|  |  |  |
| --- | --- | --- |
| **Version** | **Date** | **Changes Made** |
| 1.0 | 16/09/2024 |  |
|  |  |  |
|  |  |  |

*Prepared by the Trustworthy Digital Infrastructure for Identity Systems Team*

*This work was supported, in whole or in part, by the Gates Foundation [INV- 057591]. Under the grant conditions of the Foundation, a Creative Commons Attribution 4.0 Generic License has already been assigned to the Author’s Accepted Manuscript.*

Standard Operating Procedure - Registering Offline Biometric Collection: Facial Data

OB.1.4.B - WITH RATIONALISATION

**Version Control**

**Guidelines for Maintaining the SOP Version Control Table:**

* **Version**: Assign a new version number for every update. Minor changes can be denoted by incremental changes in decimal (e.g., 1.1, 1.2), while major changes can increment the whole number (e.g., 1.0 to 2.0).
* **Date**: The date when the changes were finalised.
* **Changes Made**: A brief description of the changes or updates made.

Table of Contents

[1. Purpose 3](#_Toc177312454)

[2. Definitions and Abbreviations 3](#_Toc177312455)

[3. Application 3](#_Toc177312456)

[3.1 Ownership and Stakeholders 3](#_Toc177312457)

[3.1.1 Digital Identity Service Providers (DISPs) 3](#_Toc177312458)

[3.1.2. IT and Security Teams 3](#_Toc177312459)

[3.1.3 Compliance and Legal Departments 4](#_Toc177312460)

[3.2 Users and Beneficiaries 4](#_Toc177312461)

[3.2.1 General Public 4](#_Toc177312462)

[3.2.2 Government Agencies 4](#_Toc177312463)

[3.2.3 Private Sector Companies 4](#_Toc177312464)

[3.3 Benefits and Impact 4](#_Toc177312465)

[3.3.1 Enhanced Security 4](#_Toc177312466)

[3.3.2 Regulatory Compliance 4](#_Toc177312467)

[3.3.3 Streamlined Processes 5](#_Toc177312468)

[3.3.4 Interoperability 5](#_Toc177312469)

[3.3.5 Data Privacy and Protection 5](#_Toc177312470)

[4. Prerequisites 5](#_Toc177312471)

[4.1 Assumptions 6](#_Toc177312472)

[4.2 Constraints 6](#_Toc177312473)

[5. Process Flow - Process and Procedures 6](#_Toc177312474)

[5.1 Applicant Actions: 6](#_Toc177312475)

[5.1.1 Start (Offline): 6](#_Toc177312476)

[5.1.2 Provide Consent (OB.1.4.A) 7](#_Toc177312477)

[5.1.3 Position Face in Front of Camera: 7](#_Toc177312478)

[5.2 Parent/Guardian/Introducer Actions 7](#_Toc177312479)

[5.2.1 Provide Consent (OB.1.4.A) 7](#_Toc177312480)

[5.2.2 Assist Applicant with Positioning 7](#_Toc177312481)

[5.2.3 Read the Consent Form: 7](#_Toc177312482)

[5.3 Administrator Actions: 7](#_Toc177312483)

[5.3.1Verify Consent Given for Biometric Collection: 7](#_Toc177312484)

[5.3.2 Verify Applicant Age 7](#_Toc177312485)

[5.3.3Request Facial Scan of Applicant 7](#_Toc177312486)

[5.3.4 Capture Facial Image of Applicant 8](#_Toc177312487)

[Capture Facial Image with Assistance: 8](#_Toc177312488)

[5.3.6 Provide Acknowledgment of Facial Biometric Capture: 8](#_Toc177312489)

[5.4 System Processing 8](#_Toc177312490)

[5.4.1 Public Network Systems (Client) 8](#_Toc177312491)

[5.4.2 Consent Form and Biometric Data Collection 8](#_Toc177312492)

[5.4.3 Private Network Systems (Server) 8](#_Toc177312493)

[5.5 User Account Creation 9](#_Toc177312494)

[5.6 Notifications and Logging 9](#_Toc177312495)

[5.7 Exceptions and Error Handling 9](#_Toc177312496)

[5.8 End of Process 9](#_Toc177312497)

[5.9 Security Measures 9](#_Toc177312498)

[6. Visualisation 10](#_Toc177312499)

[7. Rationalisation 11](#_Toc177312500)

[8. References 12](#_Toc177312501)

# 1. Purpose

This section outlines the steps required for offline biometric collection of facial data and obtaining consent for a Digital Identity (DID) account. It details the process from initiating the application to capturing facial data and updating the system records.

