|  |  |  |
| --- | --- | --- |
| **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 - PERSONAL IDENTIFICATION NUMBER BASED AUTHENTICATION

AU.1.F - 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](#_Toc177313856)

[2. Definitions and Abbreviations 3](#_Toc177313857)

[3. Application 3](#_Toc177313858)

[3.1 Ownership and Stakeholders 3](#_Toc177313859)

[3.1.1 Digital Identity Service Providers (DISPs) 3](#_Toc177313860)

[3.1.2 IT and Security Teams 3](#_Toc177313861)

[3.1.3 Compliance and Legal Departments 3](#_Toc177313862)

[3.2 Users and Beneficiaries 4](#_Toc177313863)

[3.2.1 General Public 4](#_Toc177313864)

[3.2.2 Government Agencies 4](#_Toc177313865)

[3.2.3 Private Sector Companies 4](#_Toc177313866)

[4. Prerequisites 4](#_Toc177313867)

[4.1 Assumptions 4](#_Toc177313868)

[4.2 Constraints 4](#_Toc177313869)

[5. Process Flow - Process and Procedures 4](#_Toc177313870)

[5.1. Initiation of Authentication: 4](#_Toc177313871)

[5.2. Login and Password Authentication: 5](#_Toc177313872)

[5.3. Two-Factor Authentication (2FA): 5](#_Toc177313873)

[5.4. Entering the 6-Digit PIN: 5](#_Toc177313874)

[5.5. PIN Verification: 5](#_Toc177313875)

[5.6. Handling Authentication Outcomes: 5](#_Toc177313876)

[5.7. Notification and Logging: 6](#_Toc177313877)

[5.8. Termination of Process: 6](#_Toc177313878)

[5.9. Logging and Status Reporting: 6](#_Toc177313879)

[6. Visualisation 7](#_Toc177313880)

[7. Rationalisation 8](#_Toc177313881)

[8. References 9](#_Toc177313882)

# 1. Purpose

This SOP outlines the standardised procedure for Personal Identification Number (PIN) based authentication within the Digital Identity (DID) system. It ensures secure and accurate authentication through proper credential management, verification, and error handling.

# 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

**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 authentication process.
* **Responsibilities**: Ensure secure and compliant PIN-based authentication.

### 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 using PIN-based authentication.
* **Usage**: Provide credentials and PIN to access digital identity services.

### 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 authentication process securely.
* Technological infrastructure meets current security standards.

## 4.2 Constraints

* The authentication 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. Initiation of Authentication:**

* **Subscriber/Claimant Action:**
  + The subscriber/claimant initiates the authentication by clicking on a secure link sent via QR code, email, or SMS to access the DID authenticator.
* **Verifier Action:**
  + The verifier starts the authentication process by requesting authentication via a secure link.
* **Output:** Authentication process is initiated.

## **5.2. Login and Password Authentication:**

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

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

* **System Action:**
  + After successful password authentication, the system prompts for 2FA using OTP (One-Time Password) or PIN.
* **Subscriber/Claimant Action:**
  + The subscriber enters the OTP or PIN received on their registered device.
* **System Action (Server):**
  + The server verifies the 2FA input.
* **Output:** 2FA authentication is validated. If successful, the subscriber is prompted to enter the PIN.

## **5.4. Entering the 6-Digit PIN:**

* **System Action:**
  + The system prompts the subscriber/claimant to enter their 6-digit PIN for authentication.
* **Subscriber/Claimant Action:**
  + The subscriber enters the 6-digit PIN.
* **System Action (Public Network Systems - Client):**
  + The entered PIN is masked and encrypted for secure transmission.
* **Output:** 6-digit PIN is entered and encrypted for verification.

## **5.5. PIN Verification:**

* **System Action (Server):**
  + The server decrypts the entered PIN and checks it against the stored PIN in the subscriber’s UIN (Unique Identification Number) account.
  + If the PIN matches the stored PIN, authentication is considered successful. If not, the system increments the retry counter.
* **Output:** PIN is verified. If it matches, authentication is successful.

## **5.6. Handling Authentication Outcomes:**

* **System Action (Server):**
  + If the PIN matches, the system generates a notification of authentication success.
  + If the PIN does not match:
    - The system increments the retry counter and generates a notification of authentication failure.
    - If the retry count reaches three attempts, the system locks the UIN account for 24 hours to prevent unauthorised access.
    - The system logs the reason for termination and the status.
* **Output:** Notification of authentication success or failure is generated and sent to the subscriber/claimant.

## **5.7. Notification and Logging:**

* **System Action (Public Network Systems - Client):**
  + The system sends a notification to the subscriber/claimant indicating the result of the authentication (success or failure).
  + The system logs the authentication attempt, including the outcome (success/failure) and any errors encountered.
* **Output:** Notifications are sent, and authentication attempts are logged for record-keeping.

## **5.8. Termination of Process:**

* **System Action (Server):**
  + If authentication fails after three attempts, the system terminates the process and locks the subscriber's UIN account for 24 hours.
  + If authentication is successful, the process is completed, and the user is granted access.
* **Output:** Process is terminated due to successful authentication or after multiple failed attempts.

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

* **System Action (Server):**
  + The system logs the entire authentication process, including timestamps, outcomes, and errors encountered.
  + The status is reported for audit and compliance purposes.
* **Output:** Detailed logs are maintained, and status reports are generated for security and compliance monitoring.

# 6. Visualisation

A diagram of a personal identification

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

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **AU.1.F** **PERSONAL IDENTIFICATION NUMBER BASED AUTHENTICATION** | | | | | |
| **Step** | **Description** | **Action** | **Systems Involved** | **Security Measures** | **Standards and References** |
| 1 | Start Authentication Request | Verifier initiates the authentication process | Verifier Device, Public Network | Secure Communication Link | ISO 27001 Information Security Management, eIDAS Trust Services |
| 2 | User Login | User clicks secure link and logs in | User Device, Authentication Server | HTTPS, SSL/TLS, Secure Authentication | ISO 27001 Access Control, NIST SP 800-63 Digital Identity Guidelines |
| 3 | Two-Factor Authentication | User completes 2FA using OTP and PIN | User Device, 2FA System | Two-Factor Authentication | ISO 27001 Authentication Controls, Sing Pass 2FA Mechanisms |
| 4 | Enter 6-Digit PIN | User inputs their PIN | User Device, Authentication Server | Secure Data Entry, Input Validation | ISO 27001 Data Protection, Aadhar Guidelines on Secure Authentication |
| 5 | Mask and Encrypt PIN for Authentication | Server processes and encrypts the PIN | Private Network Servers | Data Encryption, Masking | ISO 27001 Cryptography, Emirates ID Data Security Standards |
| 6 | Receive Authentication Status Notifications | Notifications sent for authentication success or failure | Notification System | Secure Notification Delivery | ISO 27001 Communications Security, Estonia ID Notification System |
| 7 | Handle Authentication Errors | Error handling and exception management | Authentication Server | Error Logging, Exception Management | ISO 27001 Event Logging and Monitoring, FATF Digital Identity Error Handling |
| 8 | Retry or Terminate Process Based on Attempts | Manage retry attempts or lock account | Authentication Server | Account Lockout, Retry Count Management | ISO 27001 Access Control Policies, NIST SP 800-63 Authenticator Management |
| 9 | 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].