

# DIGITAL SIGNATURE TRAINING

A Digital Signature unlike handwritten signature, is used documents or message while transmitting electronically gained the value equivalent of a handwritten signature feature like security, authenticity and long term This Training present an overview of digital

while sending any Today digital signature has due to various unique preservability etc. signature and its usages .



## INSIDE THIS ISSUE:

- What is Digital Signature
- Public Key Infrastructure
- Installation of USB eToken
- Digital Signing of Images
- Digital Signing of PDF
- Digital Signature in Email
- System Configuration
- Trouble Shootings



## Training Vendor

- Balajee CompuSoft P Ltd  
MP Nagar Zone 1 BHOPAL  
MP - 462001
- M.9407532405,9407532406  
,9407532409,9407532411
- Land Line – 0755-4292405
- [www.digitalsignature.net.in](http://www.digitalsignature.net.in)
- [dsc@digitalsignature.net.in](mailto:dsc@digitalsignature.net.in)

**Registration Authority  
of Digital Signatures  
and Software and  
Hardware Supplier**

## RCAI – Root Certificate Authority of India

### Authorised CA - Certifying Authorities



**Guided By –Office of A.P.C.C.F. ( Wing-Information  
Technology), Basement Floor Wing 'D', Satpura Bhawan,  
Bhopal- 462004 Phone No. : (0755) 2674302  
Fax No: (0755) 2555480 E-mail: [apccfit@mp.gov.in](mailto:apccfit@mp.gov.in)**

# PREFACE

---

**E**lectronic signature is a broader term that refers to any electronic data that carries the intent of a signature. A digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, and that it was not altered in transit (tamper-proof). Digital signatures are commonly used for software distribution, financial transactions Document Signing, and in other cases where it is important to detect forgery and tampering.

IT Act 2000/ 2008 (amended) and it also recognizes electronic records, such as, information or any other matter in electronic form. The use of electronic records and digital signatures in Government and its agencies has been approved as a policy matter within the meaning of IT Act. The Govt. of India has started using the Digital Signature across all platforms such as granting of licenses, permits, filing of applications, payment of charges and other financial transactions through electronic means. Both the central and state governments are in the midst of developing full infrastructure for all-round electronic transactions, which will see use of Digital Signature substantially.

This training material titled “**Digital Signature**” provides an overview to the digital signatures, with details about its working, components and classifications. It would surely help the participants how to install and use digital signature in dealing with e-District service delivery in electronic mode.

**Disclaimer:** The information contained herein is subject to change without notice. We shall not be liable for technical or editorial errors or omissions contained herein. The name used in the participant reference material for this course is that of a fictitious company. Any resemblance to any company name is purely coincidental. We do not believe we have used anyone's name in creating this course, but if we have, please notify us and we will change the name in the next revision of the course. Use of screenshots, photographs of another entity's products name, or service in this reference material is only for editorial purposes. No such use should be construed to imply sponsorship or endorsement of the book by, nor any affiliation of such entity. This courseware may contain links and reference from sites on the Internet that are owned and operated by third parties.

---







1. Overview of Digital Signature.....	1 -6
1. Digital Signatures	
2. Digital Signature Versus Handwritten Signatures	
3. Difference between Electronic Signatures and Digital signatures	
4. Overview of how Digital Signatures work	
5. Digital Certificate: Components	
6. Types of Digital Signature Certificate	
7. Legal Validity of Digital Signatures	
8. PUBLIC KEY INFRASTRUCTURE IN INDIA	
9. Procedure for procuring Digital Signature Certificates	
10. Certificate Revocation	
11. Media for Storage of Digital Signature Certificates-	
2. Driver Installation System Setting Java Setting.....	7 -25
1. Mandatory system Checks	
2. How to check which windows is installed in your system	
3. How to check your Internet Explorer version	
4. How to check whether USB Token driver is successfully installed and working in your system? If your USB token not working properly	
5. Do Java Settings!	
6. Finally Set your Internet Explorer now	
7. Change of Token PIN and Unblocking eToken	
3 .Successful Implementations of Digital SignaturesIn eGovernance .....	26 -27
4 . Digital Signing of Images JPEG GIF using p7signer software .....	28 -30
1. Signing of Single image	
2. Signing Bulk images into a folder	
3. Opening Signed image in p7 format	
4. Checking of signer signing authority signature	
5 Signing of PDF Documents .....	30-34
1 Convert image/doc into PDF by Software	
2 Convert image/Doc Online or By email	
3 Digital Signature option positioning of DSC	
4 Attaching image signature with digital signature	
5 Validating DSC in adobe reader	
6 Attaching Digital Signature in Outlook email .....	35
7 Definition and acronym .....	36-37
8 Frequently asked Question .....	38-40
9 References .....	41

## OVERVIEW OF DIGITAL SIGNATURES

### 1.1 Digital Signatures

A digital signature is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and to ensure that the original content of the message or document that has been sent is unchanged. Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time-stamped. A digital signature can be used with any kind of message, whether it is encrypted or plaintext. **Thus Digital Signatures provide the following three features:-**

**Authentication-** Digital signatures are used to authenticate the source of messages. The ownership of a digital signature key is bound to a specific user and thus a valid signature shows that the message was sent by that user.

**Integrity** - In many scenarios, the sender and receiver of a message need assurance that the message has not been altered during transmission. Digital Signatures provide this feature by using cryptographic message digest functions (discussed in detail in section 4.4).

**Non Repudiation** – Digital signatures ensure that the sender who has signed the information cannot at a later time deny having signed it.

### 1.2 Digital Signature Versus Handwritten Signatures

A handwritten signature scanned and digitally attached with a document **does not** qualify as a Digital Signature. A Digital Signature is a **combination of 0 & 1s** created using crypto algorithms.

An ink signature can be easily replicated from one document to another by copying the image manually or electronically. Digital Signatures cryptographically bind an electronic identity to an electronic document and the digital signature cannot be copied to another document. Further, paper contracts often have the ink signature block on the last page, allowing previous pages to be replaced after the contract has been signed. Digital signatures on the other hand compute the hash or digest of the complete document and a change of even one bit in the previous pages of the document will make the digital signature verification fail. As can be seen in the underlying figure, a Digital Signature is a string of bits appended to a document. The size of a digital signature depends on the Hash function like SHA 1 / SHA2 etc used to create the message digest and the signing key. It is usually a few bytes.

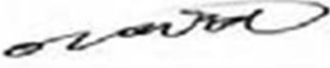
	Handwritten Signature	Digital Signature
Concept		Digital signature using asymmetric encryption / decryption method 1359829394897765839 19293923923939239239 49294994939939993999 9994394939499949994 49399234899434897999
Problem	Reusable	Impossible to reuse

Figure: Handwritten Versus Digital Signatures



### 1.3 Difference between Electronic Signatures and Digital signatures

An **electronic signature** means authentication of an electronic record by a subscriber by means of electronic techniques. An Amendment to IT Act in 2008 has introduced the term electronic signatures. The implication of this Amendment is that it has helped to broaden the scope of the IT Act to include new techniques as and when technology becomes available for signing electronic records apart from Digital Signatures.

### 1.4 Overview of how Digital Signatures work

The Digital Signatures require a key pair (asymmetric key pairs, mathematically related large numbers) called the **Public** and **Private** Keys. Just as physical keys are used for locking and unlocking, in cryptography, the equivalent functions are encryption and decryption. The private key is kept confidential with the owner usually on a secure media like crypto smart card or crypto token. The public key is shared with everyone. Information encrypted by a private key can only be decrypted using the corresponding public key.

In order to digitally sign an electronic document, the sender uses his/her **Private Key**. In order to verify the digital signature, the recipient uses the sender's **Public Key**.

Let us understand how the Digital Signatures work based on an example. Assume you are going to send the draft of a contract to your lawyer in another town. You want to give your lawyer the assurance that it was unchanged from what you had sent and that it is really from you.

1. You copy-and-paste the contract into an e-mail note. Get electronic form of a document ( eg : - word or pdf file)
2. Using special software, you obtain a message hash (fixed size bit string) of the contract.
3. You then use your private key to encrypt the hash.
4. The encrypted hash becomes your digital signature of the contract and is appended to the contract. At the other end, your lawyer receives the message.
  1. To make sure the contract is intact and from you, your lawyer generates a hash of the received contract.
  2. Your lawyer then uses your public key to decrypt the Digital Signature received with the contract.
  3. If the hash generated from the Digital Signature matches the one generated in Step 1, the integrity of the received contract is verified.

### 1.5 Digital Certificate: Components

Contents of Typical Digital Certificate:

- Serial Number: Used to uniquely identify the certificate.
- Subject: The person, or entity identified.
- Signature Algorithm: The algorithm used to create the signature.
- Signature: The actual signature to verify that it came from the issuer.



- Issuer: The entity that verified the information and issued the certificate.
- Valid-From: The date the certificate is first valid from.
- Valid-To: The expiration date.
- Key-Usage: Purpose of the public key (e.g. encipherment, signature, certificate signing).
- Public Key: Public-key encryption uses a key pair for encryption and decryption of data associated with it.
- Thumbprint Algorithm: The algorithm used to hash the public key.
- Thumbprint: The hash itself, used as an abbreviated form of the public key.

**1.6Types of Digital Signature Certificate**

Class of DSC	Assurance Level	Applicability
Class 1	Class 1 certificates shall be issued to individuals/private subscribers. These certificates will confirm that user’s name (or alias) and E-mail address form an unambiguous subject within the Certifying Authorities database.	This level provides a basic level of assurance relevant to environments where there are risks and consequences of data compromise, but they are not considered to be of major significance. This may include access to private information where the likelihood of malicious access is not high. It is assumed at this security level users are not likely to be malicious.
Class 2	These certificates will be issued for both business personnel and private individuals use. These certificates will confirm that the information in the application provided by the subscriber does not conflict with the information in well- recognized consumer databases.	This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial.
Class 3	These certificate will be issued to individuals as well as organizations. As these are high assurance certificates, primarily intended for e- commerce applications, they shall be issued to individuals only on their personal (physical) appearance before the Certifying Authorities.	This level is relevant to environments where threats to data are high or the consequences of the failure of security services are high. This may include very high value transactions or high levels of fraud risk.





## 1.7 Legal Validity of Digital Signatures

The Indian Information Technology Act 2000 (<http://www.mit.gov.in/content/information-technology-act>) came into effect from October 17, 2000. One of the primary objectives of the Information Technology Act of 2000 was to promote the use of Digital Signatures for authentication in e-commerce & e-Governance. Towards facilitating this, the office of Controller of Certifying Authorities (CCA) was set up in 2000. The CCA licenses Certifying Authorities (CAs) to issue Digital Signature Certificates (DSC) under the IT Act 2000. The standards and practices to be followed were defined in the Rules and Regulations under the Act and the Guidelines that are issued by CCA from time to time. The Root Certifying Authority of India (RCAI) was set up by the CCA to serve as the root of trust in the hierarchical Public Key Infrastructure (PKI) model that has been set up in the country. The RCAI with its self-signed Root Certificate issues Public Key Certificates to the licensed CAs and these licensed CAs in turn issue DSCs to end users.

Section 5 of the Act gives legal recognition to digital signatures based on asymmetric cryptosystems. The digital signatures are now accepted at par with the handwritten signatures and the electronic documents that have been digitally signed are treated at par with the paper based documents.

An Amendment to IT Act in 2008 has introduced the term electronic signatures. The implication of this Amendment is that it has helped to broaden the scope of the IT Act to include other techniques for signing electronic records as and when technology becomes available.

## 1.8 PUBLIC KEY INFRASTRUCTURE IN INDIA

PKI is the acronym for Public Key Infrastructure. The technology is called Public Key cryptography because unlike earlier forms of cryptography it works with a pair of keys one of which is made public and the other is kept secret. One of the two keys may be used to encrypt information which can only be decrypted with the other key. The secret key is usually called the private key. Since anyone may obtain the public key, users may initiate secure communications without having to previously share a secret through some other medium with their correspondent. PKI is thus the underlying system needed to issue keys and certificates and to publish the public information. PKI is a combination of software, encryption technologies, and services that enable enterprises to protect the security of their communications and business transactions over networks by attaching so-called “digital signatures” to them.

The Office of the Controller of Certifying Authorities (CCA), has been established under the Information Technology (IT) Act 2000 for promoting trust in the electronic environment of India. The current PKI organization structure in India consists of the Controller of Certifying Authority as the apex body and as the Root Certifying Authority of India (RCAI) (as shown in the figure on PKI Hierarchy). The CCA is entrusted with the following responsibilities : -

- Licensing Certifying Authorities (CAs) under section 21 of the IT Act and exercising supervision over their activities.
- Controller of Certifying Authorities as the “Root” Authority certifies the technologies and practices of all the Certifying Authorities licensed to issue Digital Signature Certificates
- Certifying the public keys of the CAs, as Public Key Certificates (PKCs).
  
- Laying down the standards to be maintained by the CAs.
- Conflict resolution between the CAs
- Addressing the issues related to the licensing process including:
  - a) Approving the Certification Practice Statement (CPS);
  - b) Auditing the physical and technical infrastructure of the applicants through a panel of auditors maintained by the CCA.

The RCAI is responsible for issuing Public Key Certificates to Licensed Certifying Authorities (henceforth referred to as Certifying Authorities or CA). The CAs in turn are responsible for issuing Digital Signature



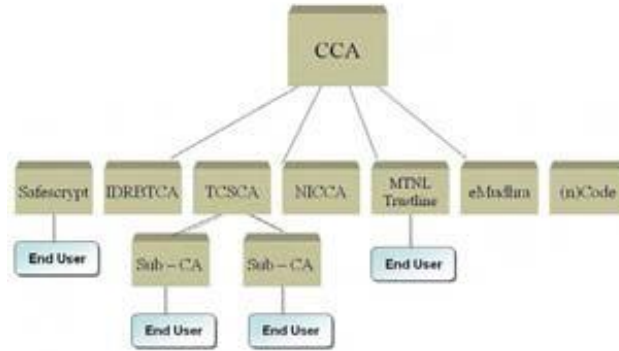
Certificates to the end users. In order to facilitate greater flexibility to Certifying Authorities, the CCA has allowed the creation of sub-CAs. As per this model, a Certifying Authority can create a sub-CA to meet its business branding requirement. However the sub-CA will be part of the same legal entity as the CA.

The sub-CA model will be based on the following principles:

The CAs must not have more than one level of sub-CA

A sub-CA certificate issued by the CA is used for issuing end entity certificates

A CA with sub-CA must necessarily issue end entity certificates only through its sub-CA. The only exception will be for code signing and time stamping certificates, which may directly be issued by the CA.



