|  |  |  |
| --- | --- | --- |
| **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 MEMORABLE SECRET

AU.1.C - 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](#_Toc177313284)

[2. Definitions and Abbreviations 3](#_Toc177313285)

[3. Application 3](#_Toc177313286)

[3.1 Ownership and Stakeholders 3](#_Toc177313287)

[3.1.1 Digital Identity Service Providers (DISPs) 3](#_Toc177313288)

[3.1.2 IT and Security Teams 3](#_Toc177313289)

[3.1.3 Compliance and Legal Departments 3](#_Toc177313290)

[3.2 Users and Beneficiaries 4](#_Toc177313291)

[3.2.1 General Public 4](#_Toc177313292)

[3.2.2 Government Agencies 4](#_Toc177313293)

[3.2.3 Private Sector Companies 4](#_Toc177313294)

[4. Prerequisites 4](#_Toc177313295)

[4.1 Assumptions 4](#_Toc177313296)

[4.2 Constraints 4](#_Toc177313297)

[5. Process Flow - Process and Procedures 4](#_Toc177313298)

[5.1 Start and Login: 4](#_Toc177313299)

[5.2 Password Authentication: 4](#_Toc177313300)

[5.3 Two-Factor Authentication (2FA): 5](#_Toc177313301)

[5.4 Navigation to Memorable Secret Configuration: 5](#_Toc177313302)

[5.5 Creation of Memorable Secret: 5](#_Toc177313303)

[5.6 Validation and Encryption: 5](#_Toc177313304)

[5.7 Notification Generation: 6](#_Toc177313305)

[5.8 Logging and Status Update: 6](#_Toc177313306)

[5.9 Termination and Retry Handling: 6](#_Toc177313307)

[6. Visualisation 7](#_Toc177313308)

[7. Rationalisation 8](#_Toc177313309)

[8. References 9](#_Toc177313310)

# 1. Purpose

This SOP outlines the standardised procedure for creating a memorable secret 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

**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 creation process of memorable secrets.
* **Responsibilities**: Ensure secure and compliant creation of memorable secrets.

### 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 memorable secrets for their DID accounts.
* **Usage**: Provide credentials and memorable secrets 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:**

* **Claimant/Subscriber Action:**
  + The claimant or subscriber starts the process by visiting the DID portal and clicking on the user login button.
* **Output:** The user login process is initiated.

## **5.2 Password Authentication:**

* **System Action:**
  + The system requests the claimant to log in using their username and password.
* **Claimant/Subscriber Action:**
  + The claimant enters their username and password to log in.
* **System Action (Server):**
  + The server validates the entered password against the records.
* **Output:** Password authentication is performed. If successful, the process moves to the next step.

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

* **System Action:**
  + If password authentication is successful, the system prompts for 2FA using OTP (One-Time Password) or PIN.
* **Claimant/Subscriber Action:**
  + The claimant enters the OTP/PIN received via their registered email or phone.
* **System Action (Server):**
  + The server verifies the 2FA input.
* **Output:** 2FA authentication is validated. If successful, the user receives a successful login notification.

## **5.4 Navigation to Memorable Secret Configuration:**

* **Claimant/Subscriber Action:**
  + After successful 2FA, the claimant navigates to the settings section and selects the "Security" tab, followed by clicking on "Memorable Secret."
* **Output:** The claimant is directed to the memorable secret configuration page.

## **5.5 Creation of Memorable Secret:**

* **Claimant/Subscriber Action:**
  + The claimant enters a new memorable secret following specified criteria:
    - At least 6 characters in length.
    - At most 25 characters in length.
    - Accepts ASCII characters, spaces, and Unicode characters.
    - No use of more than three consecutive characters, no consecutive spaces.
    - Should not be the same as the User ID or password, and not the same as the last three memorable secrets.
* **System Action (Public Network Systems - Client):**
  + The system checks if the input matches the criteria.
* **Output:** New memorable secret is entered and validated against the criteria.

## **5.6 Validation and Encryption:**

* **System Action (Public Network Systems - Client):**
  + The system validates the memorable secret. If it meets the criteria, it is masked and encrypted for secure storage.
* **System Action (Server):**
  + The encrypted memorable secret is stored in the claimant's Unique Identification Number (UIN) account with encryption and hashing.
* **Output:** Memorable secret is validated, encrypted, and securely stored.

## **5.7 Notification Generation:**

* **System Action:**
  + If the memorable secret creation is successful, the system generates a success notification.
  + If the memorable secret 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 claimant's registered email or phone indicating success or failure.

## **5.8 Logging and Status Update:**

* **System Action (Server):**
  + The system logs the process details, including the outcome of memorable secret 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.

## **5.9 Termination and Retry Handling:**

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

# 6. Visualisation

A diagram of a process

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.C** **CREATION OF MEMORABLE SECRET** | | | | | |
| **Step** | **Description** | **Action** | **Systems Involved** | **Security Measures** | **Standards and References** |
| 1 | Start User Login | User initiates session | Client Device, Public Network | HTTPS, SSL/TLS | ISO 27001 Information Security Management, eIDAS Trust Services |
| 2 | Navigate to Settings | User accesses security settings | Client Device, Web Server | Authentication, Secure Session | ISO 27001 Access Control, NIST SP 800-63 Digital Identity Guidelines |
| 3 | Configure Memorable Secret | User enters new memorable secret | Web Server | Input Validation, Encryption | ISO 27001 Data Protection, FATF Digital Identity Identity Verification |
| 4 | Memorable Secret Creation | System processes new memorable secret | Private Network Servers | Encryption, API Security | ISO 27001 Cryptography, Aadhaar Biometric Data Security |
| 5 | Authenticate Using Password | User password verification | Authentication Server | Password Policies, Rate Limiting | ISO 27001 User Access Management, eIDAS Electronic Identification |
| 6 | 2FA Using One-Time PIN | Additional authentication step with OTP | 2FA System | Two-Factor Authentication | ISO 27001 Authentication Controls, Sing Pass 2FA Mechanisms |
| 7 | Receive Notification | User receives success/failure notification | User Device, Mail Server | Secure Notification Delivery | ISO 27001 Communications Security, Estonia ID Secure Channel Communication |
| 8 | Reset Counter | System resets login attempt counter | Server | Error Handling | ISO 27001 Event Logging and Monitoring, NIST SP 800-63 Authenticator Management |
| 9 | Terminate Process | Lock out user account for 24 hours on failure | Authentication Server | Account Lockout | ISO 27001 Access Control Policies, Emirates ID User Account 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].