STANDARD OPERATING PROCEDURE- ACTIVATION OF DIGITAL ID ACCOUNT

OB.4.D

**Version Control**

|  |  |  |
| --- | --- | --- |
| **Version** | **Date** | **Changes Made** |
|  |  |  |
|  |  |  |
|  |  |  |

**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](#_Toc177261542)

[2. Definitions and Abbreviations 3](#_Toc177261543)

[3. Application 3](#_Toc177261544)

[3.1 Ownership and Stakeholders 3](#_Toc177261545)

[3.1.1 Digital Identity Service Providers (DISPs) 3](#_Toc177261546)

[3.1.2 IT and Security Teams 3](#_Toc177261547)

[3.1.3 Compliance and Legal Departments 3](#_Toc177261548)

[3.2 Users and Beneficiaries 4](#_Toc177261549)

[3.2.1 General Public 4](#_Toc177261550)

[3.1.2 Government Agencies 4](#_Toc177261551)

[3.1.3 Private Sector Companies 4](#_Toc177261552)

[4 Prerequisites 4](#_Toc177261553)

[4.1 Assumptions 4](#_Toc177261554)

[4.2 Constraints 4](#_Toc177261555)

[5. Process & Procedures 4](#_Toc177261556)

[5.1 Start and Receive DID Details 4](#_Toc177261557)

[5.2 Enter FTP and Set Up PIN 4](#_Toc177261558)

[5.3 Authenticate Using Multiple Methods 5](#_Toc177261559)

[5.4 Verify, Authenticate, and Notify 5](#_Toc177261560)

[6. Visualisation 6](#_Toc177261561)

# 1. Purpose

This SOP outlines the standardised procedure for the activation of a Digital Identity (DID) account. It ensures secure and accurate activation through proper verification, authentication, and notification mechanisms.

# 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**: Oversee the activation process.
* **Responsibilities**: Ensure secure and compliant activation of accounts.

### 3.1.2 IT and Security Teams

* **Ownership**: Manage technical infrastructure and security protocols.
* **Responsibilities**: Maintain system security, data encryption, and infrastructure.

### 3.1.3 Compliance and Legal Departments

* **Ownership**: Ensure compliance with legal and regulatory standards.
* **Responsibilities**: Oversee compliance checks, documentation, and regulatory adherence.

## 3.2 Users and Beneficiaries

### 3.2.1 General Public

* **Users**: Individuals activating their DID accounts.
* **Usage**: Provide necessary details and authentication for account activation.

### 3.1.2 Government Agencies

* **Users**: Agencies requiring verified identities for services.
* **Usage**: Utilise verified identity information for secure service delivery.

### 3.1.3 Private Sector Companies

* **Users**: Businesses requiring high-security identity verification.
* **Usage**: Use secured identities for compliance and verification purposes.

# 4 Prerequisites

## 4.1 Assumptions

* Subscribers have received their DID and FTP credentials.
* Administrators are trained to handle the activation process securely.
* Technological infrastructure meets current security standards.

## 4.2 Constraints

* The activation process may be affected by system downtimes or regulatory changes.
* Secure devices and internet access are required for administrators.

# 5. Process & Procedures

## **5.1 Start and Receive DID Details**

* **Action**:
  + The subscriber starts the process either online or by visiting the DID portal/enrollment center.
  + The subscriber receives DID and a letter with account details.
* **Output**: Subscriber is ready to proceed with account activation.

## **5.2 Enter FTP and Set Up PIN**

* **Action**:
  + The subscriber enters the FTP (temporary) received.
  + The subscriber sets up a PIN or memorable secret.
* **Output**: FTP is verified, and PIN setup is completed.

## **5.3 Authenticate Using Multiple Methods**

* **Action**:
  + The subscriber authenticates using various methods:
    - Mobile phone number or memorable secret.
    - Fingerprint, facial biometric.
    - OTP.
* **Output**: Successful multi-factor authentication.

## **5.4 Verify, Authenticate, and Notify**

* **Administrator/Verifier Actions**:
  + Verify UIN and demographic data match.
  + Request authentication.
* **Public Network Systems (Client)**:
  + Mask and encrypt UIN, demographic details, FTP details, and authentication details.
* **Private Network Systems (Server)**:
  + Verify data match and authentication.
  + Activate DID account and enable authenticators for online authentication.
  + Store authenticator status in the UIN account.
  + Generate notifications for successful activation.
  + Handle errors and retry if necessary.
  + Log the process and status in the IDA.
* **Output**: Account is activated, and the user is notified of the activation status.

# 6. Visualisation

A screenshot of a computer screen

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.