

**GEMALTO RD UTILITY
AND
BIOMETRIC ENROLMENT APPLICATION**

*Project report submitted in partial fulfilment of the requirement for the degree
of*

**BACHELOR OF TECHNOLOGY
IN
COMPUTER SCIENCE AND ENGINEERING**

By

PRIYANJUL JOHARI (141269)

UNDER THE GUIDANCE OF

Mr. SWAMI SARAN



Department of Computer Science & Engineering and Information
Technology

**Jaypee University of Information Technology Waknaghat, Solan-
173234, Himachal Pradesh**

TABLE OF CONTENTS

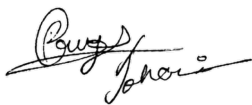
| Title | Page Number |
|--|--------------------|
| DECLARATION BY THE SCHOLAR | iv |
| SUPERVISOR’S CERTIFICATE | v |
| ACKNOWLEDGEMENT | vi |
| LIST OF ABBREVIATIONS AND ACRONYMS | vii |
| LIST OF FIGURES | ix |
| LIST OF TABLES | xi |
| ABSTRACT | xii |
| 1. CHAPTER – 1: INTRODUCTION | 1 - 4 |
| 1.1. About the Company | 1 |
| 1.2. Understanding Aadhaar Authentication | 1 |
| 1.2.1. Aadhaar Number | 1 |
| 1.2.2. Aadhaar Authentication at a Glance | 2 |
| 1.2.3. Aadhaar Authentication Usage | 2 |
| 1.3. Registered Devices | 3 |
| 1.3.1. Public Devices | 3 |
| 1.3.2. Registered Devices | 4 |
| 2. CHAPTER – 2: LITERATURE SURVEY | 5 - 6 |
| 2.1. Aadhar Authentication API Specification – Version 2.0 (Revision 1) | 5 |
| 2.2. Aadhar Registered Devices Technical Specification – Version 2.0 (Revision 2) | 5 |
| 3. CHAPTER – 3: SYSTEM DEVELOPMENT | 7 - 17 |
| 3.1. Gemalto RD Utility | 7 |
| 3.1.1. Aadhaar Authentication API | 7 |

| | | |
|-----------|--|----------------|
| 3.1.1.1. | Authentication Flow | 7 |
| 3.1.1.2. | API Protocol | 9 |
| 3.2. | Biometric Enrolment Application | 11 |
| 3.2.1. | Enrolment Devices | 11 |
| 3.2.1.1. | CSD200i | 11 |
| 3.2.1.2. | CS500e | 12 |
| 3.2.1.3. | CIS202 | 12 |
| 3.2.2. | Device SDK | 12 |
| 3.2.3. | Scanning Biometrics | 13 |
| 3.2.3.1. | Fingerprint Scanning (Geometric Accuracy Test) | 13 |
| 3.2.3.2. | Iris Scanning (Modulation Test) | 16 |
| 4. | CHAPTER – 4: PERFORMANCE ANALYSIS | 18 - 38 |
| 4.1. | Gemalto RD Utility | 18 |
| 4.1.1. | Authentication | 18 |
| 4.1.1.1. | Request Access | 19 |
| 4.1.1.2. | Grant Access | 20 |
| 4.1.2. | Development Environments | 21 |
| 4.1.2.1. | Pre-Production | 21 |
| 4.1.2.2. | Production | 22 |
| 4.1.3. | Modules | 22 |
| 4.1.3.1. | Device Status | 22 |
| 4.1.3.2. | Token Status | 24 |
| 4.1.3.3. | Device Whitelist | 26 |
| 4.1.3.4. | Device Deregistration | 28 |
| 4.1.3.5. | Token Generation | 29 |
| 4.2. | Biometric Enrolment Application | 30 |
| 4.2.1. | Applicant Form | 30 |
| 4.2.2. | Fingerprint Enrolment | 31 |
| 4.2.2.1. | CSD200i | 31 |
| 4.2.2.2. | CS500e | 33 |
| 4.2.3. | Iris Enrolment: CIS202 | 36 |

| | |
|---|-------------|
| 4.2.4. Authentication (Future Prospect) | 37 |
| 4.2.5. Acknowledgement | 37 |
| CHAPTER – 5: CONCLUSIONS | 39 |
| REFERENCES | xiii |
| LIST OF PUBLICATIONS | xiv |

DECLARATION BY THE SCHOLAR

We hereby declare that the work reported in the B-Tech thesis entitled “**Gemalto RD Utility and Biometric Enrolment Application**” submitted at **Jaypee University of Information Technology, Wagnaghat, India**, is an authentic record of my work carried out under the supervision of **MR. SWAMI SARAN**. We have not submitted this work elsewhere for any other degree or diploma.



Priyanjul Johari, 141269

Department of Computer Science and Engineering
Jaypee University of Information Technology
Wagnaghat, India

Dated:



JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY

(Established by H.P. State Legislative vide Act No. 14 of 2002)
P.O. Wahnaghat, Teh. Kandaghat, Distt. Solan - 173234 (H.P.) INDIA

Website: www.juit.ac.in

Phone No. (91) 01792-257999

Fax: +91-01792-245362

CERTIFICATE

I hereby declare that the work presented in this report entitled “**GEMALTO RD UTILITY AND BIOMETRIC ENROLMENT APPLICATION**” in partial fulfilment of the requirements for the award of the degree of **Bachelor of Technology in Computer Science and Engineering** submitted in the department of Computer Science & Engineering and Information Technology, Jaypee University of Information Technology, Wahnaghat, is an authentic record of my own work carried out over a period from February 2018 to May 2018 under the supervision of **Mr. Swami Saran**, technical manager, Department of Government Programs, Gemalto Digital Security Private Ltd.

The matter embodied in the report has not been submitted for the award of any other degree or diploma.

Priyanjul Johari, 141269

This is to certify that the above statement made by the candidate is true to the best of my knowledge.

Mr. Swami Saran

Technical Manager

Department of Government Programs

Gemalto Digital Security Private Ltd.

Bangalore

Dated:

ACKNOWLEDGEMENT

It is a pleasure to express my deep appreciation and gratitude to my mentor and to guide MR. SWAMI SARAN, Technical Director, Government Programs Department, Gemalto Digital Security Private Ltd., Bangalore, Karnataka. His dedication and keen interest, and primarily, his overwhelming attitude to help his team had been solely and mainly responsible for the completion of my work. Timely advice, meticulous review, scholarly advice and a scientific approach have helped me a lot.

I owe a deep sense of gratitude to all my team, respectful and supportive, who helped me to participate in the very early stages of project development and I expect them to continue to guide me constantly. Their prompt inspirations, timely suggestions with kindness, enthusiasm and dynamism allowed us to complete my thesis.

I thank very much MR. PARAS PATEL, Software Engineer, Government Programs Department, Gemalto Digital Security Private Ltd, Bangalore, Karnataka, for his help and cooperation throughout my development period.

PRIYANJUL JOHARI (141269)

LIST OF ABBREVIATIONS AND ACRONYMS

| | |
|--------|--|
| API | Application Program Interface |
| ASA | Authentication Service Agency |
| AUA | Authentication User Agency |
| CIDR | Central Identities Data Repository |
| CSV | Comma Separated Value |
| DLL | Digital Logic Library |
| FMR | Finger Minutiae Record |
| FP | Fingerprint |
| GDSPL | Gemalto Digital Security Private Limited |
| HSM | Hardware Security Module |
| HTTP | Hypertext Transfer Protocol |
| HTTPS | Hypertext Transfer Protocol Secure |
| HW | Hardware |
| ID | Identity |
| IIR | Iris Image Record |
| ISO | International Standards Organization |
| JSON | JavaScript Object Notation |
| MNREGA | Mahatma Gandhi National Rural Employment Guarantee Act |
| OTP | One Time Password/Pin |
| PC | Personal Computer |
| PD | Public Devices |
| PDF | Portable Document Format |
| PID | Personal Identity Data |
| PIN | Personal Identification Number |

| | |
|-------|--|
| PoS | Point of Sale |
| RD | Registered Devices |
| SDK | Software Development Kit |
| SMS | Short Message Service |
| UI | User Interface |
| UIDAI | Unique Identification Authority of India |
| URL | Uniform Resource Locator |
| UX | User Experience |
| XML | Extensible Markup Language |

LIST OF FIGURES

| Figure No. | Caption | Page no. |
|-------------------|---|-----------------|
| 1.1 | Logical Diagram of a RD | 4 |
| 3.1 | Aadhaar authentication flow under various scenarios | 9 |
| 3.2 | Gemalto Cogent Single Fingerprint Scanner CSD200i | 11 |
| 3.3 | Gemalto Cogent Tenprint Scanner CS500e | 12 |
| 3.4 | Gemalto Cogent Iris Scanner CIS202 | 12 |
| 3.5 | 1 lp/mm test card | 13 |
| 3.6 | lp/mm target | 17 |
| 4.1 | Gemalto RD Utility Sign in Page | 18 |
| 4.2 | Gemalto RD Utility Registration Page | 19 |
| 4.3 | Gemalto RD Utility Access Status Page | 20 |
| 4.4 | mLab MongoDB for Gemalto RD Utility | 20 |
| 4.5 | Android Application for granting access to Gemalto RD Utility | 21 |
| 4.6 | Gemalto RD Utility - Device Status Page (pre-prod) | 22 |
| 4.7 | Gemalto RD Utility - Device Status Bulk Mode Page (pre-prod) | 23 |
| 4.8 | Gemalto RD Utility - Token Status Page (pre-prod) | 24 |
| 4.9 | Gemalto RD Utility - Token Status Bulk Mode (pre-prod) | 25 |
| 4.10 | Gemalto RD Utility - Device Whitelist Page (pre-prod) | 26 |
| 4.11 | Gemalto RD Utility Device - Whitelist Bulk Mode Page (pre-prod) | 27 |
| 4.12 | Gemalto RD Utility - Device Deregistration (pre-prod) | 28 |
| 4.13 | Gemalto RD Utility - Token Generation Page (pre-prod) | 29 |
| 4.14 | Biometric Enrolment Application - User Form | 30 |
| 4.15 | Biometric Enrolment Application - Choose Device Pop Dialog | 31 |

| | | |
|------|---|----|
| 4.16 | Biometric Enrolment Application - CSD200i Enrolment Module | 31 |
| 4.17 | Biometric Enrolment Application - CSD200i Image boxes with Fingerprints | 32 |
| 4.18 | Biometric Enrolment Application - CS500e Enrolment Module | 33 |
| 4.19 | Biometric Enrolment Application - Device List Dialog | 33 |
| 4.20 | Biometric Enrolment Application - Initiating Capture | 34 |
| 4.21 | Biometric Enrolment Application - Capturing Right Slap | 34 |
| 4.22 | Biometric Enrolment Application - Capturing Left Slap | 34 |
| 4.23 | Biometric Enrolment Application - Capturing Thumbs | 35 |
| 4.24 | Biometric Enrolment Application - Fingerprint Card | 35 |
| 4.25 | Biometric Enrolment Application - Capture Failure | 35 |
| 4.26 | Biometric Enrolment Application - Iris Enrolment Module | 36 |
| 4.27 | Biometric Enrolment Application - Iris Preview | 37 |
| 4.28 | Biometric Enrolment Application - Acknowledgment | 37 |

LIST OF TABLES

| | | |
|-----------|--------------------------------|----|
| TABLE 4.1 | Device Status I/O | 23 |
| TABLE 4.2 | Device Status Bulk Mode I/O | 23 |
| TABLE 4.3 | Token Status I/O | 24 |
| TABLE 4.4 | Token Status Bulk Mode I/O | 25 |
| TABLE 4.5 | Device Whitelist I/O | 26 |
| TABLE 4.6 | Device Whitelist Bulk Mode I/O | 27 |
| TABLE 4.7 | Device Deregistered I/O | 28 |
| TABLE 4.8 | Token Generation I/O | 29 |

ABSTRACT

This report covers two immensely crucial desktop applications which I got a chance to develop during my internship (tentatively ending in July) in Gemalto, Bangalore. The first application is Gemalto RD Utility which assists the AUAs to perform various tasks like checking status of their biometric device, generating tokens for AUAs, checking token status and deregistering devices in pre-production and production stages. The underlying principles behind the execution of this utility is to keep devices consistent with the protocols of RD Services devised the Government of India. The desktop application communicates with the server through http requests the APIs for which have been provided by team. The second application is Biometric Enrolment Application and as the name suggests, this application communicates with fingerprint and iris scanners connected to the system and accepts the biometric signatures of the applicant. As a future prospect, this application will also authenticate the user after enrolment.

