ENROLMENT GUIDE FOR MCACert

Congratulations! You are about to become the proud owner of a Digital Signature Certificate issued by SafeScrypt, India's first Licensed Certifying Authority, under the aegis of the Indian IT Act 2000.

SafeScrypt RCAI Class 2 Certificate Hierarchy chains up to the RCAI root and is intended for use wherever the predominant requirement is for legal validity within India. This hierarchy also offers interoperability with other Licensed CA's in India through the common trust anchor of the RCAI root.

The MCACert Digital Signature Certificates are intended for use with the MCA21 portal.

You are strongly encouraged to read the contents of this Enrolment Guide before proceeding.

Stage 1: Enrolment pre-requisites

Before you commence the enrolment process, please be aware of the following.

Minimum System requirements:

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 cipher strength 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)

Stage 2: Complete MCACert DSC Application Form

The form is available on the MCACert CD or you could download it at http://mcacert.safescrypt.com.

Please remember to courier the original, completed MCACert DSC Application Form along with the attested Xerox-copy of the Photo ID to SafeScrypt

Stage 3: Install the USB Token Software

The software for the USB Token is provided on the MCACert CD or you can download it from https://mcacert.safescrypt.com.

Double click and install the software on the computer that you plan to use with the MCA application. Only after the installation is completed should you insert the USB Token into the free USB Port on your computer. This will complete the installation of the USB Token and you will now be ready to enroll for your MCACert Digital Signature Certificate.

Stage 4: Online Enrolment

Visit https://digitalid.safescrypt.com/RCAIClass2/client/userEnrollMS.htm, fill in the relevant details and have your public-private key pair generated automatically. During this process, the public key is sent to SafeScrypt CA for creation of the certificate.

Stage 5: Post-Enrolment - Validation of identity

SafeScrypt CA validates the credentials you submit before issuing your Digital Signature Certificate.

This Digital Signature Certificate provides a very high level of trust. MCA trusts and relies on the Digital Signature on the license forms, on the belief that SafeScrypt has validated the identity of the Certificate Applicant. We are therefore required to validate the credentials you submit, before we can issue this certificate to you.

ONLINE ENROLMENT PROCESS

STEP 1:

Submit information about yourself – Please submit the following information about yourself. Remember that this information must be accurate, as **it will be displayed in your Digital Certificate**. You will also have to provide this same information in your Certificate Application Attestation Form.

- **First and Last name in full**. No abbreviations are permitted (Mandatory)

- **E-mail address** (Mandatory)

  Note that the Certificate Pick-up Instructions will be sent to this e-mail id

Enter your Digital Certificate information

Fill in all required fields. Fields marked with an asterisk (*) are included with your Digital Certificate and are viewable in the certificate details. All information provided here must be identical to that provided in the Certificate Application Form.

First Name: * (required) Nickname or middle initial allowed (Example: **Anurag B.**)	
Last Name: * (required) (Example: **Shah**)	
Your E-mail Address: * (required) (Example: **anurag@safescrypt.com**)	

STEP 2:

Photo ID Number: Please Enter here the Number of a Government issued Photo ID Card that you have. Acceptable Photo ID Numbers include Passport Number, a PAN Card Number, or a Voter ID Number. Practicing Company Secretaries can enter their CP Number here.

Photo ID Details:

Please select the Type and enter the Number of a Government issued Photo ID Card that you have. Acceptable Photo IDs include Passport, PAN Card, or a Voter ID Card. Practicing Company Secretaries can enter their ICSI CP Number here. If you wish to submit any other type of Photo ID card, please enter the details of the same. Acceptance of the same will be at the discretion of SafeScrypt.

Photo ID Type and No.: (required) (Example: **PAN No., ALDPS2567K**)	PAN No. ▼ ALDPS2567K

STEP 3:

Challenge Phrase - The Challenge Phrase is a unique phrase that protects you against unauthorized action on your Digital Certificate. Do not share it with anyone. *Do not lose it*. You will need it when you want to revoke or renew your Digital Certificate. Your Challenge Phrase should not exceed 30 characters and must only be Alpha-numeric. Special characters are not permitted.

STEP 4

Cryptographic Service Provider (CSP) - Select "e-Token Base Cryptographic Provider" for the *Aladdin eToken PRO or* from the drop-down list box to store your Digital Certificate on the USB token.