### 1.9 Procedure for procuring Digital Signature Certificates

The CCA has licensed seven Certifying Authorities in India to issue Digital Signature Certificates to the end users. The National Informatics Centre issues Digital Signature Certificates primarily to the Government/ PSU's and Statutory bodies. The Institute for Development of Research in Banking Technology (IDRBT) issues Digital Signature Certificates primarily to the banking and financial sector in India. The remaining five CAs - Safescript, TCS, MTNL, n(Code) Solutions and Digital Signature issue Digital Signature Certificates to all end users across all domains. More than **16 lakh** Digital Signature Certificates have been issued by the different CA's in our country at the time of publication of this document.

#### Steps for Getting an individual Digital Signature Certificate

DSC Form **can be downloaded** from website of the CA

For **Class 3 certificate**, the applicant has to submit the **completed forms in person** at the RA

On successful processing by the RA, the **Username and password** are sent to applicant mailbox in order for him/her to log onto CA website. The **cryptographic device** is handed over to the user for storing the private key.

The **applicant installs the device drivers** for the device (for storing the private key) from CA website.

For example:- crypto token, smart card reader

User **generates the key pair** and uploads his **Certificate Signing Request (CSR)** request into his/her account on the CA Website

CA **generates the DSC** after verification. The user downloads from his/her account on the CA website.

### 1.10 Certificate Revocation

Digital Signature Certificates are issued with a planned lifetime, which is defined through a validity start date and an explicit expiration date. A certificate may be issued with a validity of upto two years. Once issued, a Certificate is valid until its expiration date.

However, various circumstances may cause a certificate to become invalid prior to the expiration of the validity period. Such circumstances include change of name (for example, change the subject of a certificate due to an employee's change of name), change of association between subject and CA (for example, when an employee terminates employment with an organization), and compromise or suspected compromise of the corresponding private key. Under such circumstances, the issuing CA needs to revoke the certificate.

In case a Digital Signature Certificate is compromised, one should immediately contact the respective CA



to initiate revocation. The CA will then put the certificate in the Certificate Revocation List. We need to have necessary processes in place defining the roles and responsibility of various government officials for the usage of Digital Signature and their revocation.

**1.11 Media for Storage of Digital Signature Certificates- PIN protected soft tokens: We Provided FIPS Level 2 Compliant ePass 2003** It is recommended to store the private key on secure medium, for example, smart cards/ crypto tokens etc. The crypto token connects to the user computer through the USB interface. For smart cards a compatible smartcard reader needs to be installed on the user computer if not already present. The secure media available for the storing the private key may vary per each Certifying Authority.

**The Private key generated is to be Password protected and kept secret.** The responsibility of the secrecy of the key lies with the owner. The key can be secured using:

**We Provide ePass 2003 eToken and a name Label Chain to Identity it**



- Auto Plug & Play- No CD required for Driver Installation.
- Supported OS: 32bit and 64bit Windows XP SP3, Server 2003 , Vista, Server 2008, Seven, Eight,
- 32bit and 64bit Linux and MAC OS X
- FIPS 140-2 Level 3 Certified and Cap for each USB Token is Included.
- Memory Space: 64KB (EEPROM) - Can store around 7-10 DSC. and Connectivity: USB 2.0 full speed, Connector type A
- Laser Printed Serial Number on each token.

Make NOTES ----




Make NOTES ----

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

2 Table of Contents

1. Mandatory system Checks ..... 3
2. How to check which windows is installed in your system?..... 3
3. How to check your Internet Explorer version?..... 4
4. How to check whether USB Token driver is successfully installed and working in your system? ..... 4
5. If your USB token not working properly..... 5
6. Do Java Settings!..... 10
7. Finally Set your Interneplorer ow. .... 13



(Please Note that we are not responsible if you delete your certificate in USB Token by your any act while following this guide. So do not click on any option which lead to initialize or format of your DSC in USB Token)

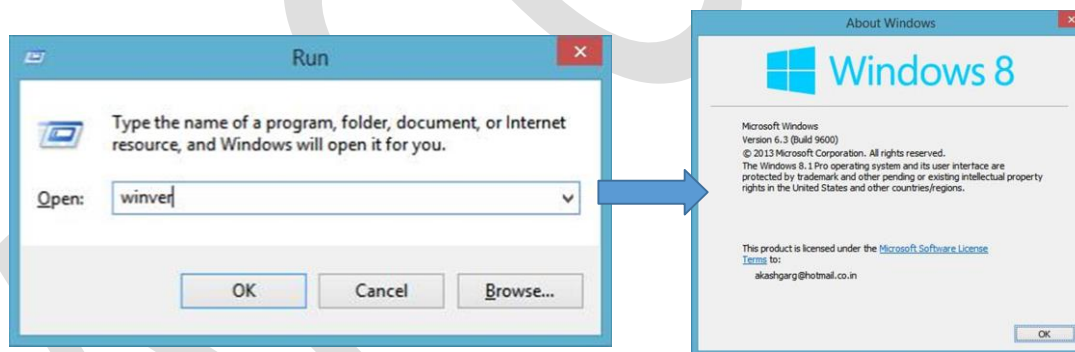
Follow the below procedure to resolve common issues while working with Digital Signature Certificates in USB Tokens on various web portals such as Income Tax e-Filing, MCA Web portal, yourself.

#### 1. Mandatory system Checks

- a. Windows XP Service Pack 3, Windows Vista, Windows 7 or Windows 8.
- b. Internet Explorer 6, 7, 8, 9 or 10. USB Tokens might not work on IE 11.
- c. USB Tokens do not work on Google Chrome or Mozilla Firefox.
- d. Only Latest Java version should be installed in your system.
- e. Always use Administrator User not limited user in your PC while working with USB Tokens.
- f. Make ensure that your USB Token software is installed properly and working fine.

#### 2. How to check which windows is installed in your system?

- a. Click Start > Run (Windows Key + R) b.
- In the Run dialog box, type winver c.
- Click on Ok
- d. A dialog box will display the version of your windows.



OR

Right click on "My Computer/ This PC" and click on properties. You can check your windows full details.

3. How to check your Internet Explorer version?

- a. Open IE in your system.
- b. Go to Help Tab> About Internet Explorer (or Press Alt + H + A).

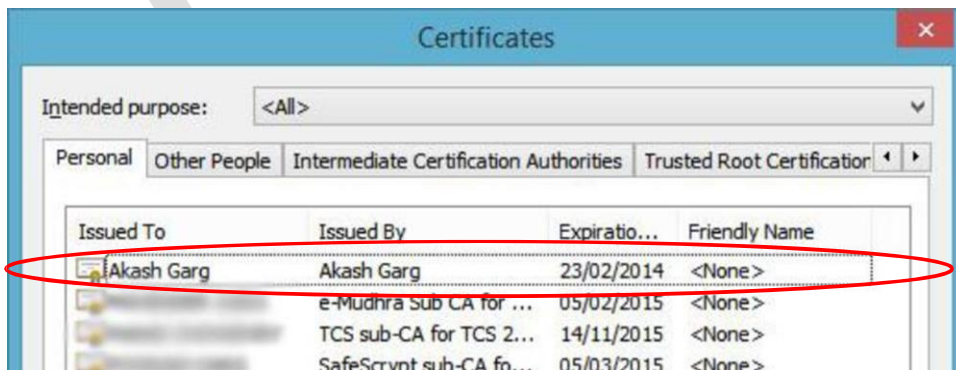


4. How to check whether USB Token driver is successfully installed and working in your system?

- a. Insert USB Token in any USB port.
- b. Wait for a while till computer recognizes and reads your USB Token.

Now open Internet Explorer Browser.

- d. Go to Tools> Internet Options (or just press Alt + T + O)
- e. Navigate to Content Tab > Certificates.
- f. If you can see your Digital Signature Certificate name here, then your USB Token is working fine. Otherwise install your USB Token driver first and then proceed with this point again.



5. If your USB token not working properly.

Driver location – [www.digitalsignature.net.in/forestit/](http://www.digitalsignature.net.in/forestit/)

Follow below steps for your ePass 2003 or ePass 2003 Auto USB tokens.

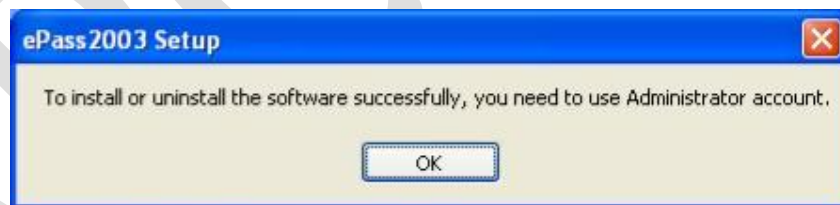
- a. Firstly identify your ePass USB Token. First one is ePass 2003 Token (Blue Colour) and other one is ePass 2003 Auto Token (Purple Colour). You can see the name clearly written on them.



- b. To install driver for above USB Tokens In your PC successfully, you need to use administrator account. You can easily check this in control panel for your user.
- c. ePass 2003 USB Token requires one time installation of a software on a PC of around 1 MB. If you have a CD with you, you can use it or otherwise you can download it from our website from the following link. <https://www.dropbox.com/s/het88bsopa28ax5/ePass2003-Setup-Latest.zip?dl=0>
- d. ePass 2003 Auto USB token has inbuilt driver in it and will install it automatically in your system if Auto-run or Auto-play is enabled in your system.

(Please note that the driver for ePass 2003 and ePass 2003 Auto is same. So if you install it by any means in your PC, you will be able to use any of the two tokens in your PC.)

- e. Now when you install ePass 2003/ ePass 2003 Auto setup, The following window may appear:



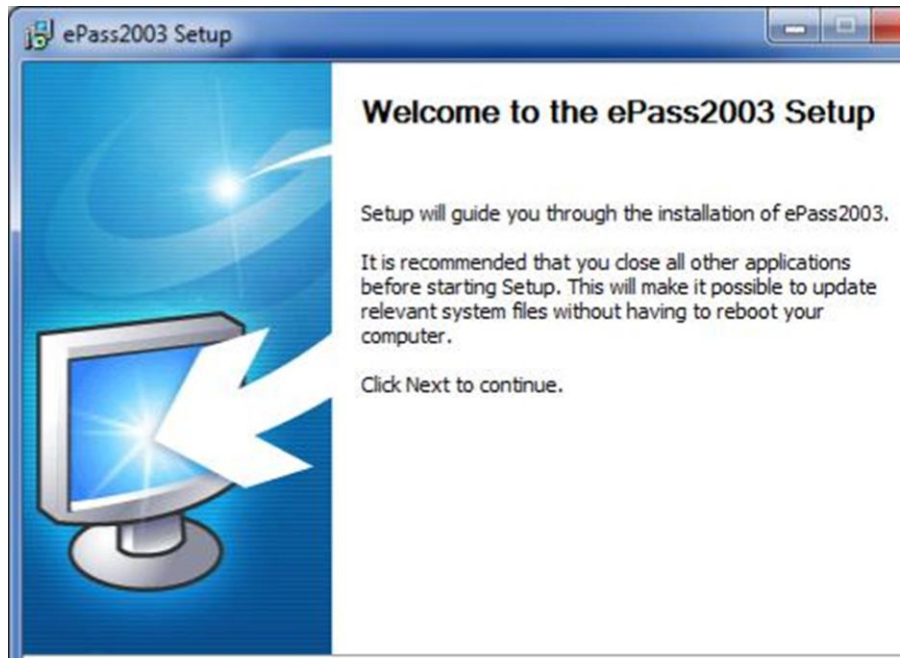
If it is so, then please logon it to your Admin user and then try to install it again. f.

When you install ePass 2003 with Admin User, following interface will appear:

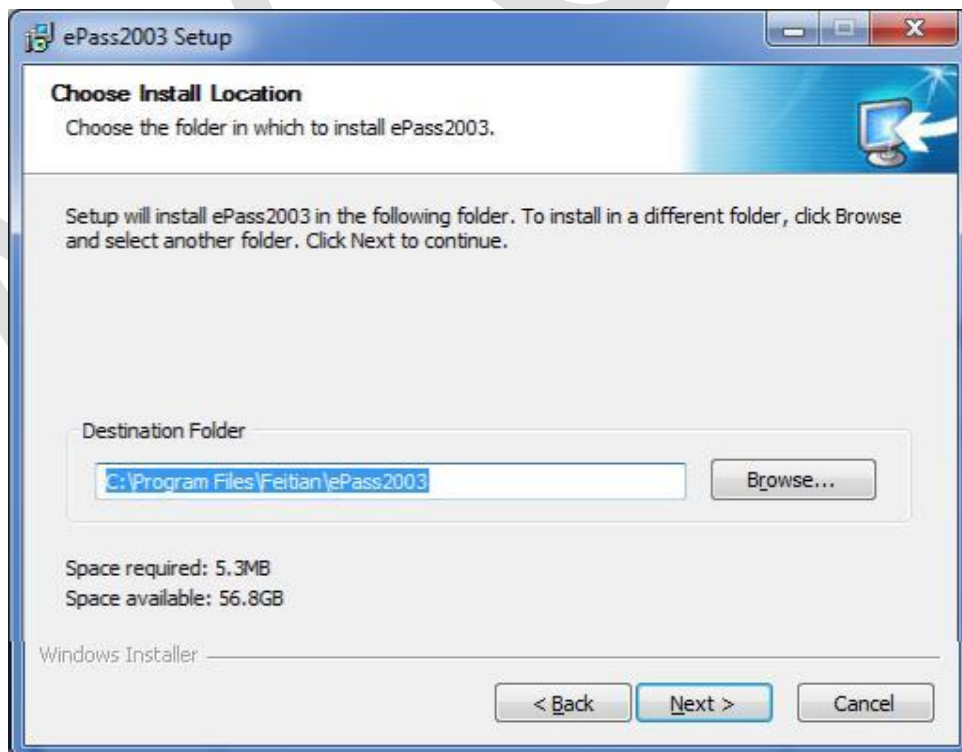




- g. After select language, click "OK", the following welcome interface appears:

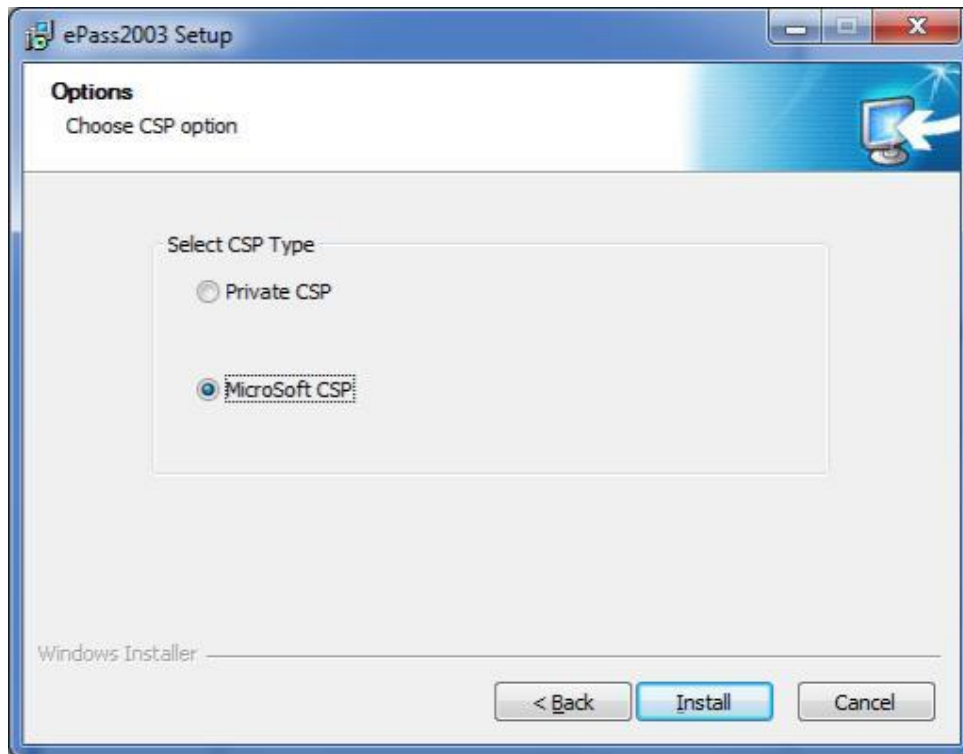


- h. Click "Next", the following select install path interface appears:





- i. Click "Next", the following choose CSP interface appears:



- j. You have to select **MicroSoft CSP** only.
- k. After selecting MicroSoft CSP, click "Install" to continue, the following interface appears after installation:



- I. Now the following two possible problems can be faced while installing this ePass 2003/ ePass 2003 Auto Software.
  - i. MicroSoft CSP option is not enabled or you cannot select it.
  - ii. Even you have installed the software successfully, still you are not able to see your Digital Signature name in Internet Options > Tools > Content > Certificates. (as described in point no 4. Above)

Solutions for both are as follows:

i. MicroSoft CSP option is not enabled.