CHAPTER – 1

INTRODUCTION

1.1 About the Company

GDSPL provides RD Services to the customers for Adhaar Authentication & Validation which is carried out by means of highly secure and tested biometric devices. These biometric devices are RDs and not PDs. In a more or less similar manner, the enrolment and authentication of the user through Biometric Enrolment Application have to be and must be carried by RDs only. Hence, before commencing and moving forward to subtle technicalities, it will be best to have an idea about basics of Adhaar Authentication, RD Services and public and registered devices.

1.2 Understanding Aadhaar Authentication

The Unique Identification Authority of India (UIDAI) was created, with the mandate to provide a unique identity (Aadhaar) to all Indian residents. UIDAI provides online authentication to verify Aadhaar holder's identity claim. Aadhaar "authentication" refers to the process by which the Aadhaar number, as well as other attributes, including biometrics, are submitted to the Central Identity Data Repository (CIDR) for verification on the basis of available information or data or documents. UIDAI provides an online service to support this process. The Aadhaar authentication service responds only with a "yes / no" and no personal identity information is returned as part of the response.

1.2.1 Aadhaar Number

The Unique Identification (Aadhaar) Number gives individuals the means to clearly establish their identity to public and private agencies across the country. Three key characteristics of Aadhaar Number are:

1. Permanency (Aadhaar number remains same during lifetime of the person)
2. Uniqueness (one Aadhaar holder has one ID and no two Aadhaar holders have same ID)

3. Global (same identifier can be used across applications and domains)

Aadhaar Number is provided during the initiation process called *enrolment* where his/her demographic and biometric information are collected and uniqueness of the provided data is

established through a process called *de-duplication*. Post de-duplication, an Aadhaar Number is issued and a letter is sent to Aadhaar holder informing the details.

1.2.2 Aadhaar Authentication at a Glance

Aadhaar authentication is the process by which the Aadhaar number, along with other attributes, including biometrics, are submitted online to CIDR for verification based on information or data or documents available with it.

Aadhaar authentication provides several ways in which an Aadhaar holder can authenticate using the system. At a high level, authentication can use demographics and / or biometric data (FP / Iris / Face) and / or OTP. Face authentication is currently not supported.

During the authentication transaction, the registration of the Aadhaar holder is first selected using the Aadhaar number, and then the demographic / biometric data is compared to the data stored in CIDR that was provided by the Aadhaar holder during the process of registration / update.

1.2.3 Aadhaar Authentication Usage

Aadhaar authentication allows agencies to verify the identity of Aadhaar holders using an online and electronic means where the agency collects Aadhaar holder's required information with the Aadhaar number and forwards it to the UIDAI systems for verification.

The Aadhaar authentication service provides services to instantly verify the identity of the Aadhaar holder against the data available in CIDR. Depending on the needs of the service, different identifiers could be used with the Aadhaar number. These identifiers can be a combination of biometric data (such as fingerprints, iris prints) and / or

demographic information (such as name, date of birth, address) and / or password(OTP/PN).

The number of Aadhaar as well as some demographic information such as name, date of birth, etc. help provide simple authentication requirements. For example, when the beneficiary MGNREGA is registered and receives a card of employment, the holder of Aadhaar can be authenticated biometrically compared to the system Aadhaar to verify his number Aadhaar with his name and his address. [1]

1.3 Registered Devices

This section describes the specification in detail for registered devices for biometric device providers and also provides details on registration flow before these can be used with larger host devices.

1.3.1 Public Devices

Before understanding the registered devices and their necessity, it is important to understand how public devices work.

Public devices are biometric capture devices that provide Aadhaar-compliant biometric data to the application, which, in turn, encrypts the data before using it for authentication purposes. Currently, AUA / Sub-AUA applications handle biometric capture return user experience, PID block validation and encryption. With public appliances, vendors may or may not provide easy-to-use libraries to application developers.

Several security measures are taken to ensure transaction security and end-to-end traceability even in public devices. These safety measures fall under prevention and traceability. This includes deployment of signed applications, AUA host and operator authentication, use of multifactor authentication, resident SMS / Email alerts on authentication, biometric locking, encryption / decryption. the signature of sensitive data, etc. [2]

1.3.2 Registered Devices

The specification of registered devices described in this document concerns the solution to eliminate the use of the stored biometry. It provides three key additional features over public devices:

- 1. Device identification** - each device having a unique identifier for traceability, analysis and fraud management.
- 2. Eliminate use of stored biometrics** - biometric data is signed inside the device using the vendor's key to ensure that they are actually captured live. Then, the device provider's registered device (RD) service must form the encrypted PID block before returning to the host application.
- 3. A standardized RD service provided by device vendors that is certified.** This RD service (exposed through the service interface defined in this specification) encapsulates biometric capture, any user experience when capturing (such as preview), and the signature and encryption of biometrics all in it.

Here is the logic diagram of a registered device (for illustrative purposes only, the actual hardware design may differ). [2]

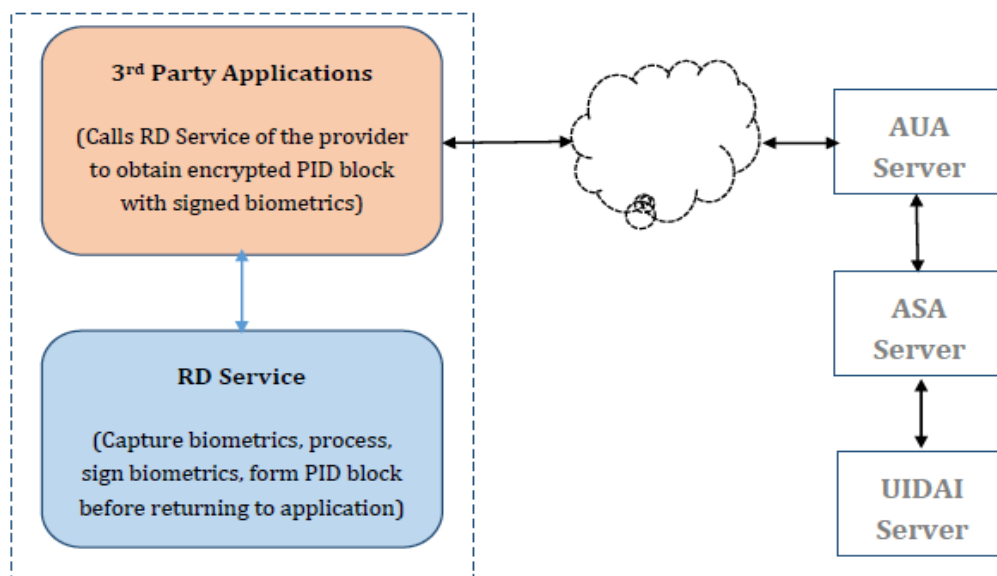


Figure 1.1 : Logical Diagram of a RD [2]

CHAPTER - 2

LITERATURE SURVEY

For the development of these applications, the basic understanding of the RD services, registered devices, workflow of API, encryption procedure and other minute details have been gained from the following documents provided to GDSPL by UIDAI:

2.1 Aadhar Authentication API Specification – Version 2.0 (Revision 1)

UIDAI.

This document provides the specification for the Aadhaar Authentication API (Application Programming Interface). It contains details, including the API data format, protocol, and security specifications. The Aadhaar Act (Targeted Supply of Grants and Other Benefits, Benefits and Services Act, 2016) was published on March 26, 2016 in a notification issued on March 27, 2016. This law provides for good governance, effective distribution, transparent and targeted grants, benefits and services to Aadhaar number holders. A gazette notice was issued by the central government on July 12, 2016 to establish UIDAI as the Authority² and to operationalize certain provisions of the Aadhaar 2016 Law. Authentication regulations are also issued under this law. These documents specify the legal framework for the use of authentication, AUA / ASA commitments, audits and other details. Detailed documents on the partners are also published. [1]

2.2 Aadhar Registered Devices Technical Specification – Version 2.0 (Revision 2)

UIDAI.

This is a technical document intended primarily for manufacturers / suppliers of biometric devices who wish to create devices registered in accordance with this

specification for the Aadhaar authentication ecosystem. This document assumes that readers are fully conversant with the Aadhaar authentication model, associated terminology, and the details of Authentication API technology. The Unique Identification Authority of India (UIDAI) was created, with the mandate to provide a unique identity (Aadhaar) to all Indian residents. UIDAI provides online authentication using demographic and biometric data. Aadhaar authentication is the process by which the Aadhaar number, along with other attributes, including biometrics, are submitted online to the Aadhaar system for verification based on information or data or documents available with the system. During the authentication transaction, the resident's record is first selected using the Aadhaar number, and then the demographic / biometric entries are compared with the stored data that was provided by the resident during the registration / upgrade process day. [2]

CHAPTER – 3

SYSTEM DEVELOPMENT

3.1 Gemalto RD Utility

RD Service is a complex system consisting of frequent to & fro calls to UIDAI database and HSM Server to accomplish validation, generation, authentication & other tasks. This is made possible by using Aadhaar Authentication APIs.

3.1.1 Aadhaar Authentication API

This chapter describes the API in detail including the authentication flow, communication protocol, and data formats.

3.1.1.1 Authentication Flow

The following diagram explains various authentication scenarios and data flows.

Scenario 1 of the diagram is a typical authentication flow and is a case of an operator assisted transaction on a PoS terminal: 1

- a) The Aadhaar holder provides the Aadhaar number or AUA / Sub-AUA identifier, demographic and biometric details required for AUA / Sub-AUA terminals (or AAU / Sub-AUA-nominated merchant / operator) to obtain a service offered by AAU / sub-AUA.
- b) The authentication-enabled Aadhaar application software that is installed on the device conditions these

TECHNOLOGY USED

| | |
|----------|-----------------|
| LANGUAGE | JAVA |
| VERSION | JDK7 |
| IDE | ECLIPSE LUNA |
| GUI TOOL | JAVA SWING |
| DATABASE | MongoDB |

input parameters, encrypts them, and sends them to the AUA server over a mobile / broadband network using a specific AUA protocol.

c) The AUA server, after validation, adds the necessary headers (AUA XML specific envelope with license key, signature, etc.), and sends the request via the ASA server to UIDAI CIDR.

d) The Aadhaar authentication server returns a "yes / no" based on the match of the input parameters.

e) Based on the response of the Aadhaar authentication server, AUA / Sub-AUA performs the transaction.

Scenario 2 below describes the holder of Aadhaar performing assisted / self-service transactions with Aadhaar authentication on their mobile or over the Internet.

a) In this case, the transaction data is captured on the mobile / internet application provided by AUA / Sub-AUA.

b) The holder of Aadhaar provides the necessary demographic data for a long time with OTP (fingerprint / iris is also possible but not yet common on mobile or PC) in addition to the specific attributes AUA (account number, password, PIN, etc.).

c) Steps c, d and e are the same as in scenario 1 above.

Scenario 3 is a slight variant of the second scenario where AUA also plays ASA and has direct connectivity to UIDAI data centers. Scenario 4 explains how AAUs and application developers can test Aadhaar authentication using the public URL.

