|  |  |  |
| --- | --- | --- |
| **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: IRIS Data

OB.1.4.D - 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](#_Toc177312200)

[2. Definitions and Abbreviations 3](#_Toc177312201)

[3. Application 3](#_Toc177312202)

[3.1 Ownership and Stakeholders 3](#_Toc177312203)

[3.1.1 Digital Identity Service Providers (DISPs) 3](#_Toc177312204)

[3.1.2 IT and Security Teams 3](#_Toc177312205)

[3.1.3 Compliance and Legal Departments 4](#_Toc177312206)

[3.2 Users and Beneficiaries 4](#_Toc177312207)

[3.2.1 General Public 4](#_Toc177312208)

[3.2.2 Government Agencies 4](#_Toc177312209)

[3.2.3 Private Sector Companies 4](#_Toc177312210)

[3.3 Benefits and Impact 4](#_Toc177312211)

[3.3.1 Enhanced Security 4](#_Toc177312212)

[3.3.2 Regulatory Compliance 5](#_Toc177312213)

[3.3.3 Streamlined Processes 5](#_Toc177312214)

[3.3.4 Interoperability 5](#_Toc177312215)

[3.3.5 Data Privacy and Protection 5](#_Toc177312216)

[4. Prerequisites 5](#_Toc177312217)

[4.1 Assumptions 6](#_Toc177312218)

[4.2 Constraints 6](#_Toc177312219)

[5. Process Flow - Process and Procedures 6](#_Toc177312220)

[5.1 Applicant Actions: 7](#_Toc177312221)

[5.1.1 Start (Offline): 7](#_Toc177312222)

[5.1.2 Provide Consent (OB.1.4.A) 7](#_Toc177312223)

[5.1.3 Position Iris in Front of Camera: 7](#_Toc177312224)

[5.2 Parent/Guardian/Introducer Actions 7](#_Toc177312225)

[5.2.1 Provide Consent (OB.1.4.A) 7](#_Toc177312226)

[5.2.2 Assist with Iris Positioning: 7](#_Toc177312227)

[5.3 Administrator Actions: 7](#_Toc177312228)

[5.3.1Verify Consent Given for Biometric Collection: 7](#_Toc177312229)

[5.3.2 Verify Applicant's Iris Presence 7](#_Toc177312230)

[5.3.3. Request Iris Scan: 7](#_Toc177312231)

[5.3.4 Capture Iris Image: 8](#_Toc177312232)

[5.3.5 Provide Acknowledgment of Iris Capture: 8](#_Toc177312233)

[5.4 System Processing 8](#_Toc177312234)

[5.4.1 Public Network Systems (Client) 8](#_Toc177312235)

[5.4.2 Consent Form and Biometric Data Collection 8](#_Toc177312236)

[5.4.3 Private Network Systems (Server) 8](#_Toc177312237)

[5.5 Exceptions and Error Handling 9](#_Toc177312238)

[5.6 End of Process 9](#_Toc177312239)

[5.7 Security Measures 9](#_Toc177312240)

[6. Visualisation 10](#_Toc177312241)

[7. Rationalisation 11](#_Toc177312242)

[8. References 12](#_Toc177312243)

# 1. Purpose

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

**AC**: Access Control

**FTP**: First Time Password

**OTP**: One-Time Password

**2FA**: Two-Factor Authentication

**API**: Application Programming Interface

**HTTPS**: Hyper Text Transfer Protocol Secure

**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.
* Oversee the development, maintenance, and updating of the system.
* Supervise 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 organization managing the DID portal play a crucial role.

**Responsibilities:**

* Manage system security, including encryption protocols, and the implementation of CAPTCHA, OTPs, and other security measures.
* Oversee the hardware and software infrastructure, ensuring system uptime and resolving technical issues.
* Conduct regular security audits and vulnerability assessments to maintain system security and adherence to the latest security standards.

### 3.1.3 Compliance and Legal Departments

* **Ownership:** These departments ensure that the biometric collection process complies with legal and regulatory requirements.
* **Responsibilities:**
  + Ensure adherence to standards such as ISO 27001, NIST, eIDAS, and other relevant regulations.
  + Participate in audits, documentation, and compliance checks.
  + Monitor and implement changes in regulatory requirements to maintain compliance.

## 3.2 Users and Beneficiaries

### 3.2.1 General Public

* **Users**: Individuals seeking to create a new digital identity account or complete biometric registration for themselves or dependents.
* **Usage:**
  + Utilize this process to provide biometric data and consent securely.
  + Access government services, financial services, or other services requiring a verified digital identity.

### 3.2.2 Government Agencies

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

### 3.2.3 Private Sector Companies

* **Users:** Businesses needing identity verification for employees or customers.
* **Usage:**
  + Use the DID portal for secure service access, employee onboarding, and compliance with various industry regulations.

## 3.3 Benefits and Impact

### 3.3.1 Enhanced Security

* **Benefit:** Provides improved security for users through advanced encryption, two-factor authentication, and robust error handling.
* **Impact:**
  + Reduces risks associated with identity theft, fraud, and unauthorized access.
  + Increases overall trust in the digital identity system.

### 3.3.2 Regulatory Compliance

* **Benefit:** Ensures adherence to international standards and regulations, minimizing legal risks.
* **Impact:**
  + Builds trust with users and regulatory bodies.
  + Facilitates smoother operations and more efficient service delivery.

### 3.3.3 Streamlined Processes

* **Benefit:** Simplifies the biometric collection and identity verification processes for users.
* **Impact:**
  + Enhances user experience, boosts adoption rates, and improves service efficiency.
  + Decreases the time and resources needed for account setup and verification.

### 3.3.4 Interoperability

* **Benefit:** Enables integration with other systems and services.
* **Impact:**
  + Allows seamless access to a variety of services across different sectors.
  + Promotes a unified digital identity system usable across multiple platforms.

