Standard Operating Procedure- ONLINE APPLICATION: APPLICATION INITIATED BY INTRODUCER

OB.1.2.C - WITH RATIONALISATION

|  |  |  |
| --- | --- | --- |
| **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.*

**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](#_Toc177312596)

[2. Definitions and Abbreviations 3](#_Toc177312597)

[3. Application 3](#_Toc177312598)

[3.1 Ownership and Stakeholders 3](#_Toc177312599)

[3.1.1 Digital Identity Service Providers (DISPs) 3](#_Toc177312600)

[3.1.2. IT and Security Teams 3](#_Toc177312601)

[3.1.3 Compliance and Legal Departments 4](#_Toc177312602)

[3.2 Users and Beneficiaries 4](#_Toc177312603)

[3.2.1 General Public 4](#_Toc177312604)

[3.2.2 Government Agencies 4](#_Toc177312605)

[3.2.3 Private Sector Companies 4](#_Toc177312606)

[3.3 Benefits and Impact 4](#_Toc177312607)

[3.3.1 Enhanced Security 4](#_Toc177312608)

[3.3.2 Regulatory Compliance 5](#_Toc177312609)

[3.3.3 Streamlined Processes 5](#_Toc177312610)

[3.3.4 Interoperability 5](#_Toc177312611)

[3.3.5 Data Privacy and Protection 5](#_Toc177312612)

[4. Prerequisites 5](#_Toc177312613)

[4.1 Assumptions and Constraints 6](#_Toc177312614)

[4.1.1 Assumptions 6](#_Toc177312615)

[4.1.2 Constraints 6](#_Toc177312616)

[5. Process Flow - Process and Procedures 6](#_Toc177312617)

[5.1 Start 6](#_Toc177312618)

[5.2 Initial Online Application 6](#_Toc177312619)

[5.3 Form Filling 6](#_Toc177312620)

[5.4 Document Upload 6](#_Toc177312621)

[5.5 Review and Confirmation 7](#_Toc177312622)

[5.6 Public Network Systems (Client) - File Size and Format Check 7](#_Toc177312623)

[5.7 Public Network Systems (Client) - Masking and Encrypting 7](#_Toc177312624)

[5.8 Public Network Systems (Client) - Image Quality Check 7](#_Toc177312625)

[5.9 Public Network Systems (Client) - Face Verification 7](#_Toc177312626)

[5.10 Private Network Systems (Server) - Unique Applicant Check 7](#_Toc177312627)

[5.11 Private Network Systems (Server) – Request Evidence Documents 7](#_Toc177312628)

[5.12 Private Network Systems (Server) - Liveness Detection Test 7](#_Toc177312629)

[5.13 Private Network Systems (Server) - Exception and Error Handling 8](#_Toc177312630)

[5.14 Private Network Systems (Server) - Appointment Slot Check 8](#_Toc177312631)

[5.15 Notifications and Logging 8](#_Toc177312632)

[5.16 End of Process 8](#_Toc177312633)

[5.17 Security Measures 8](#_Toc177312634)

[6. Visualisation 9](#_Toc177312635)

[7. Rationalisation 10](#_Toc177312636)

[8. References 11](#_Toc177312637)

# 1. Purpose

This SOP outlines the steps for registering a new account on the Digital Identity (DID) portal. It details the process flow from the initial visit to the portal to the successful creation of a new user account or termination due to errors.

# 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

**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 create a new digital identity account.
* **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 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 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 *OB.1.4.A OFFLINE BIOMETRIC COLLECTION CONSENT.*

## 4.1 Assumptions and Constraints

This subsection describes underlying assumptions and potential constraints that could influence the effectiveness of the SOP.

### 4.1.1 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.

### 4.1.2 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 registration process from the initial online application to the confirmation of an appointment.

## 5.1 Start

* **Action**: The introducer begins the online application.
* **Output**: The registration process begins.

## 5.2 Initial Online Application

* **Action**: The introducer selects the application type (OB.1.1.B).
* **Output**: Application type is selected.

## 5.3 Form Filling

* **Action**: The introducer fills out the form with the applicant's details (given name, family name, address, claimed phone number).
* **Output**: The form with the applicant's details is completed.

## 5.4 Document Upload

* **Action**: The introducer uploads documents for ID verification (scanned copies).
* **Output**: Documents are uploaded for verification.

## 5.5 Review and Confirmation

* **Action** The introducer reviews the application and clicks confirm.
* **Output**: The application is reviewed and submitted.