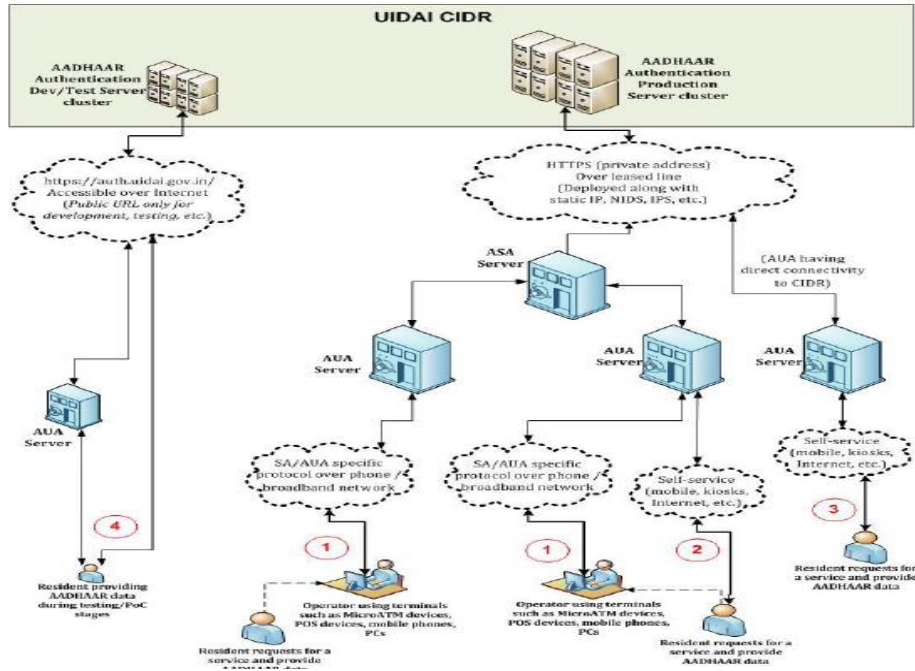


Figure 3. 1: Aadhaar authentication flow under various scenarios.

3.1.1.2 API Protocol

Aadhaar authentication service is exposed as stateless service over HTTPS. Usage of open data format in XML and widely used protocol such as HTTP allows easy adoption and deployment of Aadhaar authentication. To support strong end to end security and avoid request tampering and man-in-the-middle attacks, it is essential that encryption of data happens at the time of capture on the capture device.

Following is the URL format for Aadhaar authentication service:

`https://<host>/<ver>/<ac>/<uid[0]>/<uid[1]>/<asalk>`

The API input data must be sent to this URL as an XML document using the content type "application / xml" or "text / xml".

Here are detailed explanations of what the different tags in the URL format for the Aadhaar Authentication Service really mean and what role they play in the RD service environment:

- host - Aadhaar authentication server address. The actual address of the production server will be provided to the ASAs. Note that production servers can only be accessed via a private secure connection. The ASA server must ensure that the actual URL is

configurable. (For development and testing purposes, the public URL "auth.uidai.gov.in" can be used.)

- worm - Authentication API version (optional). If not provided, the URL points to the current version. UIDAI can host multiple versions to support progressive migration. From this specification, the default production version is "2.0".
- ac - A unique code for AUA assigned by UIDAI. This is an alphanumeric string with a maximum length of 10. (A "public" default value is available for testing.)
- uid [0] and uid [1] - first 2 digits of the Aadhaar number. Used for load balancing.
- asalk - A valid ASA license key. ASAs must send one of their valid license keys at the end of the URL. It is important that license keys are kept safe.

When you add a license key to the URL, make sure that it is URL encoded to handle special characters.

For all valid responses, the HTTP 200 response code is used. All application error codes are encapsulated in the response XML element. In case of connection and other server errors, standard HTTP error response codes are used (4xx codes such as 403, 404, etc.). Automatic HTTP redirects must also be handled by the ASA server.

Another important aspect of Authentication and RD Services is creation of PID block which contains all the encrypted information about the session including biometrics which need to be sent to UIDAI database where they are compared with data stored in CIDR and authentication is performed thereafter. The entire process is not discussed in the report as it is beyond the scope of it.

3.2 Biometric Enrolment Application

As discussed earlier, the Biometric Enrolment Application communicates with the biometric devices connected with the computer and captures biometric signatures. This is achieved by classes and functions defined in the DLLs present in the device SDK developed by the research and development team. One major prerequisite of using Biometric Enrolment Application is to have biometric devices and buy RD Services. A license is also required for enrolment and authentication which can be bought (or a demo can also be provided for 90 days) from the RD service vendor.

TECHNOLOGY USED

| | |
|-----------|-----------------------|
| LANGUAGE | .NET (C#) |
| FRAMEWORK | .NET 4.0 |
| IDE | VISUAL STUDIO 2010 |
| GUI TOOL | WPF |

3.2.1 Enrolment Devices

A brief description of the enrolment devices compatible with the application is given below.

3.2.1.1 CSD200i

- 500ppi resolution
- USB 2.0 interface
- Ambient light rejection
- Large active platen area
- 10 frames/second image capture
- Fully featured with auto capture, adjustable brightness, contrast and gain functions
- FBI PIV-071006
- Mobile ID FAP20



Figure 3. 2: Gemalto Cogent Single Fingerprint Scanner CSD200i

3.2.1.2 CS500e

- Supports flat and/or rolled capture capabilities
- Automatic calibration and table updates
- Preformatted data fields based on predefined lists
- Configurable data input features to meet state and federal specifications
- Fully compliant with ANSI/NIST standards
- FBI Appendix F
- Submission acknowledgement, tracking, and reporting
- Lightweight, compact design



Figure 3. 3: Gemalto Cogent Tenprint Scanner CS500e

3.2.1.3 CIS202

- Simultaneous dual iris capture
- IP 54 rating, optional IP 65 hardened housing available
- Unaffected by ambient lighting
- Adjustable interpupillary distance
- Compliant with NIST SAP Level 40
- Compliant with ANSI NIST and ISO image interchange format
- Meets safety standards for LED products
- Easy-to-clean housing



Figure 3. 4: Gemalto Cogent Iris Scanner CIS202

3.2.2 Device SDK

The SDK for the devices listed above have been developed by our research and development team. This SDK contains DLLs for interacting with the respective biometric devices :

- **CgtFpAccessCSD200Dotnet.dll** : This dll file contains classes, methods and interfaces to initialize, calibrate and capture fingerprint from CSD200i device in .bmp format.

- **CLSFPCaptureDllWrapper.dll** : This dll file is a wrapper file built on top of *CLSFPCaptureDLL.dll* which contains classes, methods and interfaces to initialize, calibrate, capture and save segmented and unsegmented fingerprints in .bmp format from CS500e device in .bmp format.
- **CG4IrisApi.dll** : This dll file contains classes, methods and interfaces to initialize, calibrate and capture iris from CIS202 device in .bmp format.
- **BioSdk710Wrapper.dll** : This dll file generates .fmr(for fingerprints)/.iir(for iris) file from the .bmp biometric image files captured from devices already listed above. A .fmr/.iir file is also called ISO Template and is used to match biometrics for authentication purpose. The phenomenon of generation of ISO Template(.fmr/.iir) from Bitmap Image(.bmp) is called FMR/IIR Extraction.

3.2.3 Scanning Biometrics

Scanning human biometric data is a tricky and intricate task and requires utmost accuracy. Here's a synopsis how this is achieved.

3.2.3.1 Fingerprint Scanning (Geometric Accuracy Test)

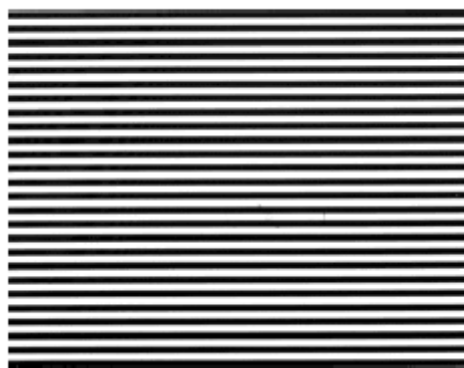


Figure 3. 5: 1 lp/mm test card.

Scanner resolution and geometric accuracy are measured using a precision Ronchi target having a constant spatial frequency of 1.0 cy/mm; i.e., the combined width of one black bar plus one adjacent white space is 1.0 mm, which is one cycle, or one period.

Test Procedures

1. Clean the prism surface
2. Run the testing software ScanTest.exe, which is located in “C:\Gemalto Cogent-STQC-Testing\FingerprintScanner_CS500e\CaptureSoftware\ScanTest”.
3. Click “Connect”, wait for the scanner initialization until the preview screen is displayed.
4. Drop some water on the prism surface and carefully put the 1 lp/mm test card on the prism in horizontal direction, make sure no air gap (bubbles) between the test card and prism. If there’s wrap on the corner or edge of target card, put some flat object on the card to ensure the close contact between card and prism.
5. Click button “Save Image”. The target image is saved to “C:\Gemalto Cogent-STQC-Testing\FingerprintScanner_CS500e\CaptureSoftware\ScanTest\Pics\- 6. Copy this target image to folder “C:\Gemalto Cogent-STQC-Testing\FingerprintScanner_CS500e\2. GEO\”, and rename it to “H.raw”.
- 7. Run MITRE testing program runGeoH.bat, which is on “C:\Gemalto Cogent-STQC-Testing\FingerprintScanner_CS500e\2. GEO\”. A report will be generated.
- 8. Remove the target from platen, and clean the surface.
- 9. Drop some water on the prism surface and carefully put the 1 lp/mm test card on the prism in vertical direction, make sure no air gap (bubbles) between the test card and prism. If there’s wrap on the corner or edge of target card, put some flat object on the card to ensure the close contact between card and prism.
- 10. Click button “Save Image”. The target image is saved to “C:\Gemalto Cogent-STQC-Testing\FingerprintScanner_CS500e\CaptureSoftware\ScanTest\Pics\- 11. Copy this target image to folder “C:\Gemalto Cogent-STQC-Testing\FingerprintScanner_CS500e\2. GEO\”, and rename it to “V.raw”.
- 12. Run MITRE testing program runGeoV.bat, which is on “C:\Gemalto Cogent-STQC-Testing\FingerprintScanner_CS500e\2. GEO\”. A report will be generated.

Requirements Compliance

1. The resolution should be between 495.0 and 505.0 ppi
2. The across-bar geometric accuracy requirement is complied with if at least 99.0 percent of the tested cases, in each print block measurement area, and in each direction, are within the minimum and maximum distance limits defined in following table
3. The along-bar geometric accuracy requirement is complied with if at least 99.0 percent of the test measurement values, in each print block measurement area and in each direction, are less than 0.016 inches.

The output of geo.exe looks like

Grand Totals

Horizontal Test Measurement Areas

1-Bar Distance

No horizontal 1-bar tests performed

6-Bar Distance

No horizontal 6-bar tests performed

Resolution

Horizontal resolution not checked

No Distortion Tests Performed

Vertical Test Measurement Areas

1-Bar Distance

0 out of 270 checks (0.0%) fail the F Spec (0.0007")

6-Bar Distance

0 out of 45 checks (0.0%) fail the F Spec (0.0023622")

Resolution

Out of 45 checks (0.0%) fail Resolution (500 +/-5)

No Distortion Tests Performed

Resolution Summary

Vertical

min 501.299 max 502.238 mean 501.794 std dev 0.249

3.2.3.2 Iris Scanning (Modulation Test)

1. Mount target on CIS-202, connect target to power supply so LED is on.
2. Launch the testing program CDualIris.exe, which is located in “C:\Gemalto Cogent-STQC-Testing\IrisScanner_CIS202\Software\CDualIris\”.
 - a. Click button “Visual Light off” and “NIR Light off” to turn off the white light and NIR light.
 - b. Adjust the Exposure value, so that the gray scale of the white block on result image is close to 250.
 - c. Click “Manual Capture” to force taking result image, which is stored to local disk automatically. The result images are located in “C:\Gemalto Cogent-STQC-Testing\IrisScanner_CIS202\Software\CDualIris\Images\”.
 - d. Check the mean gray scale value of white block on the target result image.
 - e. If the mean gray scale value is larger than 250, lower the exposure value and repeat the step c and d.
 - f. If the mean gray scale value is lower than 235, increase the exposure value and repeat the step c and d.