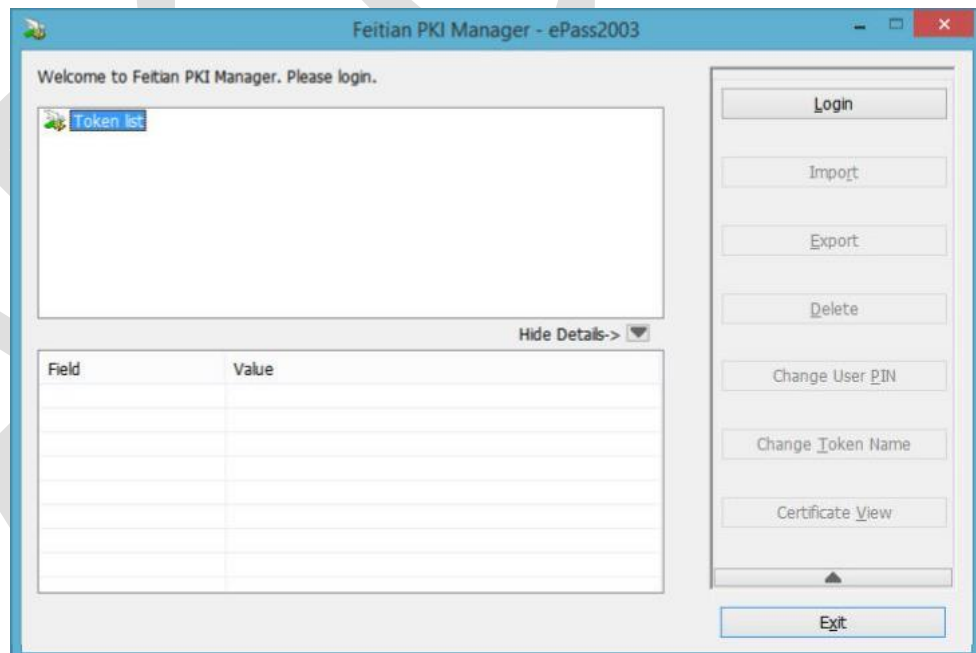
- This error generally occurs in some XP windows system. Stop the installation of your ePass 2003 Setup here and exit the setup.
- You need to install an additional patch (setup) for your windows. For 32 Bit system [Click here to download](#)  
For 64 Bit system [Click here to download](#)

(You can check your system bit using following link or can follow Point No. 2 of this document. <http://support.microsoft.com/kb/827218>)

- After installing above patch, try again to install ePass 2003 setup. Now you will be able to select MicroSoft CSP.

ii. Even after successful installation of your ePass driver, your token not working properly.

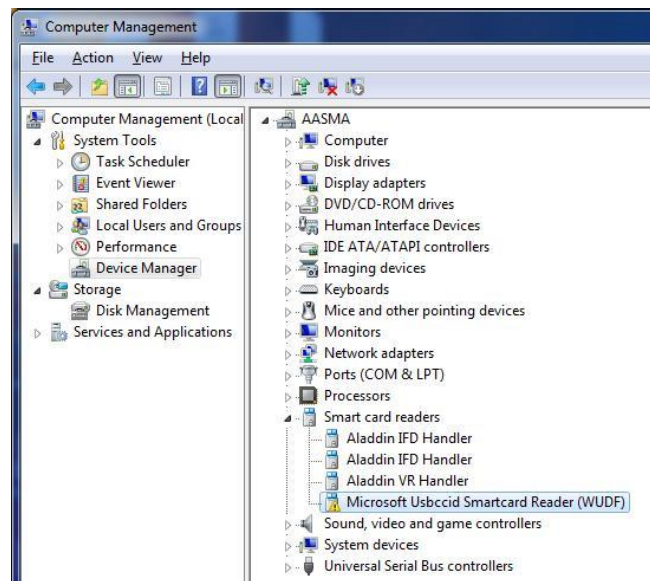
You may face this possible issue – When you open ePass 2003 / ePass 2003 Auto software after installation of it and insert your USB Token in your PC, after waiting for a while, you are not able to view your token name in Token list. The following screen may appear in this situation.



Now Close this window and do not remove the USB Token from your PC.

Now this may be tricky one for you. The procedure to solve this issue is quite different, so suggest you to follow our instructions very carefully.

- Right Click on My Computer or This PC on your Desktop and select Manage > Device Manager.



- You must be seeing an option with a yellow critical symbol. The name may be Microsoft Usbccid Smartcard Reader (WUDF) as you can see in image above or it can be USB Token or ePass 2003 USB, etc. The name must be related to your Token only.
- Select it and then Right Click on it.
- Go to Properties > Driver > Update Driver.
- When prompted, Select Browse option and do not select Search Automatically option.
- Then Browse to My computer > C:\ Drive > Program Files > Feitian > ePass 2003 > CCID.
- Select CCID and then click Ok and Finish the process.
- The system will automatically update the driver for ePass 2003 / ePass 2003 Auto USB Tokens. And
- then you will be prompted to install a certificate of CCA, please install it and do not cancel it. Your
- problem must be resolved and now you can also see your DSC in Internet Explorer also.
- You will also be prompted for Change user pin as below:

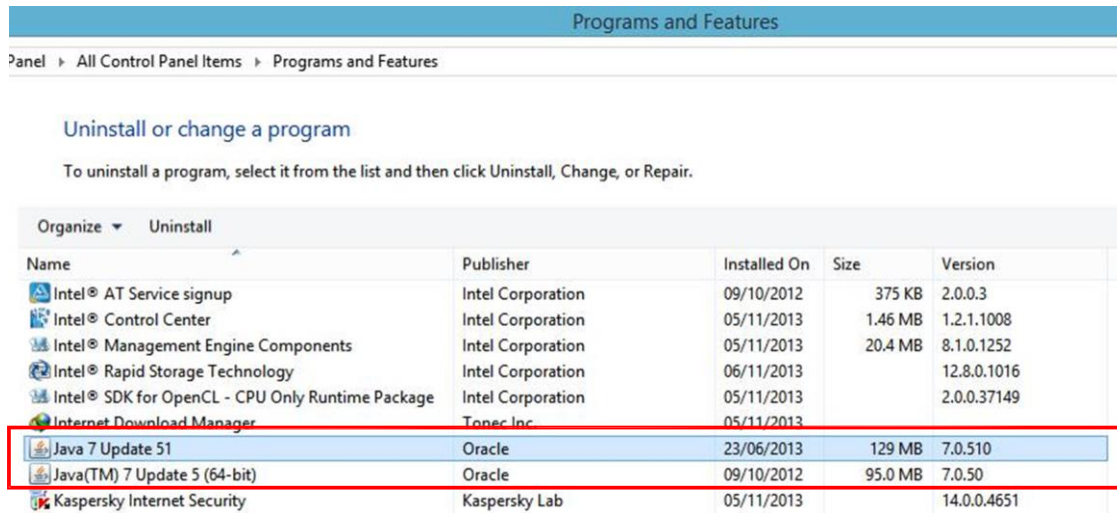


We suggest you not to change it as in any case if you forget your PIN then your USB Token will be blocked after entering wrong PIN 10 Times. Then you will have to send it to us for unblock if possible.

Also do not initialize the USB Token ever in ePass 2003/ ePass 2003 Auto software as it will delete and format your USB Token permanently and we do not have the backup for it. In that case you have to apply for new one with same procedure as you have followed before.

## 6. Do Java Settings!

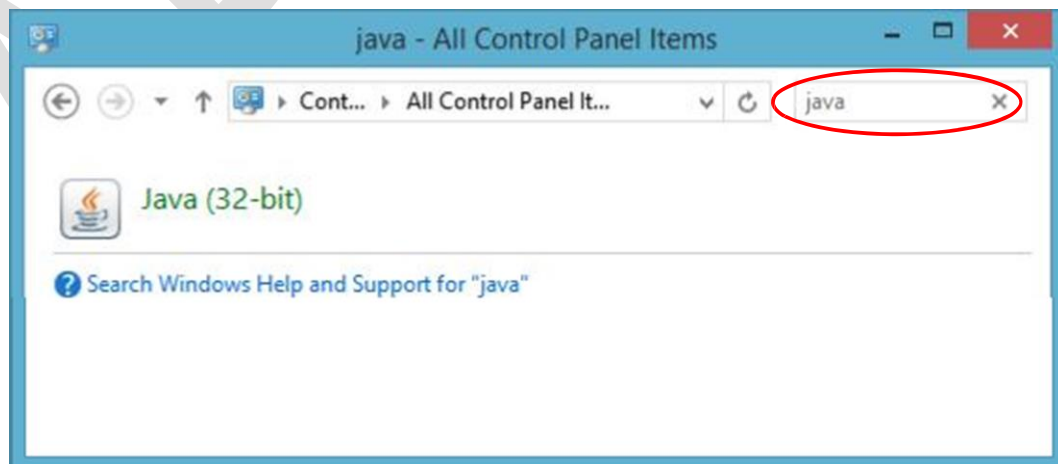
- a. Firstly check which versions of JAVA are installed in your system.
- b. Open Control Panel > Add/remove program or Uninstall a program.
- c. A list will open in a dialog box.
- d. Search for all Java Versions installed in your system.



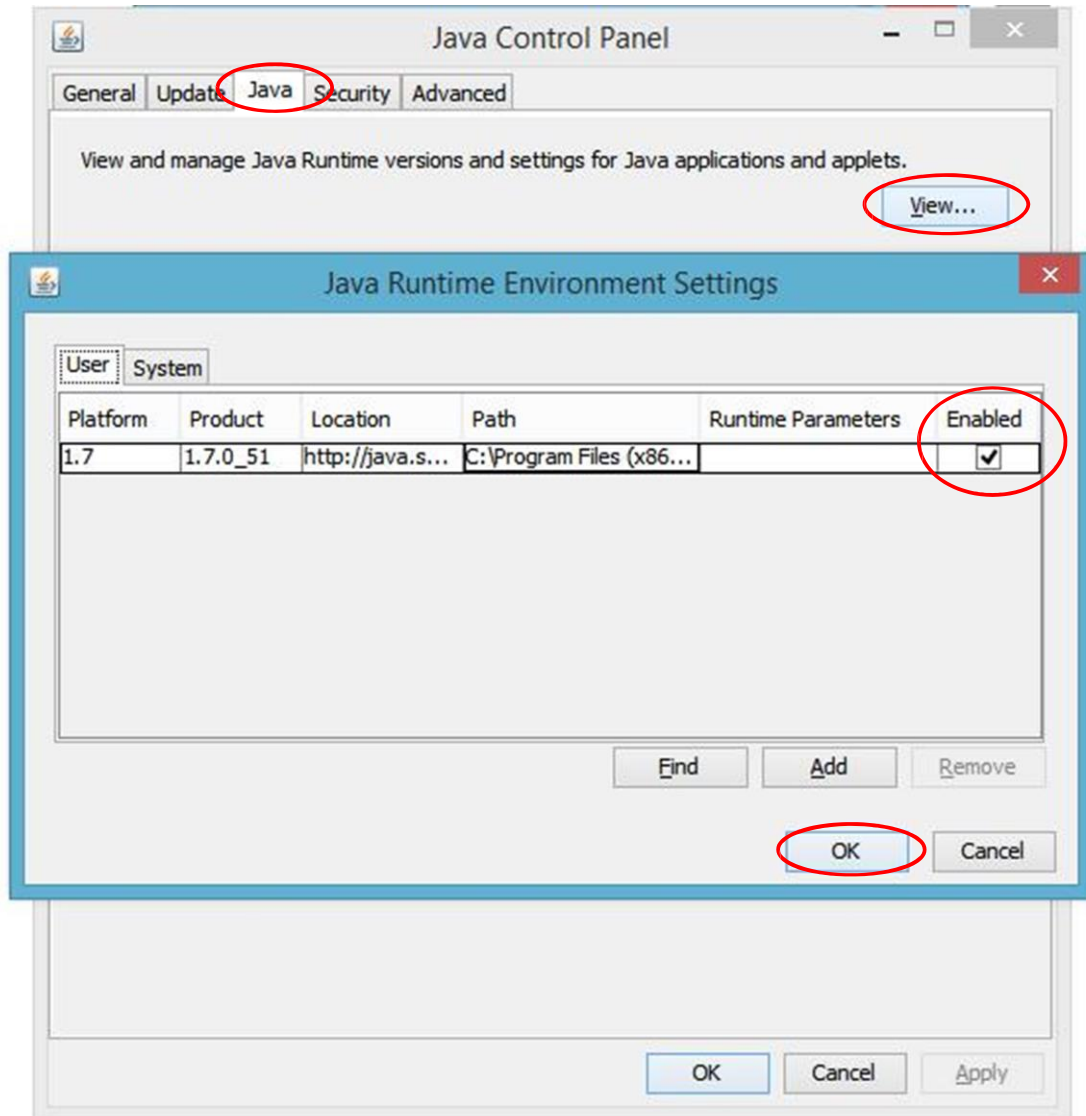
- e. If there is more than one JAVA installed, remove all JAVA versions from your system by uninstalling all of them.
- f. After uninstalling all java, download and install latest java version of 32 bit only. It does not matter if your system is 64 bit. At present latest JAVA is JRE 7 update 51.
- g.