# 2. Definitions and Abbreviations

**DID**: Digital Identity

**KM**: Key Manager

**KR**: Key Revocation

**HSM**: Hardware Security Module

**CA**: Certificate Authority

**IDA**: ID Authentication Database

**OTP**: One-Time Password

**API**: Application Programming Interface

**SSL/TLS**: Secure Sockets Layer / Transport Layer Security

**IDS**: Intrusion Detection System

**IPS**: Intrusion Prevention System

# 3. Application

## 3.1 Ownership and Stakeholders

### 3.1.1 Digital Identity Service Providers (DISPs)

* **Ownership:** The primary owners of this process are the digital identity service providers responsible for managing the DID portal.
* **Responsibilities:**
  + Ensure the process is secure, compliant with regulatory standards, and efficiently managed.
  + Responsible for the development, maintenance, and updating of the system.
  + Oversee the integration of new technologies and updates to enhance the system’s functionality and security.

### 3.1.2. IT and Security Teams

* **Ownership:** IT and security teams within the organisation managing the DID portal play a crucial role.
* Responsibilities:
  + Handle system security, encryption protocols, and the implementation of CAPTCHA, OTPs, and other security measures.
  + Manage the hardware and software infrastructure, ensuring uptime and handling technical issues.
  + Conduct regular security audits and vulnerability assessments to ensure the system remains secure and up-to-date with the latest security standards.

### 3.1.3 Compliance and Legal Departments

* Ownership: These departments ensure that the registration process complies with legal and regulatory requirements.
* Responsibilities:
  + Oversee adherence to standards like ISO 27001, NIST, eIDAS, and others.
  + Involved in audits, documentation, and compliance checks.
  + Monitor changes in regulatory requirements and update the process to remain compliant.

## 3.2 Users and Beneficiaries

### 3.2.1 General Public

* Users: Individuals looking to create a new digital identity account or complete biometric registration for themselves or dependents usage:
  + Use this process to register and authenticate their identity securely on the DID portal.
  + Access government services, financial services, or any other service requiring a verified digital identity.

### 3.2.2 Government Agencies

* Users: Various government departments and agencies that require citizens and residents to have a verified digital identity for accessing services.
* Usage: Rely on the DID portal to streamline service delivery, ensure secure access to services, and manage identity verification efficiently.

### 3.2.3 Private Sector Companies

* Users: Businesses requiring identity verification for employees or customers.
* Usage: They use the DID portal for secure access to services, employee onboarding, and ensuring compliance with various industry regulations.

## 3.3 Benefits and Impact

### 3.3.1 Enhanced Security

* Benefit: Improved security for users through advanced encryption, two-factor authentication, and robust error handling.
* Impact:
  + Reduces the risk of identity theft, fraud, and unauthorised access.
  + Enhances the overall trust in the digital identity system.

### 3.3.2 Regulatory Compliance

* Benefit: Ensures compliance with international standards and regulations, minimising legal risks.
* Impact: Builds trust with users and regulatory bodies, facilitating smoother operations and service delivery.

### 3.3.3 Streamlined Processes

* Benefit: Simplifies the registration and identity verification process for users.
* Impact:
  + Enhances user experience, increases adoption rates, and improves service efficiency.
  + Reduces the time and resources required for account setup and verification.

### 3.3.4 Interoperability

* Benefit: Allows for integration with other systems and services.
* Impact:
  + Facilitates seamless access to a wide range of services across different sectors.
  + Promotes a unified digital identity system that can be used across various platforms

### 3.3.5 Data Privacy and Protection

* Benefit: Ensures user data is securely stored and handled, complying with data protection laws.
* Impact:
  + Builds user confidence in the system and safeguards sensitive information.
  + Safeguards sensitive information, reducing the risk of data breaches and privacy violations.

# 4. Prerequisites

This section outlines the essential conditions and resources required before initiating the offline biometric collection and consent process for the Digital Identity (DID) portal. Prerequisites act as the foundational parameters necessary for the SOP to function effectively within the broader SOP collection.