Note: The different iris scanner might need different exposure value. So this process may need several iterations to get desired target result image.

3. Test optical resolution (at least 60% modulation)
 - a. Open the result image in Photoshop
 - b. Pick up a block in white area and calculate the mean gray scale level W1 using Adobe Photoshop or similar image analysis software.
 - c. Pick up a black block near to white area, and calculate the mean gray scale level B1
 - d. Pick up a line pair on 4lp/mm area whose contrast is biggest and calculate the mean gray scale level W2 and B2. Note: this might need several attempts to find the best pair.
 - e. Calculate the modulation using formula $(W2-B2)/(W2+B2)/((W1-B1)/(W1+B1))$. The expected value should be greater than 0.6.

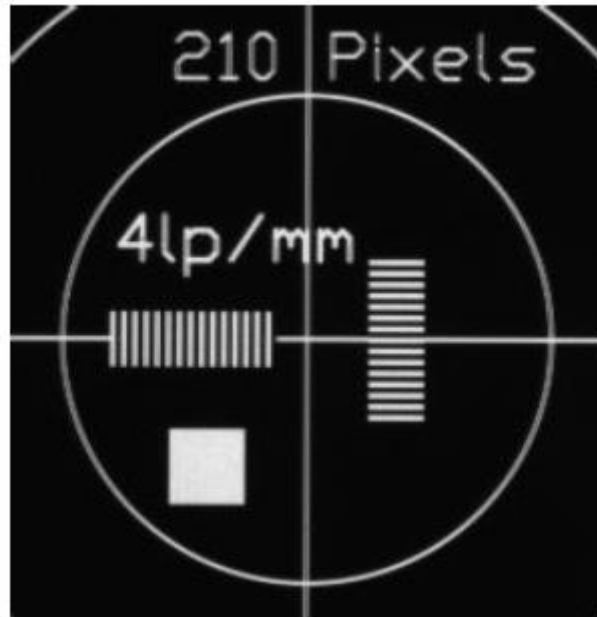


Figure 3.6: lp/mm target

4. As shown above, Fig 3.6, test the pixel resolution.

- a. Get the diameter of inner circle in pixel from the result image.
 - b. Divide this value by 12. (The physical diameter of the inner circle is 12mm.)
 - c. The expected result should be greater than 16.7.
- : Inner Circle Diameter = 236
 = 236/12=19.66

RESULT:

$$W1=240 \quad B1=4$$

$$W2=190 \quad B2=55$$

$$= ((190-55) / (190+55)) / ((240-4) / (240+4))$$

$$= 0.729$$

CHAPTER – 4

PERFORMANCE ANALYSIS

This section of report describes a modular breakdown of the applications (Gemalto RD Utility and Biometric Enrolment Application) throwing a light on all the basic and advanced functionalities, various use cases, communication between the data and user interface and their binding along with other subtle details.

4.1 Gemalto RD Utility

This application performs it's functionalities under two very different development environments (both of which are explained ahead) and an user can avail it's features only upon being granted access by a Gemalto authorised personnel.

4.1.1 Authentication

In order to use the utility, users are required to enter their username and user-handle (explained later). Only a user authorized by a trusted Gemalto personnel can sign in.



Figure 4. 1: Gemalto RD Utility Sign in Page

Steps to get access to the utility are explained in the *Request Access* Section ahead while the database administrator's part which involves granting access is elaborated in *Grant Access* section.

4.1.1.1 Request Access



Figure 4. 2: Gemalto RD Utility Registration Page

New users are required to register themselves by providing a username and an email-id. The username need not be unique but a redundant email-id is unacceptable. Once the user provides suitable data for registration, she/he receives a mail having a *user handle* which is unique to each user and is meant to be kept confidential. This is the same user handle which is used for signing in later. Once the sign-up request has been successfully submitted, the user has to wait for some time for the access to be approved by database administrator.

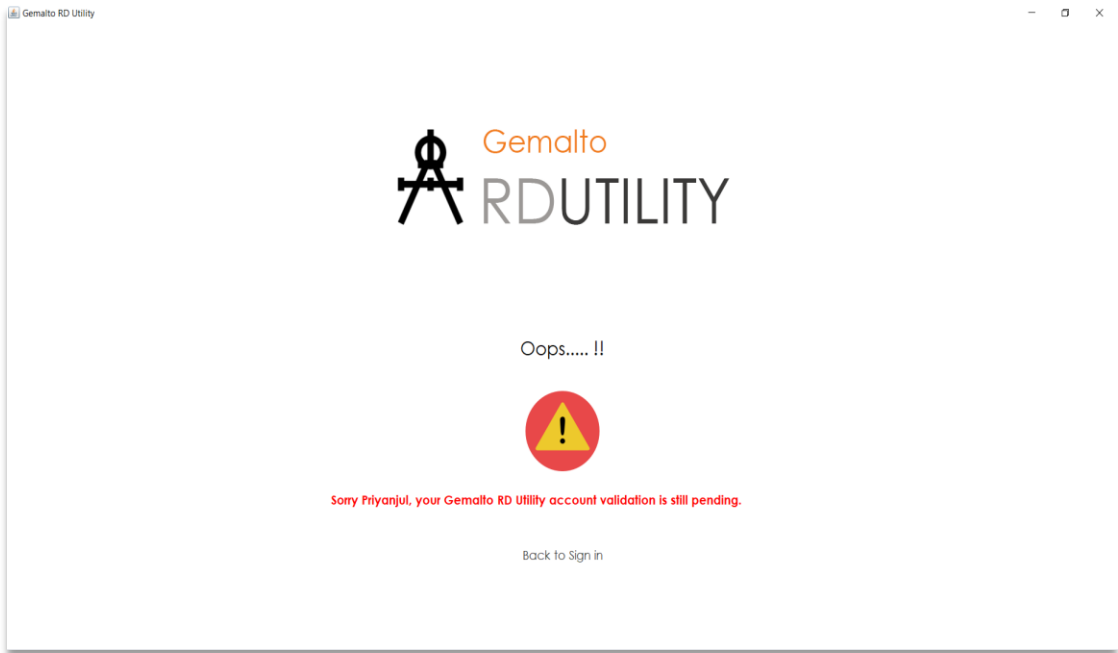


Figure 4. 3: Gemalto RD Utility Access Status Page

Once sign-up has been completed, user can try signing-in to the utility again. If a user is valid but has not been granted access by the database administrator, then she/he will see a message like this and have a wait for access to be granted. Hence, it is recommended to wait for 12-18 working hours or register well in advance to avoid hot delays.

4.1.1.2 Grant Access

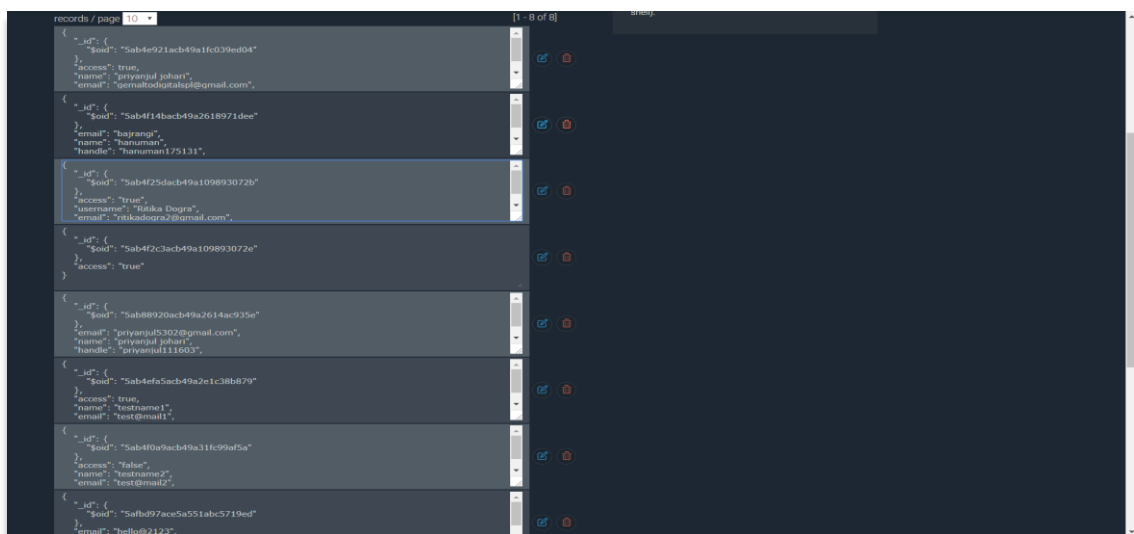


Figure 4. 4: mLab MongoDB for Gemalto RD Utility

On receiving a sign-up request, the database administrator does a little background check about the applicant and once the applicant is declared as a valid applicant, the access is granted. This is done by making direct changes into the database.

But working on database through a browser to regularly check updated requests is not a convenient task. Hence, an android application is under development to make the task handy & fast. As of now, the android app provides only basic features and is not available for full-fledged usage.

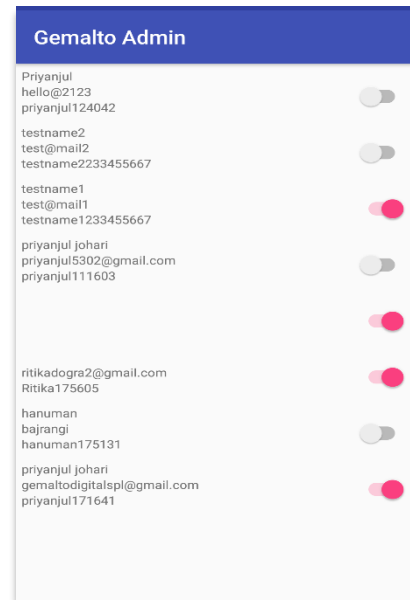


Figure 4. 5: Android Application for granting access to Gemalto RD Utility

4.1.2 Development Environments

Development environments are basically a combination of database and environment state parameters of UIDAI which depict the suitable conditions for testing and processing of various data and requests.

4.1.2.1 Pre-Production

Pre-production is most suited for testing and data processing through the web APIs. Any changes or requests made in pre-production state do not impact the users in real time. Some sensitive tasks like token generation (explained later) can be easily carried out in pre-production state as it will not have any implications to the token vendor.

4.1.1.1 Production

Production is very sensitive and live state and should not be used for testing of any request as it may have direct implications to the user and the vendor in return. As a best example, it is never advised to test token generation in production mode as tokens are only to be generated on the demands of AUAs and randomly generated tokens in production mode may be misused.

4.1.3 Modules

This section provides in-depth overview of all the different modules present in the utility. These modules are exactly same for production and pre-production except pre-production sends its HTTP requests to UIDAI server with *pre-prod* parameter and vice-versa. All the responses of HTTP requests are fetched as JSON responses and are parsed to more comprehensible data.

4.1.3.1 Device Status

This tells the status of a registered device along with its whitelisted status and UIDAI registration date. This however works only for L0 compliance level as L1 is under development.

The screenshot shows a web application window titled "RDService UI" with two tabs: "Pre-Production" and "Production". The "Pre-Production" tab is active. On the left, there is a vertical sidebar with five buttons: "Device Status" (purple), "Token Status" (blue), "Device Whitelist" (green), "Deregistration" (red), and "Token Generation" (dark blue). The main content area is light purple and contains a form for "Device Status". The form has the following elements:

- Compliance Level:** A dropdown menu set to "LO" and a yellow button labeled "SWITCH TO BULK MODE!".
- Device Serial No.:** A text input field containing "P031721828".
- Model:** A dropdown menu set to "CSD200i".
- Submit:** A purple button.
- Device Code:** An empty text input field.
- Device Status:** A text input field containing "notFound".
- Device Whitelisted:** A text input field containing "false".
- Model ID:** An empty text input field.
- UIDAI Registratio...:** An empty text input field.