Then restart your system.

- h. After restart, open Java in control panel.
- i. Double Click on Java (32-bit) icon. A dialog box will appear



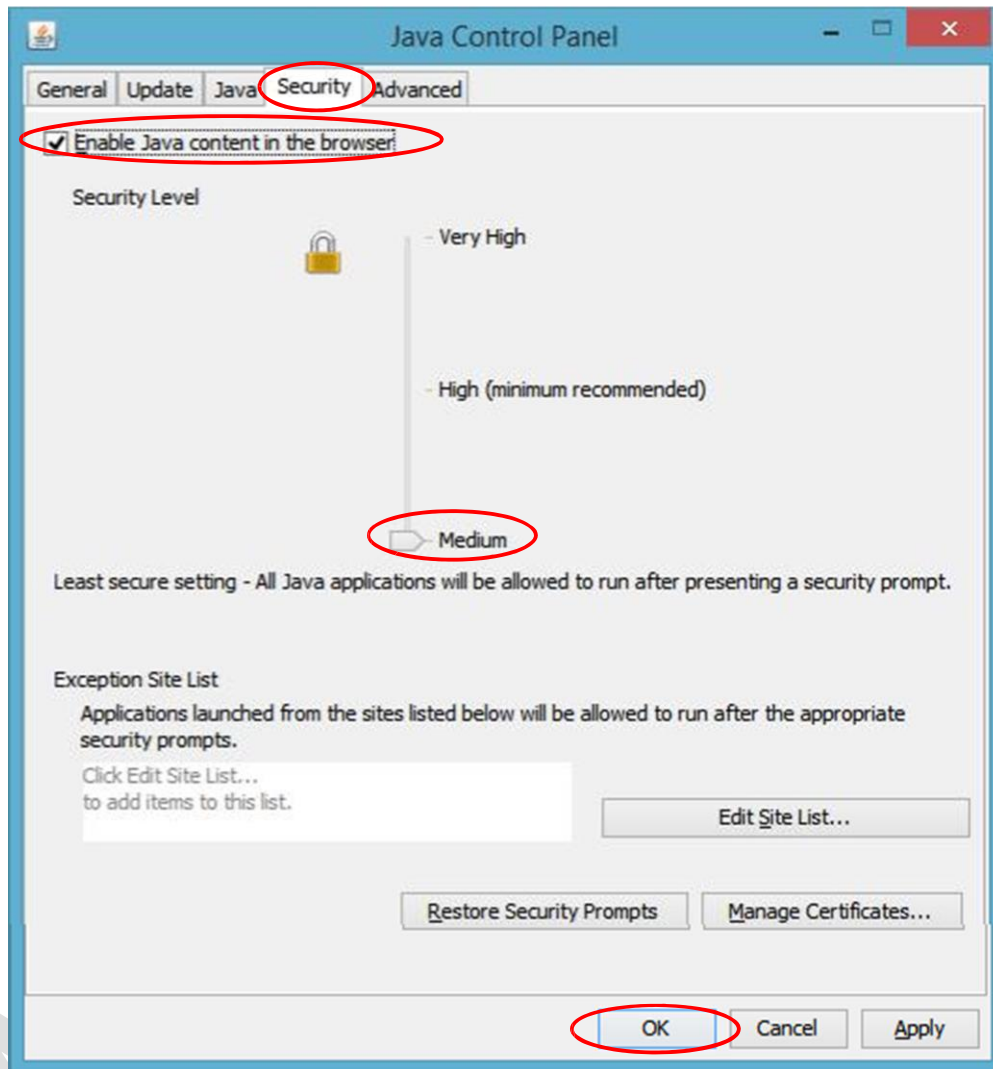
- j. Click on Java Tab > View button.



- k. You must see latest java version in the list. It should be enabled.

(If you still see more than one Java version or old Java versions, then you might not have uninstalled all Java Versions completely. So suggest you to repeat point no 6 again carefully.)

1. Click OK and now click on Security Tab. Java Content in the browser should be enabled and Drag security level to medium. Click Apply and OK.

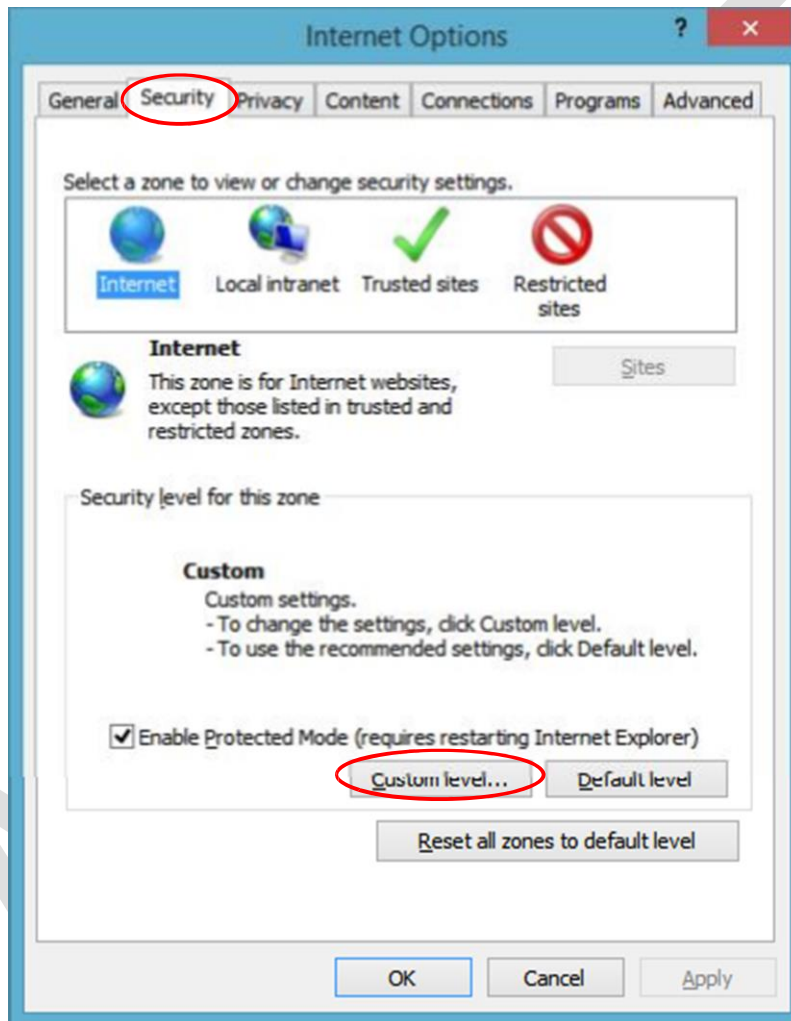


m. Your JAVA settings are now done!

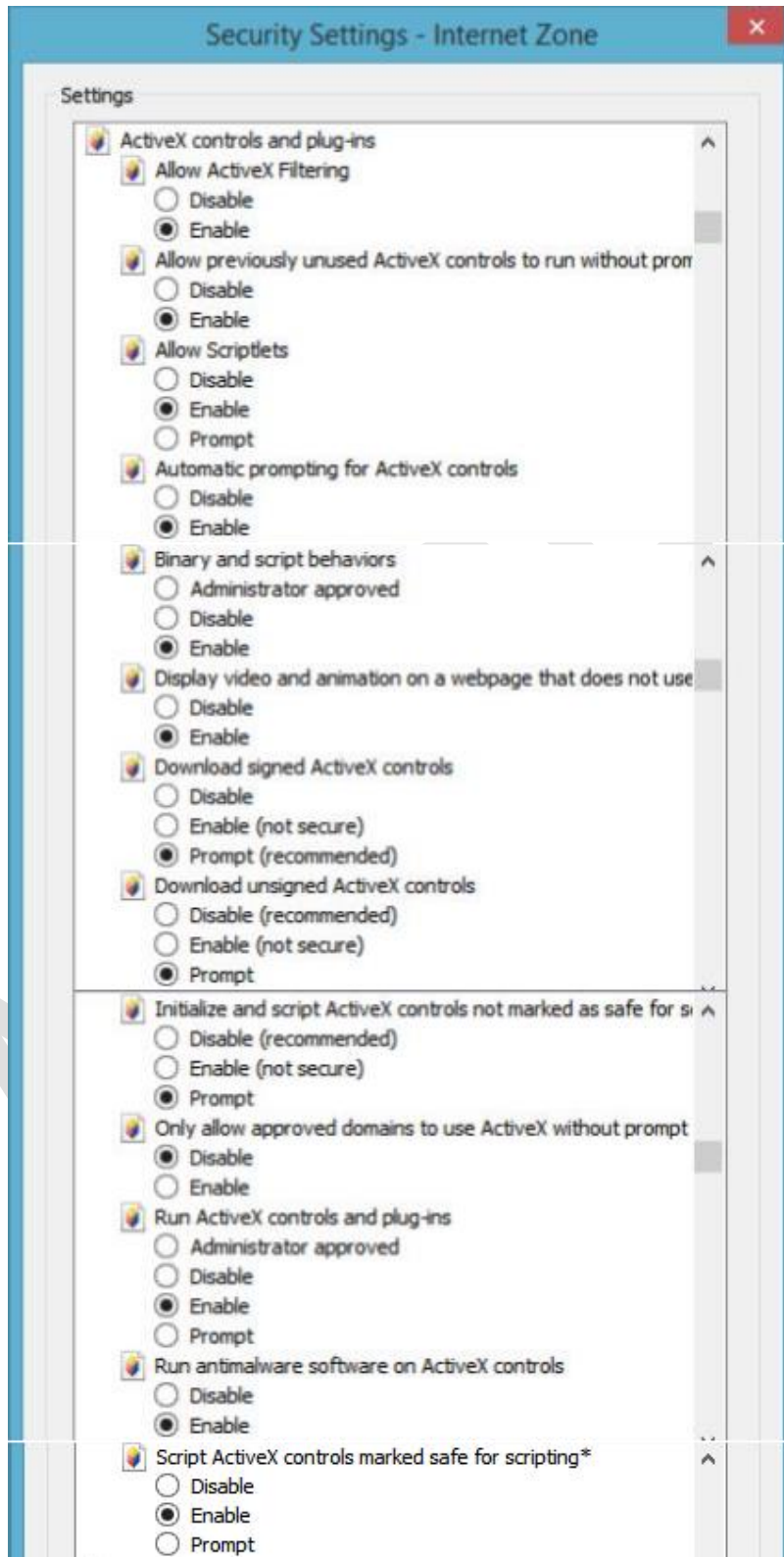
Make NOTES ----

7. Finally Set your Internet Explorer now.

- a. Open internet explorer.
- b. Open Internet Options in Tools menu (or simply press Alt+T+O)
- c. Go to security Tab.
- d. Click on custom level.

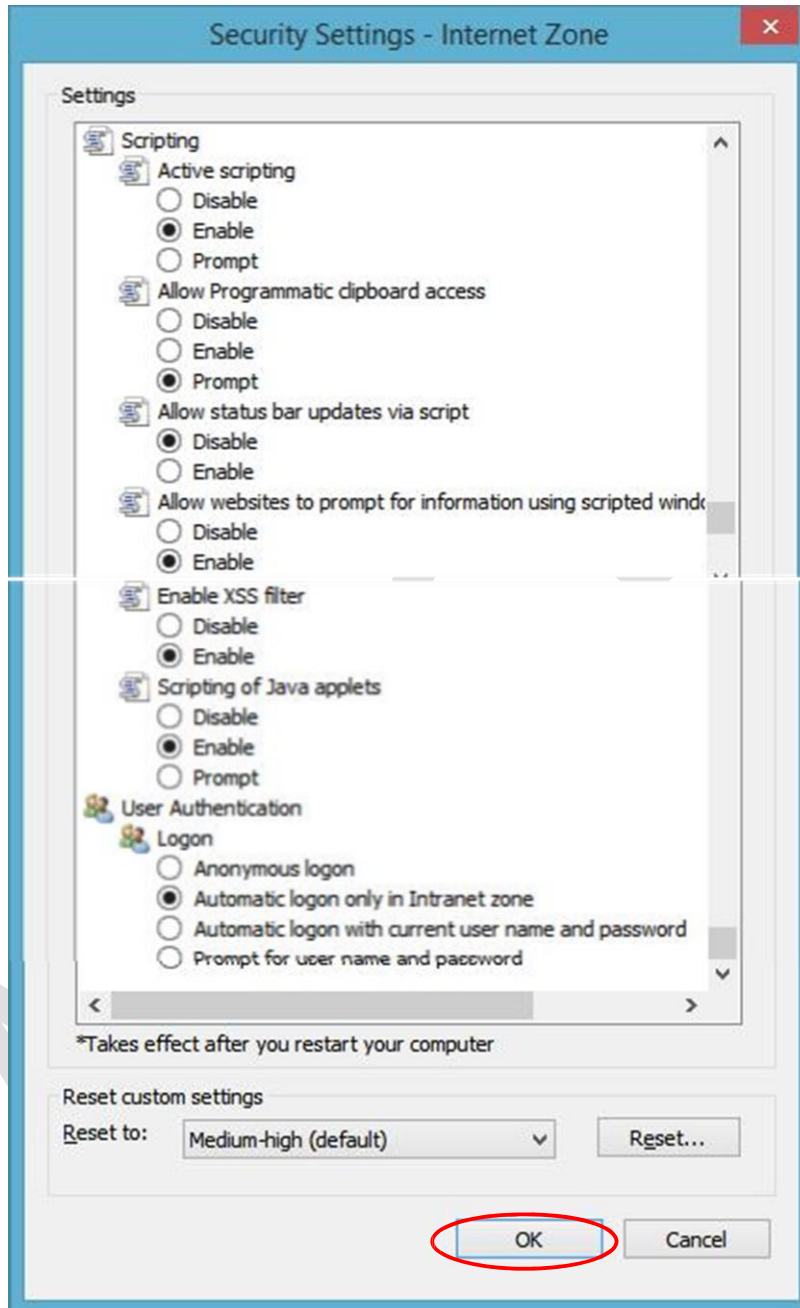


f. Set all ActiveX controls and plug-ins options as selected in screenshots below.



