|  |  |  |
| --- | --- | --- |
| **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: Consent

OB.1.4.A - 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](#_Toc177311082)

[2. Definitions and Abbreviations 3](#_Toc177311083)

[3. Application 3](#_Toc177311084)

[3.1 Ownership and Stakeholders 3](#_Toc177311085)

[3.1.1 Digital Identity Service Providers (DISPs) 3](#_Toc177311086)

[3.1.2. IT and Security Teams 3](#_Toc177311087)

[3.1.3 Compliance and Legal Departments 4](#_Toc177311088)

[3.2 Users and Beneficiaries 4](#_Toc177311089)

[3.2.1 General Public 4](#_Toc177311090)

[3.2.2 Government Agencies 4](#_Toc177311091)

[3.2.3 Private Sector Companies 4](#_Toc177311092)

[3.3 Benefits and Impact 4](#_Toc177311093)

[3.3.1 Enhanced Security 4](#_Toc177311094)

[3.3.2 Regulatory Compliance 4](#_Toc177311095)

[3.3.3 Streamlined Processes 5](#_Toc177311096)

[3.3.4 Interoperability 5](#_Toc177311097)

[3.3.5 Data Privacy and Protection 5](#_Toc177311098)

[4. Prerequisites 5](#_Toc177311099)

[4.1 Assumptions 6](#_Toc177311100)

[4.2 Constraints 6](#_Toc177311101)

[5. Process Flow - Process and Procedures 6](#_Toc177311102)

[5.1 Applicant Actions: 6](#_Toc177311103)

[5.1.1 Start (Offline): 6](#_Toc177311104)

[5.1.2 Visit Third Party/Enrolment Centre 7](#_Toc177311105)

[5.1.3 Read the Consent Form 7](#_Toc177311106)

[5.2 Parent/Guardian/Introducer Actions 7](#_Toc177311107)

[5.2.1 Start (Offline) 7](#_Toc177311108)

[5.2.2 Visit Third Party/Enrollment Center 7](#_Toc177311109)

[5.1.4 Read the Consent Form: 7](#_Toc177311110)

[5.3 Administrator Actions: 7](#_Toc177311111)

[5.3.1Verify Time, Centre, and RID 7](#_Toc177311112)

[5.3.2 Wait for All Participants to Arrive 7](#_Toc177311113)

[5.3.3Provide Document Detailing Biometric Collection 7](#_Toc177311114)

[5.3.4 Offer Support for Questions 8](#_Toc177311115)

[5.4 System Processing 8](#_Toc177311116)

[5.4.1 Public Network Systems (Client) 8](#_Toc177311117)

[5.4.2 Consent Form and Biometric Data Collection 8](#_Toc177311118)

[5.4.3 Private Network Systems (Server) 8](#_Toc177311119)

[5.5 User Account Creation 8](#_Toc177311120)

[5.6 Notifications and Logging 9](#_Toc177311121)

[5.7 Exceptions and Error Handling 9](#_Toc177311122)

[5.8 End of Process 9](#_Toc177311123)

[5.9 Security Measures 9](#_Toc177311124)

[6. Visualisation 10](#_Toc177311125)

[7. Rationalisation 11](#_Toc177311126)

[8. References 12](#_Toc177311127)

# 1. Purpose

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

# 2. Definitions and Abbreviations

**DID**: Digital Identity

**KM**: Key Manager

**HSM**: Hardware Security Module

**CA**: Certificate Authority

**IDA**: ID Authentication Database

**AC**: Access Control

**OTP**: One-Time Password

**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.
* 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.
* **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.1.1.B Initiating an Online Application*

## 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.

## 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 Visit Third Party/Enrolment Centre

* **Action**: Applicant visits the designated third-party or enrolment canter with the appointment confirmation letter.
* **Output**: Applicant is at the centre for biometric collection.

### 5.1.3 Read the Consent Form

* **Action**: Applicant reads the consent form provided at the centre.
* **Output**: Consent form reviewed

## 5.2 Parent/Guardian/Introducer Actions

### 5.2.1 Start (Offline)

* **Action:** Parent/guardian or introducer begins the process with the applicant
* **Output:** Process initiated for applicant with support.

### 5.2.2 Visit Third Party/Enrollment Center

* **Action:** Accompany applicant to the center with the appointment confirmation letter.
* **Output:** Both parties are at the center for biometric collection.

### 5.1.4 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:

### 5.3.1 **Verify Time, Centre, and RID**

* **Action:** Verify the appointment time, centre, and Registration ID (RID).
* **Output:** Verification completed.

### 5.3.2 **Wait for All Participants to Arrive**

* **Action:** Ensure all participants (applicant and parent/guardian/introducer) are present.
* **Output:** Participants are ready for the process.

### 5.3.3 **Provide Document Detailing Biometric Collection**

* **Action:** Provide a document detailing the process, storage, and usage of biometric data.
* **Output:** Document provided.

### 5.3.4 **Offer Support for Questions**

* **Action:** Offer support and answer any questions regarding the consent form.
* **Output:** Questions addressed.

## 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:** Capture and encrypt the consent form and biometric data.
* **Output:** Data sent to the server for processing.

### 5.4.3 Private Network Systems (Server)

**Verify RID and Appointment Details Match:**

* **Action:** System verifies if RID and appointment details match.
* **Output:** If matched, proceed with updating arrival status.

**Update Arrival Status in RID Account:**

* **Action:** Update the arrival status in the RID account.
* **Output:** Arrival status updated.

**Store Consent Document Securely:**

* **Action:** Store the scanned and encrypted consent document securely in the RID account.
* **Output:** Consent document stored.

**Generate Notifications:**

* **Action:** Generate notifications for successful or failed consent processes.
* **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 diagram of a flowchart

Description automatically generated

Please refer to the [GitHub](https://github.com/carstenmaple/Standard-Operating-Procedures-for-Digital-Identity-Systems/blob/main/Standard%20Operating%20Procedures/Phase%20A%20-%20Onboarding/1.%20Collection%20and%20Resolution/Collection%20and%20Resolution.pdf) 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].