|  |  |  |
| --- | --- | --- |
| **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- Initiating an online application

OB.1.1.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 3](#_Toc177311413)

[2. Definitions and Abbreviations 3](#_Toc177311414)

[3. Application 3](#_Toc177311415)

[3.1 Ownership and Stakeholders 3](#_Toc177311416)

[3.1.1 Digital Identity Service Providers (DISPs) 3](#_Toc177311417)

[3.1.2. IT and Security Teams 3](#_Toc177311418)

[3.1.3 Compliance and Legal Departments 4](#_Toc177311419)

[3.2 Users and Beneficiaries 4](#_Toc177311420)

[3.2.1 General Public 4](#_Toc177311421)

[3.2.2 Government Agencies 4](#_Toc177311422)

[3.2.3 Private Sector Companies 4](#_Toc177311423)

[3.3 Benefits and Impact 4](#_Toc177311424)

[3.3.1 Enhanced Security 4](#_Toc177311425)

[3.3.2 Regulatory Compliance 4](#_Toc177311426)

[3.3.3 Streamlined Processes 4](#_Toc177311427)

[3.3.4 Interoperability 4](#_Toc177311428)

[3.3.5 Data Privacy and Protection 5](#_Toc177311429)

[4. Prerequisites 5](#_Toc177311430)

[4.1 Assumptions 5](#_Toc177311431)

[4.2 Constraints 5](#_Toc177311432)

[5. Process Flow - Process and Procedures 6](#_Toc177311433)

[5.1 Visit DID Portal 6](#_Toc177311434)

[5.2 Click Login 6](#_Toc177311435)

[5.3 Enter Email and Password: 6](#_Toc177311436)

[5.4 Password Authentication (B.1.4.1.A) 6](#_Toc177311437)

[5.5 Authenticate using OTP (B.2.4.1.B): 6](#_Toc177311438)

[5.6 Home Page: Click Start Application 6](#_Toc177311439)

[5.7 Select Type of Application: 6](#_Toc177311440)

[5.8 System Processing 6](#_Toc177311441)

[5.8.1 Public Network Systems (Client): Mask & Encrypt Application Details: 6](#_Toc177311442)

[5.8.2 Private Network Systems (Server) 7](#_Toc177311443)

[5.9 Exceptions and Error Handling 7](#_Toc177311444)

[5.10 End of Process 7](#_Toc177311445)

[5.11 Security Measures 7](#_Toc177311446)

[6. Visualisation 9](#_Toc177311447)

[7. Rationalisation 10](#_Toc177311448)

[8. References 11](#_Toc177311449)

# 1. Purpose

This SOP outlines the steps required for initiating an online application for a Digital Identity (DID) account, detailing the process from logging into the DID portal to the receipt of application notifications.

# 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**: They ensure the process is secure, compliant with regulatory standards, and efficiently managed. They are responsible for the development, maintenance, and updating of the system.

### 3.1.2. IT and Security Teams

* **Ownership**: IT and security teams within the organisation managing the DID portal play a crucial role.
* **Responsibilities**: These teams handle system security, encryption protocols, and the implementation of CAPTCHA, OTPs, and other security measures. They also manage the hardware and software infrastructure, ensuring uptime and handling technical issues.

### 3.1.3 Compliance and Legal Departments

* **Ownership**: These departments ensure that the registration process complies with legal and regulatory requirements.
* **Responsibilities**: They oversee adherence to standards like ISO 27001, NIST, eIDAS, and others. They are involved in audits, documentation, and compliance checks.

## 3.2 Users and Beneficiaries

### 3.2.1 General Public

* **Users**: Individuals looking to create a new digital identity account.
* **Usage**: They use this process to register and authenticate their identity securely on the DID portal. This includes anyone needing to 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**: They 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.

### 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.

### 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.

### 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.

# 4. Prerequisites

This section outlines the essential conditions and resources required before initiating the registration 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 applicant 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 *OB.1.2.A ONLINE APPLICATION SELF INITIATED, OB.1.2.B ONLINE APPLICATION BY PARENT/GUARDIAN, OB.1.2.C ONLINE APPLICATION INITIATED BY INTRODUCER.*

## 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

The process involves interactions between the applicant, public network systems (client-side), and private network systems (server-side). Security measures such as encryption, OTP verification, and firewalls are integral throughout the process.

## 5.1 Visit DID Portal

* **Action:** User visits the Digital Identity (DID) portal.
* **Output:** The registration process begins

## 5.2 Click Login

* **Action:**User clicks on the login button.
* **Output:**Redirects to the login page.

