|  |  |  |
| --- | --- | --- |
| **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- Registering a new account

OB.1.1.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](#_Toc177309673)

[2. Definitions and Abbreviations 3](#_Toc177309674)

[3. Application 3](#_Toc177309675)

[3.1 Ownership and Stakeholders 3](#_Toc177309676)

[3.1.1 Digital Identity Service Providers (DISPs) 3](#_Toc177309677)

[3.1.2. IT and Security Teams 3](#_Toc177309678)

[3.1.3 Compliance and Legal Departments 4](#_Toc177309679)

[3.2 Users and Beneficiaries 4](#_Toc177309680)

[3.2.1 General Public 4](#_Toc177309681)

[3.2.2 Government Agencies 4](#_Toc177309682)

[3.2.3 Private Sector Companies 4](#_Toc177309683)

[3.3 Benefits and Impact 4](#_Toc177309684)

[3.3.1 Enhanced Security 4](#_Toc177309685)

[3.3.2 Regulatory Compliance 5](#_Toc177309686)

[3.3.3 Streamlined Processes 5](#_Toc177309687)

[3.3.4 Interoperability 5](#_Toc177309688)

[3.3.5 Data Privacy and Protection 5](#_Toc177309689)

[4. Prerequisites 5](#_Toc177309690)

[4.1 Assumptions 6](#_Toc177309691)

[4.2 Constraints 6](#_Toc177309692)

[5. Process Flow - Process and Procedures 6](#_Toc177309693)

[5.1 Start 6](#_Toc177309694)

[5.2 Applicant Registration 6](#_Toc177309695)

[5.3 Password Creation 6](#_Toc177309696)

[5.4 Acceptance of Terms and Conditions 6](#_Toc177309697)

[5.5 Captcha Verification 7](#_Toc177309698)

[5.6 One-Time Password (OTP) Verification 7](#_Toc177309699)

[5.7 System Processing 7](#_Toc177309700)

[5.7.1 Public Network Systems (Client) 7](#_Toc177309701)

[5.7.2 Private Network Systems (Server) 7](#_Toc177309702)

[5.8 User Account Creation 7](#_Toc177309703)

[5.9 Notifications and Logging 7](#_Toc177309704)

[5.10 Exceptions and Error Handling 8](#_Toc177309705)

[5.11 End of Process 8](#_Toc177309706)

[5.12 Security Measures 8](#_Toc177309707)

[6. Visualisation 9](#_Toc177309708)

[7. Rationalisation 10](#_Toc177309709)

[8. References 11](#_Toc177309710)

# 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

**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:**
  + 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**: 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 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 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.1.1.B Initiating an Online Application*

## 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 registration process from the initial visit to the DID portal to the successful creation of a new account.

## 5.1 Start

* **Action**: The user visits the DID portal.
* **Output**: The registration process begins.

## 5.2 Applicant Registration

* **Action**: The user clicks on the new applicant sign-up link.
* **Action**: The user fills in personal details such as given name, family name, date of birth (DOB), email, and phone number.
* **Output**: The personal details form is submitted.

## 5.3 Password Creation

* **Action**: The user creates a strong password (without using FTP).
* **Output**: The password is securely stored.

## 5.4 Acceptance of Terms and Conditions

* **Action**: The user accepts the terms and conditions for the new account.
* **Output**: The acceptance is recorded.

## 5.5 Captcha Verification

* **Action**: The user performs a CAPTCHA test to prove they are not a robot.
* **Output**: The CAPTCHA test is passed.

## 5.6 One-Time Password (OTP) Verification

* **Action**: The system sends two distinct OTPs to the user's email and phone.
* **Action**: The user enters the OTPs received on their email and phone.
* **Output**: The OTP authentication (2FA) is completed successfully.

## 5.7 System Processing

### 5.7.1 Public Network Systems (Client)

* **Action**: The system checks if the applicant is older than 16 years.
* **Action**: The system masks and encrypts user details using KM, HSM, and CA.
* **Output**: The encrypted details are sent to the server.

### 5.7.2 Private Network Systems (Server)

* **Action**: The server checks if the provided email and phone number have not been used previously.
* **Output**: If they have been used previously, the process redirects to the login page with a reason.

## 5.8 User Account Creation

* **Action**: If the CAPTCHA test is passed and the email and phone number are verified, the server generates OTPs for email and phone.
* **Action**: If the OTPs are authenticated successfully, a new user account is created.
* **Action**: The user's information is stored securely with encryption and hashing using KM and HSM.
* **Output**: The new account is created successfully.

## 5.9 Notifications and Logging

* **Action**: The system generates a notification for successful account creation and sends it to the user's email and phone.
* **Action**: If the account creation 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 account status.

## 5.10 Exceptions and Error Handling

* **Action**: If an error occurs, the system handles exceptions and increments the retry counter.
* **Output**: If the retry count exceeds three, the process is terminated with an error message.

## 5.11 End of Process

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

## 5.12 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 unauthorized 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 REGISTER NEW ACCOUNT** | | | | | |
| **Step** | **Description** | **Action** | **Systems Involved** | **Security Measures** | **Standards and References** |
| 1. Start and Input | Applicant initiates the registration online. | Visit DID portal and input personal details. | Applicant Interface | Age verification (>16 years). | NIST Digital Identity: Age verification guidance; eIDAS: Identity proofing requirements. |
| 2. Account Creation | Create a new account with security protocols. | Agree to T&Cs, create strong password, perform CAPTCHA test. | Public Network Systems Client | CAPTCHA to prevent bots, strong password enforcement. | ISO 27001: Secure system access control; AADHAR & SingPass: Best practices in account creation and management. |
| 3. Two-Factor Authentication | Secure account with OTPs. | Enter OTPs received by email and phone. | Public Network Systems Client | OTP for email and phone to verify identity. | FATF Digital Identity Guidance: Authentication mechanisms; NIST Digital Identity: 2FA requirements. |
| 4. Data Encryption and Protection | Secure transmission and storage of data. | Encrypt user details using HSM managed by KM. | Public & Private Network Systems, HSM, KM, CA | SSL/TLS for secure API calls, use of IDS, IPS, and honeypots. | ISO 27001: Encryption and key management; Estonia ID & Emirates ID: Data protection practices. |
| 5. Account Validation and Finalisation | Verify details and finalise account creation. | Create new user account if all validations are passed. | Private Network Systems Server, IDA | Logging of processes and status, secure account creation. | eIDAS & NIST Digital Identity: Compliance with registration processes; SingPass & Aadhar: Identity verification protocols. |
| 6. Error Handling and Termination | Manage errors and terminate if necessary. | Redirect to login page or display error message upon failure. | Error Handling System | Reset error counter, terminate process with error explanation. | ISO 27001: Incident management; FATF Digital Identity Guidance: Error management and user notification. |
| 7. Notification and Completion | Notify the applicant of the outcome. | Send notification of account creation or failure. | Notification Generator | Secure notification delivery on email and phone. | Estonia ID, Emirates ID, eIDAS: Notification standards for 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].