If you do not have USB token Internet Explorer (IE) browser users will have to select the *Microsoft Enhanced Cryptographic Provider* option from the drop-down list box. Remember that this option generates and stores your Private Key in the browser itself.

NOTE: If your IE CSP options do not include either the Microsoft Enhanced Cryptographic Provider or the eToken Base Cryptographic Provider, then you must update your browser with the appropriate service packs from the Microsoft Windows Update site (these are free updates) before you continue with the enrolment.
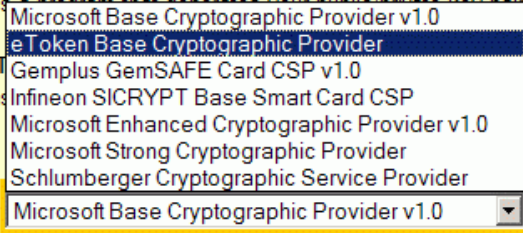
Only these CSP's will give you Private Keys that are 1024 bits in length. The Indian IT Act 2000 specifies that Digital Signatures will be awarded legal recognition only if they are created with Private Keys that are 1024 bits in length.

STEP 5

Submit your Payment Information

Token Redemption Number (TRN)	Please enter the token number correctly. The token number is case and space sensitive, which means that you will need to enter it exactly as it is given to you. Ensure that you do not leave any blank spaces. If you make a mistake while entering the token number, your enrolment will not be submitted. If you do not have a TRN, please visit http://mcacert.safescrypt.com to purchase it.
CD Serial Number	Key in the unique CD Serial No. here. The CD Serial No. must also be entered correctly in the Certificate Application Form.

Enter Payment Information

You can pay for and purchase a Digital Certificate via any of our authorized partners. To have one of our partners get in touch with you, give us a call at any of the following or mail us at mcacert@safescrypt.com.

Delhi	+91-11-41017439 / 41039457
Mumbai	+91-22-56772424
Chennai	+91-44-22540770, extn:2005
Bangalore	+91-80-26555095

Toll Free Numbers
1901 425 3330
1600 345 3330

On payment realization, you will be issued a unique 16-Digit Token Redemption Number (or TRN). This TRN is required to be entered below while enrolling for your Digital Certificate.

Token Redemption Number: (required)
Key in your Token Redemption Number here. The TRN will automatically determine the validity of your Digital Certificate. Please ensure that there are no spaces in the Token Number.

CD Serial Number: (required)
Key in the unique CD Serial No. here. This Number will be used to track your application.
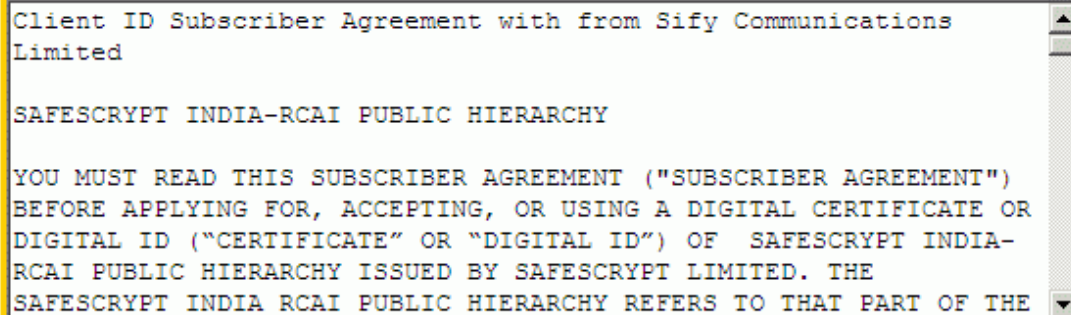
STEP 6

Digital Certificate Subscriber Agreement: You must read this subscriber agreement before applying for, accepting, or using a Digital Certificate. If you do not agree to the terms of this subscriber agreement, do not apply for, accept, or use the Digital Certificate. Read the Subscriber Agreement and click the "Submit" button. This will submit your registration information to SafeScrypt.

Note: As your enrolment is getting submitted, the Web page will display a few popup windows that tell you that your Key-Pair is getting generated and will be stored in the certificate store you selected (i.e. IE, Netscape or I-Key, E-Token). Please select "Yes" or "Accept", wherever you are prompted to do so.