## 5.3 Enter Email and Password:

* **Action:** User enters their email and password.
* **Output:** The login details are submitted for authentication.

## 5.4 Password Authentication (B.1.4.1.A)

* **Action:** System verifies the entered email and password.
* **Output:** If successful, proceeds to OTP generation.

## 5.5 Authenticate using OTP (B.2.4.1.B):

* **Action:** System sends OTP to user's registered email and phone. User enters OTP.
* **Output:** OTP authentication is completed.

## 5.6 Home Page: Click Start Application

* **Action:** User clicks the start application button on the homepage.
* **Output:** Redirects to application type selection.

## 5.7 Select Type of Application:

* **Action:** User selects the type of application (Self, Parent/Guardian, Introducer).
* **Output:** Based on selection, directs to appropriate application form.

## 5.8 System Processing

### 5.8.1 Public Network Systems (Client): Mask & Encrypt Application Details:

* **Action:** System masks and encrypts user details using KM, HSM, and CA.
* **Output:** Encrypted details are sent to the server.

### 5.8.2 Private Network Systems (Server)

**Generate OTP (B.2.4.1.A):**

* **Action:** Generates OTP for email and phone verification.
* **Output:** OTPs are sent to user.

**Verify OTP Authentication:**

* **Action:** Verifies if OTP entered by user matches.
* **Output:** If successful, proceeds with application creation.

**Create New RID for the Application:**

* **Action:** Creates a new Registration ID (RID) for the application.
* **Output:** RID and application details are securely stored.

**Store RID & Application Information:**

* **Action:** Stores the generated RID and application details.
* **Output:** Information is securely stored using KM and HSM.

**Notification Generator:**

* **Action:** Generates notification for successful or failed application creation.
* **Output:** Notification sent to user's email and phone.

## 5.9 Exceptions and Error Handling

**Terminate Process with Error Message:**

* **Action:** If any step fails, the process is terminated and an error message is displayed.
* **Output:** Error message sent to user, process logs update.

## 5.10 End of Process

**End of Process:**

* **If Successful**
  + **Action:** User is redirected to the application dashboard.
  + **Output:** Process ends with successful application initiation.
* **If Failed**
  + **Action:** User is notified of the failure.
  + **Output:** Process terminates with error handling.

## 5.11 Security Measures

* **Encryption and Hashing:** All user information is encrypted and hashed using advanced security protocols.
* **Network Security:** Utilises SSL/TLS for secure communication, IDS/IPS for intrusion detection and prevention.
* **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/alan-turing-institute/Standard-Operating-Procedures-for-Digital-Identity-Systems) repository for further information.

# 7. Rationalisation

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **OB.1.1.b INITIATING AN ONLINE APPLICATION** | | | | | |
| **Step** | **Description** | **Action** | **Systems Involved** | **Security Measures** | **Standards and References** |
| 1. Initial Access | User starts the application process online. | Visit DID portal, click login, enter email and password. | Applicant Interface | Password authentication. | NIST Digital Identity: Guidelines on secure login and authentication. |
| 2. Authentication | Secure the login with two-factor authentication. | Authenticate using OTP sent to email or phone. | Public Network Systems Client | Two-factor authentication with OTP. | ISO 27001: Controls for user access management; FATF Digital Identity Guidance: Enhancing security via multi-factor authentication. |
| 3. Application Type Selection | Applicant chooses the type of application. | Select application as self, by parent/guardian, or with introducer. | Public Network Systems Client | Data handling and access control at selection. | Estonia ID, eIDAS: Data integrity and choice handling in digital processes. |
| 4. Application Encryption | Encrypt and mask application details for protection. | Mask and encrypt application details using KM and HSM. | Private Network Systems Server, KM, HSM, CA | SSL/TLS for data transmission; encryption using HSM. | ISO 27001: Data encryption and secure key management practices. |
| 5. Application Processing | Handle the application based on type selected. | Generate new RID for the application, create application, or terminate with error message. | Private Network Systems Server, IDA, KM, HSM | Log and store RID and application information securely. | NIST Digital Identity, Aadhar: Secure processing and storage of application details. |
| 6. Notification and Logging | Notify the applicant of the application status. | Generate notifications of application initiation or failure. | Notification Generator, IDA | Notifications ensure transparency and inform the applicant. | SingPass, Emirates ID: Best practices for user notifications in digital identity systems. |

# 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].