Guidelines for installing biometric device for Aadhar Verification of Beneficiaries on BIS

The biometric devices provided for Aadhar verification of beneficiaries on BIS portal is **Startek FM 220U**

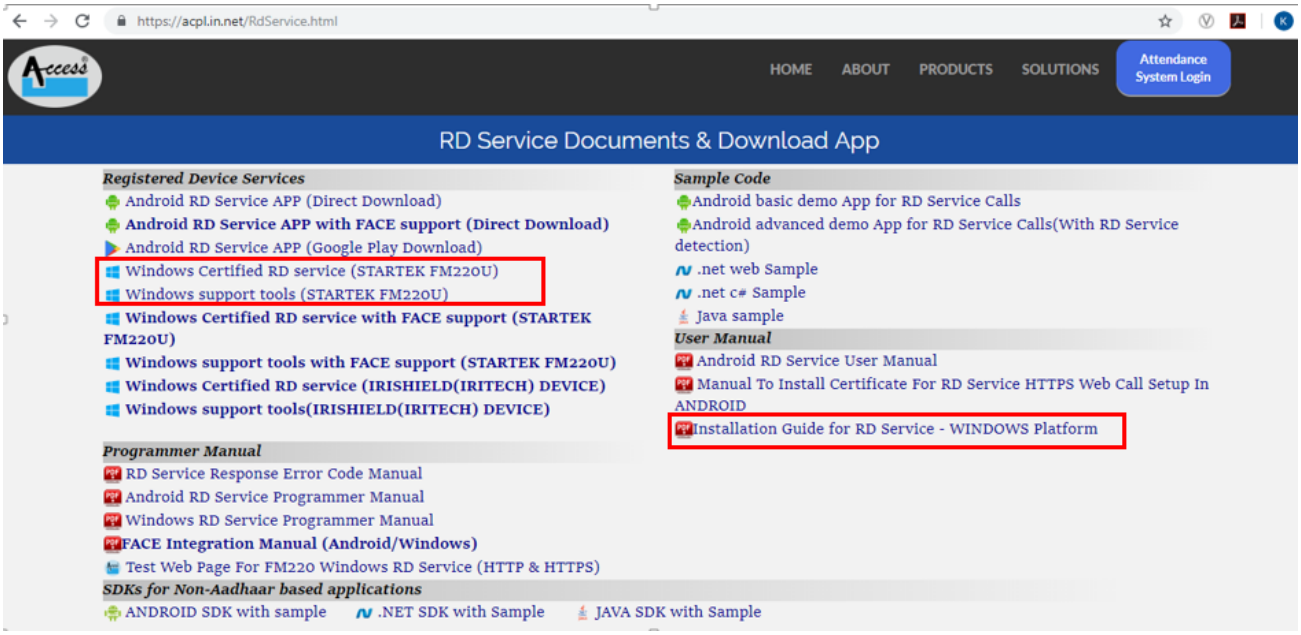
This device has to be installed and registered with UIDAI for it to work properly on BIS portal. Following are the steps to install and register the finger print device.

1. Open the following link on Google Chrome

   https://acpl.in.net/RdService.html

2. Download the following software/RD services (please refer the screenshot for more details)

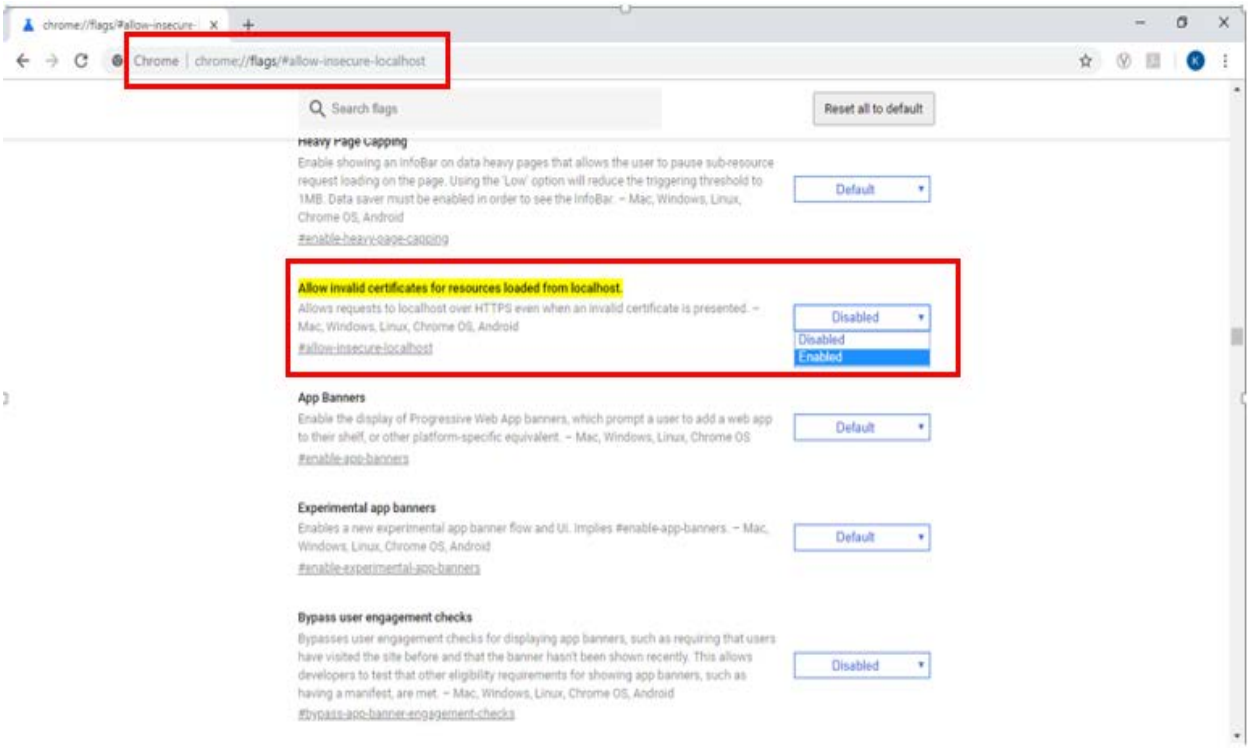
   i. Windows Certified RD service
   ii. Windows support tools
   iii. Installation guide for RD service–Windows platform (for any clarification on RD service)



3. After installation of relevant Biometric device, please open Google Chrome and type the following where URL is typed (place where we type the link of any website)

   chrome://flags/#allow-insecure-localhost

4. Select **"*ENABLED*"** option for Allow invalid certificates for resources loaded from localhost



With the above steps executed successfully, the biometric device should work on the BIS portal and the section on BIS where Aadhar number is to be entered will become enabled and the font will turn Green.

Further details on RD services are as follow:-

Below is the list of some UID complaint biometric devices used in Jeevan Pramaan https://jeevanpramaan.gov.in and link for registration of device.

Importance of Registered Device Services are as follow:-

All biometric devices for Aadhaar authentication are mandatory to be registered with UIDAI w.e.f. 01-Oct-17.

Registered devices addresses the solution to eliminate the use of stored biometrics. It provides three key additional features compared to public devices:

1. Device identification – every device having a unique identifier allowing traceability, analytics,

and fraud management.

2. Eliminating use of stored biometrics – biometric data is signed within the device using the provider key to ensure it is indeed captured live. Then the Registered Device (RD) Service of the device provider must form the encrypted PID block before returning to the host application.

3. A standardized RD Service provided by the device providers that is certified.