|  |  |  |
| --- | --- | --- |
| **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 - MEMORABLE SECRET BASED AUTHENTICATION

AU.1.D - 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](#_Toc177314011)

[2. Definitions and Abbreviations 3](#_Toc177314012)

[3. Application 3](#_Toc177314013)

[3.1 Ownership and Stakeholders 3](#_Toc177314014)

[3.1.1 Digital Identity Service Providers (DISPs) 3](#_Toc177314015)

[3.1.2 IT and Security Teams 3](#_Toc177314016)

[3.1.3 Compliance and Legal Departments 3](#_Toc177314017)

[3.2 Users and Beneficiaries 4](#_Toc177314018)

[3.2.1 General Public 4](#_Toc177314019)

[3.2.2 Government Agencies 4](#_Toc177314020)

[3.2.3 Private Sector Companies 4](#_Toc177314021)

[4. Prerequisites 4](#_Toc177314022)

[4.1 Assumptions 4](#_Toc177314023)

[4.2 Constraints 4](#_Toc177314024)

[5. Process Flow - Process and Procedures 4](#_Toc177314025)

[5.1 Initiation of Authentication: 4](#_Toc177314026)

[5.2 Login and Password Authentication: 4](#_Toc177314027)

[5.3 Two-Factor Authentication (2FA): 5](#_Toc177314028)

[5.4 Entering Memorable Secret: 5](#_Toc177314029)

[5.5 Verification of Memorable Secret: 5](#_Toc177314030)

[5.6 Handling Authentication Outcomes: 6](#_Toc177314031)

[5.7 Notification and Logging: 6](#_Toc177314032)

[5.8 Termination of Process: 6](#_Toc177314033)

[5.9 Logging and Status Reporting: 6](#_Toc177314034)

[6. Visualisation 7](#_Toc177314035)

[7. Rationalisation 8](#_Toc177314036)

[8. References 9](#_Toc177314037)

# 1. Purpose

This SOP outlines the standardised procedure for memorable secret-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 memorable secret-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 memorable secret-based authentication.
* **Usage**: Provide credentials and memorable secret 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 clicks on a secure link sent via QR, email, or SMS to initiate authentication using the DID authenticator.
* **Verifier Action:**
  + The verifier requests authentication by sending a secure link to the subscriber/claimant.
* **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 to log in.
* **System Action (Server):**
  + The server validates the entered credentials against the 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 PIN.
* **Subscriber/Claimant Action:**
  + The claimant enters the OTP or PIN received on their registered email or phone.
* **System Action (Server):**
  + The server verifies the 2FA input.
* **Output:** 2FA authentication is validated. If successful, the process moves forward.

## **5.4 Entering Memorable Secret:**

* **System Action:**
  + After successful 2FA, the system requests the subscriber/claimant to enter specific characters from their memorable secret.
* **Subscriber/Claimant Action:**
  + The subscriber enters the requested characters from their memorable secret.
* **System Action (Public Network Systems - Client):**
  + The system masks and encrypts the entered memorable secret for secure transmission.
* **Output:** Specific characters from the memorable secret are entered and encrypted for verification.

## **5.5 Verification of Memorable Secret:**

* **System Action (Server):**
  + The server receives the encrypted memorable secret and decrypts it for verification.
  + The system checks if the entered characters match the stored memorable secret for the claimant's UIN (Unique Identification Number) account.
* **Output:** The system verifies the memorable secret. If the characters match, the process is authenticated successfully.

## **5.6 Handling Authentication Outcomes:**

* **System Action (Server):**
  + If the memorable secret matches, the system generates a notification of authentication success.
  + If the memorable secret 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 secret authentication

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.D MEMORABLE SECRET-BASED AUTHENTICATION** | | | | | |
| **Step** | **Description** | **Action** | **Systems Involved** | **Security Measures** | **Standards and References** |
| 1 | Request Authentication Start | Verifier starts authentication with secure link | Verifier Device, Public Network | Secure Communication Link | ISO 27001 Information Security Management, eIDAS Trust Services |
| 2 | User Login | User clicks secure link to initiate login | User Device, Authentication Server | HTTPS, SSL/TLS | ISO 27001 Access Control, eIDAS Electronic Identification |
| 3 | Two-Factor Authentication | 2FA using OTP | User Device, 2FA System | Two-Factor Authentication | ISO 27001 Authentication Controls, Sing Pass 2FA Mechanisms |
| 4 | Enter Memorable Secret | User enters requested characters from secret | User Device, Authentication Server | Data Encryption, Input Validation | ISO 27001 Data Protection, NIST SP 800-63 Digital Identity Guidelines |
| 5 | Memorable Secret Authentication | Server masks and encrypts entered secret | Private Network Servers | Masking, Encryption | ISO 27001 Cryptography, Aadhaar Biometric Data Security |
| 6 | Notification of Authentication Status | Server sends success or failure notification | Notification System, User Device | Secure Notification Delivery | ISO 27001 Communications Security, Estonia ID Secure Channel Communication |
| 7 | Handle Authentication Failures | Exception and error handling for failed attempts | Authentication Server | Error Handling, Account Lockout Policy | ISO 27001 Event Logging and Monitoring, Emirates ID User Account Management |
| 8 | Terminate or Continue Process | Lock out or reset process based on attempts | Authentication Server | Account Lockout, Error Handling | ISO 27001 Access Control Policies, FATF Digital Identity Identity Verification |
| 9 | End Process | Logs the process status and ends | Authentication Server | Logging | NIST SP 800-63 Authenticator Management, Estonia ID Secure Channel Communication |

# 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].