STANDARD OPERATING PROCEDURE ACTIVATION OF DIGITAL ID ACCOUNT

OB.4.D - 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**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Version | Date | Changes Made | Updated By | Approved By | Remarks |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**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.
* **Updated By**: The name of the individual who made the changes.
* **Approved By**: The name of the person who reviewed and approved the changes.
* **Remarks**: Any additional notes about the update, such as the reason for changes or the impact on the procedures.

Table of Contents

[1. Purpose 3](#_Toc177312368)

[2. Definitions and Abbreviations 3](#_Toc177312369)

[3. Application 3](#_Toc177312370)

[3.1 Ownership and Stakeholders 3](#_Toc177312371)

[3.1.1 Digital Identity Service Providers (DISPs) 3](#_Toc177312372)

[3.1.2 IT and Security Teams 3](#_Toc177312373)

[3.1.3 Compliance and Legal Departments 3](#_Toc177312374)

[3.2 Users and Beneficiaries 4](#_Toc177312375)

[3.2.1 General Public 4](#_Toc177312376)

[3.1.2 Government Agencies 4](#_Toc177312377)

[3.1.3 Private Sector Companies 4](#_Toc177312378)

[4 Prerequisites 4](#_Toc177312379)

[4.1 Assumptions 4](#_Toc177312380)

[4.2 Constraints 4](#_Toc177312381)

[5. Process & Procedures 4](#_Toc177312382)

[5.1 Start and Receive DID Details 4](#_Toc177312383)

[5.2 Enter FTP and Set Up PIN 4](#_Toc177312384)

[5.3 Authenticate Using Multiple Methods 5](#_Toc177312385)

[5.4 Verify, Authenticate, and Notify 5](#_Toc177312386)

[6. Visualisation 6](#_Toc177312387)

[7. Rationalisation 7](#_Toc177312388)

[8. References 7](#_Toc177312389)

# 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.

# 7. Rationalisation

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **OB.4.D ACTIVATION OF DIGITAL ID ACCOUNT** | | | | | |
| **Step** | **Description** | **Action** | **Systems Involved** | **Security Measures** | **Standards and References** |
| 1. Start Process | Initiate delivery process online. | Administrator starts the credential delivery process upon successful application approval. | Public Network Systems Client | Secure data transmission. | ISO/IEC 27001 for data security |
| 2. Print and Encrypt Credentials | Print physical ID and password letters. | Print credentials and use encryption for transmitting digital ID attributes and FTP credentials. | Public/Private Network Systems | Encryption of sensitive data. | ISO/IEC 27001, eIDAS for secure document management |
| 3. Notification and Tracking | Send credentials via post with tracking. | Generate a tracking number, notify the subscriber, and encrypt the tracking information. | Notification Generator, Private Network Systems Server | Secure tracking and notification delivery. | ISO/IEC 27001 for secure communications, NIST Digital Identity Guidelines |
| 4. Delivery Confirmation | Confirm receipt and verify identity. | Subscriber receives the credentials, verifies through provided methods, and confirms receipt. | Public/Private Network Systems | Two-factor authentication and receipt confirmation. | GDPR for data protection, ISO/IEC 27001 for authentication procedures |
| 5. Log and Update Status | Update and log the delivery status. | Log the process and update the status in the digital ID account. | IDA (Identity Authentication Database), Notification Generator | Logging for audit and compliance, secure data storage. | ISO/IEC 27001 for maintaining secure audit logs; FATF Digital Identity Guidance for reliable electronic records |

# 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].