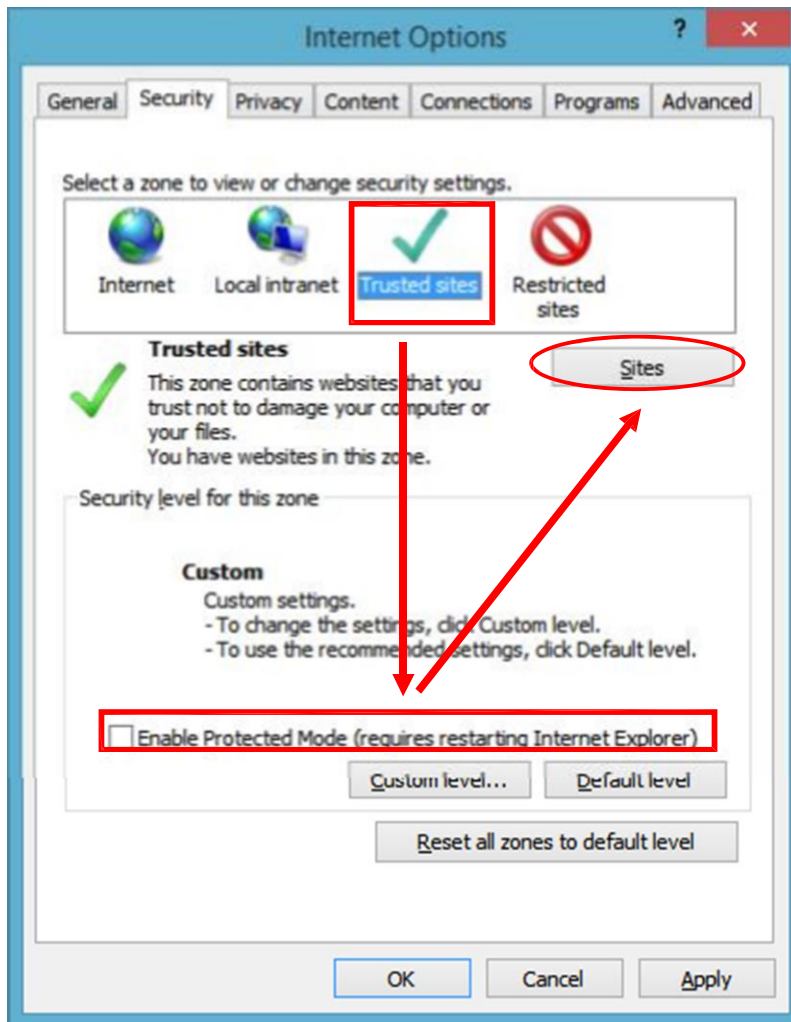


- g. Now Scroll down to Scripting options in same dialog box and set all as below:



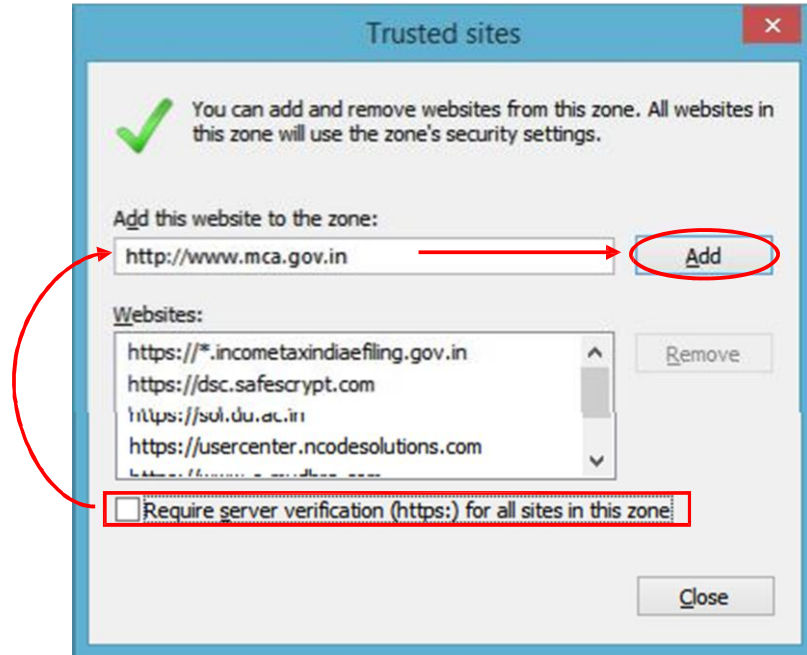
- h. Now Press OK.  
i. Click Yes to the Warning Message "Are you sure to change the security settings for this zone", if prompted.  
j. Click on Apply Button.

- l. Un-tick Enable Protected Mode option.
- m. Then click on Sites Button.



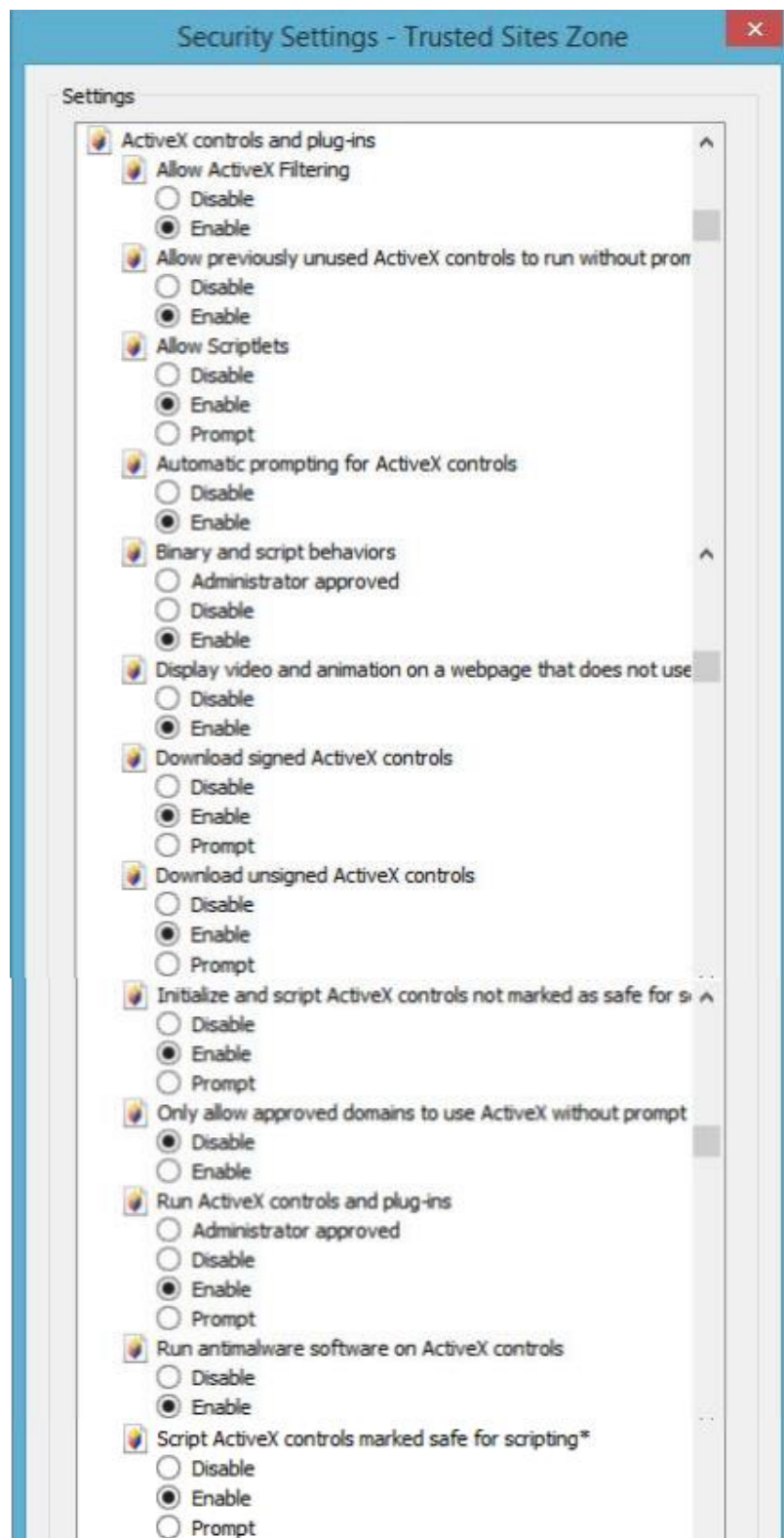
Make NOTES ----

- n. Here, Firstly un- tick “Require server verification (https:) for all sites in this zone” option
- o. Then add the full name of website where you are using your Digital Signature Certificates and Click Add Button. Then close this box.

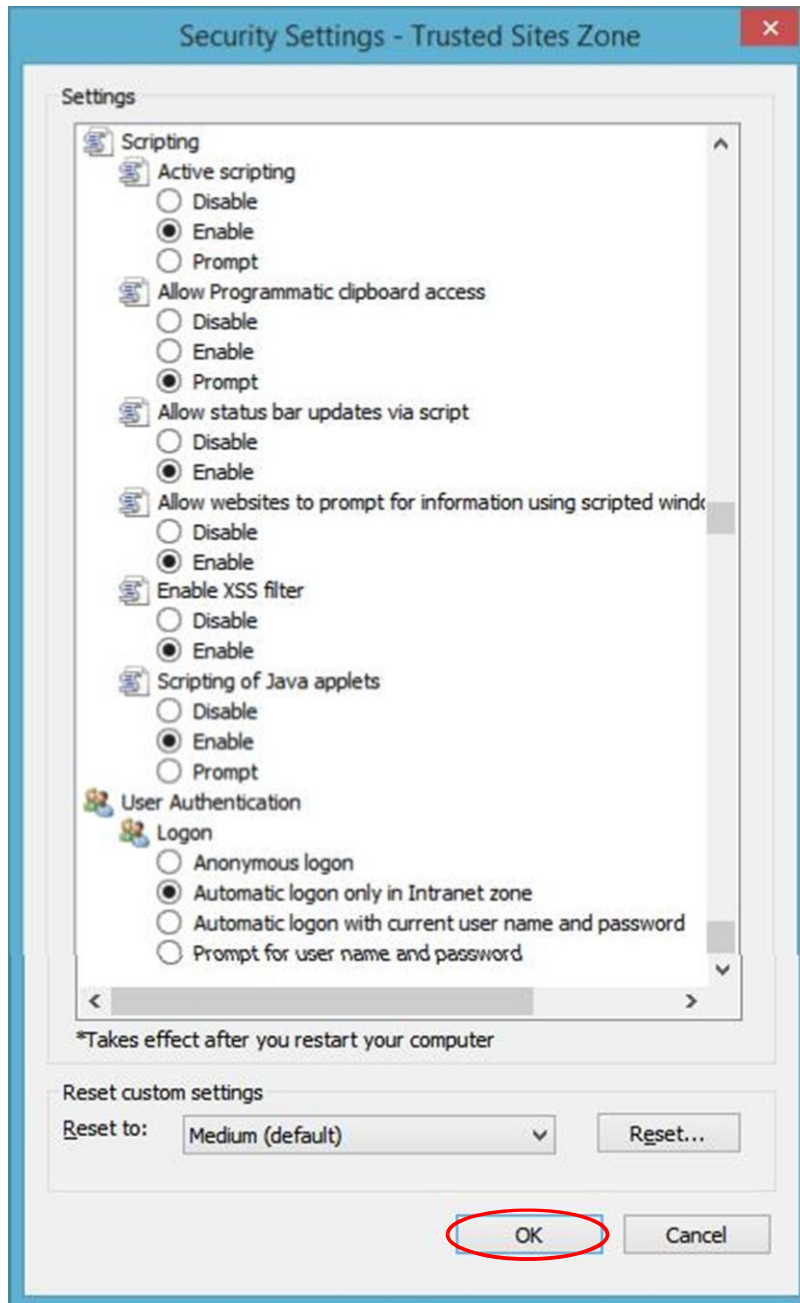


Make NOTES ----

- p. Click on custom Level Button.
- q. Scroll down to ActiveX controls and plug-ins again.
- r. Set all ActiveX controls and plug-ins options as selected in screenshots below.



- s. Now Scroll down to Scripting options in same dialog box and set all as below:



- t. Now after doing all setting as shown in images above, click on OK
- u. Click Yes to the Warning Message "Are you sure to change the security settings for this zone", if prompted.
- v. Now Finally Click on Apply and then OK.

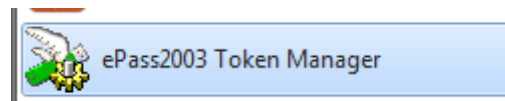


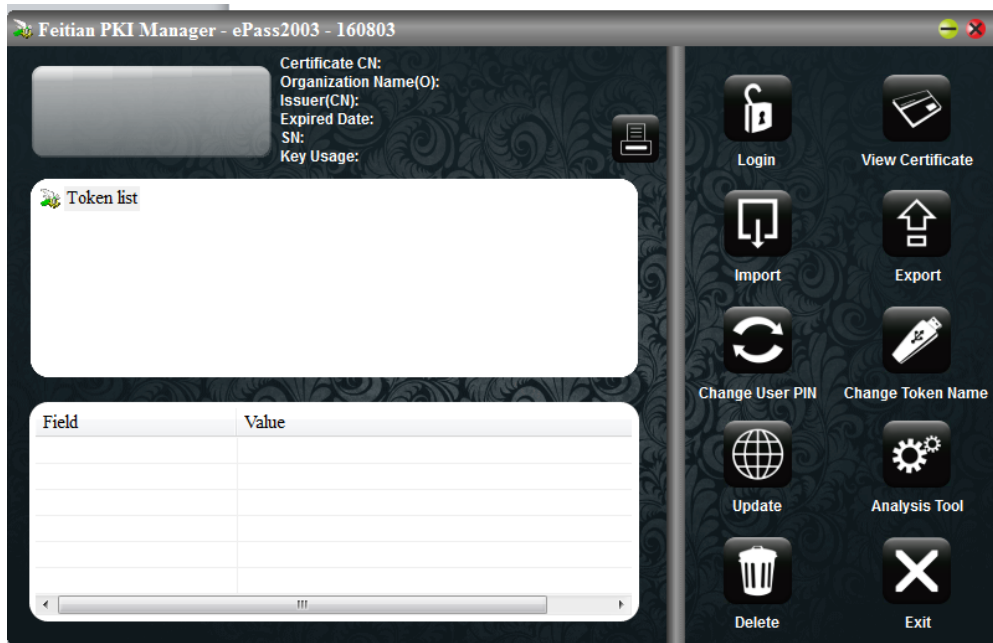
Now you have to restart your system again and hopefully your most of the issue regarding non-working of any USB token is resolved now.

Email us with screenshots of your problem if it still persists or Contact us with full details of your Digital Email ID is [dsc@digitalsignature.net.in](mailto:dsc@digitalsignature.net.in)  
Raise a Ticket atomically when you email here

#### OPEN THE TOKEN MANAGER TO SET PASSWORD AND CHECK THE DIGITAL SIGNATURE

1. Click the ICON to OPEN Token Manager





## You Can Change Token Pin and Name if Desired

What if etoken is Blocked ?

