eMudhra.mu DTM

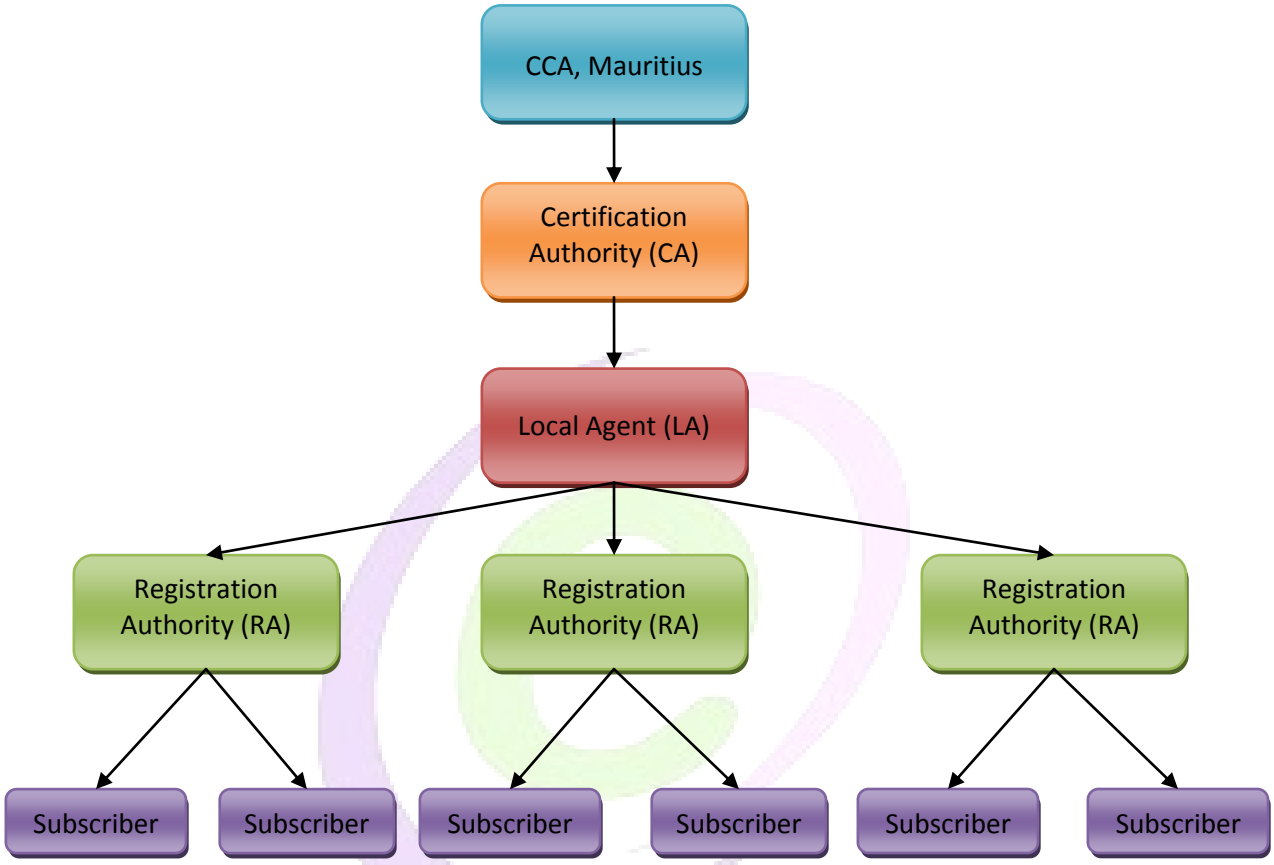
eMudhra DSC TRAINING MANUAL

VERSION
(eMudhra/DOC/DTM/1.0)

Date of Publication: 2nd May 2013

Table of Contents

I. PKI Eco System in Mauritius



Controller of Certification Authorities (CCA)

The ICT Authority, in the exercise of its statutory function as CCA, is the apex body of the Mauritian PKI. The Electronic Transactions Act, 2000 (as amended), and its regulations, provide the required legal sanctity to the digital signatures based on asymmetric cryptosystems. It also provides for the Controller of Certification Authorities (CCA) to license and regulate the working of Certification Authorities. The Certification Authorities (CAs) issue digital signature certificates to users.