Figure 4. 6: Gemalto RD Utility - Device Status Page (pre-prod)

| INPUTS | OUTPUTS |
|---|--|
| <ul style="list-style-type: none"> • Compliance Level • Device Serial Number • Model | <ul style="list-style-type: none"> ✓ Device Code ✓ Device Status ✓ Device Whitelisted Status ✓ Model ID ✓ UIDAI Registration Date |

Table 4.1: Device Status I/O

Bulk Mode provides a privilege to upload a csv containing relevant inputs and automatically sends multiple requests to server and saves result in an excel sheet which can be viewed from the utility UI itself.

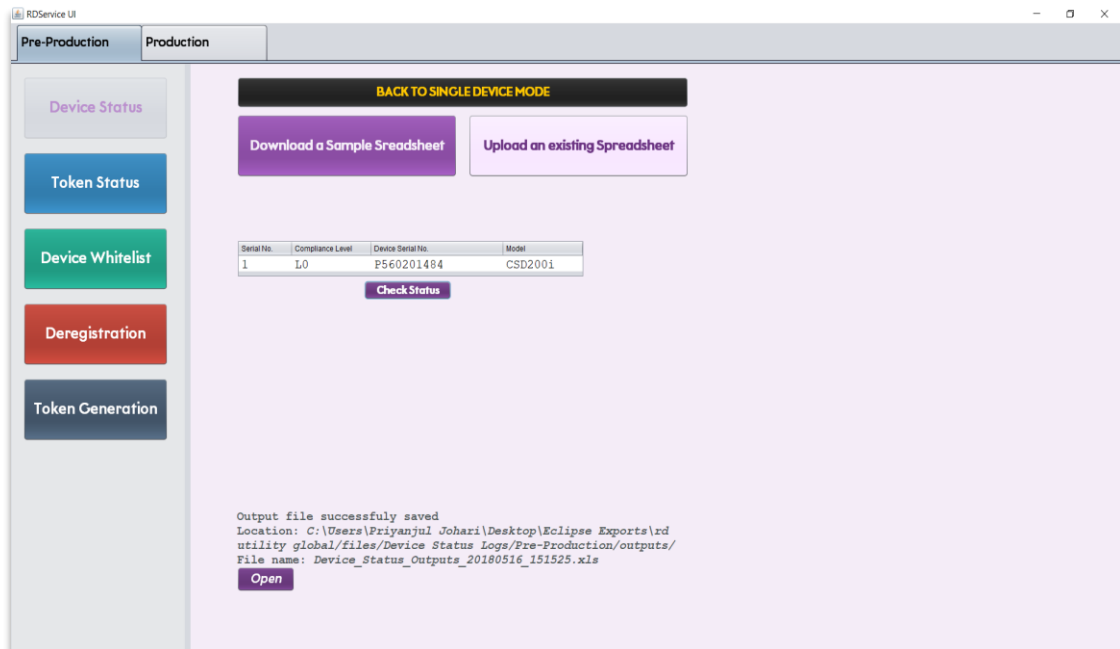


Figure 4. 7: Gemalto RD Utility - Device Status Bulk Mode Page (pre-prod)

| INPUTS | OUTPUTS |
|--|---|
| <p>A csv file containing list of:</p> <ul style="list-style-type: none"> • Compliance Levels • Device Serial Numbers • Models | <p>An excel sheet containing corresponding:</p> <ul style="list-style-type: none"> ✓ Device Codes ✓ Device Statuses ✓ Device Whitelisted Statuses ✓ Model IDs ✓ UIDAI Registration Dates |

Table 4.2: Device Status Bulk Mode I/O

4.1.3.2 Token Status

Tokens are like passcodes for the customers as they are required to provide a valid token in order to activate their device. Number of tokens generated to a customer is dependent on number of devices bought by the customer. Token status tells the activation status of token, whether it is used or not, if it's overridden or invalid and many other attributes.

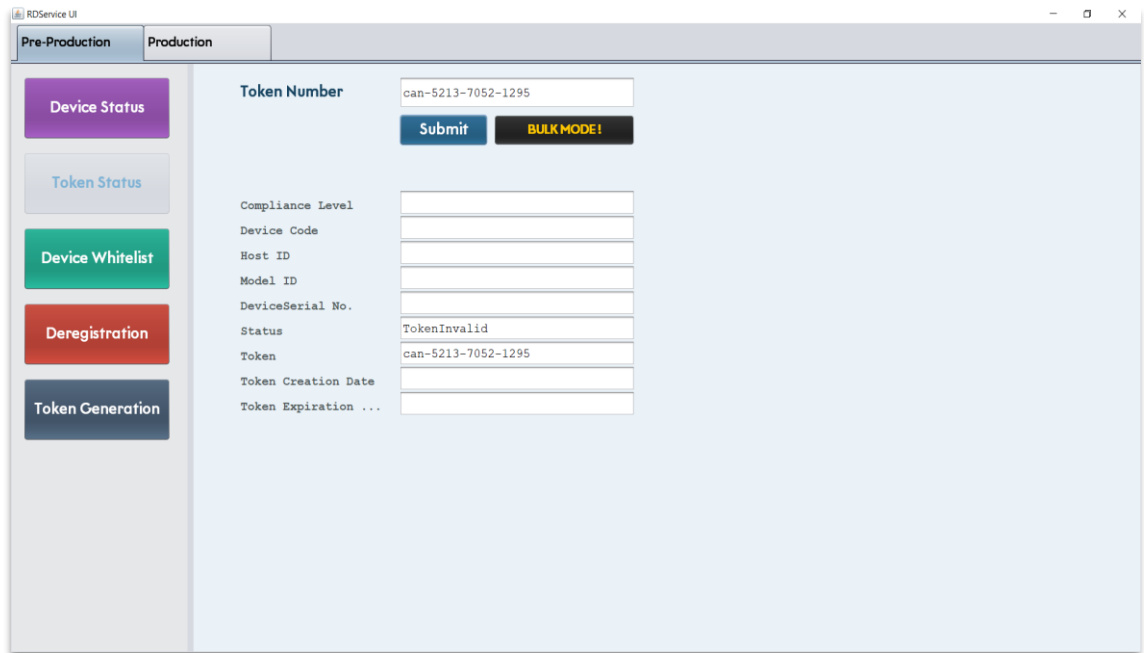


Figure 4. 8: Gemalto RD Utility - Token Status Page (pre-prod)

| INPUTS | OUTPUTS |
|--|---|
| <ul style="list-style-type: none"> • Token Number | <ul style="list-style-type: none"> ✓ Compliance Level ✓ Device Code ✓ Host ID ✓ Model ID ✓ Device Serial Number ✓ Status ✓ Token ✓ Token Creation Date ✓ Token Expiration Date |

Table 4.3: Token Status I/O

Bulk Mode provides a privilege to upload a csv containing list of tokens to be checked and automatically sends multiple requests to server and saves result in an excel sheet which can be viewed from the utility UI itself.

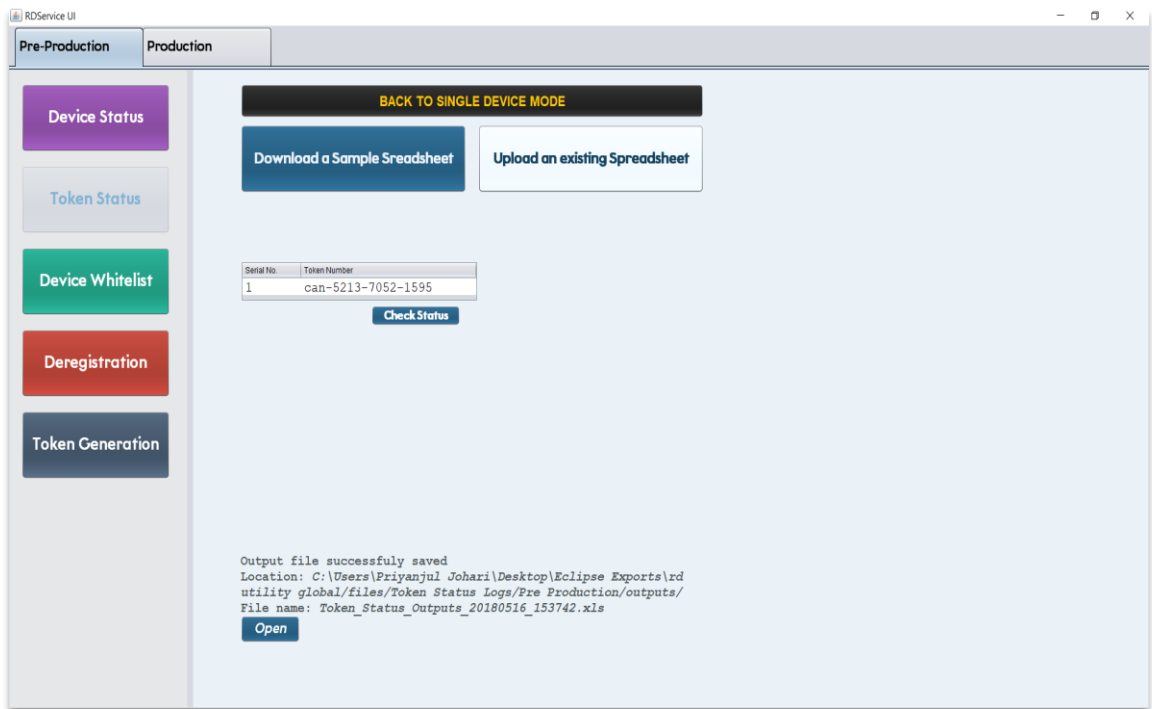


Figure 4. 9: Gemalto RD Utility - Token Status Bulk Mode (pre-prod)

| INPUTS | OUTPUTS |
|---|---|
| <p>A csv file containing:</p> <ul style="list-style-type: none"> • Token Numbers | <p>An excel sheet containing corresponding:</p> <ul style="list-style-type: none"> ✓ Compliance Levels ✓ Device Codes ✓ Host IDs ✓ Model IDs ✓ Device Serial Numbers ✓ Statuses ✓ Tokens ✓ Token Creation Dates ✓ Token Expiration Dates |

Table 4. 4: Token Status Bulk Mode I/O

4.1.3.3 Device Whitelist

Whitelisting a device means to activate a device without the use of token. This can be thought of as a privilege or an emergency backup option or even a shortcut so that the device can be activated without any hustle. Though it is recommended to do with special grants from vendor only.

