|  |  |  |
| --- | --- | --- |
| **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- PASSWORD: BASED AUTHENTICATION

AU.1.B - 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](#_Toc177313356)

[2. Definitions and Abbreviations 3](#_Toc177313357)

[3 Application 3](#_Toc177313358)

[3.1 Ownership and Stakeholders 3](#_Toc177313359)

[3.1.1 Digital Identity Service Providers (DISPs) 3](#_Toc177313360)

[3.1.2 IT and Security Teams 3](#_Toc177313361)

[3.1.3 Compliance and Legal Departments 3](#_Toc177313362)

[3.2 Users and Beneficiaries 4](#_Toc177313363)

[3.2.1 General Public 4](#_Toc177313364)

[3.2.2 Government Agencies 4](#_Toc177313365)

[3.2.3 Private Sector Companies 4](#_Toc177313366)

[4. Prerequisites 4](#_Toc177313367)

[4.1 Assumptions 4](#_Toc177313368)

[4.2 Constraints 4](#_Toc177313369)

[5. Process Flow - Process and Procedures 4](#_Toc177313370)

[5.1. Authentication Initiation: 4](#_Toc177313371)

[5.2. Entering Credentials: 5](#_Toc177313372)

[5.3. Credential Encryption and Transmission: 5](#_Toc177313373)

[5.4. Credential Verification: 5](#_Toc177313374)

[5.5. Handling Authentication Outcomes: 5](#_Toc177313375)

[5.6. Notification and Logging: 6](#_Toc177313376)

[5.7. Termination of Process: 6](#_Toc177313377)

[5.8. Logging and Status Reporting: 6](#_Toc177313378)

[6. Visualisation 7](#_Toc177313379)

[7. Rationalisation 8](#_Toc177313380)

[8. References 8](#_Toc177313381)

# 1. Purpose

This SOP outlines the standardised procedure for password-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

**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 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**: 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. Authentication Initiation:

* **Subscriber/Claimant Action:**
  + The subscriber or claimant clicks on a secure link sent via email or SMS to initiate authentication through the DID authenticator.
  + The action can be started by the subscriber directly or through a request made by a verifier.
* **Verifier Action:**
  + The verifier requests authentication for the subscriber/claimant by providing a secure link.
* **Output:** Authentication process is initiated, and the subscriber/claimant proceeds to the next step.

## 5.2. Entering Credentials:

* **Subscriber/Claimant Action:**
  + The subscriber enters their email address and password in the provided fields on the authentication page.
  + After entering the credentials, the subscriber clicks the "Submit" button to proceed.
* **Output:** Credentials (email and password) are entered and submitted for verification.

## 5.3. Credential Encryption and Transmission:

* **System Action (Public Network Systems - Client):**
  + The system masks and encrypts the subscriber's email and password to ensure secure transmission.
  + Data encryption is performed using SSL/TLS protocols.
* **Output:** Encrypted credentials are securely transmitted to the server for verification.

## 5.4. Credential Verification:

* **System Action (Private Network Systems - Server):**
  + The server receives the encrypted credentials and decrypts them for verification.
  + The system checks if the email and password match the records in the DID database.
  + If the credentials match, authentication is considered successful. If they do not match, the system increments the retry counter.
* **Output:** The system verifies whether the credentials are correct or not.

## 5.5. Handling Authentication Outcomes:

* **System Action (Private Network Systems - Server):**
  + If the email and password match the records, the system generates a notification of authentication success.
  + If the credentials do not match:
    - The system increments the retry counter and generates a notification of authentication failure.
    - If the retry count reaches 3, the system terminates the authentication process and locks the account.
    - 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.

## 5.6. Notification and Logging:

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

## 5.7. Termination of Process:

* **System Action (Private Network Systems - Server):**
  + If the authentication fails after three attempts, the system terminates the process and marks the user account as locked.
  + If authentication is successful, the process is completed, and the user is granted access.
* **Output:** Process is terminated either due to successful authentication or after multiple failed attempts.

## 5.8. Logging and Status Reporting:

* **System Action (Private Network Systems - 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 screenshot of a computer

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.B PASSWORD-BASED AUTHENTICATION** | | | | | |
| **Step** | **Description** | **Action** | **Systems Involved** | **Security Measures** | **Standards and References** |
| 1. Start Authentication | Subscriber initiates login process. | Enter UIN and password on the secure login page. | Public Network Systems Client | Secure login interface and HTTPS encryption. | ISO/IEC 27001, eIDAS for secure digital interactions |
| 2. Secure Transmission | Securely transmit login details. | Encrypt and send UIN and password for authentication. | Public Network Systems Client | Data encryption during transmission. | ISO/IEC 27001 for data encryption; NIST Digital Identity Guidelines for secure transmission |
| 3. Verify Credentials | Authenticate user's credentials. | Verify UIN and password match with the database records. | Private Network Systems Server | Access control and credential verification. | FATF Digital Identity Guidance, ISO/IEC 27001 for access control measures |
| 4. Handle Authentication Results | Process authentication outcomes. | Generate notifications based on authentication success or failure. | Notification Generator | Real-time response and error handling. | ISO/IEC 27001 for incident management |
| 5. Log Activities | Document the authentication process. | Log the outcome and details of the authentication attempt. | IDA (Identity Database) | Secure logging and compliance with data retention policies. | ISO/IEC 27001 for audit trails; GDPR for data privacy |
| 6. Error and Retry Handling | Manage errors and retry attempts. | Apply error handling protocols and allow retries, terminating after excessive attempts. | Private Network Systems Server | Robust security protocols to prevent unauthorised access. | NIST Digital Identity Guidelines, ISO/IEC 27001 for error handling |

# 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].