|  |  |  |
| --- | --- | --- |
| **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 -OFFLINE BIOMETRIC COLLECTION: APPOINTMENT

OB.1.3.E - 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 4](#_Toc177311149)

[2. Definitions and Abbreviations 4](#_Toc177311150)

[3. Application 4](#_Toc177311151)

[3.1 Ownership and Stakeholders 4](#_Toc177311152)

[3.1.1 Digital Identity Service Providers (DISPs) 4](#_Toc177311153)

[3.1.2. IT and Security Teams 4](#_Toc177311154)

[3.1.3 Compliance and Legal Departments 5](#_Toc177311155)

[3.2 Users and Beneficiaries 5](#_Toc177311156)

[3.2.1 General Public 5](#_Toc177311157)

[3.2.2 Government Agencies 5](#_Toc177311158)

[3.2.3 Private Sector Companies 5](#_Toc177311159)

[3.3 Benefits and Impact 5](#_Toc177311160)

[3.3.1 Enhanced Security 5](#_Toc177311161)

[3.3.2 Regulatory Compliance 6](#_Toc177311162)

[3.3.3 Streamlined Processes 6](#_Toc177311163)

[3.3.4 Interoperability 6](#_Toc177311164)

[3.3.5 Data Privacy and Protection 6](#_Toc177311165)

[4. Prerequisites 6](#_Toc177311166)

[4.1 Assumptions 7](#_Toc177311167)

[4.2 Constraints 7](#_Toc177311168)

[5. Process Flow - Process and Procedures 7](#_Toc177311169)

[5.1 Start 7](#_Toc177311170)

[5.2 Submit Acknowledgement Letter 7](#_Toc177311171)

[5.3 Receive Acknowledgement Letter 7](#_Toc177311172)

[5.4 Check Availability 8](#_Toc177311173)

[5.5 Select Appointment Time 8](#_Toc177311174)

[5.6 Confirm Appointment 8](#_Toc177311175)

[5.7 Print Confirmation Letter 8](#_Toc177311176)

[5.8 Print Failure Letter 8](#_Toc177311177)

[5.9 Mask and Encrypt Appointment Details 8](#_Toc177311178)

[5.10 Verify RID and Details 8](#_Toc177311179)

[5.11 Notify Available Appointments 8](#_Toc177311180)

[5.12 Update Appointment Details 9](#_Toc177311181)

[5.13 Store Appointment Details 9](#_Toc177311182)

[5.14 Exception and Error Handling 9](#_Toc177311183)

[5.15 Notification and Logging 9](#_Toc177311184)

[6. Visualisation 10](#_Toc177311185)

[7. Rationalisation 11](#_Toc177311186)

[8. References 12](#_Toc177311187)

# 1. Purpose

This SOP outlines the steps for the offline biometric collection appointment process. It covers the process from approaching the booking counter to receiving the appointment confirmation letter.

# 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.
  + 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 book an appointment for creating a new digital identity account.
* **Usage**:
  + Use this process to pre-register and book an appointment 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 pre-registration and appointment booking process on 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 administrator must have access to a device capable of connecting to the internet, equipped with updated security features.
* **Technical Setup:** Access to the DID portal server and backend systems, including database servers for storing encrypted user 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 *1.4.A OFFLINE BIOMETRIC COLLECTION CONSENT.*

## 4.1 Assumptions

* Users possess a basic understanding of how to navigate internet applications and complete digital forms.
* The technological infrastructure (servers, network, security systems) is maintained to current standards and is operational without significant downtime.

## 4.2 Constraints

* Limitations due to scheduled system maintenance or unexpected outages, which may temporarily hinder the application process.
* Any regulatory changes or updates in technology that require adjustments in the SOP before proceeding with user applications.

# 5. Process Flow - Process and Procedures

This section provides a high-level overview of the biometric collection appointment booking process from approaching the booking counter to receiving the appointment confirmation letter.

## 5.1 Start

* **Action**: The applicant, parent/guardian, or introducer approaches the booking counter attendant.
* **Output**: The appointment booking process begins.

## 5.2 Submit Acknowledgement Letter

* **Action**: The applicant submits the acknowledgement letter with the RID for appointment booking.
* **Output**: The acknowledgement letter is submitted.

