|  |  |  |
| --- | --- | --- |
| **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 - CREATION OF PERSONAL IDENTIFICATION NUMBER

AU.1.E - 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](#_Toc176257011)

[2. Definitions and Abbreviations 3](#_Toc176257012)

[3 Application 3](#_Toc176257013)

[3.1 Ownership and Stakeholders 3](#_Toc176257014)

[3.1.1 Digital Identity Service Providers (DISPs) 3](#_Toc176257015)

[3.1.2 IT and Security Teams 3](#_Toc176257016)

[3.1.3 Compliance and Legal Departments 3](#_Toc176257017)

[3.2 Users and Beneficiaries 4](#_Toc176257018)

[3.2.1 General Public 4](#_Toc176257019)

[3.2.2 Government Agencies 4](#_Toc176257020)

[3.2.3 Private Sector Companies 4](#_Toc176257021)

[4. Prerequisites 4](#_Toc176257022)

[4.1 Assumptions 4](#_Toc176257023)

[4.2 Constraints 4](#_Toc176257024)

[5. Process Flow - Process and Procedures 4](#_Toc176257025)

[5.1. Start and Login: 4](#_Toc176257026)

[5.2. Password Authentication: 4](#_Toc176257027)

[5.3. Two-Factor Authentication (2FA): 5](#_Toc176257028)

[5.4. Navigation to PIN Configuration: 5](#_Toc176257029)

[5.5. Authentication for PIN Setup: 5](#_Toc176257030)

[5.6. Creation of New PIN: 5](#_Toc176257031)

[5.7. Validation and Encryption: 6](#_Toc176257032)

[5.8. Notification Generation: 6](#_Toc176257033)

[5.9. Logging and Status Update: 6](#_Toc176257034)

[5.10. Termination and Retry Handling: 6](#_Toc176257035)

[6. Resources 7](#_Toc176257036)

[6.1 Visualisation 7](#_Toc176257037)

[6.2 Rationalisation 8](#_Toc176257038)

[7. References 9](#_Toc176257039)

# 1. Purpose

This SOP outlines the standardised procedure for creating a Personal Identification Number (PIN) within the Digital Identity (DID) system. It ensures secure and accurate creation through proper verification, encryption, and error handling.

# 2. Definitions and Abbreviations

**DID**: Digital Identity

**KM**: Key Manager

**KR**: Key Revocation

**HSM**: Hardware Security Module

**IDA**: ID Authentication Database

**AC**: Access Control

**FTP**: First Time Password

**OTP**: One-Time Password

**2FA**: Two-Factor Authentication

**HTTPS**: Hyper Text Transfer Protocol Secure

**SSL/TLS**: Secure Sockets Layer / Transport Layer Security

# 3 Application

## 3.1 Ownership and Stakeholders

### 3.1.1 Digital Identity Service Providers (DISPs)

* **Ownership**: Oversee the creation process of PINs.
* **Responsibilities**: Ensure secure and compliant creation of PINs.

### 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 creating PINs for their DID accounts.
* **Usage**: Provide credentials and create a PIN to enhance account security.

### 3.2.2 Government Agencies

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

### 3.2.3 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 creation process securely.
* Technological infrastructure meets current security standards.

## 4.2 Constraints

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

# 5. Process Flow - Process and Procedures

## **5.1. Start and Login:**

* **Subscriber Action:**
  + The subscriber begins by visiting the DID portal and clicking on the user login button.
* **Output:** The login process is initiated.

## **5.2. Password Authentication:**

* **System Action:**
  + The system prompts the subscriber to log in using their username and password.
* **Subscriber Action:**
  + The subscriber enters their username and password to log in.
* **System Action (Server):**
  + The server validates the entered credentials against stored records.
* **Output:** Password authentication is validated. If successful, proceed to the next step.

## **5.3. Two-Factor Authentication (2FA):**

* **System Action:**
  + Upon successful password authentication, the system prompts for 2FA using OTP (One-Time Password) or Memorable Secret.
* **Subscriber Action:**
  + The subscriber enters the OTP or Memorable Secret as part of the 2FA process.
* **System Action (Server):**
  + The server verifies the 2FA input.
* **Output:** 2FA authentication is validated. If successful, the subscriber receives a successful login status.

## **5.4. Navigation to PIN Configuration:**

* **Subscriber Action:**
  + After successful 2FA, the subscriber navigates to the settings section, selects "Security," and clicks on "PIN."
* **Output:** The subscriber is directed to the PIN configuration page.

