|  |  |  |
| --- | --- | --- |
| **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: Self Initiated

OB.1.2.A - 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](#_Toc177311587)

[2. Definitions and Abbreviations 3](#_Toc177311588)

[3. Application 3](#_Toc177311589)

[3.1 Ownership and Stakeholders 3](#_Toc177311590)

[3.1.1 Digital Identity Service Providers (DISPs) 3](#_Toc177311591)

[3.1.2. IT and Security Teams 3](#_Toc177311592)

[3.1.3 Compliance and Legal Departments 4](#_Toc177311593)

[3.2 Users and Beneficiaries 4](#_Toc177311594)

[3.2.1 General Public 4](#_Toc177311595)

[3.2.2 Government Agencies 4](#_Toc177311596)

[3.2.3 Private Sector Companies 4](#_Toc177311597)

[3.3 Benefits and Impact 4](#_Toc177311598)

[3.3.1 Enhanced Security 4](#_Toc177311599)

[3.3.2 Regulatory Compliance 4](#_Toc177311600)

[3.3.3 Streamlined Processes 5](#_Toc177311601)

[3.3.4 Interoperability 5](#_Toc177311602)

[3.3.5 Data Privacy and Protection 5](#_Toc177311603)

[4. Prerequisites 5](#_Toc177311604)

[4.1 Assumptions 5](#_Toc177311605)

[4.2 Constraints 6](#_Toc177311606)

[5. Process Flow - Process and Procedures 6](#_Toc177311607)

[5.1 Initiate Online Application 6](#_Toc177311608)

[5.2 Selects Application for Self 6](#_Toc177311609)

[5.3 Fill Application Form 6](#_Toc177311610)

[5.4 Upload Supporting Documents: 6](#_Toc177311611)

[5.5 Click Start to Capture Face for Liveness Check: 6](#_Toc177311612)

[5.6 Download Application with Filled Details 6](#_Toc177311613)

[5.7 Select Appointment Center & Time: 6](#_Toc177311614)

[5.8 System Processing 7](#_Toc177311615)

[5.8.1 Public Network Systems (Client): 7](#_Toc177311616)

[5.8.2 Private Network Systems (Server) 7](#_Toc177311617)

[5.9 Exceptions and Error Handling 8](#_Toc177311618)

[5.10 End of Process 8](#_Toc177311619)

[5.11 Security Measures 8](#_Toc177311620)

[6. Visualisation 9](#_Toc177311621)

[7. Rationalisation 10](#_Toc177311622)

[8. References 11](#_Toc177311623)

# 1. Purpose

This SOP outlines the steps required for a self-initiated online application for a Digital Identity (DID) account. It details the process from initiating the application to receiving confirmation or termination notifications.

# 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**: 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.

### 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.1.4.A OFFLINE BIOMETRIC COLLECTION CONSENT.*

## 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, firewalls, and liveness checks are integral throughout the process.

## 5.1 Initiate Online Application

* **Action:** User initiates the online application process.
* **Output:** The application process begins.

## 5.2 Selects Application for Self

* **Action:**User selects the option to apply for themselves.
* **Output:**Redirects to the application form.

## 5.3 Fill Application Form

* **Action:** User enters personal details (given name, family name, DOB, address, etc.) and clicks confirm.
* **Output:** Application form is submitted for review.

## 5.4 Upload Supporting Documents:

* **Action:** User uploads required documents for verification
* **Output:** Documents are submitted for verification.

## 5.5 Click Start to Capture Face for Liveness Check:

* **Action:** User starts the liveness check by capturing their face
* **Output:** Liveness check is initiated.

## 5.6 Download Application with Filled Details

* **Action:** User downloads the application with all filled details for offline use.
* **Output:** Application downloaded successfully.

## 5.7 Select Appointment Center & Time:

* **Action:** User selects a convenient center and time for an appointment
* **Output:** Appointment is scheduled.

## 5.8 System Processing

### 5.8.1 Public Network Systems (Client):

**Mask & Encrypt Application Details:**

* **Action:** System masks and encrypts user details.
* **Output:** Encrypted details are sent to the server.

**File Upload Verification:**

* **Action:** System verifies the size and format of uploaded files.
* **Output:** Valid files are encrypted and sent to the server.

