|  |  |  |
| --- | --- | --- |
| **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 Strong Password AU.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](#_Toc177314121)

[2. Definitions and Abbreviations 3](#_Toc177314122)

[3. Application 3](#_Toc177314123)

[3.1 Ownership and Stakeholders 3](#_Toc177314124)

[3.1.1 Digital Identity Service Providers (DISPs) 3](#_Toc177314125)

[3.1.2 IT and Security Teams 3](#_Toc177314126)

[3.1.3 Compliance and Legal Departments 3](#_Toc177314127)

[3.2 Users and Beneficiaries 4](#_Toc177314128)

[3.2.1 General Public 4](#_Toc177314129)

[3.2.2 Government Agencies 4](#_Toc177314130)

[3.2.3 Private Sector Companies 4](#_Toc177314131)

[4. Prerequisites 4](#_Toc177314132)

[4.1 Assumptions 4](#_Toc177314133)

[4.2 Constraints 4](#_Toc177314134)

[5. Process Flow - Process and Procedures 4](#_Toc177314135)

[5.1 Start 4](#_Toc177314136)

[5.2 Subscriber Authentication 4](#_Toc177314137)

[5.3 Password Entry 4](#_Toc177314138)

[5.4 System Processing 5](#_Toc177314139)

[5.4.1 Public Network Systems (Client) 5](#_Toc177314140)

[5.4.2 Private Network Systems (Server) 5](#_Toc177314141)

[5.5 Password Creation 5](#_Toc177314142)

[5.6 Notifications and Logging 5](#_Toc177314143)

[5.7 Exceptions and Error Handling 5](#_Toc177314144)

[5.8 End of Process 5](#_Toc177314145)

[5.9 Security Measures 5](#_Toc177314146)

[6. Visualisation 7](#_Toc177314147)

[7. Rationalisation 8](#_Toc177314148)

[8. References 9](#_Toc177314149)

# 1. Purpose

This SOP outlines the process for creating a strong password on the Digital Identity (DID) portal. It includes all procedures from the initial login to the final confirmation of password change, ensuring security and compliance with defined password criteria.

# 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**: HyperText 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 authentication process.
* **Responsibilities:** Ensure secure and compliant password-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 password-based authentication.
* **Usage**: Provide credentials to access digital identity services.

### 3.2.2 Government Agencies

* **Users**: Agencies requiring verified identities for services.
* **Usage**: Utilize 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**

* + The subscriber must have a valid DID account and login credentials.
  + The subscriber should have access to the registered email address and phone number for OTP verification.
  + 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 Start

* **Action:** The user visits the DID portal login page.
* **Output:** The password creation process is initiated.

## 5.2 Subscriber Authentication

* **Action**: The user enters their User Identification Number (UIN) and receives an FTP (temporary password).
* **Action**: The user authenticates using OTP (B.2.4.1.B).
* **Output**: The user is authenticated successfully.

## 5.3 Password Entry

* **Action**: The user enters the desired password following specified criteria.
* **Action**: The user re-enters the same password for confirmation.
* **Output**: Both entered passwords are matched.

## 5.4 System Processing

### 5.4.1 Public Network Systems (Client)

* **Action**: The system checks if both entered passwords match.
* **Action**: The system masks and encrypts the password for creation using KM, HSM, and CA.
* **Output**: The encrypted password is securely sent to the server.

### 5.4.2 Private Network Systems (Server)

* **Action**: The server verifies if the entered password matches the criteria.
* **Output**: If the criteria are met, the password is stored in the user's account with encryption and hashing.

## 5.5 Password Creation

* **Action**: The user creates a new password without using FTP, updating the process.
* **Output**: The password is successfully created and stored.

## 5.6 Notifications and Logging

* **Action**: The system generates a notification for successful password change and sends it to the user's email and phone with a timestamp.
* **Action**: If the password change 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 password change status.

## 5.7 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, and the user's account is locked for 24 hours.

## 5.8 End of Process

* **Action**: If the password creation is successful, the process concludes, and the user is notified.
* **Output**: The process ends with a successful password creation or terminates with an error message and account lock.

## 5.9 Security Measures

* **Encryption and Hashing**: All passwords are 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 unauthorised access.

# 6. Visualisation

A diagram of a password

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.A CREATION OF STRONG PASSWORD** | | | | | |
| **Step** | **Description** | **Action** | **Systems Involved** | **Security Measures** | **Standards and References** |
| 1. Start Process | Subscriber starts password creation online. | Enter UID and received temporary password via login page. | Public Network Systems Client | Secure login and data transmission. | ISO/IEC 27001 for data security; eIDAS for electronic transactions |
| 2. Authenticate | Verify user's identity using OTP. | Authenticate user by sending and validating OTP. | Public/Private Network Systems | Two-factor authentication to enhance security. | ISO/IEC 27001, NIST Digital Identity Guidelines for authentication standards |
| 3. Enter New Password | User enters a new password based on specified criteria. | Ensure the password meets security criteria before acceptance. | Public Network Systems Client | Enforcement of strong password policies. | NIST SP 800-63B for password guidelines |
| 4. Encrypt and Store Password | Encrypt and securely store the new password. | Mask and encrypt the password for creation; store securely in the DID account. | Private Network Systems Server, KM, HSM | Use of encryption and secure storage practices. | ISO/IEC 27001 for encryption and data storage; GDPR for data protection |
| 5. Notify User | Send notification of password change status. | Notify user via email/phone about the password change success or failure. | Notification Generator | Secure notification delivery systems. | ISO/IEC 27001 for secure communication protocols |
| 6. Error Handling | Manage errors and retries in password creation. | Provide retries for password entry; lock account temporarily if excessive failures. | Private Network Systems Server | Robust error handling and account lockout mechanisms. | ISO/IEC 27001 for access control and error management |

# 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].