## **5.5. Authentication for PIN Setup:**

* **System Action:**
  + The system requests the subscriber to authenticate using their password again to confirm the identity before PIN setup.
* **Subscriber Action:**
  + The subscriber re-enters their password.
* **System Action (Server):**
  + The server validates the password.
* **Output:** Password re-authentication is successful, allowing PIN creation to proceed.

## **5.6. Creation of New PIN:**

* **Subscriber Action:**
  + The subscriber is prompted to enter a new 6-digit PIN twice for confirmation, following specific criteria:
    - Must be exactly 6 digits in length.
    - No consecutive numbers or repetitive digits.
* **System Action (Public Network Systems - Client):**
  + The system checks if both entered PINs match and meet the criteria.
* **Output:** New PIN is entered and validated against the specified criteria.

## **5.7. Validation and Encryption:**

* **System Action (Public Network Systems - Client):**
  + The system validates the PIN. If it meets the criteria and both entries match, it proceeds to encryption.
* **System Action (Server):**
  + The encrypted PIN is securely stored in the subscriber's UIN (Unique Identification Number) account with encryption and hashing.
* **Output:** PIN is validated, encrypted, and securely stored.

## **5.8. Notification Generation:**

* **System Action:**
  + If the PIN creation is successful, the system generates a success notification.
  + If the PIN fails to meet criteria after three attempts, a failure notification is generated, and the process may be terminated with account lock.
* **Output:** Notifications are sent to the subscriber's registered email or phone indicating success or failure.

## **5.9. Logging and Status Update:**

* **System Action (Server):**
  + The system logs the process details, including the outcome of PIN creation.
  + If the process fails after three attempts, the system locks the UIN account for 24 hours to prevent unauthorised access.
* **Output:** Process completion is logged, and status is updated in the system.

## **5.10. Termination and Retry Handling:**

* **System Action:**
  + If the PIN creation fails after three retries, the process is terminated, and the subscriber's account is temporarily locked for 24 hours.
* **Output:** The account is locked for 24 hours, and the subscriber is notified of the lock status.

# 6. Visualisation

A diagram of a process

Description automatically generated

Please refer to the [GitHub](https://github.com/carstenmaple/Standard-Operating-Procedures-for-Digital-Identity-Systems/blob/main/Standard%20Operating%20Procedures/Phase%20A%20-%20Onboarding/1.%20Collection%20and%20Resolution/Collection%20and%20Resolution.pdf) repository for further information.

# 7. Rationalisation

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **AU.1.E CREATION OF PERSONAL IDENTIFICATION NUMBER** | | | | | |
| **Step** | **Description** | **Action** | **Systems Involved** | **Security Measures** | **Standards and References** |
| 1 | Start Process | User logs in to start PIN creation | User Device, Public Network | Secure Login | ISO 27001 Information Security Management, eIDAS Trust Services |
| 2 | Authenticate User | User provides password and undergoes 2FA | Authentication Server | Two-Factor Authentication | ISO 27001 Access Control, NIST SP 800-63 Digital Identity Guidelines |
| 3 | Navigate to Security Settings | User navigates to configure PIN | User Device, Web Server | Secure Session, HTTPS | ISO 27001 Access Control, FATF Digital Identity Guidelines |
| 4 | Enter New PIN | User inputs new 6-digit PIN | User Device, Authentication Server | Input Validation, Secure Data Entry | ISO 27001 Data Protection, Aadhaar Guidelines on Secure Authentication |
| 5 | Confirm New PIN | User re-enters PIN for verification | Authentication Server | Data Matching, Secure Data Processing | ISO 27001 Data Integrity, NIST SP 800-63 User Authentication |
| 6 | PIN Creation Success | System confirms PIN setup success | Notification System | Secure Notification Delivery | ISO 27001 Communications Security, Estonia ID Notification System |
| 7 | Store PIN Securely | Encrypted PIN storage in database | Database Server | Encryption, Hashing | ISO 27001 Cryptography, Emirates ID Data Storage Standards |
| 8 | Handle Errors and Exceptions | Manage errors and exceptions during setup | Authentication Server | Error Handling, Logging | ISO 27001 Event Logging and Monitoring, FATF Digital Identity Error Handling |
| 9 | Terminate or Reset Process Based on Attempts | Lock account or reset attempt counter | Authentication Server | Account Lockout, Counter Reset | ISO 27001 Access Control Policies, Sing Pass Account Management |
| 10 | End Process | Log process status and conclude | Authentication Server | Process Logging | NIST SP 800-63 Authenticator Management, Estonia ID Secure Logging |

# 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].