The CCA certifies the public keys of CAs using its own private key, which enables users in the cyberspace to verify that a given certificate is issued by a licensed CA.

Certification Authority

Certification Authority is the entity, recognized by Controller of Certification Authorities (CCA). Certification Authority is entrusted to issue, revoke, renew digital signature certificates, Maintains online access to the public key certificates issued, Assures the identity of the parties to whom it issues certificates and publishes CRL (Certificate Revocation List). eMudhra is the recognized Certification Authority by CCA.

Local Agent (LA)

Local Agent (LA) is a local person or entity of Mauritius, appointed by eMudhra CA to carry out the role of Local Agent as detailed but not limited to below. NCB is the Local Agent for eMudhra CA:

- To ensure data confidentiality both digital as well as physical data in compliance with this CPS, ETA, Data Protection Act of Mauritius or any other local laws.
- To ensure security levels in storage of data, IT infrastructure, physical access and so on as is applicable to a CA in Mauritius.
- Storing of the customer data including the physical application forms and supporting documents as a custodian of CA
- Creating and maintaining various records and related audit trails of various transactions
- Ensuring full compliance with all the local laws and regulations of Mauritius.

Registration Authority (RA)

Registration Authority is the entity appointed by eMudhra to evaluate and either approve or reject digital signature certificate applications in accordance with the CPS (Certification Practice Statement). Following are the activities performed.

- Collect, Verify and validate the application forms and relevant supporting documents provided by the applicant
- Processing revocation or renewal of the Digital Signature Certificate upon the request from the subscriber
- Forward the physical application forms to LA for storage and record keeping.
- Distribution of Crypto USB tokens to the applicants and maintaining inventory for the same.

Mauritius Post is the Registration Authority.

Subscriber

A Subscriber is a person, entity, or authorized representative of an organization that has been issued a eMudhra Digital Signature Certificate.

- To ensure that the information / data provided in the application for certificate request is true, accurate, current and without errors, omissions or misrepresentations.
- Use secure medium as specified in the eMudhra CPS to generate the key pair
- To protect the generated private key in a trustworthy, secure medium.
- To keep the private key safe and protect it from any disclosure or unintended use
- Notify eMudhra immediately when the information included in the Subscriber's Digital Signature Certificate is inaccurate, false or incomplete.
- Notify eMudhra immediately upon any actual or suspected compromise of the Subscriber's private key.
- Comply with any other additional obligations as mentioned in the Subscriber agreement.
- Read and accept the policies and procedures as specified in this CPS.

II. What is a Digital Signature Certificate?

- Digital Identity equivalent of paper certificate like Driver's license and Passport that establishes your credentials when doing business or other transactions on the Web
- Issued by a Certification Authority (CA) like eMudhra CA
- Contains your name, serial number, expiration dates, public key, signature of CA
- As per ETA, Digital signatures are accepted at par with handwritten signatures

The certificate and private key are stored in a TOKEN called crypto token. These tokens are FIPS certified. The keys are generated in the token and cannot be extracted out of the token.