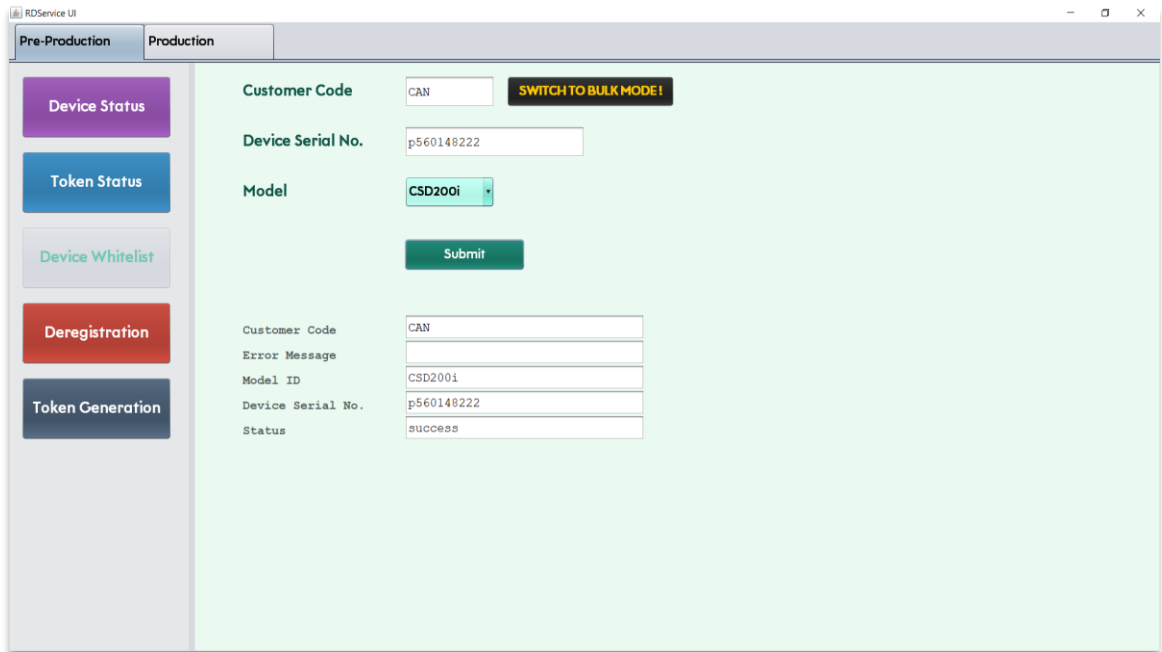


Figure 4. 10: Gemalto RD Utility - Device Whitelist Page (pre-prod)

| INPUTS | OUTPUTS |
|--|--|
| <ul style="list-style-type: none"> • Customer Code • Device Serial Number • Model | <ul style="list-style-type: none"> ✓ Customer Code ✓ Error Message ✓ Model ID ✓ Device Serial Number ✓ Status |

Table 4. 5: Device Whitelist I/O

Bulk Mode provides a privilege to upload a csv containing relevant inputs and automatically sends multiple requests to server and activates all the devices.

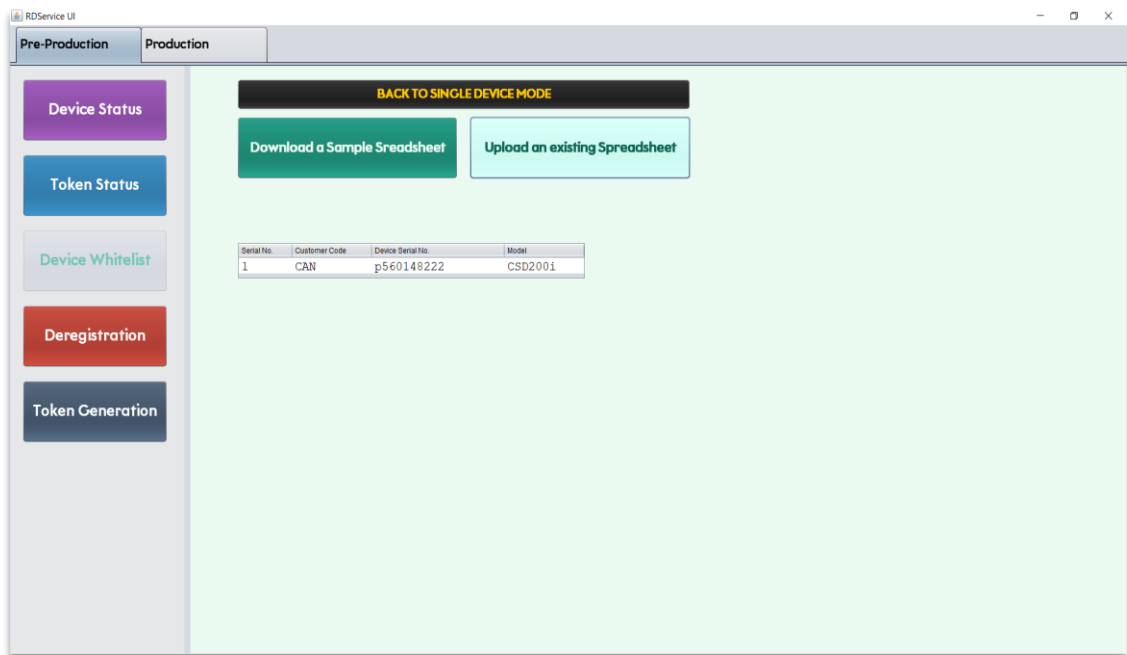


Figure 4. 11: Gemalto RD Utility Device - Whitelist Bulk Mode Page (pre-prod)

| INPUTS | OUTPUTS |
|---|--|
| <p>A csv file containing:</p> <ul style="list-style-type: none"> • Customer Codes • Device Serial Numbers • Models | <p>An excel sheet containing corresponding:</p> <ul style="list-style-type: none"> ✓ Customer Codes ✓ Error Messages ✓ Model IDs ✓ Device Serial Numbers ✓ Statuses |

Table 4. 6: Device Whitelist Bulk Mode I/O

4.1.3.4 Device Deregistration

As the name suggests, it performs deregistration of device from UIDAI database. But only a valid device can be deregistered, any random deregistration requests result in a prompt indicating “*Device not found!!*”.

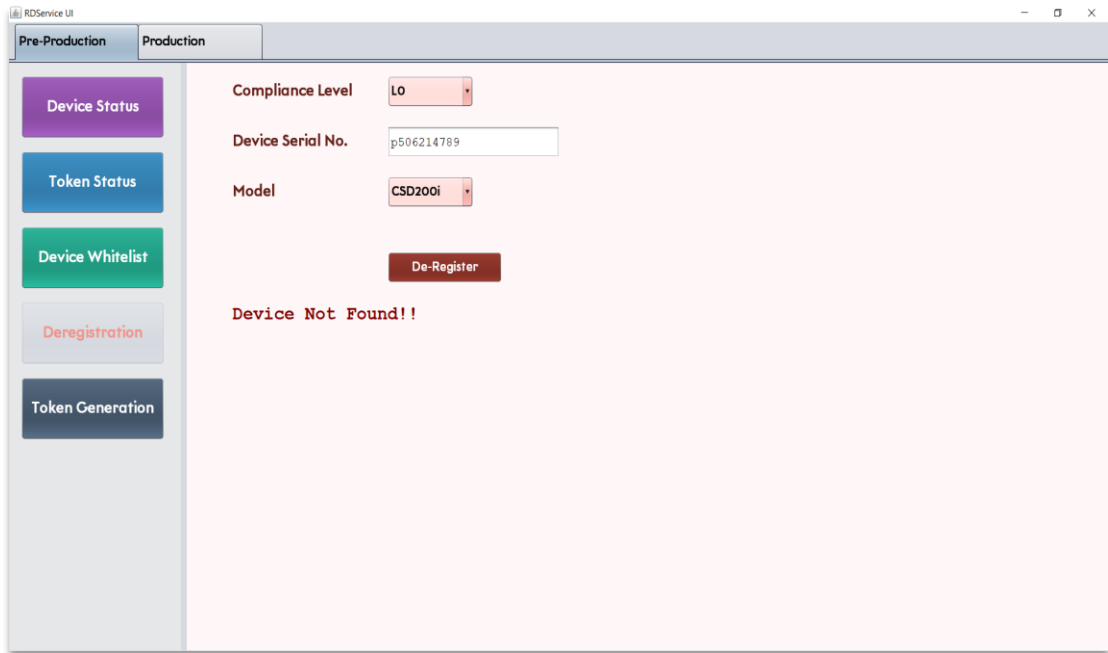


Figure 4. 12: Gemalto RD Utility - Device Deregistration (pre-prod)

| INPUTS | OUTPUTS |
|---|--|
| <ul style="list-style-type: none">• Compliance Level• Device Serial Number• Model | ✓ Prompt stating Device Deregistered or Not !! |

Table 4. 7: Device Deregistered I/O

4.1.3.5 Token Generation

Token generation is perhaps the most sensitive module of this utility as tokens are a confidential chunk of data and any garbage generation of tokens will increase the chances of token misuse potentially. Tokens are generated on demand of customers.

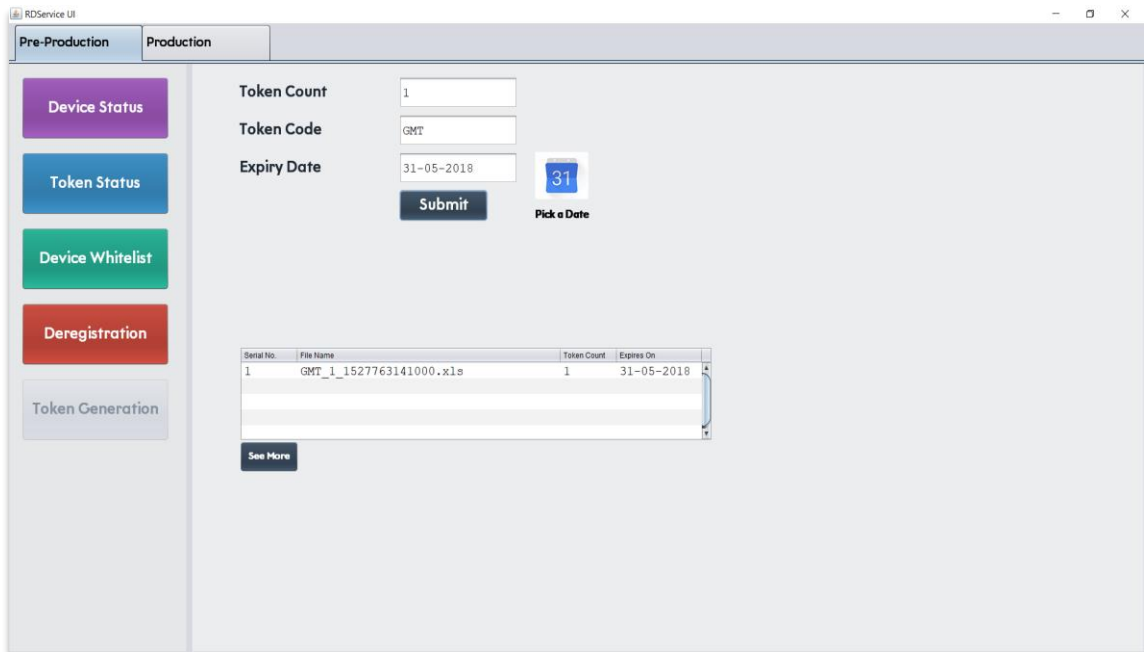


Figure 4. 13: Gemalto RD Utility - Token Generation Page (pre-prod)

| INPUTS | OUTPUTS |
|--|--|
| <ul style="list-style-type: none"> • Token Count (say 'n') • Token Code • Expiry Date | <p>An excel sheet containing 'n' number of:</p> <ul style="list-style-type: none"> ✓ Tokens ✓ Creation Dates ✓ Expiration Dates |

Table 4. 8: Token Generation I/O

4.2 Biometric Enrolment Application

As mentioned earlier, this application has three distinct steps out of which completing first step is mandatory to proceed ahead, upcoming two steps may be skipped and the final step is an acknowledgement of the whole enrolment session for a particular user.

