Checklist for MCACert Installation

Step 1	***IMPORTANT* : Pre-requisites**	**Tick (√)**
	Ensure that the Computer has Internet Explorer (IE) Browser Version 5.5 or 6.0 with 128 bit Cipher Strength or Netscape Navigator 4.7x, 4.8 or 7.x. If the computer does not have a supported browser version, please upgrade the browser with IE 6.0. (Software provided on the MCACert CD)	
	For Windows 95/98 users - MSI 1.1 or higher version should be pre-installed on the computer. (Software provided on the MCACert CD)	
	Hardware - 1 free USB Port should be enabled on the computer	
Step 2	**Complete MCACert Application Form** (Form provided on the MCACert CD)	
	Enter Partner Code, City of Applicant, Date of Application and CD Serial Number	
	Select Certificate Validity, based on payment made	
	Enter the Personal Details of the Applicant. Paste recent Passport Photo of the applicant and have him Sign across the picture and the application form	
	Enter the Contact Details of the Applicant, as per banking records and which must be attested by the Banker. Please ensure Accuracy of the details for Identity Validation purposes	
	Submit Applicant's e-mail ID. Please ensure Accuracy of the details as the DSC will be sent to the applicant only on this e-mail ID	
	Enter the ID Number of any one of the Photo IDs mentioned in the application form. Attach a Xerox-copy of the same Photo ID after having it attested by a Notary or Gazetted Officer or the Banker. **Note:** Without this attested Xerox-copy of the Photo ID, the MCACert DSC Application will be rejected	
	Have the applicant Sign the MCACert DSC Application Form	
	This MCACert DSC Application Form must now be presented to the Bank Manager of the Bank where the applicant holds a valid account. Instruct the Bank Manager to verify that the Signature of the applicant in the application form is the same as per the Bank records. Instruct the Bank Manager to affix his Signature and other details as required	
	Courier the original, completed MCACert DSC Application Form along with the attested Xerox-copy of the Photo ID to SafeScrypt	
Step 3	**Install USB Token Software** (Software provided on the MCACert CD)	
	Install the USB Token software. If the Aladdin eToken PRO USB Token software does not install, please download and install MSI Version 1.1 or higher version and re-start the installation.	
	Insert the USB Token into the computer only after this step and personalize the USB token by changing the Default Password from 1234567890. **Note:** The new password must be entered by the user only and will be required every time the user accesses the MCA application.	
Step 4	**Enrol for the MCACert Digital Signature Certificate**	
	Online Enrolment link: **https://digitalid.safescrypt.com/RCAIClass2/client/userEnrollMS.htm**	

Ensure that USB Token is plugged into the computer	
Enter Applicant information	
Enter Token Redemption Number	
Enter CD Serial Number	
Important Challenge Phrase to be entered only by Applicant	
Select ‘eToken Base Cryptographic Provider’	
Read the Subscriber Agreement and click the "**Accept**" button	

Minimum System Requirements for MCACert DSC Installation

Operating System: SafeScrypt recommends use of the following Operating systems only

- Windows 2000
- Windows 2003 Enterprise
- Windows ME
- Windows XP

Supported Browsers: Browser with 128-bit crypto and Javascript enabled

- Netscape Communicator 4.7x, 4.8, 7.x
- Internet Explorer 5.5, 6.x

Minimum Hardware

- Intel-based PC, 866Mhz Pentium or faster
- 128MB RAM
- 50MB free disk space

Required for USB Token Users

- CD-ROM drive
- USB token, drivers and software
- One available USB port for connecting the token
- Microsoft Windows Installer (MSI) 1.1 or later utility (for Windows 98/95 users only http://support.microsoft.com/default.aspx?scid=kb;en-us;292539)

MCACert Digital Signature Certificate: Do's and Don’ts

Proper security procedures require that users of MCACert Digital Signature Certificates follow safe practices. Just as one keeps ones driver’s license and credit cards safe, every user should be aware of the possibility of theft of their electronic digital certificates and take reasonable precautions to prevent it.

1. Please ensure that the USB Token software is installed before the token is inserted into the USB Port of the computer. The USB Token must be inserted before the user enrols and pickup the Digital Signature Certificate
2. To view the status of the MCACert Digital Signature Certificate enrolment, please perform a “Search” at https://digitalid.safescrypt.com/RCAIClass2/client/search.htm
3. Use difficult-to-guess passwords while personalizing the USB Token and while enrolling for the Digital Certificate. Do not leave the Challenge Phrase blank when enrolling for the Digital Certificate
4. Do not reveal the Digital Certificate Challenge Phrase or USB Token Password to anyone.

5. Ensure that the user remembers the Digital Certificate Challenge Phrase which was given while enrolling for the certificate online. This Challenge Phrase is required at a later date for revoking or renewing the Digital Certificate.
6. Ensure that the Digital Certificate is used only for Authorized and Legal purposes. The user is legally responsible for all Digital Signatures created using the Digital Certificate.
7. When the user is not transacting with the MCA using the Digital Certificate, please ensure that the USB Token is removed from the USB Port of the computer. Store the USB Token safely when it's not being used. Remember that if the USB token is lost or gets stolen, it is not possible to retrieve the Digital Certificate.
8. If the user suspects that the Digital Certificate has been tampered with or stolen, inform us at SafeScrypt immediately or the user can personally revoke the certificate online using the Challenge Phrase. Visit the following URL for revoking the Digital Certificate.
   https://digitalid.safescrypt.com/RCAIClass2/client/revoke.htm