## 5.3 Receive Acknowledgement Letter

* **Action**: The administrator receives the acknowledgement letter with the RID for appointment booking.
* **Output**: The acknowledgement letter is received.

## 5.4 Check Availability

* **Action**: The administrator checks the availability of the center and time for biometric collection appointment.
* **Output**: Availability is checked.

## 5.5 Select Appointment Time

* **Action**: The applicant selects the desired appointment center and time.
* **Output**: The appointment center and time are selected.

## 5.6 Confirm Appointment

* **Action**: The administrator confirms the selected appointment center and time.
* **Output**: The appointment is confirmed.

## 5.7 Print Confirmation Letter

* **Action**: The administrator prints the appointment confirmation letter with the RID.
* **Output**: The appointment confirmation letter is printed.

## 5.8 Print Failure Letter

* **Action**: If there is an error, the administrator prints an appointment failure letter with the error.
* **Output**: The appointment failure letter is printed.

## 5.9 Mask and Encrypt Appointment Details

* **Action**: The public network system masks and encrypts the appointment details using KM, HSM, and CA.
* **Output**: The encrypted appointment details are ready for server processing.

## 5.10 Verify RID and Details

* **Action**: The private network system verifies if the RID and details match.
* **Output**: If details match, the process continues; otherwise, it redirects to error handling.

## 5.11 Notify Available Appointments

* **Action**: The system notifies the available appointments.
* **Output**: Available appointments are notified.

## 5.12 Update Appointment Details

* **Action**: The system updates the appointment details.
* **Output**: Appointment details are updated.

## 5.13 Store Appointment Details

* **Action**: The private network system stores the appointment details in the RID account securely with encryption and hashing.
* **Output**: The appointment details are stored securely.

## 5.14 Exception and Error Handling

* **Action**: The system handles exceptions and increments the retry counter if needed.
* **Output**: If the retry count exceeds the limit, the process terminates with an error message.

## 5.15 Notification and Logging

* **Action**: The system generates a notification for successful appointment booking and sends it to the applicant.
* **Action**: If the process fails, the system sends a failure notification with the reason to the applicant.
* **Action**: The system logs the process and status in the IDA.
* **Output**: The applicant is notified of the appointment status.

# 6. Visualisation

A diagram of a flowchart

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.1.3.E OFFLINE BIOMETRIC COLLECTION APPOINTMENT** | | | | | |
| Step | Description | Action | Systems Involved | Security Measures | Standards and References |
| 1. Start Process | Applicant approaches the booking counter. | Submit acknowledgment letter with RID to the booking counter attendant. | Enrollment Center | Initial verification of acknowledgment letter and RID. | ISO 27001: Verification and validation procedures. |
| 2. Check Availability | Administrator checks appointment availability. | Check availability of center and time for biometric collection appointment. | Public Network Systems Client | Secure handling of appointment scheduling information. | NIST Digital Identity: Secure management of biometric collection scheduling. |
| 3. Digitise and Secure Data | Secure and process appointment data. | Mask and encrypt appointment details and RID; update appointment details in the system. | Public Network Systems Server, KM, HSM | Encryption and secure handling of personal and appointment data. | ISO 27001: Data encryption and secure data handling protocols. |
| 4. Approve or Reject Application | Approve or reject the application based on the validation and verification of the details. | Print appointment confirmation letter with RID if approved, or generate a rejection notice if rejected; handle errors if any. | Public and Private Network Systems | Error handling and secure printing of confirmation details. | FATF Digital Identity Guidance: Secure document issuance and error management. |
| 5. Notification and Error Handling | Manage notifications and potential errors. | Notify about available appointments; manage exceptions and retry operations if necessary. | Private Network Systems Server | Notification generation and error logging for auditing purposes. | ISO 27001: Incident and error management; notification security. |
| 5. Notification and Error Handling | Manage notifications and potential errors. | Notify about available appointments; manage exceptions and retry operations if necessary. | Private Network Systems Server | Notification generation and error logging for auditing purposes. | ISO 27001: Incident and error management; notification security. |

# 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].