Components of Digital Signature Certificate

Component	Details

Certificate Standard	X.509
Key length	2048 bits
Issuer of certificate	eMudhra CA
Key usage	Digital Signature, Non-repudiation & Key encipherment
Validity	2 or 3 years
Subject DN	Certificate owner details

Keypair with 2048 bit length

Public Key – Known by everyone

Private Key – Known only by the owner

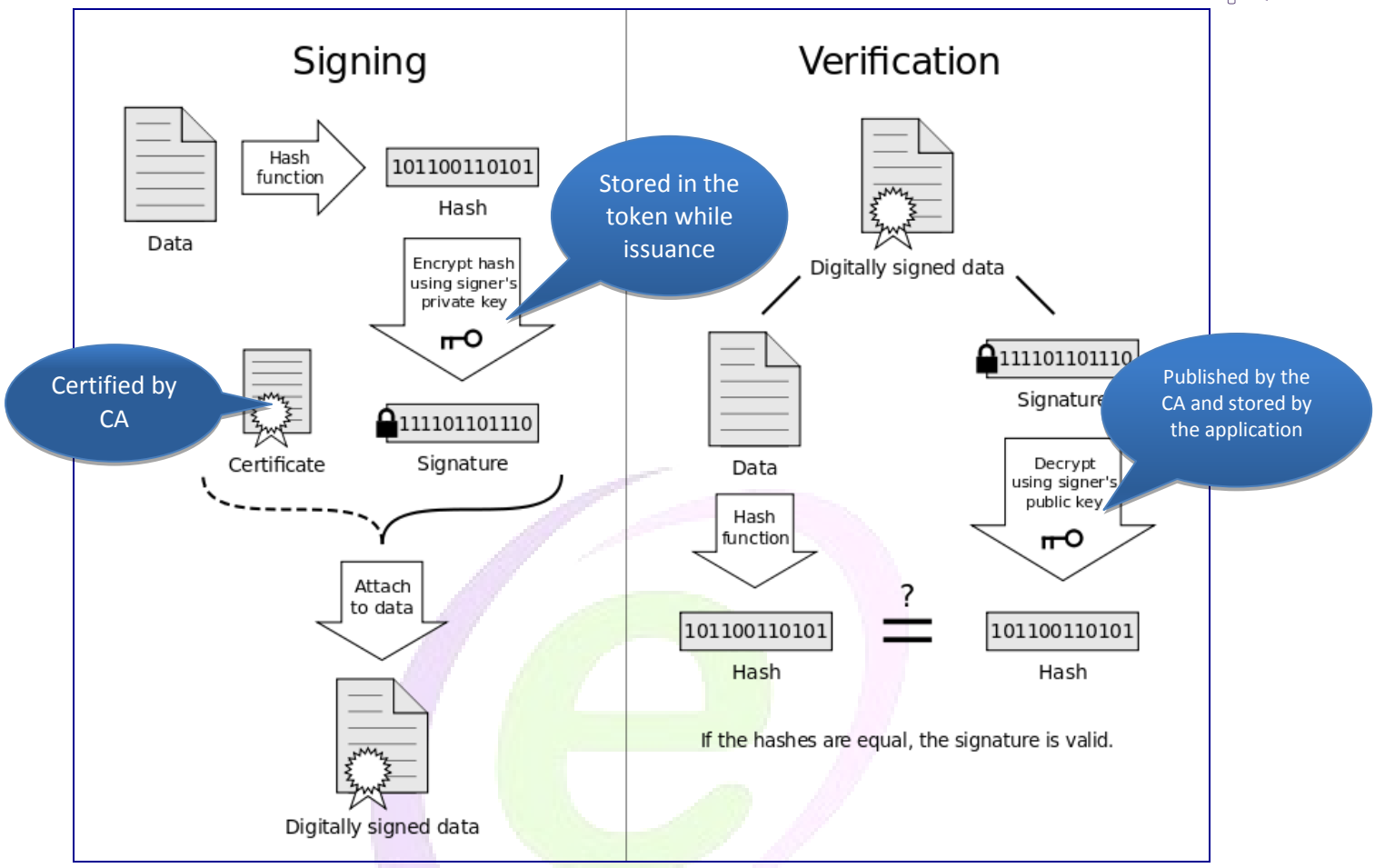
Contents of Digital Signature Certificate

A certificate includes:

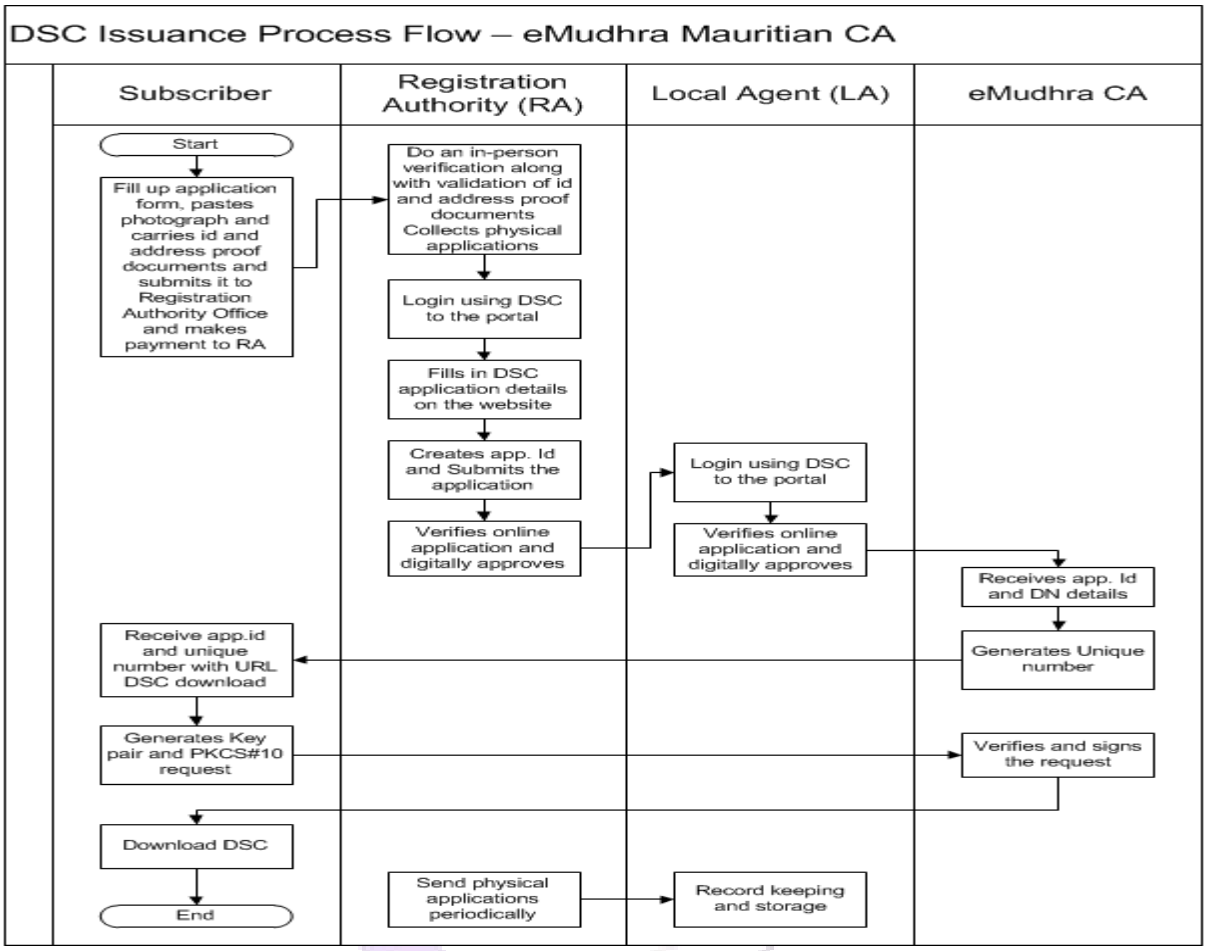
- The distinguished name (DN) of the owner. A DN is a unique identifier, a fully qualified name including not only the common name (CN) of the owner but also the owner's organization and other distinguishing information.
- The public key of the owner.
- The date on which the certificate is issued.
- The date on which the certificate expires.
- The distinguished name of the issuing CA.
- The digital signature of the issuing CA.