THERE ARE LIMITED USAGE AT A TIME 5 CONSECUTIVE WRONG PASSWORD WILL BLOCK YOU ETOKEN  
 CONTACT THE SUPPLIER TO UNBLOCK THE ETOKEN  
 USE REMOTE SOFTWARE LIKE AMMY ADMIN OR TEAMVIEWER TO HAVE HELP  
 DROP A EMAIL [dsc@digitalsignature.net.in](mailto:dsc@digitalsignature.net.in) to raise Ticket

What if the etoken is Stolen or Compromised ?

In Case token is lost or compromised Please drop email at [dsc@digitalsignature.net.in](mailto:dsc@digitalsignature.net.in) with the Approval from APCCFIT to Block and revoke the etoken

Step: 8 You can also view the details of the certificate by opening the Feitian PKI Manager as shown in the figure below:

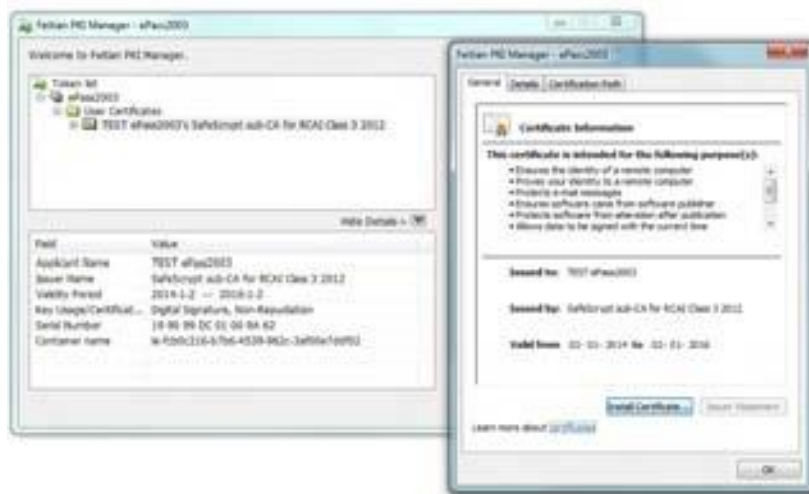


Fig. 1.25: Certificate details from the Feitian PKI Manager ePass 2003

**E**-Governance is at the center of Digital Transformation for Governments and digital signatures can enable Digital Transformation by making Government to Citizen services and vice versa completely paperless.

The following are the lessons learnt and the road ahead suggested for implementation of digital signatures in the e-Governance programmes:-

The digital signature implementation must be end to end available without any dependency on proprietary OS.

The verifications must happen on the local application servers, else the implementation model may fail in the remote applications in the rural landscape.

The State Government needs to develop its own franchisee model for management of digital signatures on a day to day basis, else it may impede decision making.

No physical signature should be promoted on print outs of any digitally signed certificates/ documents

Awareness campaign should be launched in national and local media (in local languages) regarding what is digital signature and how it benefits the citizens.

**GOVERNMENT OF ASSAM  
OFFICE OF THE SUB-DIVISIONAL OFFICER  
BISWANATH CHARIALI II, SONITPUR DISTRICT**

**PERMANENT RESIDENT CERTIFICATE**

Date: 17-06-2010

This is to certify that the person with the following details :

Name	BABLY KHATUN
Name of Father	MD. ABDUL DAREK DEPARI
Name of Mother	SALEMA KHATUN
Revenue Circle	BISWANATH
Village / Town	AMBARI PAVOURGAD
Post Office	CHARIALI
Police Station	BISWANATH CHARIALI I
Sub - Division	BISWANATH CHARIALI
Purpose of Issue	Admission into higher educational Institutions

is Permanent Resident of **SONITPUR**

This certificate shall not be valid for any other purpose other than the purpose stated above.

**Signature valid**  
Digitally signed by [Name] Prukar  
Date: 2010.06.17 11:29:42 IST  
Reason: e-District Portal  
Location: Assam

**NOTE :**

- This order is digitally signed and therefore needs no physical signature.
- Authenticity of this order can be verified from <http://cdistrict.assamgovt.in>. This Order is legally valid as per the Information Technology ACT, 2008 and its subsequent amendments.
- Tampering of this order will attract penal action.

**Figure: Screenshot of a Digitally Signed Residence Certificate**



### 3 Successful Implementations of Digital Signatures

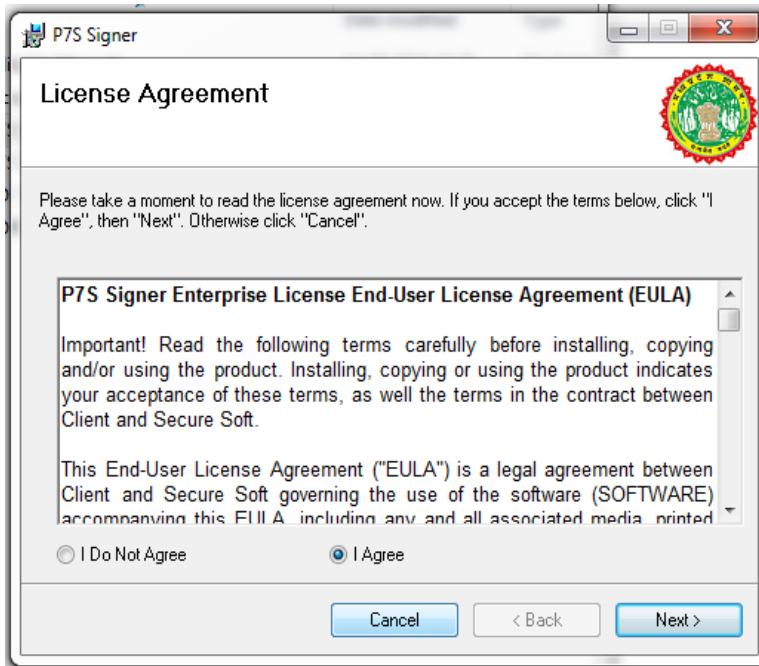
Some of the successful implementation of Digital Signatures in Uttar Pradesh include -

S.No	Project	Use of Digital Signatures	No of DSC issued
1.	<b>eDistrict</b> – implemented in six pilot districts. More than 18 lakh Digitally Signed Certificates/ Service already delivered to citizens	Digital Signatures are being used for electronically signing the Certificates being issued through eDistrict Centres / CSCs etc The approving authority puts his Digital Signatures at the time of approving the certificate and the related information is printed on the certificate also.  This not only ensures that the details of the signing authority is displayed, even the DSC of the signatory can be verified over the Internet.	500 to various Govt. district functionaries such as DM, SDM, Tehsildar, DSO, DSWO etc for issuance of services
2	<b>Online Counselling</b> for admission to more than 1 lakh seats of Engineering, Medical, Polytechnic & B.Ed. courses.	The Digital Signatures are being used by the Counselling In-charge for document verification, fee submission, registration & for choice locking opted by the candidates which are finally locked by the invigilators using DSC. Class II DSC are being used for these activities  In case of any modification in the student record, the same can be carried out only through digital signatures in order to ensure the same is recorded in the	<b>1264</b>  B.Ed – 438 UPTU - 433 Medical -433 Polytechnic – 220
3	<b>eProcurement</b> is an online tender processing system for the state government departments. More than 1000 tenders published so far.	The Digital Signatures are being used both by the vendors and government officials for tender submission and processing. The vendors/traders are using it for applying tenders online, while the government officials are using it at time of opening the tenders and during finalizing of the tenders.  Class II signatures are being used both for	About 500 to Govt. officials and Around 3000 to bidders
4	<b>Voters List Preparation</b> – The State Election Commission has issued a GO that the field data along with the photo ID will be digitized and the same will be digitally signed assuring the	The DSC will be used to counter verify the digitised data of voters list and the photo ID. This can be used by other applications such as eDistrict for online verification of citizen details.	Under Process
5	Many other departments are using DSC such as  1. CPWD	1. Class III Signing	

#### 4. DIGITAL SIGNING OF IMAGES GIF/JPEG

**STEP INSTALL P7S SIGNER SOFTWARE** –This is registered to MP Forest and can be obtained from Forest Website by Contacting IT Department APCCFIT

Click ICON to install p7s Signing SW and select I agree to install it



*Image Signer Software is  
Registered Software for MP  
Forest Department  
Images of JPEG and GIF  
Format will be saved in p7s  
format with Authentication  
provided from Digital  
Signature of Signing Officer*

Once you have installed the SW it will be saved in DESKTOP

**STEP 2** – OPEN DESKTOP SHORTCUT TO OPEN SW

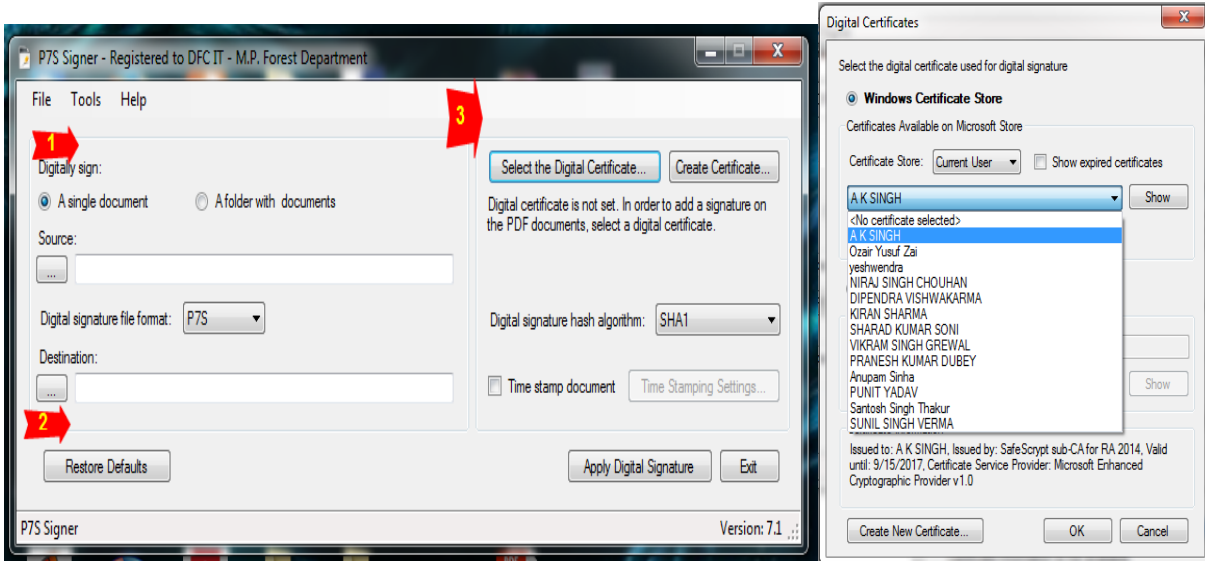
**STEP 3** .

1 SELECT SINGLE OR FOLDER OF IMAGE

STEP 3.2 SELECT DESTINATION OF IMAGE SIGNED

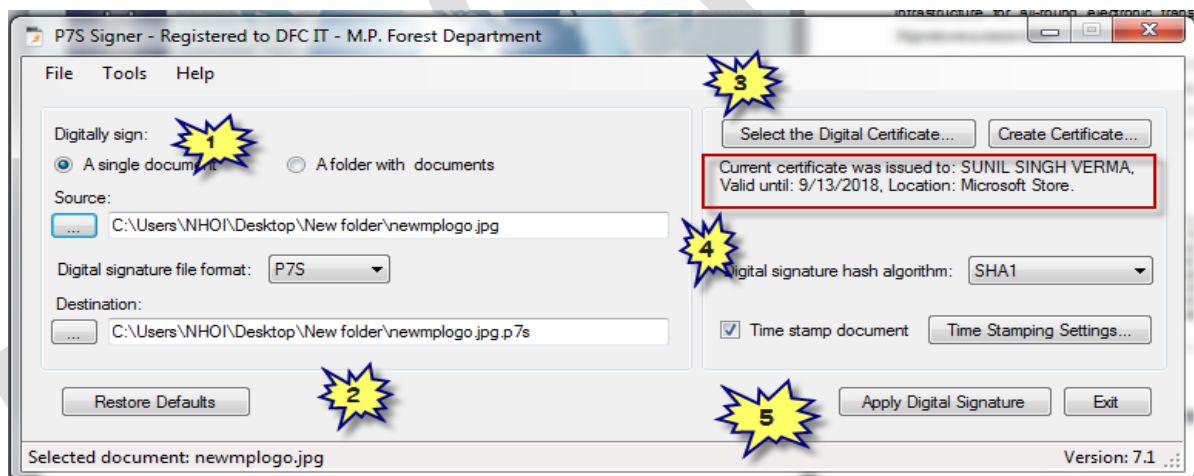
STEP 3.3 SELECT THE DIGITAL SIGNING OFFICER TO APPLY



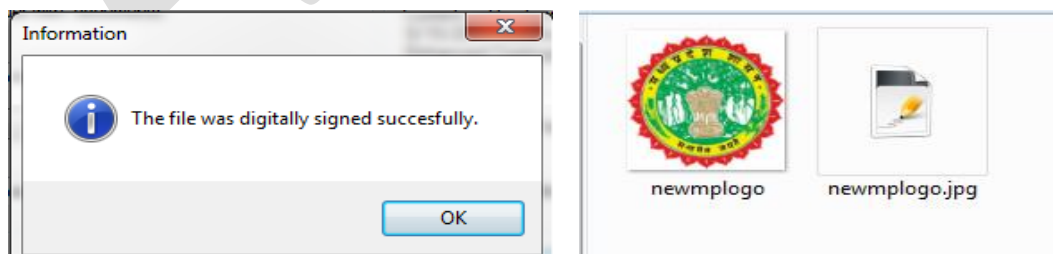


ONCE YOU HAVE SELECTED SIGNATURE YOU CAN SEE THE DETAILS AS IN POINT NO 4

5. APPLY THE SIGNATURE AS IN POINT 5



AFTER FEW SECOND THE FILE WILL BE SIGNED AND WILL BE SAVED IN DESIRED LOCATION AS HERE BELOW



YOU CAN CLICK SIGNATURE DETAILS BY DOUBLE CLICK THE FILE AND THEN SAVE THE UNSIGNED FILE AS YOU MAY NEED

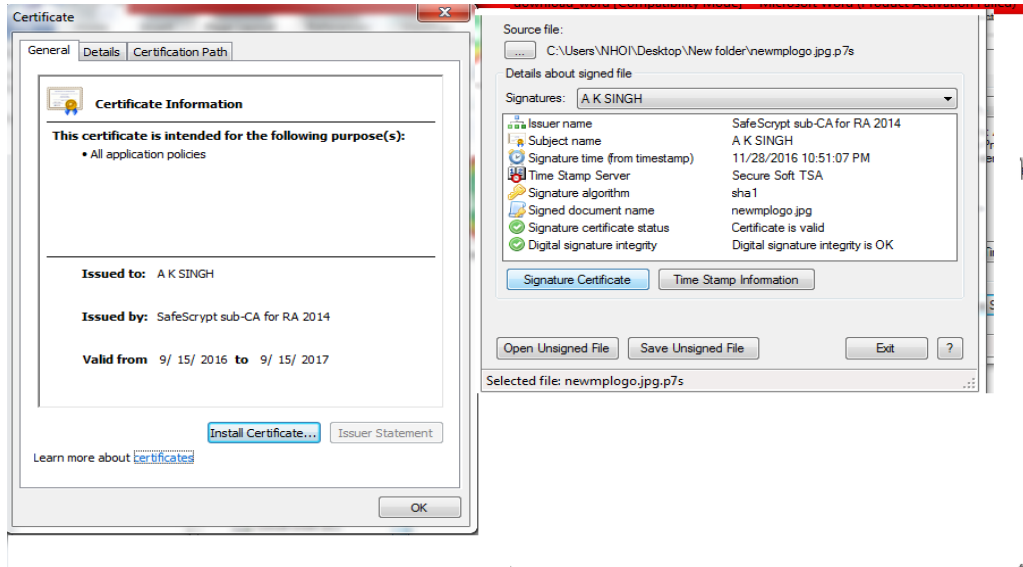


Image Signing Format is p7s p7m which you may select Custom Configuration

In some cases, you will need a different signature configuration (e.g. different signature appearance and digital certificates) for different files/folders.