* **System Requirements:** The applicant must have access to a device capable of connecting to the internet, equipped with updated security features for initial setup and communication.
* **Technical Setup:**
  + Access to the DID portal server and backend systems, including database servers for storing encrypted user data and consent documents.
  + Equipment and software at the enrollment center for capturing biometric data and consent forms. A camera at the enrollment center to capture facial biometric data.
* **Interdependencies:** This SOP operates in conjunction with other processes, such as system maintenance SOPs and security protocol SOPs. It relies on these interconnected systems from onboarding, authentication, and lifecycle management phases to ensure seamless operation and security compliance. The next immediate SOP to be followed would be *OB.1.4.E Application Approval Rejection*

## 4.1 Assumptions

* User Proficiency:
  + Users (applicants, parents/guardians, introducers) possess a basic understanding of how to navigate internet applications and complete digital forms.
  + Administrators are trained to handle biometric collection equipment and explain consent forms.
* Technological Infrastructure:
  + The technological infrastructure (servers, network, security systems) is maintained to current standards and is operational without significant downtime.
  + Enrollment centers are equipped with the necessary hardware and software for biometric data collection and consent management, including a camera for capturing facial data.

## 4.2 Constraints

* Limitations due to scheduled system maintenance or unexpected outages, which may temporarily hinder the biometric collection process.
* Any regulatory changes or updates in technology that require adjustments in the SOP before proceeding with biometric data collection and consent processing.

# 5. Process Flow - Process and Procedures

The process involves interactions between the applicant, parent/guardian/introducer, and administrators, with support from public network systems (client-side) and private network systems (server-side). Security measures such as encryption, consent verification, and data storage are integral throughout the process.

## 5.1 Applicant Actions:

### 5.1.1 Start (Offline):

* **Action:** Applicant begins the offline biometric collection process with their documents.
* **Output**: Process initiated.

### 5.1.2 Provide Consent (OB.1.4.A)

* **Action**: Applicant provides consent for biometric data collection
* **Output**: Consent provided.

### 5.1.3 Position Face in Front of Camera:

* **Action**: Applicant positions their face in front of the camera for facial data capture.
* **Output**: Face positioned correctly for data capture.

## 5.2 Parent/Guardian/Introducer Actions

### 5.2.1 Provide Consent (OB.1.4.A)

* **Action:** Parent/guardian or introducer provides consent for the applicant.
* **Output:** Consent Provided

### 5.2.2 Assist Applicant with Positioning

* **Action:** Assist the applicant in positioning their face in front of the camera if necessary.
* **Output:** Face positioned correctly for data capture with assistance.

### 5.2.3 Read the Consent Form:

* **Action:** Parent/guardian or introducer reads the consent form provided at the center.
* **Output**: Consent form reviewed.

## 5.3 Administrator Actions:

### 5.3.1Verify Consent Given for Biometric Collection:

* **Action:** Verify that consent has been provided by the applicant and parent/guardian/introducer.
* **Output:**  Consent verified

### 5.3.2 Verify Applicant Age

* **Action:** Verify the age of the applicant to ensure eligibility.
* **Output:** Participants are ready for the process.

### 5.3.3Request Facial Scan of Applicant

* **Action:** Request the applicant to position their face for facial scanning.
* **Output:** Facial scan initiated.

### 5.3.4 Capture Facial Image of Applicant

* **Action:** Capture the facial image of the applicant
* **Output:** Facial image captured.

### Capture Facial Image with Assistance:

* **Action:** If necessary, capture the facial image of the applicant with assistance from the parent/guardian/introducer.
* **Output:** Facial image captured with assistance.

### 5.3.6 **Provide Acknowledgment of Facial Biometric Capture:**

* **Action:** Provide acknowledgment of successful facial biometric capture to the applicant.
* **Output:** Acknowledgment provided.

## 5.4 System Processing

### 5.4.1 Public Network Systems (Client)

* **Action**: The system masks and encrypts user details using KM, HSM, and CA.
* **Output**: The encrypted details are sent to the server.

### 5.4.2 Consent Form and Biometric Data Collection

* **Action:** System processes facial scan data.
* **Output:** Facial Scan Data sent to the server for processing.

### 5.4.3 Private Network Systems (Server)

**Initiate Facial Biometric Collection:**

* **Action:** System initiates the process for collecting facial biometric data.
* **Output:** Facial biometric collection initiated.

**Store Facial Biometric Data Securely:**

* A**ction:** Store the collected facial biometric data securely in the RID account with encryption and hashing.
* **Output:** Data securely stored.

**Generate Notifications:**

* **Action:** Generate notifications for successful or failed facial data collection.
* **Output:** Notifications sent to the applicant.

## 5.5 User Account Creation

* **Action**: If the CAPTCHA test is passed and the email and phone number are verified, the server generates OTPs for email and phone.
* **Action**: If the OTPs are authenticated successfully, a new user account is created.
* **Action**: The user's information is stored securely with encryption and hashing using KM and HSM.
* **Output**: The new account is created successfully.