4.2.1 Applicant Form

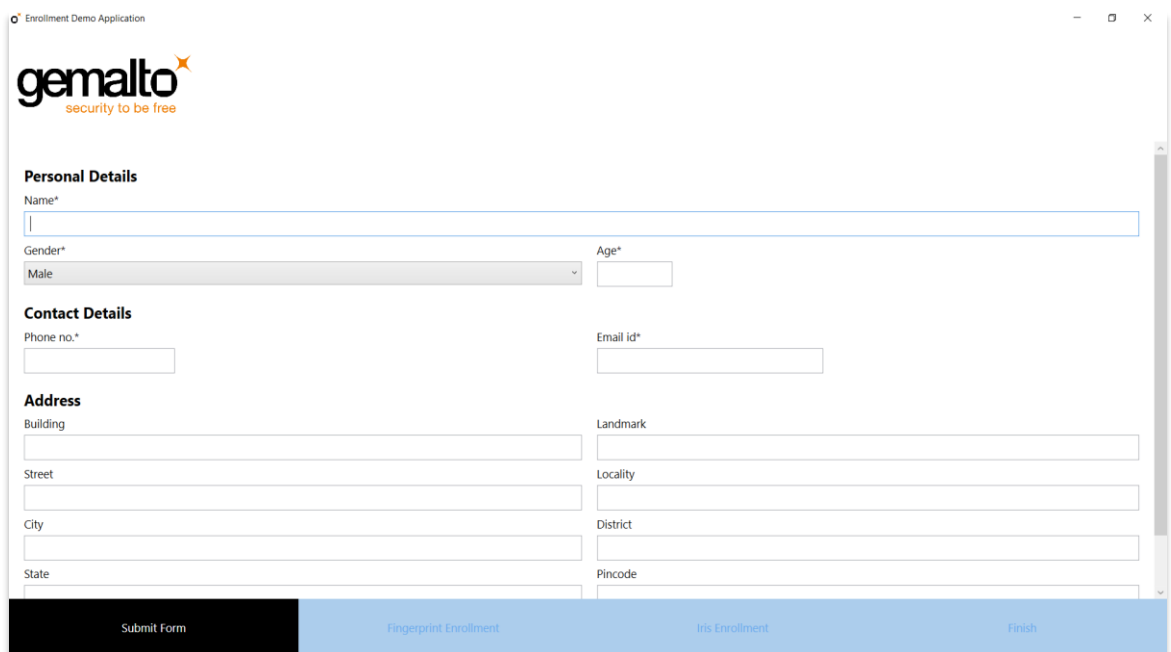


Figure 4. 14: Biometric Enrolment Application - User Form

The application form asks the user to fill his basic personal details and some demographic data to proceed with enrolment process. The personal details (marked with *) are mandatory fields and must be provided for maintaining the authenticity and uniqueness of user. The mobile number provided by the user acts as transaction ID for the whole session. Once form has been filled and user presses next, its has to choose an appropriate device for fingerprint enrolment.

SPECIAL USE CASE #1

- Before moving on to fingerprint enrolment, make sure that form is filled correctly because there's no way to redo it once moved ahead.
- It is advised not to leave demographic data blank in order to get a proper enrolment receipt.

4.2.2 Fingerprint Enrolment

Before commencing fingerprint enrolment, users are asked to make a choice of device. Users are free to choose any device depending on the physical availability of the device and proficiency to use it.

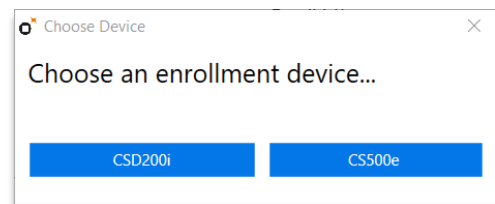


Figure 4. 15: Biometric Enrolment Application - Choose Device Pop Dialog

4.2.2.1 CSD200i

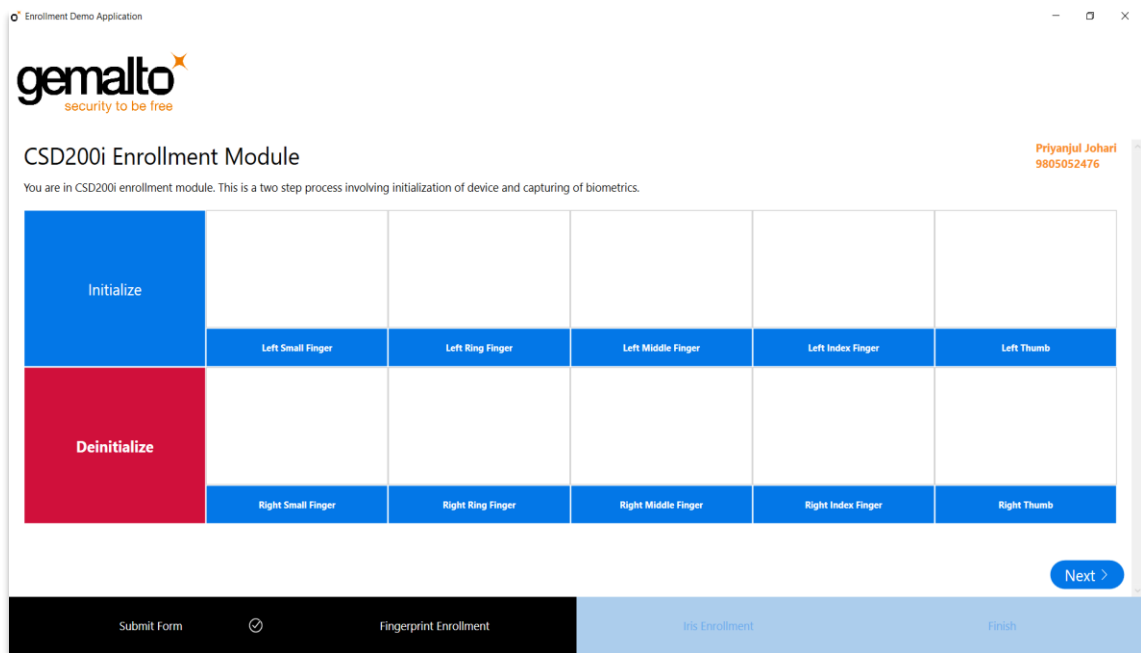


Figure 4. 16: Biometric Enrolment Application - CSD200i Enrolment Module

CSD200i Enrolment Module welcomes you with a heading on top left stating the purpose, session details like applicant name and transaction id on top right and the centre which contains the main part to interact with the device. The initialize button initializes the device and a green LED blinks for about 5-10 seconds indicating successful initialization.

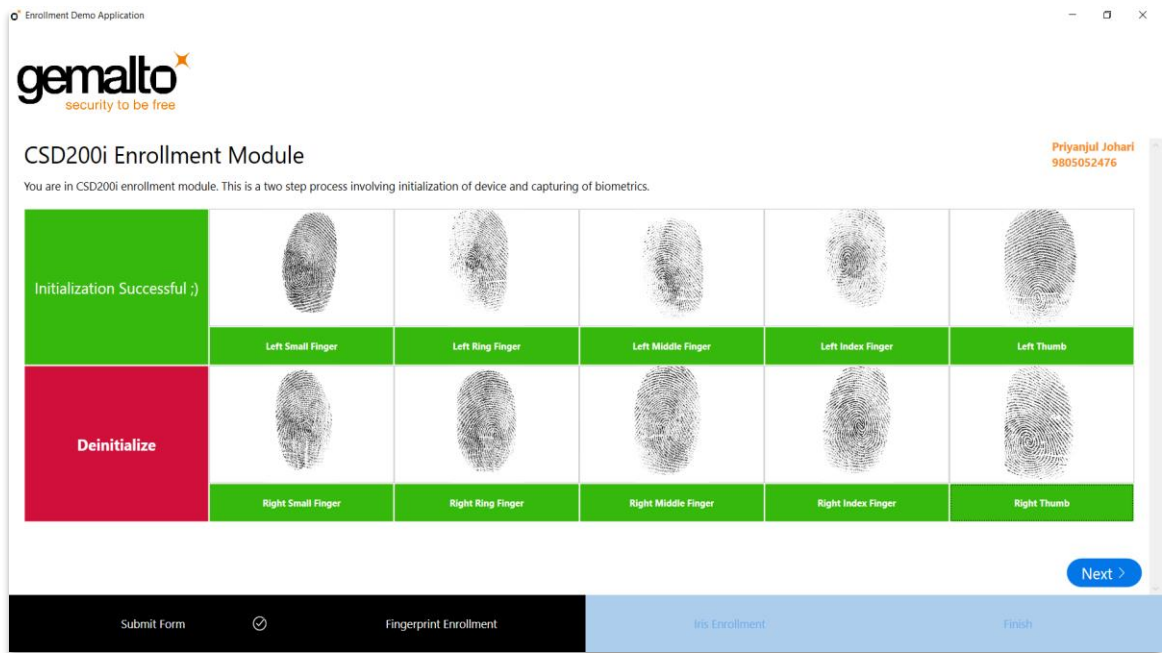


Figure 4. 17: Biometric Enrolment Application - CSD200i Image boxes with Fingerprints

Once the initialization is completed, fingerprints can be captured sequentially or randomly however suitable. The preview appears in the image box after successful capture. Re-capturing overrides the old fingerprint with new one. Once all fingerprints have been captured, you can move forward to next stage.

SPECIAL USE CASE #2

- In case of initialization failure or capture failure, it is recommended to de-initialize device and re-start process.
- Enrolment is considered successful once all the 10 distinct fingerprints have been captured; any subsequent captures will override the old copies. This condition holds even if user switches back from iris enrolment module to fingerprint module again, any number of times.

4.2.2.2 CS500e

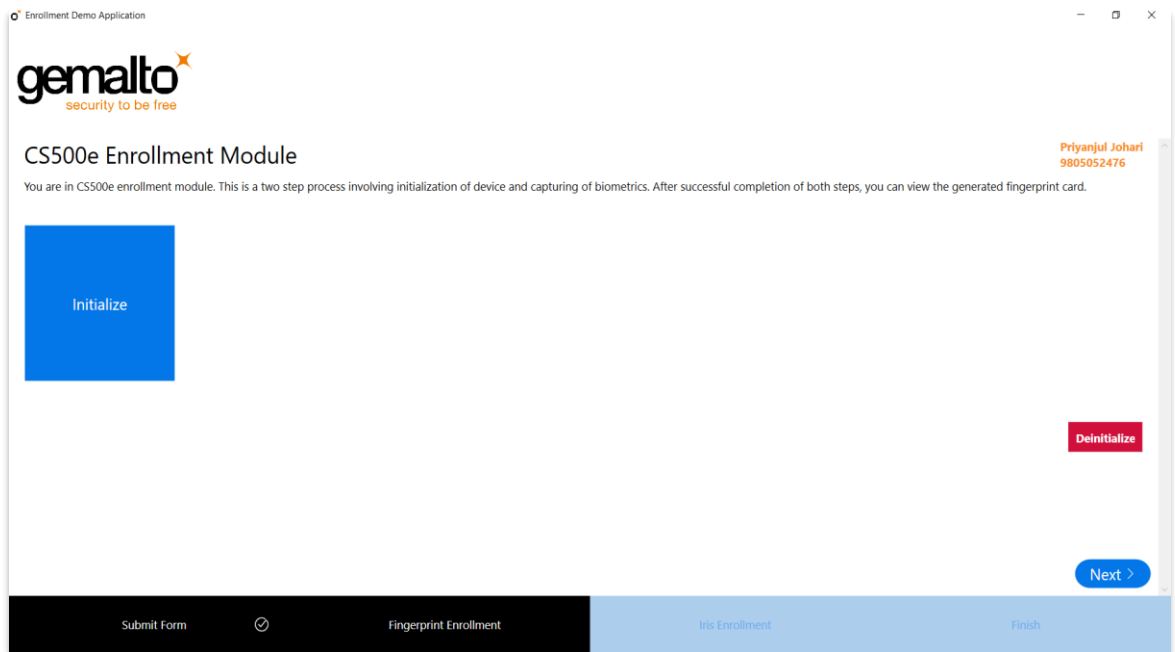


Figure 4. 18: Biometric Enrolment Application - CS500e Enrolment Module

CS500e Enrolment module welcomes user with a similar UI and as usual, process begins with device initialization. In order to use CS500e Fingerprint Scanner, user requires a license; it can be a paid license or just a demo license.