**Image Quality Check:**

* **Action:** System checks the quality of the captured image.
* **Output:** Accepted images are encrypted and sent to the server.

### 5.8.2 Private Network Systems (Server)

**Verify Applicant Age:**

* **Action:** System checks if the applicant is older than 16 years.
* **Output:** Proceeds if age criteria are met.

**Check for Unique Applicant Details:**

* **Action:** System verifies if the applicant's details are unique.
* **Output:** If unique, proceeds; otherwise, requests document re-upload.

**Request Upload of Evidence Documents:**

* **Action:** If necessary, system requests additional evidence documents.
* **Output:** Applicant uploads additional documents.

**Store Information Securely:**

* **Action:** Stores application details securely with encryption and hashing.
* **Output:** Information is securely stored in the database.

**Liveness Test Verification:**

* **Action:** System verifies the liveness test.
* **Output:** If successful, proceeds to appointment scheduling.

**Generate Notifications:**

* **Action:** Generates notifications for successful or failed processes.
* **Output:** Notifications are sent to the applicant.

**Check Appointment Slot Availability:**

* **Action:** System checks available slots and books the appointment.
* **Output:** Appointment confirmation is sent.

## 5.9 Exceptions and Error Handling

**Exception and Error Handling:**

* **Action:** Handles exceptions and errors, increments retry counter if necessary.
* **Output:** Process retries up to three times before termination.

**Terminate Process with Error Message:**

* **Action:** If errors persist, the process is terminated with an error message.
* **Output:** Applicant is notified of the termination.

## 5.10 End of Process

**Successful Completion:**

* **Action:** Applicant receives a confirmation notification and is redirected to the next steps.
* **Output:** Process ends successfully.

**Failure Notification:**

* **Action:** Applicant is notified of the failure and provided with instructions.
* **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.
* F**irewalls:** Single or dual firewalls protect the network from unauthorised access.

# 6. Visualisation

A diagram of a process

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.A INITIATING AN ONLINE APPLICATION: SELF INITIATED** | | | | | |
| **Step** | **Description** | **Action** | **Systems Involved** | **Security Measures** | **Standards and References** |
| 1. Application Initiation | User starts the application process. | Initiate online application: enter personal details (family name, DOB, address, etc.). | Applicant Interface | Ensure personal details are complete and accurate. | NIST Digital Identity: Guidelines on personal data entry; eIDAS: Identity proofing requirements. |
| 2. Document Submission | Upload necessary supporting documents. | Upload documents needed for application. Check file size and format. | Public Network Systems Client | Mask and encrypt uploaded files. | ISO 27001: Secure data handling and encryption; FATF: Secure management of documents. |
| 3. Accept Terms and Conditions | Agree to proceed under set conditions. | Click to accept terms and then initiate liveness check. | Public Network Systems Client | Secure data transaction protocols. | GDPR, eIDAS: Compliance with data protection and user consent. |
| 4. Liveness Detection | Perform a liveness check to validate identity. | Prompt for a liveness test and validate the image quality. | Private Network Systems Server | Image encryption and quality check against fraud. | ISO/IEC 30107-3: Biometric presentation attack detection; NIST: Biometric data security. |
| 5. Application Review and Processing | Process and verify the application details. | Store and mask application details; manage RID and notification generation. | Private Network Systems Server, KM, HSM | SSL/TLS for data transmission; IDS, IPS, and honeypot for security. | ISO 27001: Information security management; AADHAR: Data privacy and security protocols. |
| 6. Appointment Scheduling | Schedule an appointment for further processing. | Select appointment center and time. Receive confirmation. | Notification Generator | Secure notification delivery on email. | SingPass, Emirates ID: Efficient and secure scheduling systems. |
| 7. Exception and Error Handling | Manage errors and terminate if necessary. | Handle exceptions, reset counters, and terminate process with an error message if issues persist. | Error Handling System | Detailed error logging and user notification of failures. | ISO 27001: Incident response management; FATF Digital Identity Guidance: Error management protocols. |
| 8. Completion | Notify the applicant of the outcome. | Notify the applicant whether the application is successful or not. | Notification Generator, IDA | Logging of the entire process for audit and security compliance. | Estonia ID, eIDAS: Best practices for transparency and notification in digital identity services. |

# 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].