|  |  |  |
| --- | --- | --- |
| **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 -PRE-REGISTRATION: APPOINTMENT BOOKING

OB.1.3.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 4](#_Toc177311206)

[2. Definitions and Abbreviations 4](#_Toc177311207)

[3. Application 4](#_Toc177311208)

[3.1 Ownership and Stakeholders 4](#_Toc177311209)

[3.1.1 Digital Identity Service Providers (DISPs) 4](#_Toc177311210)

[3.1.2. IT and Security Teams 4](#_Toc177311211)

[3.1.3 Compliance and Legal Departments 5](#_Toc177311212)

[3.2 Users and Beneficiaries 5](#_Toc177311213)

[3.2.1 General Public 5](#_Toc177311214)

[3.2.2 Government Agencies 5](#_Toc177311215)

[3.2.3 Private Sector Companies 5](#_Toc177311216)

[3.3 Benefits and Impact 5](#_Toc177311217)

[3.3.1 Enhanced Security 5](#_Toc177311218)

[3.3.2 Regulatory Compliance 6](#_Toc177311219)

[3.3.3 Streamlined Processes 6](#_Toc177311220)

[3.3.4 Interoperability 6](#_Toc177311221)

[3.3.5 Data Privacy and Protection 6](#_Toc177311222)

[4. Prerequisites 6](#_Toc177311223)

[4.1 Assumptions 7](#_Toc177311224)

[4.2 Constraints 7](#_Toc177311225)

[5. Process Flow - Process and Procedures 7](#_Toc177311226)

[5.1 Start 7](#_Toc177311227)

[5.2 Evaluate Application Form 7](#_Toc177311228)

[5.3 Digitise Application Form 7](#_Toc177311229)

[5.4 Scan Supporting Documents 8](#_Toc177311230)

[5.5 Mask and Encrypt Application Details 8](#_Toc177311231)

[5.6 Verify RID and Applicant Details 8](#_Toc177311232)

[5.7 Generate New RID 8](#_Toc177311233)

[5.8 Store Application Details 8](#_Toc177311234)

[5.9 Exception and Error Handling 8](#_Toc177311235)

[5.10 Notification and Logging 8](#_Toc177311236)

[6. Visualisation 9](#_Toc177311237)

[7. Rationalisation 10](#_Toc177311238)

[8. References 11](#_Toc177311239)

# 1. Purpose

This SOP outlines the steps for pre-registering and booking an appointment through an offline process. It covers the process from receiving the signed application form to the final booking of the appointment.

# 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 *1.3.E OFFLINE BIOMETRIC COLLECTION – APPOINTMENT.*

## 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 offline application process from the initial visit to the enrollment center to the pre-registration for appointment.

## 5.1 Start

* **Action**: The administrator starts the process offline by receiving the signed application form along with supporting documents.
* **Output**: The pre-registration process begins.

## 5.2 Evaluate Application Form

* **Action**: The administrator evaluates the application form for completeness.
* **Output**: The application form is evaluated for completeness.

## 5.3 Digitise Application Form

* **Action**: The administrator digitises the application form details and uploads them to the system.
* **Output**: The application form details are digitised and uploaded.

## 5.4 Scan Supporting Documents

* **Action**: The administrator scans photocopies of supporting documents.
* **Output**: Supporting documents are scanned and digitised.

## 5.5 Mask and Encrypt Application Details

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

## 5.6 Verify RID and Applicant Details

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

## 5.7 Generate New RID

* **Action**: The system generates a new RID for the applicant if necessary.
* **Output**: A new RID is generated for the applicant.

## 5.8 Store Application Details

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

## 5.9 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.

## 5.10 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 work flow

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.D PRE-REGISTRATION\_APPOINTMENT BOOKING** | | | | | |
| Step | Description | Action | Systems Involved | Security Measures | Standards and References |
| 1. Start Process | Administrator receives the application offline. | Receive signed application form with supporting documents. | Enrollment Center | Initial review for completeness and authenticity. | eIDAS: Standards for document handling and verification. |
| 2. Digitise Application | Convert physical documents into digital format. | Digitise application details and upload to the system; scan supporting documents. | Public Network Systems Client | Encrypt application and document details. | ISO 27001: Secure handling and encryption of digital data. |
| 3. Verify and Process Application | Ensure all details are correct and complete. | Check if the RID exists and matches the applicant’s details. | Private Network Systems Server | Use of secure channels (SSL/TLS) for data transmission; data masking and encryption. | NIST Digital Identity: Verification of identity details. |
| 4. RID Management | Handle Registration Identification (RID) details. | Generate new RID for the applicant if not existing; store securely in the DID user database. | Private Network Systems Server, IDA | Encryption and hashing of RID details. | ISO 27001: Secure storage and integrity of registration details. |
| 5. Exception and Error Handling | Manage errors in data processing. | Handle exceptions and errors; reset counters if necessary; terminate process with reason if issues are not resolved. | Error Handling System | Error logging and detailed notification of issues. | FATF Digital Identity Guidance: Error management and process integrity. |
| 6. Appointment Booking and Notification | Confirm the booking and notify the applicant. | Print acknowledgment with RID for appointment booking; if rejected, provide a reason. | Notification Generator | Secure generation of notifications and acknowledgments. | AADHAR: Notification protocols and secure document handling. |
| 7. Finalisation | Log the completed process. | Log the process and status in the IDA system. | IDA | Logging for audit and compliance, ensuring all steps are recorded. | ISO 27001: Compliance with information security management practices; NIST Digital Identity: Logging and auditing processes. |

# 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].