## 5.6 Notifications and Logging

* **Action**: The system generates a notification for successful account creation and sends it to the user's email and phone.
* **Action**: If the account creation fails, the system sends a failure notification with the reason to the user's email and phone.
* **Action**: The system logs the process and status in the IDA.
* **Output**: The user is notified of the account status.

## 5.7 Exceptions and Error Handling

* **Action**: If an error occurs, the system handles exceptions and increments the retry counter.
* **Output**: If the retry count exceeds three, the process is terminated with an error message.

## 5.8 End of Process

* **Action**: If the account creation is successful, the user is redirected to the login page.
* **Output**: The process ends with a successful account creation or terminates with an error message.

## 5.9 Security Measures

* **Encryption and Hashing**: All user information, including consent forms and biometric data, is encrypted and hashed using advanced security protocols.
* **Network Security**: The system employs SSL/TLS for secure communication, and IDS/IPS to detect and prevent intrusions.
* **Firewalls**: Single or dual firewalls protect the network from unauthorised access

# 6. Visualisation

A screenshot of a computer screen

Description automatically generated

Please refer to the [GitHub](https://github.com/alan-turing-institute/Standard-Operating-Procedures-for-Digital-Identity-Systems) repository for further information.

# 7. Rationalisation

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **OB.1.4.B OFFLINE BIOMETRIC COLLECTION FACIAL DATA** | | | | | |
| Step | Description | Action | Systems Involved | Security Measures | Standards and References |
| 1. Start Process | Applicant begins the facial data collection process. | Provide consent and initiate facial data collection. | Enrollment Center | Consent verification before proceeding. | GDPR: Informed consent for processing biometric data. |
| 2. Positioning for Scan | Proper positioning before capturing facial data. | Position the camera and ensure applicant is correctly positioned for facial scan. | Public Network Systems Client | Ensure accuracy and quality of biometric capture. | ISO/IEC 19794-5: Technical specifications for facial image data. |
| 3. Capture Facial Data | Capture facial image of the applicant. | Request and capture facial scan; assist if needed for proper capture. | Public Network Systems Client | Quality control and compliance with biometric data standards. | ISO/IEC 29794-5: Facial recognition data quality requirements. |
| 4. Data Encryption and Upload | Secure and upload facial data. | Mask and encrypt facial scan data before uploading to the system. | Public Network Systems Server, KM, HSM | Data encryption to ensure confidentiality and integrity. | ISO/IEC 27001: Secure handling of sensitive data. |
| 5. Success and Failure Notifications | Handle scan success or failure. | Receive notification of successful or unsuccessful capture; manage errors as needed. | Private Network Systems Server | Responsive handling of capture outcomes and errors. | ISO/IEC 27001: Incident and error management standards. |
| 6. Store Biometric Data | Securely store facial biometric data. | Store facial scan in RID account with encryption and hashing. | Private Network Systems Server, IDA | Secure storage practices to protect biometric data. | ISO/IEC 27040: Storage security management for sensitive data. |
| 7. Notification and Logging | Finalise process and notify applicant. | Notify the participants of the outcome and log the process and status. | Notification Generator, IDA | Compliance with data privacy and security logging requirements. | GDPR, ISO/IEC 27001: Notification and logging of processing activities. |
| 8. Error Handling and Termination | Manage process termination or continuation. | Handle exceptions, reset and retry if necessary, or terminate the process with a reason if unresolved. | Error Handling System | Efficient management of retries and terminations. | ISO/IEC 27001: Error handling and business continuity protocols. |

# 8. References

1. NIST. Digital Identity Guidelines: Age Verification Guidance. Available at: [https://pages.nist.gov/800-63-3/].
2. eIDAS. Identity Proofing Requirements. Available at: [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L\_.2014.257.01.0073.01.ENG].
3. ISO. 27001, Secure System Access Control. Available at: [https://www.iso.org/standard/27001].
4. Aadhaar. Account Creation and Management. Available at: [https://uidai.gov.in/en/my-aadhaar/about-your-aadhaar/aadhaar-enrolment.html].
5. SingPass. Account Creation and Management. Available at: [https://www.singpass.gov.sg/home/ui/assets/pdf/Singpass\_Registration\_Guide.pdf].
6. FATF. Digital Identity Guidance: Authentication Mechanisms. Available at: [https://www.fatf-gafi.org/en/publications/Financialinclusionandnpoissues/Digital-identity-guidance.html].
7. Estonia ID. Data Protection Practices. Available at: [https://toolbox.estonia.ee/asset-page/252494-e-estonia-guide-full-brochure].
8. Emirates ID. Available at: [https://u.ae/en/information-and-services/visa-and-emirates-id/emirates-id].