AUDIT PROCEDURES

for

REGISTRATION AUTHORITY OFFICE

(Operating under IDRBT CA Office)

INF/PKI/06.03/261/30.0

IDRBT,
Castle Hills, Road No. 1
Masab Tank, Hyderabad,
Andhra Pradesh – 500057, India
Ph: 040 23294217, 19 & 21
Fax: 040 23535157
Email: cahelp@idrbt.ac.in

A Certifying Authority (CA) is a body that fulfills the need for trusted third party services in electronic commerce by issuing Digital Certificates that attest to some fact about the subject of the Certificate. A Certificate is a digitally signed statement by a CA that provides independent confirmation of an attribute claimed by a person offering a Digital Signature. As a Certifying Authority licensed by the Controller of Certifying Authorities (CCA), Government of India, IDRBT CA issues, administers and revokes Digital Certificates of subscribers who are members of INFINET.

The Certificate management involves interaction between entities (called 'end entities' or 'Users') identified by Certificates and CA. These interactions include operations such as registration for certification, Certificate retrieval, Certificate renewal, Certificate revocation and key back-up & recovery. In order to provide maximum operational flexibility, the interactions with end entities or Users are handled by a separate service called Registration Authority (RA).

The RA is an entity dedicated to user registration and accepts requests for digital certificates. User registration is the process of collecting user information and verifying user credentials which is then used to register a user according to the policy of IDRBT CA. The credibility of a certificate issued by IDRBT CA depends on the authentication process adopted by the RA. The Registration Authority Office consists of at least one RA Administrator and at least one RA Officer. The RA Officials verify the certificate/revocation request(s), corresponding credentials of the user, digitally sign the request(s) and submit to IDRBT CA for issuance/revocation of certificate(s). Banks may appoint multiple RA Administrators and RA Officers under the same organization as also may set up multiple RA Offices.

As the RA Office is part and parcel of IDRBT CA, they are to get audited as per the Information Technology Act 2000, Rules and Regulations for Certifying Authorities 2001. IDRBT CA advises the RA Offices to carry out audit as per CCA guidelines issued from time to time.

Audit Requirements

Given below is the audit checklist to be maintained by the RA Office:

1. Certificate Request Details / Application ID

   Checklist of certificate requests as per Annexure-1. This list is to be prepared every six months and has to verified by RA Auditor with subject as "Audit document for xxxxx RA Office during the period of DD/MM/YYYY to DD/MM/YYYY".

- Subscriber application form filled and duly signed by subscriber and approved by RA Officer/RA Administrator as per Appendix-3 of Rules and Guidelines for RA Office document.

- Class 2 certificates are issued to individuals and to the servers used in financial transactions. IDRBT CA is furnishing below various options to RAs to fulfil CCA guidelines with regard to Physical Verification of Class 2 DSC subscribers.

  Option 1: The subscriber will present himself/herself at the respective Bank's RA office physically with required documents as stipulated in CA application form.

  Option 2: The video verification of subscriber should be carried out by RA in accordance with the guidelines specified under IVG and the recording must be preserved by respective RA office for seven years. On demand, the video recording must be shown to auditors during the audit.

  Option 3: The subscriber should submit a letter duly authorized by the subscriber's superior authority to the respective RA. The format of the letter is available at https://idrbtca.org.in. This option should be allowed by RA only in selective and exceptional cases on his/her satisfaction of the circumstances stated in the superior authorization letter and not as a matter of routine.

- Copy of documents of PAN Card or Aadhar and Bank's ID Card attested by Superior Authority With seal are essential for verifying subscriber credentials according to Class of certificate.

- While issuing SSL Certificates, the guidelines issued by CCA that has been circulated to all RAs are to be strictly followed.

2. Revocation Details

   Checklist of Revocation requests as per Annexure-2. This list is to be maintained once in every six months and has to be verified by RA Auditor with subject as "Audit document for xxxxx RA Office during the period of DD/MM/YYYY to DD/MM/YYYY".

   .

   - Certificate Revocation/Suspension form as per Appendix-4 of Rules and Guidelines for RA Office document.

3. Copy of Master Agreement as per Appendix-2 of Rules and Guidelines for RA Office document. In case of multiple RA Offices in the same organization, the **copy of the agreement** should be kept at each RA Office location.

4. Copy of communication with subscriber in paper/electronic media (if any).

5. Copy of communication with IDRBT CA office in paper/electronic media.

6. Financial records should be maintained as per Annexure- 3 as applicable.

7. Details of transfer/termination of duty/revocation of RA Officials'.