To save a specific configuration, go to File – Save Configuration As and save the configuration on a file. Later, you can use that file in batch mode to apply different signature configuration on your signed file.

## **5. DIGITAL SIGNING OF PDF DOCUMENTS –PDF SIGNER SOFTWARE**

–This is registered to MP Forest and can be obtained from Forest Website by Contacting IT Department APCCFIT

- Portable Document Format (PDF) is best and suitable format to Sign Files Digitally as the Signature Details is Visible in the Documents and it can be validated also .

STORED IMAGES MAPS DOCUMENTS LETTER CAN BE CONVERTED INTO PDF EASILY

- Use GOOGLE CHROME ----Open Google Chrome DRAG n DROP Image into chrome → Click CTRL + P ( File→ Print) .
- In Print Option Choose Save AS PDF and the file is stored as PDF
- USE FREE PDF CONVERT SOFTWARE LIKE do pdf ,icecreampdf ,pdf maker etc
- Use Free Online PDF Converting Website Like <https://www.freepdfconvert.com/> <https://online2pdf.com> <https://www.wordtopdf.com> [convertonlinefree.com](http://convertonlinefree.com) etc etc
- RECEIVE CONVERTED FILE IN YOUR EMAIL - Alternatively, you can forward the original email message to pdfconvert@pdfconvert.me and the service will send a PDF version of the message back to you in a second or two.
- If there are any Word, Excel or Powerpoint attachments inside the mail, you can forward the files to attachconvert@pdfconvert.me and they'll come back to you in PDF format.

ONCE YOUR PDF IS READY YOU CAN USE PDF SIGNER TO AUTHENTICATE IT

- **Install the Software PDF Signer → Agree → Install → Shortcut is created @DT**
- **Select PDF Single Document or Folder Origin and Destination Both**
- **Select Reason and Place of Signing if needed**
- **Select Digital Signature to sign the Documents**
- **You Can configure signature appearance by Checking into Visible Sign Box and include adobe Right Tick and Question mark Status for validation also**

## Digital Signature Options

### Digital Signature Rectangle

If the checkbox Visible signature box is checked, a signature rectangle will be inserted on the PDF document. The appearance of the digital signature can be customized from the Signature Appearance section.

The default text direction is left to right. To change the text direction to right to left (e.g. for Hebrew language) checkbox Right to Left text must be checked.

The default font file for the digital signature rectangle is Helvetica. It is possible that this font to not include all necessary UNICODE characters like ä, à, â. On this case you will need to use an external font.

The font size is calculated based on the signature rectangle size in order to fit on the signature rectangle (it not have a fixed size). If you want to use a specific font size, it can be specified on the Font size section.

Observation: If the custom position will be used, the corner (0,0) is on the bottom left of the page.

### **Basic appearance settings**

Signature Page: First Page

Position: Top Right

Large signature box

Custom position

X-axis:  Width:

Y-axis:  Height:

Include Adobe signature status images (e.g. question mark)

Fonts

Font size: 10  Right to Left text

Standard fonts: Helvetica

Use a custom font

C:\signFont.ttf

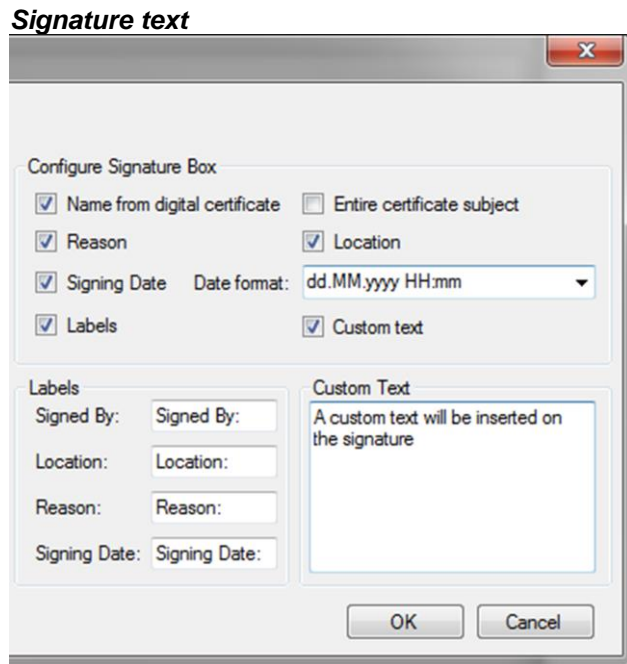
Place an image on the signature box

C:\signature.jpg

Image and text  Image as background  Image with no text

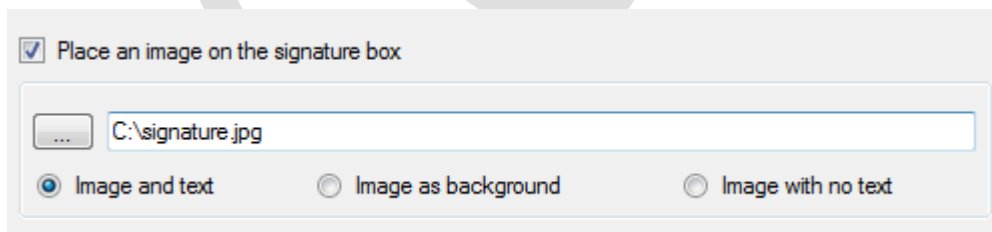
Restore Defaults

The default digital signature text contains information extracted from the signing certificate, signing date, signing reason and signing location but the digital signature text can be easily customized.



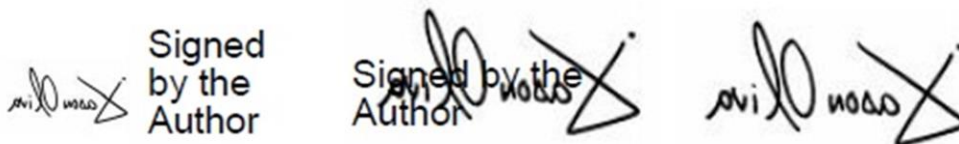
#### Set the Digital Signature Graphic

The digital signature rectangle can contain text, graphic or text with graphic. To add an image on the digital signature rectangle, you can do that from the Place an image on the signature box section.



These types of signatures are shown below:

- 1. Image and text,    2. Image as background,    3. Image with no text**



#### Signing Reason and Location

The signing reason and location attributes can be set from the main interface.

Signing reason: I approve this document

Signing location: Europe branch

**Signed by, Reason, Location and Date properties in Adobe**

Signature is VALID, signed by Test Certificate <test@test.com>.

Summary Document Signer Date/Time Legal

Signed by: Test Certificate <test@test.com> Show Certificate...

Reason: I approve this document

Date: 2011/06/20 13:00:00 +03'00' Location: Europe branch

Test Certificate  
2011.06.20 13:00  
I approve this document  
Europe branch  
This is a demo version

**Using SHA256, SHA512 Hash Algorithms**

The default hash algorithm used by the library is SHA1 but in some cases, SHA256/384/512 must be used for the digital signature and the Time Stamp Request.

Attention: SHA-256 and SHA-512 hash algorithms are not supported by Windows XP. Note that some smart cards and USB tokens not support SHA-256 and SHA-512 hash algorithms.

**Set the hash algorithm**

Select the Digital Certificate... Create Certificate...

Current certificate was issued to: Secure Soft S.R.L., Valid until: 5/28/2016, Certificate Service Provider: Microsoft Enhanced Cryptographic Provider v1.0, Location: Microsoft Store.

Digital signature hash algorithm: SHA1

Certify PDF document

No changes allowed

Visible signature box Signature Appearance...

Time stamp document Time Stamping Settings...

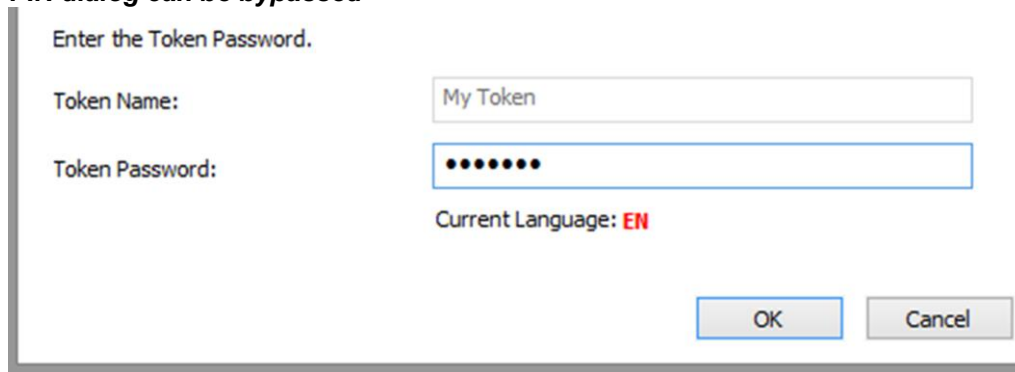
Encrypt document Encryption Settings...

Apply Digital Signature Exit

## Bypassing the Smart Card PIN

In case the digital signature must be made without user intervention and the certificate is stored on a smart card or USB token, the PIN dialog might be automatically bypassed for some models.

### ***PIN dialog can be bypassed***



Enter the Token Password.

Token Name: My Token

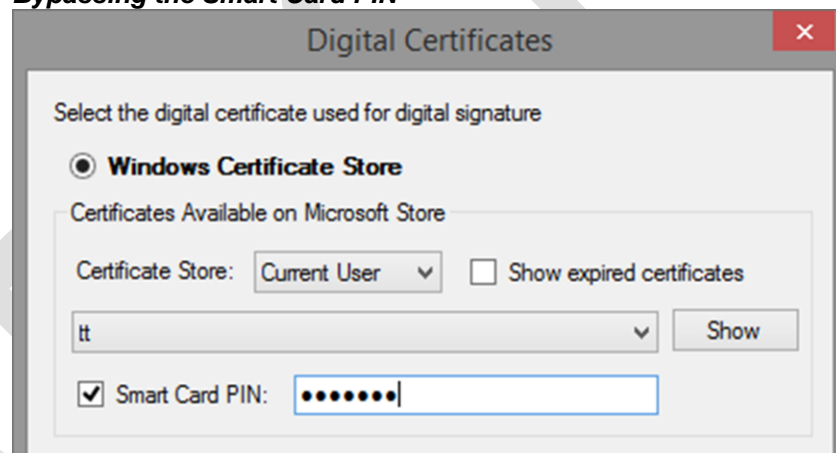
Token Password: ●●●●●●

Current Language: EN

OK Cancel

In order to bypass the PIN dialog window, the Smart Card PIN checkbox must be checked and the right PIN to be entered. `DigitalCertificate.SmartCardPin` property must be set. This option bypass the PIN dialog and the file is automatically signed without any user intervention.

### ***Bypassing the Smart Card PIN***



Digital Certificates

Select the digital certificate used for digital signature

Windows Certificate Store

Certificates Available on Microsoft Store

Certificate Store: Current User  Show expired certificates

tt Show

Smart Card PIN: ●●●●●●


Attention: This feature will NOT work for all available smart card/USB tokens because of the drivers or other security measures. Use this property carefully.



## 6. ATTACHING DIGITAL SIGNATURE IN EMAIL BY USING OUTLOOK USING OUTLOOK TO SEND DIGITALLY SIGNED EMAIL

Digitally sign a single message

In the message, on the Options tab, in the Permission group, click Sign Message.

- If you don't see the Sign Message button, do the following:
- In the message, click Options.
- In the More Options group, click the dialog box launcher  in the lower-right corner.
- Click Security Settings, and then select the Add digital signature to this message check box.
- Click OK, and then click Close.
- If you don't see the Sign Message button, you might not have a digital ID configured to digitally sign messages, and you need to do the following to install a digital signature.
- On the File menu, click Options > Trust Center.
- Under Microsoft Outlook Trust Center, click Trust Center Settings > Email Security
- Click Import/Export to import a digital ID from a file on your computer, or click Get digital IDs to find a list of services that issue digital IDs for your use.

Compose your message, and then send it.

Digitally sign all messages

1. On the File tab, click Options > Trust Center.
2. Under Microsoft Outlook Trust Center, click Trust Center Settings.
3. On the Email Security tab, under Encrypted Mail, select the Add digital signature to outgoing messages check box.
4. If available, you can select one of the following options:
5. If you want recipients who don't have S/MIME security to be able to read the message, select the Send clear text signed message when sending signed messages check box. By default, this check box is selected.
6. To verify that your digitally signed message was received unaltered by the intended recipients, select the Request S/MIME receipt for all S/MIME signed messages check box. You can request notification telling you who opened the message and when it was opened, When you send a message that uses an S/MIME return receipt request, this verification information is returned as a message sent to your Inbox.
7. To change additional settings, such as choosing between multiple certificates to use, click Settings.
8. Click OK on each open dialog box.

## 7 - Definitions and Acronyms

### Cryptography

The art of protecting information by transforming it (encrypting it) into an unreadable format, called cipher text. Only those who possess a secret key can decipher (or decrypt) the message into plain text. Cryptography systems can be broadly classified into **symmetric-key systems** and **public-key systems**.