Digital Certificate Subscriber Agreement
You must read this subscriber agreement before applying for, accepting, or using a Digital Certificate. If you do not agree to the terms of this subscriber agreement, do not apply for, accept, or use the Digital Certificate.

```
Client ID Subscriber Agreement with from Sify Communications
Limited

SAFESCRYPT INDIA-RCAI 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") OF  SAFESCRYPT INDIA-
RCAI PUBLIC HIERARCHY ISSUED BY SAFESCRYPT LIMITED. THE
SAFESCRYPT INDIA RCAI PUBLIC HIERARCHY REFERS TO THAT PART OF THE
```

POST-ENROLMENT PROCESS

Once you have completed the online enrolment, the last screen that will be displayed will confirm your enrolment and will also explain the post-enrolment procedures. If you experience any difficulty submitting your order, please contact SafeScrypt by sending us mail at **support@safescrypt.com**

Note: You will need to reference the following information when you contact SafeScrypt for support.

1. Serial Number from the back of the MCACert DSC Pack
2. Token Redemption Number used for the enrolment
3. Full Name of the applicant as given in the enrolment
4. E-mail ID of the applicant as given in the enrolment
5. Error messages (send screenshots if possible) and action that caused the error

Step 1: Documents to be submitted - You need to submit the documents as mentioned below. The documents will enable SafeScrypt to validate your application for the Digital Certificate.

1. **Certificate Application Form for Individuals** - SafeScrypt requires this form for validating your identity prior to issuing your Digital Certificate.

   The format of the Certificate Application Form may be downloaded from the website http://mcacert.safescrypt.com or taken from the MCACert CD.

   You will need to complete the form as per the instructions given. To ease of use, the form is available as a PDF form which can be filled electronically and printed. If you have a scanned electronic copy of your latest passport sized photograph, you can attach the same in the PDF form before printing it out. Alternatively, you can print a copy of the Application form and fill it with a pen. All the fields marked with a '*' are mandatory and must be filled.

   There are 4 Sections in the form.

   Section 1 captures your personal details. These details are required as per the rules defined under the IT Act.

   Please ensure that you fill in your contact address as per your banking records. Your bank manager should be able to verify this address as correct and attest the same in Section 4. If you are a practicing Company Secretary, you will NOT be required to provide a banker attestation (Section 4). However, please ensure that the address that you provide here is correct and is as per information available in the ICSI Database.

   You will also need to sign across your photograph as a self attestation of the same.

Section 2 captures your email address. Please ensure that the email address is the same that you will be using for your online enrolment. The email address will appear in your certificate. A PIN number will be sent to this email address to enable you to pick up your certificate.

Section 3 of the Application Form captures details of proof of your Identity. You are required to key in details of a Government issued ID that you hold. Acceptable IDs include Passport, Voter ID or a PAN Card. If you wish to submit any other type of ID, please provide details of the same. SafeScrypt will recognize only Government issued IDs as valid.

Practicing Company Secretaries can provide their ICSI CP number here. A SafeScrypt validation team member will make an outbound call based on the phone number listed in the ICSI member database to confirm details with the applicant before issuing the Digital Certificate.

Section 3 also contains a self attestation for the accuracy of the details provided in form. Please ensure that all the details above are filled correctly and you sign the form. Unsigned forms will be rejected.

Section 4 is an attestation by your banker for the following details. (This section is not applicable to ICSI members)

  i. The Contact Address provided by you

  ii. Your Name and Signature

SafeScrypt at its discretion will make an outbound call to the banker to confirm details of the attestation.

After completing the Application Form Submit all documentation to SafeScrypt either directly or through the SafeScrypt partner you have interacted with.

Important: Your Name and E-mail ID that you enter in this form must be exactly as you have provided in the online enrolment. If these details do not match or if the details are found to be false, we will not be able to complete the validation and your certificate will not be issued.

Certificate Issuance - SafeScrypt will begin the validation process after all the duly completed documents have been received.

If there is any discrepancy in the information received by way of the online enrolment and the documents you submitted, SafeScrypt will send you an e-mail with the instructions to either re-enroll with the correct details or to submit corrected documents. The validation will resume only after the corrected information has been received. Once the validation has been completed and payment has been confirmed, SafeScrypt will issue your Digital Certificate. You will receive an e-mail with a URL, a PIN number and the instructions to pick up your Digital Certificate.

Note: Please remember to pick up the Digital Certificate using the same computer and USB Token/browser that were used to enroll for the Digital Certificate.