



Registration Authority (RA) Guide – Version 1.0

Notations used in the document:

- RA/RA Operator: Registration Authority
- End Entity: User, who is requesting for User/Host Certificate.
- **Brown coloured text** - Highlights the RA activities.
- **Red coloured text** - Indicates Mistakes

Qualification of RA:

1. Every Institution/Organization has only one RA personnel.
2. RA personnel must be the institution/organization employee
3. RA personnel must provide the photo ID.
4. RA personnel must agree to the responsibilities of being RA and maintain the institution/organization activities.

Responsibilities of RA:

1. **Help IGCA to verify the End entity** identity;
2. **RA must meet with end user face to face** (interview).
3. Assist end entities with IGCA services.
4. **Insist end entity to protect his/her private key.**
5. When **RA leaves his/her organization**, should **inform IGCA**.
6. **Report to IGCA**, if any **unusual certificate activities** found.
7. Inform IGCA of any changes to the contact (like email address) or personnel information of the end entities.
8. RA should **inform IGCA**, when the **End Entity leaves the organization**. So that IGCA will revoke the end entities certificates.

9. Archive all activity records and send it to IGCA each year. **RA Record** Form can be found at <http://ca.garudaindia.in/docs/RA-Record.xls>.
10. Should communicate with IGCA securely. (Using **signed emails** - <http://ca.garudaindia.in/index.php/information/faq/how-to-send-digitally-signed-e-mails/>)
11. Also, **record** all **email messages** sent to IGCA.

Face to Face Interview: (RA & subscriber)

If the End Entity applies for User Certificate

1. Make sure the **End Entity prepares the following documents** before the interview:
 - a. Filled user certificate application form.
 - b. Photo ID (Passport, PAN Card, Work ID or Drivier's License)
2. **Verify the User application form with his/her Photo ID.**
3. Verify the Name of the Applicant. **Name should be specific and should not be generic (bioinfo, testing, climate etc.....)**
4. **Verify the CSR No.** field in the application form with the Serial No in <https://ca.garudaindia.in/cgi-bin/pub/pki?cmd=lists;action=newReqs>

(If the above link does not work, Browse - <https://ca.garudaindia.in/pub> → Requests → Certificate Requests). If CSR No. is not filled or incorrect, reject the request and advice the end entity to follow the procedure in <http://ca.garudaindia.in/index.php/certificate/request-a-new-certificate/>
5. **If the information** in the application form **found to be correct** and accurate, **Approve the request** (Check the Approve check box in the application form).
6. Advise the End Entity to protect his/her private key (secure with passphrase of minimum 12 characters in length) and inform RA in case of private key loss.
7. **If the information** in the application form **found to be incorrect, reject the request.**
8. If you have any comment, mention in the comments field and **sign the request.**

9. **Record the events** in the **RA Record Form** (<http://ca.garudaindia.in/docs/RA-Record.xls>) and save it in your machine. (This form is required to be sent to IGCA every year, upon request)

If the End Entity applies for Host Certificate

1. **End Entity** requesting for Host Certificate should have **User Certificate**.
2. If the End Entity applies for host certificate **without having User Certificate**, **reject the request** and advice to follow the procedure defined in <http://ca.garudaindia.in/index.php/certificate/host-certificate-request-process/>
3. If the End Entity has User Certificate and applies for Host Certificate, RA should **verify the User cert. no** in the application. (Can be compared with list of issued certificates found at <https://ca.garudaindia.in/cgi-bin/pub/pki?cmd=lists;action=certslist> . Click on the Serial no of the certificate, which you like to verify and confirm the details.
4. **Verify the Certificate Request No (CSR No.)** for each hostname in the application form. Verify the CSR No. with Serial in <https://ca.garudaindia.in/cgi-bin/pub/pki?cmd=lists;action=newReqs>. Confirm with End Entity about the Fully Qualified Domain Name (FQDN) that he/she would like to request certificate. FQDN should be valid one as e.g.:
gridfs.ctsf.cdac.org.in
5. **If the information** in the application form **found to be correct** and accurate, **Accept the request** (Check the Accept check box in the application form - Refer RA Operator Column).
6. **If the information** in the application form **found to be incorrect**, **reject the request**.
7. If you have any comments, mention in the comments field and **sign the request**.
8. **Record the events** in the **RA Record Form** (<http://ca.garudaindia.in/docs/RA-Record.xls>) and save it in your machine. (This form is required to be sent to IGCA every year, upon request)

In Case, if the End Entity leaves the organization

1. RA should **inform IGCA** with following information's,
 - a. Name of the User leaving the organization.
 - b. Information of the Certificates, he holds.
2. If RA has user certificate, can send the signed e-mails.
(<http://ca.garudaindia.in/index.php/information/faq/how-to-send-digitally-signed-e-mails/> - procedure to send signed emails).

In case, if the End Entity requests for Re-key

This procedure will be available in RA Guide V1.1

IGCA: Contact Information

Email: igca@cdacb.ernet.in

Phone No: 080-66116511, 080-66116502

Website: <http://ca.garudaindia.in>