For a licensed user, it asks you to choose the device to initialise in case you have attached both CSD200i and CS500e (as shown in figure 4.19) to your system. Choose CS500e here and a capture button as in figure 4.20. User may now proceed to capture.

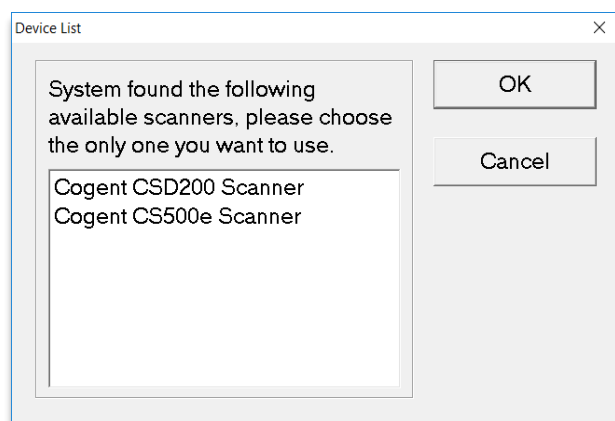


Figure 4. 19: Biometric Enrolment Application - Device List Dialog

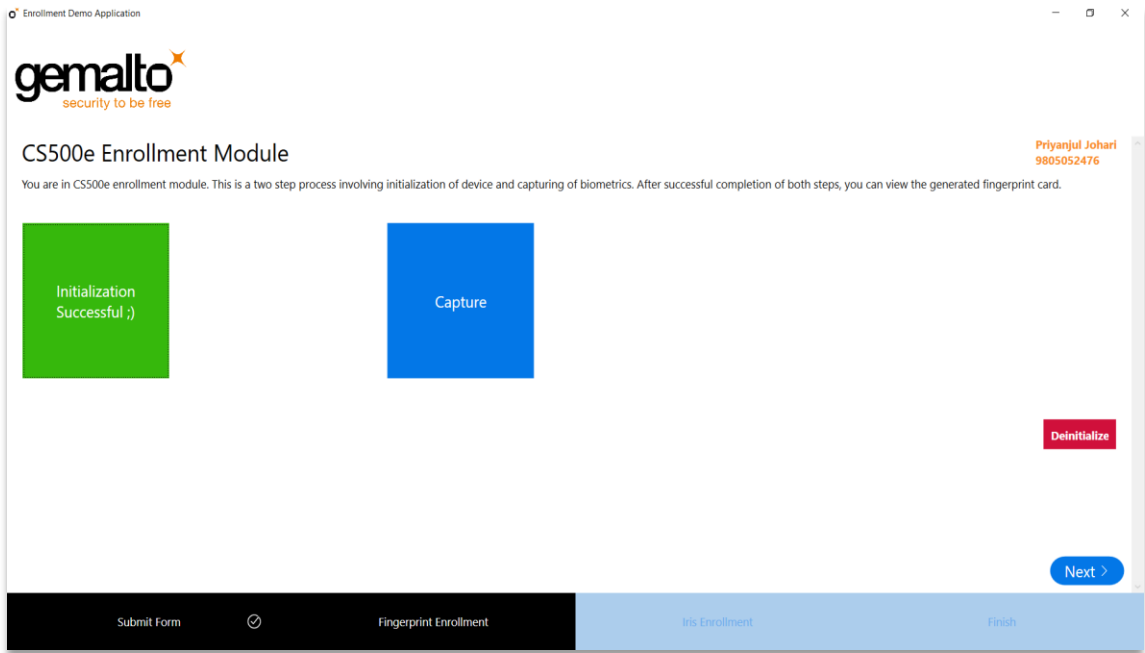


Figure 4. 20: Biometric Enrolment Application - Initiating Capture

After clicking on the capture button, a new window opens up and graphically guides you in the enrolment process as shown in figures 4.21 – 4.23. After completing the enrolment, a fingerprint card is generated which contains all the images including right slap, left slap, thumbs and their segmented images as well as shown in figure 4.24.

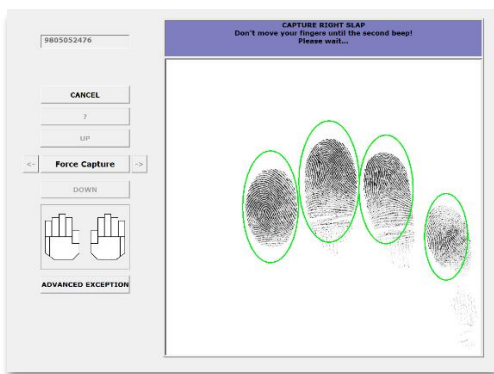


Figure 4. 21: Biometric Enrolment Application - Capturing Right Slap



Figure 4. 22: Biometric Enrolment Application - Capturing Left Slap



Figure 4. 22: Biometric Enrolment Application - Capturing Thumbs

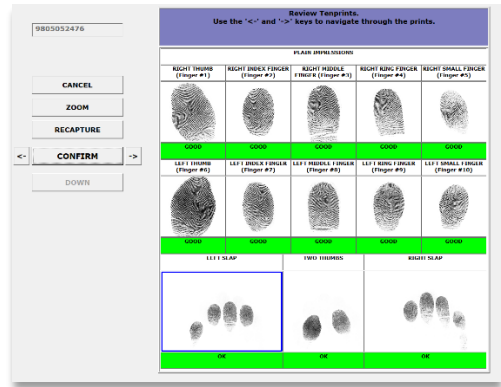


Figure 4. 24: Biometric Enrolment Application - Fingerprint Card

Upon completion of enrolment procedure, the users can also access the fingerprint card to have glimpse of the fingerprint bitmap images.

SPECIAL USE CASE #3

Something seems fishy. Deinitianlize and Try again

Capture Failed due to initialization failure. Retry :(

Figure 4. 23: Biometric Enrolment Application - Capture Failure

- In case the capture gets interrupted due to machine failure or unintentional activities of the user, the operation is aborted and can be restarted by de-initializing the device and starting again.
- While choosing enrolment device as in figure 4.19, do not choose CSD200i or operation will get aborted.

4.2.3 Iris Enrolment: CIS202



Figure 4. 24: Biometric Enrolment Application - Iris Enrolment Module

For Iris Enrolment, initialise the iris scanner and two red LEDs will glow. Click on the capture button and place the scanner as told in the instructions in a dialog box the appears. Now look into the scanner and wait till a white LED flashes. It indicates a successful capture. The live preview and captured iris can be viewed in the image box as shown in figure 4.25.

SPECIAL USE CASE #4

- For a clear and vivid iris capture, keep the iris at about 4cm from your eyes or the it would capture a hazy image. Also do not shake the device shake the device while capturing.
- If capturing takes unexpectedly long, de-initialize device and try again.
- User can go back and forth as many number of times from iris to finger (and vice-versa) but only the latest captured biometrics will be considered valid.



Figure 4. 25: Biometric Enrolment Application - Iris Preview

4.2.4 Authentication (Future Prospect)

Authentication Module is under development phase as of now. This module authenticates user after enrolment by comparing the ISO templates of the biometrics and calculating a similarity index called Match Score. For a successful match, Match Score should be 10,000+. Otherwise authentication fails. Although, authentication can only be carried out on systems with paid license activated on them.

4.2.5 Acknowledgement

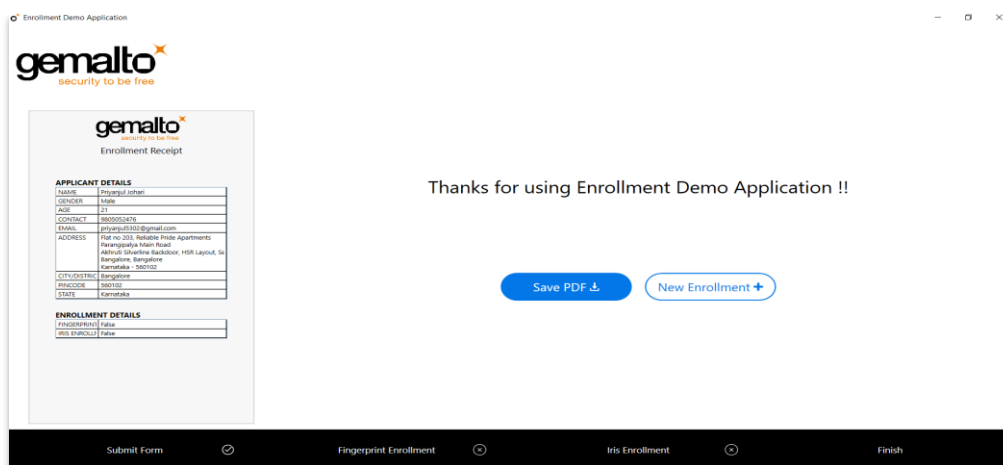


Figure 4. 26: Biometric Enrolment Application - Acknowledgment

Acknowledgement page provides a zest of whole session and generates a receipt containing all your personal details, demographic details and enrolment status depending on the data from user form and enrolment modules. It generates a PDF file and provides an option to view it straightaway. Besides generating and viewing PDF file, it also provides option to begin a new enrolment by resetting the application.

SPECIAL USE CASE #5

- There is no going back from this stage so be sure you have completed all necessary enrolments.
- If you try to enrol an existing user in a new enrolment, then the data gets overridden, as said many times earlier.

CHAPTER – 5

CONCLUSIONS

Working at Gemalto Digital Security Private Ltd. Has as been as fun and productive as it has been working on these projects. Gemalto RD Utility and Biometric Enrolment Application are equally significant in their own places. The former provides ease of operation to the technical team while the latter gives an insight into the enrolment procedure to a layman who's from a minimal technical background.

Gemalto RD Utility has been the most extensive application of the two as it processes complex and heavy server requests. The application needs more modifications for increasing efficiency. Also, there are certain bugs which need to be dealt with to make it deployable to the technical team of the Government Programmes department of GDSPL. After the aforementioned changes, the application will go through an extensive modular and system testing to make it work at it's best efficiency.

Biometric Enrolment Application on the other hand was a top level development with it's foundations in the low level SDKs containing DLLs for interaction with the biometric devices. The DLLs are full fledged and capable of exception handling and failure management which prevents application from crashing and providing a detailed error log instead. This application has a slightly flashy UI and a relatively smoother UX as it is meant to be used by users of all domains irrespective of their technical background.

Biometric Enrolment Application has been deployed successfully on our cloud storage SharePoint and is being tested and used by the sales team of GDSPL for demonstration to future customers. While Gemalto RD Utility, on the other hand, needs a bit of debugging and improvisation before staging it to SharePoint.

Overall, development of these applications has been a really learning experience in terms of writing legible, comprehensible and maintainable code, debugging to an extent that each and every module knows how to handle exceptional situations, creating a UI that is not just good to look but is equally good to use and work with.

There are indeed places which need extemporization and diligence to reach the mark of perfection and excellence. I've been working hard to reach there and will confidently accomplish it some day. I will keep these precious learnings with me forever and hope to flourish more with Gemalto.

REFERENCES

1. http://www.controldeasistencia.mx/uploads/5/8/3/3/58339667/3m_csd_200i_single-digit_optical_fingerprint_scanner_v122015.pdf
2. <https://www.gemalto.com/brochures-site/download-site/Documents/gov-cogent-CIS202-TDS.pdf>
3. <https://www.gemalto.com/govt/biometrics/biometric-fingerprint-scanners/iris-scanner>
4. <https://www.gemalto.com/govt/biometrics/biometric-fingerprint-scanners/fingerprint-scanners>
5. <https://www.gemalto.com/govt/biometrics/biometric-fingerprint-scanners/palm-tenprint-scanners/cs500e>

LIST OF PUBLICATIONS

1. Dr. Pramod Varma, “Aadhaar Registered Devices Specification” July 7th, 2017.
2. Dr. Pramod K. Varma, “Aadhaar Authentication API 1.6” February 26th, 2017.