|  |  |  |
| --- | --- | --- |
| **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 - Application approval or Rejection

OB.1.4.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 3](#_Toc177312029)

[2. Definitions and Abbreviations 3](#_Toc177312030)

[3. Application 3](#_Toc177312031)

[3.1 Ownership and Stakeholders 3](#_Toc177312032)

[3.1.1 Digital Identity Service Providers (DISPs) 3](#_Toc177312033)

[3.1.2 IT and Security Teams 3](#_Toc177312034)

[3.1.3 Compliance and Legal Departments 4](#_Toc177312035)

[3.2 Users and Beneficiaries 4](#_Toc177312036)

[3.2.1 General Public 4](#_Toc177312037)

[3.2.2 Government Agencies 4](#_Toc177312038)

[3.2.3 Private Sector Companies 4](#_Toc177312039)

[3.3 Benefits and Impact 4](#_Toc177312040)

[3.3.1 Enhanced Security 4](#_Toc177312041)

[3.3.2 Regulatory Compliance 4](#_Toc177312042)

[3.3.3 Streamlined Processes 4](#_Toc177312043)

[3.3.4 Data Privacy and Protection 5](#_Toc177312044)

[4. Prerequisites 5](#_Toc177312045)

[4.1 Assumptions 5](#_Toc177312046)

[4.2 Constraints 5](#_Toc177312047)

[5. Process Flow - Process and Procedures 6](#_Toc177312048)

[5.1. Application Data Review: 6](#_Toc177312049)

[5.2. Handling Missing Data: 6](#_Toc177312050)

[5.3. Biometric Data Verification: 6](#_Toc177312051)

[5.4. Special Case Handling: 6](#_Toc177312052)

[5.5. Authentication: 6](#_Toc177312053)

[5.6. Approval/Rejection Decision: 6](#_Toc177312054)

[5.7. Notification: 6](#_Toc177312055)

[5.8. Data Logging: 6](#_Toc177312056)

[5.9 Security Measures 7](#_Toc177312057)

[6. Visualisation 8](#_Toc177312058)

[7. Rationalisation 9](#_Toc177312059)

[8. References 10](#_Toc177312060)

# 1. Purpose

The purpose of this SOP is to provide a standardised procedure for the approval or rejection of applications for Digital Identity (DID) accounts. It ensures secure and consistent processing, verifies data completeness, and manages special cases. This SOP outlines stakeholder responsibilities, prerequisites, and security measures, ensuring a transparent and efficient experience for applicants while protecting their data.

# 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:** Responsible for overseeing the application approval/rejection process for the DID portal.
* **Responsibilities:** Ensure secure, compliant, and efficient management of application data and decision-making processes.

### 3.1.2 IT and Security Teams

* **Ownership:** Handle the technical infrastructure supporting the DID portal's application processes.
* **Responsibilities:** Manage system security, including data encryption, and maintain the hardware and software infrastructure.

### 3.1.3 Compliance and Legal Departments

* **Ownership:** Ensure the application process adheres to legal and regulatory standards.
* **Responsibilities:** Oversee compliance with relevant laws and standards, including conducting audits and compliance checks.

## 3.2 Users and Beneficiaries

### 3.2.1 General Public

* **Users:** Individuals applying for a new digital identity account.
* **Usage:** Use the application process to submit their biometric and demographic information for identity proofing.

### Government Agencies

* **Users:** Departments requiring verified digital identities for service access.
* **Usage:** Rely on the approved digital identities for secure access to services.

### 3.2.3 Private Sector Companies

* **Users:** Businesses needing verified identities for employee or customer onboarding.
* **Usage:** Use the DID portal for secure verification and compliance with industry regulations.

## 3.3 Benefits and Impact

### 3.3.1 Enhanced Security

* **Benefit:** Secure handling of biometric and demographic data.
* **Impact:** Reduces risks of data breaches and unauthorised access.

### 3.3.2 Regulatory Compliance

* **Benefit:** Adherence to international and local regulations.
* **Impact:** Mitigates legal risks and builds trust with stakeholders.

### 3.3.3 Streamlined Processes

* **Benefit:** Efficient application approval/rejection workflow.
* **Impact:** Reduces processing time and enhances user experience.

## 3.3.4 Data Privacy and Protection

* **Benefit:** Secure storage and handling of sensitive information.
* **Impact:** Protects user data and maintains privacy.

