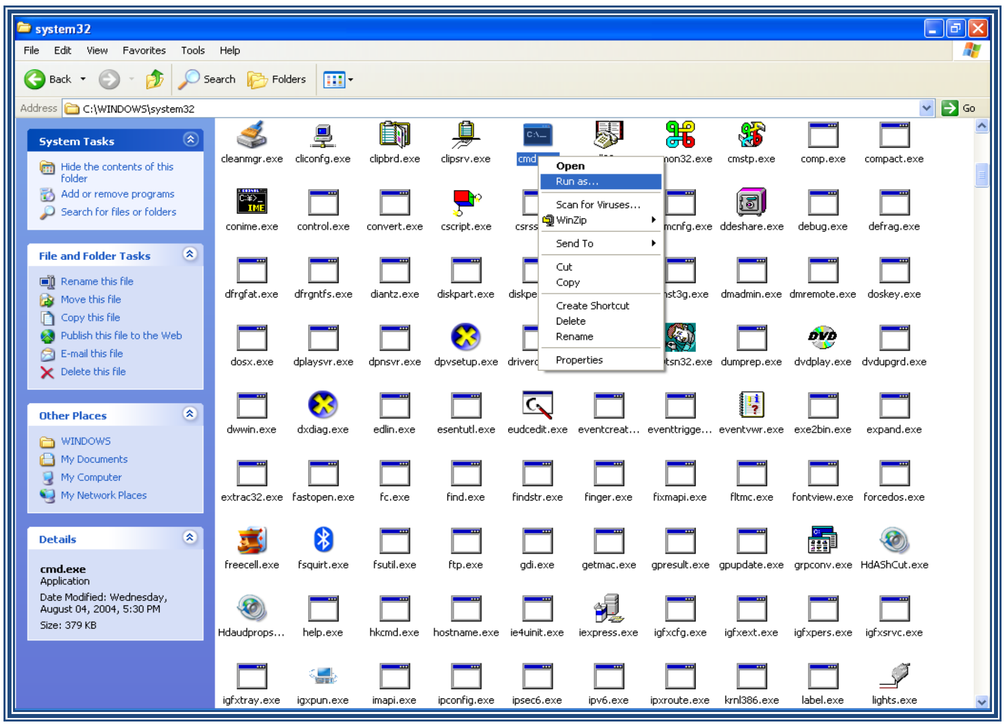
- Go to My Computer/ Local Disk ***(C:) / Windows/ System32***



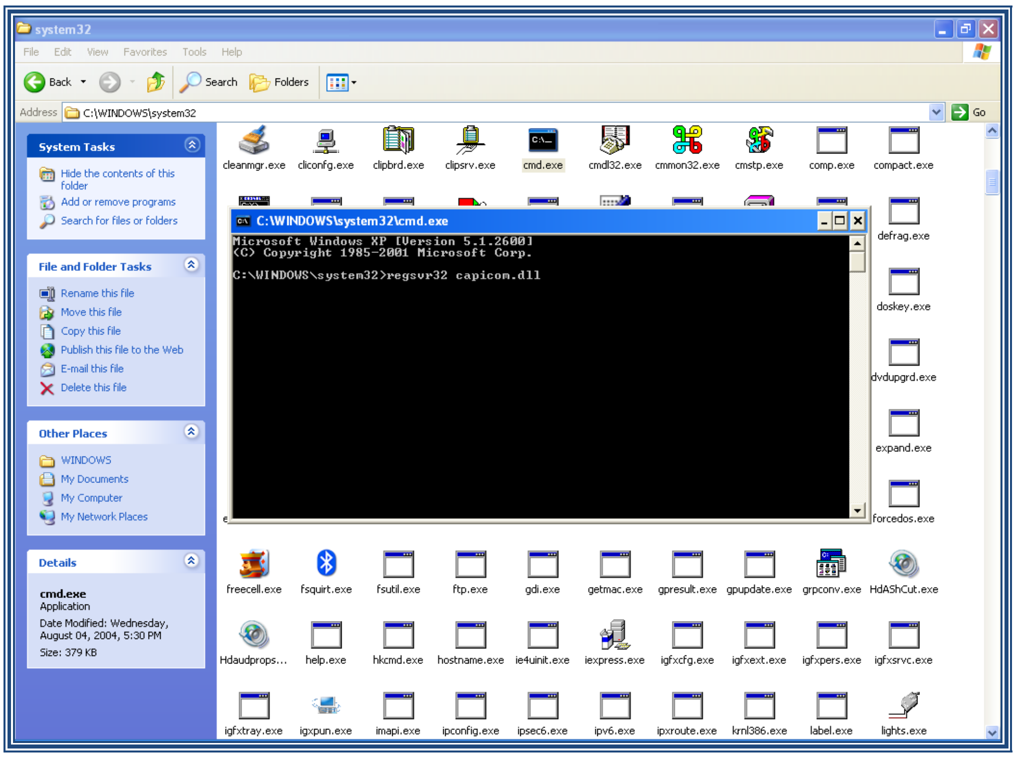
Address C:\WINDOWS\system32

capicom.dll
Application Extension
Date Modified: Monday, June 30, 2008, 4:36 PM
Size: 499 KB

- Search ***CMD*** file.
- Right Click on ***CMD*** file and click on ***Run*** option.



- Type command - ***regsvr32 Capicom.dll***



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>regsvr32 capicom.dll
```

- On clicking the '***Enter***' button, the successful installation message displays.

➢ For Windows Vista, Windows 7 (64 bit)

- Click on windows Start button
- Type ***"%systemroot%\SysWoW64\"*** in the search text box to open system folder
- Copy the corresponding capicom.dll to following folder ***"%systemroot%\SysWoW64\"***

- Open the ***cmd*** prompt in administrator mode
- Goto folder ***"%systemroot%\SysWoW64"*** from ***cmd*** prompt
- Run command ***"regsvr32 capicom.dll"***
- On clicking the ***'Enter'*** button, the successful installation message displays.