|  |  |  |
| --- | --- | --- |
| **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 APPLICATION: APPLICATION BY PARENT or GUARDIAN

OB.1.3.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 4](#_Toc177309855)

[2. Definitions and Abbreviations 4](#_Toc177309856)

[3. Application 4](#_Toc177309857)

[3.1 Ownership and Stakeholders 4](#_Toc177309858)

[3.1.1 Digital Identity Service Providers (DISPs) 4](#_Toc177309859)

[3.1.2. IT and Security Teams 4](#_Toc177309860)

[3.1.3 Compliance and Legal Departments 5](#_Toc177309861)

[3.2 Users and Beneficiaries 5](#_Toc177309862)

[3.2.1 General Public 5](#_Toc177309863)

[3.2.2 Government Agencies 5](#_Toc177309864)

[3.2.3 Private Sector Companies 5](#_Toc177309865)

[3.3 Benefits and Impact 5](#_Toc177309866)

[3.3.1 Enhanced Security 5](#_Toc177309867)

[3.3.2 Regulatory Compliance 5](#_Toc177309868)

[3.3.3 Streamlined Processes 6](#_Toc177309869)

[3.3.4 Interoperability 6](#_Toc177309870)

[3.3.5 Data Privacy and Protection 6](#_Toc177309871)

[4. Prerequisites 6](#_Toc177309872)

[4.1 Assumptions 7](#_Toc177309873)

[4.2 Constraints 7](#_Toc177309874)

[5. Process Flow - Process and Procedures 7](#_Toc177309875)

[5.1 Start 7](#_Toc177309876)

[5.2 Request Application Form 7](#_Toc177309877)

[5.3 Fill Application Form 7](#_Toc177309878)

[5.4 Submit Documents 7](#_Toc177309879)

[5.5 Document Verification 8](#_Toc177309880)

[5.6 Mask and Encrypt Application Details 8](#_Toc177309881)

[5.7 Check for Matching Details 8](#_Toc177309882)

[5.8 Exception and Error Handling 8](#_Toc177309883)

[5.9 Notification and Logging 8](#_Toc177309884)

[5.10 Pre-Registration for Appointment 8](#_Toc177309885)

[6. Visualisation 9](#_Toc177309886)

[7. Rationalisation 10](#_Toc177309887)

[8. References 11](#_Toc177309888)

# 1. Purpose

This SOP outlines the steps for initiating and completing an offline application for a new account by a parent or guardian. It covers the process from visiting the enrolment centre to the submission and verification of the application.

# 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

# 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 organization 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**: Parents or guardians looking to create a new digital identity account for their 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 unauthorized access.
  + Enhances the overall trust in the digital identity system.

### 3.3.2 Regulatory Compliance

* **Benefit**: Ensures compliance with international standards and regulations, minimizing 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 application 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 introducer 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.D PRE-REGISTRATION. - APPOINTMENT BOOKING.*

## 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 registration process.
* Any regulatory changes or updates in technology that require adjustments in the SOP before proceeding with user registrations.

# 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 parent or guardian visits the enrollment center.
* **Output**: The application process begins.

## 5.2 Request Application Form

* **Action**: The parent or guardian requests a new application form.
* **Output**: The physical copy of the application form is handed over to the parent or guardian.

## 5.3 Fill Application Form

* **Action**: If requested for assistance, the administrator helps the parent or guardian fill out the form.
* **Output**: The form is filled with details such as given name, family name, date of birth (DOB), address, POI, POA, RID, UID, email, and phone number.

## 5.4 Submit Documents

* **Action**: The parent or guardian provides photocopies of POI, POA, and POR, and submits the completed form.
* **Output**: The documents are submitted and acknowledged.

## 5.5 Document Verification

* **Action**: The administrator verifies if the parent or guardian’s RID/UID matches and if the applicant is older than 5 years.
* **Output**: The application is accepted if the age requirement and relationship verification are met.

## 5.6 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.

## 5.7 Check for Matching Details

* **Action**: The private network system checks if the applicant’s name, demographic, and contact details do not exist in the DID database.
* **Output**: If details are unique, the process continues; otherwise, it redirects to error handling.

## 5.8 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.

## 5.9 Notification and Logging

* **Action**: The system generates a notification for successful pre-registration 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 application status.

## 5.10 Pre-Registration for Appointment

* **Action**: The process proceeds to pre-registration for an appointment (OB.1.3.D).
* **Output**: The appointment is pre-registered successfully.

# 6. Visualisation

A diagram of a workflow

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.B OFFLINE APPLICATION\_APPLICATION BY PARENT\_GUARDIAN** | | | | | |
| Step | Description | Action | Systems Involved | Security Measures | Standards and References |
| 1. Visit Enrollment Center | Parent or guardian begins the process in person. | Visit an enrollment center; request an application form for parent/guardian. | Enrollment Center | Personal interaction ensures the presence and intent of the guardian. | eIDAS: Physical verification standards. |
| 2. Form Filling | Fill out the application form. | Complete the form with applicant’s details and guardian’s details; if needed, get assistance from the administrator. | Applicant and Administrator | Manual entry of accurate information for both applicant and guardian. | NIST Digital Identity: Accurate data entry guidelines. |
| 3. Document Submission | Provide necessary documents. | Confirm details and provide photocopies of proof of identity (POI), proof of address (POA), and proof of relationship (POR). | Enrollment Center | Ensure all provided documents are verified and copied securely. | ISO 27001: Handling and security of sensitive documents. |
| 4. Application Processing | Process the application form. | Submit the application and attached documents; receive an acknowledgement. | Enrollment Center | Secure handling and processing of application forms. | FATF Digital Identity Guidance: Secure document processing. |
| 5. Data Encryption and Transfer | Secure and transfer application data. | Encrypt application details before digital transmission to servers. | Public Network Systems Client, KM, HSM | Encryption using HSM; data transmitted via secure channels (SSL/TLS). | ISO 27001: Encryption and secure transmission protocols. |
| 6. Verification and Error Handling | Verify application details in the database. | Check if parent/guardian’s RID matches; verify if applicant’s details are unique in the DID database; manage errors if details are incorrect. | Private Network Systems Server, IDA | Verification against existing records; detailed error logging and handling. | eIDAS & NIST Digital Identity: Verification processes and error management. |
| 7. Notification and Finalization | Notify parent/guardian of application status. | Generate notification of the process completion; log the process and status. | Notification Generator, IDA | Secure notification delivery; logging for audit and compliance. | ISO 27001: Compliance with information security management practices; AADHAR: Logging and notification 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].