### 3.3.5 Data Privacy and Protection

* **Benefit:** Ensures that user data is securely stored and managed in compliance with data protection laws.
* **Impact**:
  + Increases user confidence in the system by safeguarding sensitive information.
  + Mitigates 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. These prerequisites serve as the foundational parameters necessary for the SOP to function effectively within the broader SOP framework.

**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, including iris scanners and other necessary hardware.

**Interdependencies:**

* This SOP operates in conjunction with other processes, such as system maintenance SOPs and security protocol SOPs. It relies on these interconnected systems throughout the onboarding, authentication, and lifecycle management phases to ensure seamless operation and security compliance. The next immediate SOPs to be followed are:

OB.1.4.E Application Approval/Rejection

## 4.1 Assumptions

**User Proficiency:**

* Users (applicants, parents/guardians, introducers) are expected to have a basic understanding of navigating internet applications and completing digital forms.
* Administrators are trained to operate biometric collection equipment and to explain consent forms to participants.

**Technological Infrastructure:**

* The technological infrastructure, including servers, networks, and security systems, is maintained to current standards and operates without significant downtime.
* Enrollment centers are equipped with the necessary hardware and software for efficient biometric data collection and consent management.

## 4.2 Constraints

**System Maintenance and Outages:**

* The biometric collection process may be temporarily hindered by scheduled system maintenance or unexpected outages.

**Regulatory and Technological Changes:**

* The SOP may require adjustments in response to regulatory changes or technological advancements 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, supported by 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 Iris in Front of Camera:

* **Action**: Applicant positions their eyes in front of the camera for iris data capture.
* **Output**: Iris are correctly positioned 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 with Iris Positioning:

* **Action:** Assist the applicant in positioning their Iris on the camera if necessary.
* **Output:** Iris are correctly positioned for data capture with assistance.

## 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's Iris Presence

* **Action:** Confirm the presence of the applicant's iris for scanning.
* **Output:**  Iris presence confirmed

### 5.3.3. Request Iris Scan:

* **Action:** Request the applicant to position their eyes for iris scanning
* **Output:** Iris scan initiated.

### 5.3.4 Capture Iris Image:

* **Action:** Capture the iris images of the applicant.
* **Output:** Iris images captured.

### 5.3.5 Provide Acknowledgment of Iris Capture:

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

## 5.4 System Processing

### 5.4.1 Public Network Systems (Client)

**Mask & Encrypt RID and Applicant Details:**

* **Action:** System masks and encrypts the Registration ID (RID) and applicant details.
* **Output:** Encrypted details are transmitted to the server.

**Iris Scan Processing:**

* **Action:** System processes the iris scan data.
* **Output:** Iris scan data is processed and transmitted to the server.

### 5.4.2 Consent Form and Biometric Data Collection

* **Action:** System processes iris scan data.
* **Output:** Iris Scan Data is processed and transmitted to the server.

### 5.4.3 Private Network Systems (Server)

**Initiate Iris Biometric Collection:**

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

**Store Iris Biometric Data Securely:**

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

**Generate Notifications:**

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

## 5.5 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.

## 5.6 End of Process

**Success Notification:**

* **Action**: Applicant receives acknowledgment of successful iris data collection and is directed to the next steps.
* **Output**: Process ends successfully.

**Failure Notification:**

* **Action:** Applicant is notified of the failure and provided with instructions.
* **Output:** Output terminates with error handling.

## 5.7 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 unauthorized access

# 6. Visualisation

A screenshot of a computer

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.A OFFLINE BIOMETRIC COLLECTION\_CONSENT** | | | | | |
| Step | Description | Action | Systems Involved | Security Measures | Standards and References |
| 1. Arrival and Verification | Applicant arrives at the enrollment center. | Verify appointment time and RID at the center. | Enrollment Center | Verification of identification and appointment details. | ISO/IEC 27001: Verification of user identity and data integrity. |
| 2. Reading Consent Form | Applicant reads the consent form. | Provide the consent form; ensure all parties (applicant, parent/guardian, or introducer) read it. | Public Network Systems Client | Compliance with data protection laws (e.g., GDPR). | GDPR: Ensuring informed consent for data processing. |
| 3. Q&A Session | Address any questions regarding the consent form. | Offer Q&A session to clarify consent document details and usage of biometric data. | Enrollment Center | Providing clear and accessible information. | GDPR: Right to clear information about data processing. |
| 4. Consent Confirmation | Confirming explicit consent. | Request explicit consent for biometric data collection; handle special cases. | Public Network Systems Client | Secure handling of consent forms; explicit consent recording. | GDPR: Explicit consent requirements for sensitive data. |
| 5. Document Scanning and Encryption | Scan and secure the consent document. | Scan the signed consent document; mask and encrypt before uploading. | Public Network Systems Server, KM, HSM | Encryption and secure data storage of consent forms. | ISO/IEC 27001: Encryption and confidentiality of sensitive documents. |
| 6. Update and Store Consent | Update consent status in the system. | Update RID account with consent status; store scanned document securely. | Private Network Systems Server, IDA | Secure storage and access control for documented consent. | ISO/IEC 27001, GDPR: Secure storage and processing of consent records. |
| 7. Exception Handling | Manage any exceptions or errors. | Handle exceptions and errors; terminate or reschedule appointment if necessary. | Error Handling System | Error and exception management procedures in place. | ISO/IEC 27001: Incident and error management standards. |
| 8. Notification and Completion | Notify and conclude the process. | Generate notifications regarding the process; log the entire process and status. | Notification Generator, IDA | Secure logging and notification processes. | ISO/IEC 27001: Compliance with auditing and logging procedures. |

# 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].