The information in a certificate helps an application to determine whether to honor the certificate. With the expiration date, the application can determine if the certificate is still valid. With the name of the issuing CA, the application can check that the CA is considered trustworthy by the site.

III. How do digital signatures work?



IV. What is the digital signature certificate application process?



1. Subscribers can either download application from emudhra.mu or visit Mauritius Post Branch office. Subscriber fills up the application form, and attaches copy of photo identification document as well as address proof documents. The same is submitted to the Registration Authority (RA) i.e. Mauritius Post.
2. The Mauritius Post in turn does in-person verification and also verifies photo identification as well as address proof documents. On successful verification, the subscriber is issued a crypto token for downloading digital signature certificate on to it.
3. Mauritius Post logs into emudhra.mu portal as RA and keys in subscriber details as provided in the application form; digitally signs and approves the online application.
4. Mauritius Post sends the physical application form to Local Agent i.e. NCB for further verification and processing.

5. On receipt of the physical application form from the RA, LA in turn verifies for completeness of the application form along with the validation and verification of documentary evidence provided as part of the application.
6. On successful verification, LA logs into eMudhra.mu portal using digital signature certificate and cross verifies physical application vis-à-vis online application form that is approved by RA.
7. On successful verification, LA digitally signs and provides final approval. The physical application form is then stored at LA for record keeping.
8. On approval by LA, eMudhra CA system generates user credentials and the same is sent to the subscriber by email.
9. On receipt of email from eMudhra CA, subscriber logs into eMudhra.mu portal by providing the credentials received in email.
10. Checks for the user details that are going to be part of digital signature certificate and clicks on download DSC. Before downloading DSC, subscriber has to make sure that token is plugged into USB port and the respective token drivers are installed.
11. On clicking download DSC, the user generates key pair either onto crypto token or PC and request. The request is sent to eMudhra CA for issuance of DSC.
12. On issuance of DSC, subscriber downloads the DSC either onto crypto token or PC. This happens real time.

V. What is a Certificate Revocation and process to revoke certificate

A Digital Signature Certificate can be revoked under circumstances such as the following

- Users suspect compromise of certificate private key
- Change of personal data
- Change of relationship with the organization

Subscriber can directly revoke his/her digital signature certificate by visiting portal (emudhra.mu) -> click on Revoke and provide following details.

- Application No.
- Certificate Serial Number
- Date of Birth
- Revocation Reason
- Remarks
- Verification Code

On successful validation of credentials by eMudhra CA system, the system then revokes the DSC and the same published in the respective CRL. On revocation of DSC, an email is sent to the subscriber confirming revocation of DSC.

VI. What is a crypto token?

A crypto token is a specific token that can be only used for secure storage of digital signature certificate as well as keypairs. The crypto token is FIPS 140-2 Level 2 certified and supports USB port 2.0. It is one of the best and highly secure way of storing the keypair.

VII. From where can I download Application form

Go to www.emudhra.mu -> Quick Links -> Application Forms

VIII. Procedure for downloading digital signature certificate

Detailed documentation on DSC download procedure is available at http://emudhra.mu/repository/eMudhra_DSC_Download_Manual.pdf

IX. Procedure for configuring DSC on MS Outlook

Detailed documentation on configuring DSC on MS Outlook is available at http://emudhra.mu/repository/ConfiguringDigitalsignaturecertificateinMicrosoftOutlook.pdf

X. Procedure for digitally signing MS Word Document

Detailed documentation on digitally signing MS Word Document is available at http://emudhra.mu/repository/Digitally_Signing_a_Microsoft_Word_Document.pdf

XI. What is the alternate source for downloading crypto token drivers

Crypto Token drivers are available at http://emudhra.mu/downloads.html under Utilities section

XII. From where can I download Root certificates?

Go to www.emudhra.mu -> Three certificates will be available under CA Certificates Section