## 5.6 Public Network Systems (Client) - File Size and Format Check

* **Action**: The system checks the file size and format.
* **Output**: File size and format are accepted.

## 5.7 Public Network Systems (Client) - Masking and Encrypting

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

## 5.8 Public Network Systems (Client) - Image Quality Check

* **Action**: The system checks the quality of the uploaded image.
* **Output**: Image quality is accepted.

## 5.9 Public Network Systems (Client) - Face Verification

* **Action**: The introducer clicks start to capture the introducer's face along with the face of the applicant.
* **Output**: Face images are captured and processed.

## 5.10 Private Network Systems (Server) - Unique Applicant Check

* **Action**: The server checks if the applicant details are unique and if the introducer exists in the authorised introducer database
* **Output**: Applicant details are unique, or the process is redirected to error handling.

## 5.11 Private Network Systems (Server) – Request Evidence Documents

* **Action**: The system requests the upload of evidence documents if necessary.
* **Output**: Additional evidence documents are uploaded.

## 5.12 Private Network Systems (Server) - Liveness Detection Test

* **Action:** The system prompts for a liveness test to ensure the authenticity of the applicant.
* **Output:** Liveness detection is successful.

## 5.13 Private Network Systems (Server) - 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.

## 5.14 Private Network Systems (Server) - Appointment Slot Check

* **Action**: The system checks appointment slot availability and blocks the appointment.
* **Output**: Appointment is confirmed and blocked.

## 5.15 Notifications and Logging

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

## 5.16 End of Process

* **Action**: If the process is successful, the user is redirected to the appointment confirmation page.
* **Output**: The process ends with a successful appointment confirmation or terminates with an error message.

## 5.17 Security Measures

* **Encryption and Hashing**: All user information is encrypted and hashed using advanced security protocols.
* **Network Security**: The system employs SSL/TLS for secure communication and IDS/IPS to detect and prevent intrusions
* **Firewalls**: Single or dual firewalls protect the network from unauthorised access

# 6. Visualisation

A diagram of a application

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.1.2.C ONLINE APPLICATION APPLICATION INITIATED BY INTRODUCER** | | | | | |
| **Step** | **Description** | **Action** | **Systems Involved** | **Security Measures** | **Standards and References** |
| 1. Application Initiation by Introducer | Introducer starts the application process for the applicant. | Fill forms with applicant's and self (introducer's) details, initiate application. | Applicant Interface | Accurate entry of personal details for both parties. | NIST Digital Identity: Guidelines on data entry; eIDAS: Identity proofing requirements. |
| 2. Document Submission | Submit required identity documents. | Upload proof of identity documents for the introducer. If the applicant has no official documentation, only the introducer's documents are uploaded unless the applicant provides unofficial documentation. | Public Network Systems Client | Check file size and format; mask and encrypt uploaded files. | ISO 27001: Secure handling and encryption of data; FATF: Management of identity documents. |
| 3. Terms Acceptance and Biometric Check | Agree to terms and verify biometric data. | Accept terms and conditions; initiate biometric liveness check for both the introducer and the applicant. | Public Network Systems Client | Secure biometric data transmission and storage; image quality check. | ISO/IEC 30107-3: Biometric presentation attack detection; GDPR: Data protection for biometrics. |
| 4. Application Processing and Encryption | Secure and process application details. | Encrypt and store all application details and images. | Private Network Systems Server, KM, HSM | Use of SSL/TLS for data transmission; data encryption using HSM. | ISO 27001: Data encryption and security management; NIST: Secure storage practices. |
| 5. Verification and Notification | Validate details and notify parties involved. | Check if introducer is authorised and if applicant's details are unique; generate notifications. | Private Network Systems Server, IDA | Verification against database for duplicates; secure notification process. | eIDAS & Estonia ID: Verification protocols; notification standards. |
| 6. Appointment Scheduling | Schedule an appointment for further processing. | Select appointment center and time; confirm via notifications. | Notification Generator | Efficient and secure scheduling system. | SingPass, Emirates ID: Best practices for digital appointment systems. |
| 7. Exception Handling and Error Management | Handle potential errors and issues. | Manage exceptions, reset counters, and terminate the process if necessary with an error message. | Error Handling System | Error logging and detailed user notification of failures. | ISO 27001: Incident and error management; AADHAR: Protocols for handling errors. |
| 8. Completion | Conclude the application process. | Log the process status and end the session upon successful or failed application. | IDA | Secure logging and auditing of the process. | NIST Digital Identity, FATF Digital Identity Guidance: Compliance with secure process completion and auditing. |

# 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].