#### Secret key (Symmetric/Conventional) cryptography

This is a system based on the sender and receiver of a message knowing and using the same secret key to encrypt and decrypt their messages. One weakness of this system is that the sender and receiver must trust some communications channel to transmit the secret key to prevent from disclosure. This form of cryptography ensures data integrity, data authentication and confidentiality.

#### Public – Key (Asymmetric Key) Cryptography

This system is based on pairs of keys called public key and private key. The public key is published and known to everyone while the private key is kept secret with the owner. The need for a sender and a receiver to share a secret key and trust some communications channel is eliminated. This concept was introduced in 1976 by Whitfield Diffie and Martin Hellman.

### Hash Function

A cryptographic hash function is a deterministic procedure that takes an arbitrary block of data and returns a fixed-size bit string, the (cryptographic) hash value, such that an accidental or intentional change to the data will change the hash value. The data to be encoded is often called the "message", and the hash value is sometimes called the message digest or digest or hash.

### Cryptotoken

Cryptotoken is a security token used to store cryptographic keys for digitally signing the documents. They are typically small enough to be carried in a pocket or purse or keychain. For example : - USB

### Digital Signature Certificates (DSC)

Certificates serve as identity of an individual for a certain purpose, e.g. a driver's license identifies someone who can legally drive in a particular country. Likewise, a Digital Signature Certificate (DSC) can be presented electronically to prove your identity or your right to access information or services on the Internet.

### Certificate Revocation List (CRL)

A CRL is a list of certificates (or more specifically, a list of serial numbers for certificates) that have been revoked, and therefore should not be relied upon. A CRL is generated and published periodically, often at a defined interval. The CRL is always issued by the CA which issues the corresponding certificates. All CRLs have a lifetime during which they are valid. During a CRL's validity period, it may be consulted by a PKI-enabled application to verify a certificate prior to use.

**Public Key Infrastructure (PKI)**

PKI is a combination of software, encryption technologies, and services that enable enterprises to protect the security of their communications and business transactions over networks by attaching so-called “digital signatures” to them.

**Certifying Authority (CA)**

This is an entity that issues Digital Signature Certificate to the end users. The digital certificate certifies the ownership of a public key by the named subject of the certificate. This allows others (relying parties) to rely upon signatures or assertions made by the private key that corresponds to the public key that is certified. In this model of trust relationships, a CA is a trusted third party that is trusted by both the subject (owner) of the certificate and the party relying upon the certificate.

**Registration Authority (RA)**

This is an entity within the CA that acts as the verifier for the Certifying Authority before a Digital Signature Certificate is issued to a requestor. The Registration Authority (RA) processes user requests, confirm their identities, and induct them into the user database.

**Root Certifying Authority of India (RCAI)**

This entity is created under CCA and is responsible for issuing Public Key Certificates to Licensed Certifying Authorities. This serves as the root of the trust chain in India. The requirements fulfilled by the RCAI include the following:

The licence issued to the CA is digitally signed by the CCA.

All public keys corresponding to the signing private keys of a CA are digitally signed by the CCA.

That these keys are signed by the CCA can be verified by a relying party through the CCA's website or CA's own website.

Make NOTES ----

## 9. Frequently Asked Questions

### Q1. What is Cryptography?

Cryptography is the science of enabling secure communications between a sender and one or more recipients. This is achieved by the sender scrambling a message (with a computer program and a secret key) and leaving the recipient to unscramble the message (with the same computer program and a key, which may or may not be the same as the sender's key).

### Q2. How do I get a Digital Signature Certificate?

The Office of Controller of Certifying Authorities (CCA), issues Certificate only to Certifying Authorities. The CAs in turn issue Digital Signature Certificates to the end-users. You can approach any of the CAs for getting the Digital Signature Certificate. For more information about the respective CAs kindly visit their websites (provided below)

### Q3. What is a Certifying Authority (CA)?

A CA is a trusted third party willing to verify the ID of entities and their association with a given key, and later issue certificates attesting to that identity. In the passport analogy, the CA is similar to the Ministry of External Affairs, which verifies your identification, creates a recognized and trusted document which certifies who you are, and issues the document to you.

### Q4. Who are the CAs licensed by the CCA?

- a. Safescrypt
- b. NIC
- c. IDRBT
- d. TCS
- e. CapricornIdentity .
- g. e-MudhraCA

### Q5. If CA is out of business then if the subscriber is told to move to another CA then the subscriber has to get a new digital certificate. What happens to his/her earlier transactions? Does this not create a legal and financial problem?

Prior to cessation of operations the CA has to follow procedures as laid down under the IT Act. Such problems should not therefore exist.

### Q6. Can one authorize someone to use DSC?

In case a person wants to authorize someone else to sign on his/her behalf, then the person being authorized should use their own PKI credentials to sign the respective documents.

### Q7. Can a person have two digital signatures say one for official use and other one for personal use?

Yes.

### Q8. In paper world, date and the place where the paper has been signed is recorded and court proceedings are followed on that basis. What mechanism is being followed for dispute settlements in the case of digital signatures?

Under the IT Act, 2000 Digital Signatures are at par with hand written signatures. Therefore, similar court proceedings will be followed.

### Q9. Is there a "Specimen Digital Signature" like Paper Signature?

No. The Digital signature changes with content of the message.

### Q10. If somebody uses others computer, instead of his own computer, then is there any possibility of threat to the security of the owners/users digital signature?

No, there is no threat to the security of the owner / users digital signature, if the private key lies on the smartcard /crypto token and does not leave the SmartCard/crypto token.

**Q11. Is it possible for someone to use your Digital Signature without your knowledge?** It depends upon the how the signer has kept his private key. If private key is not stored securely, then it can be misused without the knowledge of the owner. As per the IT Act 2000, the owner of the private key will be held responsible in the Court of Law for any electronic transactions undertaken using his/her PKI credentials(public/private keys).

**Q12. When you cancel an earlier communication you can get it back, how does this work in e- environment?**

A new message saying that the current message supersedes the earlier one can be sent to the recipient(s). This assumes that all messages are time stamped.

**Q13. When can a DSC be revoked?**

The DSC can be revoked when an officer is transferred, suspended or his/her key is compromised.

**Q14. How do digital certificates work in e-mail correspondence?**

Suppose Sender wants to send a signed data/message to the recipient. He creates a message digest (which serves as a "digital fingerprint") by using a hash function on the message. Sender then encrypts the data/message digest with his own private key. This encrypted message digest is called a Digital Signature and is attached to sender's original message, resulting in a signed data/message. The sender sends his signed data/message to the recipient.

When the recipient receives the signed data/message, he detaches sender's digital signature from the data/message and decrypts the signature with the sender's public key, thus revealing the message digest.

The data/message part will have to be re-hashed by the recipient to get the message digest. The recipient then compares this result to the message digest he receives from the sender. If they are exactly equal, the recipient can be confident that the message has come from the sender and has not changed since he signed it. If the message digests are not equal, the message may not have come from the sender of the data/message, or was altered by someone, or was accidentally corrupted after it was signed.

**Q15. How do Digital Certificates work in a web site?**

When a Certificate is installed in a web server, it allows users to check the server's authenticity (server authentication), ensures that the server is operated by an organization with the right to use the name associated with the server's digital certificate. This safeguard's the users from trusting unauthorized sites.

A secure web server can control access and check the identity of a client by referring to the client certificate (client authentication), this eliminates the use of password dialogs that restrict access to particular users.

The phenomenon that allows the identities of both the server and client to be authenticated through exchange and verification of their digital certificate is called mutual server-client authentication. The technology to ensure mutual server-client authentication is Secure Sockets Layer (SSL) encryption scheme

**Q16. What clause an eGovernance project should have to ensure that the PKI implementation meets the requirement of the IT Act 2000?**

The eGovernance applications have to be developed in compliance with RFC5280 certificate profile. A number of commercial and open source PKI toolkits are available which can be used to develop a standard validation process. Eg : - Microsoft CNG, Sun Java Toolkit. Please refer to Annexure IV of the Digital Signature Certificate Interoperability Guidelines (<http://cca.gov.in/rw/pages/index.en.do>) for further details.

**Q17. Can I use the certificate issued by a CA across eGovernance applications ?**

Yes

**Q18. What are the key sizes in India?**

CA Key is 2048 bits and the end user keys are 1024 bits. However from 1 Jan 2011, the end user keys will be 2048 bits as well as per the notification by CCA.

**Q19. What is the size of digital signatures?**

The size of the Digital Signatures varies with the size of the keys used for generation of the message digest or hash. It can be a few bytes.

**Q20. What is the Key Escrow ?**

Key escrow (also known as a fair cryptosystem) is an arrangement in which the keys needed to decrypt encrypted data are held in escrow so that, under certain circumstances, an authorized third party may gain access to those keys. These third parties may include businesses, who may want access to employees' private communications, or governments, who may wish to be able to view the contents of encrypted communications.

**Q21. How do applications use the CRLs?**

The applications download the CRLs from the respective CA sites at a specified frequency. The applications then verify the public keys against this CRL at the time of Digital Signature verification. The CCA is in the process of implementation of the OCVS (Online Certificate Verification Service) . This will ensure online verifications of the CRLs by the applications.

**Q22. How long do the CAs' in India preserve the Public Keys of the end users?**

As per the IT Act 2000, each CA stores the Public Key in their repository for a period of 7 years from the date of expiration of the Certificate.

**Q23. Should e-Governance applications archive the Digital Signature Certificates as well?**

In view of the fact that the CAs have a mandate to save the DSCs for a period of 7 years, it may be advisable for the eGovernance applications which would need to verify the records for authenticity for periods beyond 7 years.

**Q24. Can I have multiple Digital Signatures to a document?**

Yes one can have multiple Digital Signatures to a document. For eg: - in the MCA21 application the forms are signed by different Directors as part of the application workflow.

**Q25. What are the types of applications that should use Digital Signatures?**

The eGovernance applications mainly provide:

1. Information Services
2. Interactive Services (downloading of forms etc)
3. Transaction Services with or without payments like issuance of various Certificates etc

The category 3 services (transaction based) can benefit from the use of digital signatures. In general wherever a eGovernance application requires handwritten signatures during the workflow of a document in the approval process, we should replace them with Digital Signatures.

**Q26. What are cryptotokens?**

They are hardware security tokens used to store cryptographic keys and certificates. Eg :- USB etc

**Q27. What are the different ways of authenticating content of digitally signed documents issued to the citizen?**

There are different ways of verifying the content and the digital signatures of the document. Some of the mechanisms are enlisted below:-

**1. Via Unique Request ID (manual content verification only)** - In this process the user can verify the validity of his/her document by logging onto the Department website and providing the unique request number printed on the document. The Department application will display the electronic version of the document stored in the application repository. However in this process since the digital signature on the document is not verified, the contents have to be verified manually by the user by comparing the online document from the website with the hardcopy of the document. This process thus provides content verification only. The verification of the Digital Signature does not take place in this process.

**2. Verification by the 2D Barcode** – In this process, the barcode printed at the bottom of the document is used for the digital signature verification. The barcode has the Digital Signature embedded in it. The two verification mechanisms enlisted below verify the Digital Signature only. Since the complete content of the document is not being scanned, the content verification has to be done manually.

**a) Online Verification**

In this process, a barcode reader is used to scan the 2-D bar code printed at the bottom of the certificate. The verification utility of the Departmental application would verify the digital signature embedded in the document and after successful verification, show the corresponding electronic record on their website. However the user needs to compare the contents of the electronic record and the hardcopy. This method requires a computer, an internet connection and a 2D bar code reader.

**b) Offline Verification**

In this process, the user can verify the digital signature embedded in the barcode without connecting to the Department website. Thereby this process is called as "offline" verification. The user needs to download and install the verification utility custom developed by the Department (downloadable from their website). The user also needs to download the root chain certificates of CCA and NIC and the public key of the authorised taluka and the taluka official onto the computer. Once these items are installed

on the computer, the user can scan the 2D barcode on the document and the verification utility will check the validity of the digital signature embedded in the document thereby proving the authenticity of the document. However, the content of the hardcopy of the document will have to be manually verified by the comparing with the electronic version available at the Department website as the content of the hardcopy is not being scanned in this process.

**Q28. How can a digitally signed document be verified after the DSC associated with the Public Key has expired?**

The digital signature verification process for a document requires the public key, root chains and the CRL. The eGovernance application should therefore have a repository of public key certificates, root chains and the CRL's of the time the document was digitally signed. The CA's as of now are mandated to store the Digital Signature

Certificates, root chains and the CRLs for a period of 7 years as per the Rules of the IT Act. Therefore the Digital Signature Certificates can be downloaded from the CAs for a period of 7 years. However, if the digital signature on the document needs to be verified after this period, the eGovernance applications will have to have a provision to store the DSCs, root chains and the CRLs in a repository and undertaking the verification of digitally signed document against this repository. However, it may be a cumbersome process to get the CRLs' from the respective CAs for a specific period ( in the past).

**Q29. How can Departments ensure that their Government officers authorized to sign the Certificates do not misuse their Digital Signature Certificates after being transferred from a given place?**

It is recommended that as part of the handing over of charge of a given officer, the DSC issued to the officer be revoked. Further his user credentials in the respective eGovernance applications should be deactivated so that he can no longer access the application while the Certificate revocation is under process with the CA. Once the DSC is successfully revoked, the officer will be no longer able to sign the documents.

**Q30. How can a citizen be assured that the document has been digitally signed by the appropriate authorized Government officer?**

In order to ensure that the documents are signed by authorized individuals only, the Departments should maintain a repository having a mapping between the DSC and the respective roles assigned to the officers of the Departments. The eGovernance application should check against this repository for the various documents before allowing an officer to digitally sign the document. This mechanism has been implemented in MCA21 application wherein multiple directors sign the eforms for the application. The key challenge with this approach is to be able to maintain an updated repository at all times.

The Government of India is currently looking into the proposal for creation of a central repository of Digital Signature Certificates and CRLs' in order to ensure that digitally signed documents can be verified at a later date ( greater than 7 years).

## SOURCES AND REFERENCES

**CCA website:** <http://cca.gov.in>

**NIC- CA website:** <http://nicca.nic.in>

**Interoperability Guidelines for Digital Signature Certificates:**  
<http://cca.gov.in/rw/pages/index.en.do>

**IT ACT 2000** <http://www.mit.gov.in/content/information-technology-act>

**Wikipedia** <http://www.wikipedia.org>

**Nemmadi** <http://nemmadi.karnataka.gov.in/>

## COMPILATIONS –

- **SUNIL SINGH VERMA ( TECHNICAL INCHARGE BCSPL) BE.CS**
- **SUPPORTING STAFF – AMLESH SINGH ( TECHNICAL ASSISTANT )BE.EC**
- **DEEPENDRA – BCOM KAJOL ( BCOM PGDCA)**

-----\*\*\*\*\*Thank you Very Much \*\*\*\*\*-----







**SPACE FOR MAKING NOTES**