# 4. Prerequisites

This section outlines the conditions required before starting the application approval/rejection process on the DID portal. These prerequisites are essential for ensuring the SOP functions effectively within the broader procedural framework.

**System Requirements:**

* Access to devices with internet capabilities and updated security features for data entry and communication.

**Technical Setup:**

* Access to the DID portal's server and backend systems for secure data storage.
* Necessary hardware and software to review and process applications

**Interdependencies:**

* The process relies on interconnected systems, including data encryption protocols, security audits, and system maintenance SOPs. It requires coordination with systems handling biometric data collection and identity verification. The next immediate SOPs to be followed are:

OB.2.A Validation of Proof of Identity and Proof of Address

## 4.1 Assumptions

* Administrators are trained to handle data securely and assess applications accurately.
* The technological infrastructure is up-to-date and functioning without significant downtime.

**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

* The process may be impacted by system maintenance or regulatory changes that necessitate adjustments in the SOP.

# 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. Application Data Review:

* **Action:** Administrator receives the applicant's Registration ID (RID) and verifies the completeness of the data submitted.
* **Output:** Completeness of the application data is confirmed.

## 5.2. Handling Missing Data:

* **Action:** If biometric data is missing, the administrator records the reason.
* **Output:** Reason for missing data is documented and encrypted.

## 5.3. Biometric Data Verification:

* **Action:** Verify the completeness of the biometric data. If data is complete, proceed to authentication.
* **Output:** Verification of biometric data completeness.

## 5.4. Special Case Handling:

* **Action:** For special cases where biometric data is missing, store the reason securely.
* **Output:** Special case reasons are stored in the RID account.

## 5.5. Authentication:

* **Action:** Authenticate the application using biometric data (fingerprint, iris, facial).
* **Output:** Authentication results are determined.

## 5.6. Approval/Rejection Decision:

* **Action:** Approve or reject the application based on the authentication results and completeness of data.
* **Output:** Application status is decided.

## 5.7. Notification:

* **Action:** Notify the applicant of the application outcome via email and phone.
* **Output:** Applicant is informed of approval or rejection.

## 5.8. Data Logging:

* **Action:** Log the process and status in the system.
* **Output:** Process completion is recorded.

## 5.9 Security Measures

* Encryption and Hashing: All sensitive data is encrypted and securely stored.
* Network Security: Secure channels and firewalls protect data during transmission and storage.

# 6. Visualisation

A diagram of a process 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.1.4.E OFFLINE BIOMETRIC COLLECTION\_CONSENT** | | | | | |
| Step | Description | Action | Systems Involved | Security Measures | Standards and References |
| 1. Start Process | Begin the approval/rejection process. | Administrator receives RID of applicant and checks completeness of data. | Admin Interface | Verification of data completeness and integrity. | ISO/IEC 27001: Information security management; eIDAS: Data integrity and authenticity. |
| 2. Check Biometric Data | Determine if biometric data is missing. | Fill appropriate reason for missing biometric data, if any. | Public Network Systems Client | Secure entry and encryption of reasons for missing data. | GDPR: Secure processing of personal data; NIST Digital Identity: Handling of biometric data. |
| 3. Authenticate Applicant | Use biometric data for authentication. | Authenticate using one or more biometric methods: fingerprint, facial recognition. | Biometric Authentication System | Secure biometric authentication processes. | ISO/IEC 19794: Biometric data interchange standards; Aadhar, SingPass: Biometric verification protocols. |
| 4. Decision Making | Approve or reject the application. | Approve the application if all conditions are met, otherwise reject with reasons. | Private Network Systems Server | Access control and decision integrity. | FATF Digital Identity Guidance: Decision-making criteria; Estonia ID, Emirates ID: Compliance with national identity standards. |
| 5. Notification of Decision | Inform the applicant of the decision. | Send notification via email and phone about the application approval or rejection. | Notification Generator | Secure notification delivery. | ISO/IEC 27001: Security of communications; eIDAS: Electronic identification and trust services. |
| 6. Log and Close | Log the process and conclude. | Store the decision and notify the applicant; log all process details for auditing. | IDA, Logging System | Secure logging and data retention. | ISO/IEC 27001: Logging and monitoring; GDPR: Data retention and transparency requirements. |

# 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].