Standard Operating Procedure - Generation of One-Time Password

AU.2.A

**Version Control**

|  |  |  |
| --- | --- | --- |
| Version | Date | Changes Made |
|  |  |  |
|  |  |  |
|  |  |  |

**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](#_Toc177285120)

[2. Definitions and Abbreviations 3](#_Toc177285121)

[3 Application 3](#_Toc177285122)

[3.1 Ownership and Stakeholders 3](#_Toc177285123)

[3.1.1 Digital Identity Service Providers (DISPs) 3](#_Toc177285124)

[3.1.2 IT and Security Teams 3](#_Toc177285125)

[3.1.3 Compliance and Legal Departments 3](#_Toc177285126)

[3.2 Users and Beneficiaries 4](#_Toc177285127)

[3.2.1 General Public 4](#_Toc177285128)

[3.2.2 Government Agencies 4](#_Toc177285129)

[3.2.3 Private Sector Companies 4](#_Toc177285130)

[4. Prerequisites 4](#_Toc177285131)

[4.1 Assumptions 4](#_Toc177285132)

[4.2 Constraints 4](#_Toc177285133)

[5. Process Flow - Process and Procedures 4](#_Toc177285134)

[5.1. Start and Access Portal: 4](#_Toc177285135)

[5.2. Login and Password Authentication: 4](#_Toc177285136)

[5.3. Provide UIN and Demographic Data: 5](#_Toc177285137)

[5.4. Request Authentication via Secure Link: 5](#_Toc177285138)

[5.5. Verification of UIN and Demographic Data: 5](#_Toc177285139)

[5.6. OTP Generation: 5](#_Toc177285140)

[5.7. OTP Delivery: 5](#_Toc177285141)

[5.8. OTP Resend Request (if applicable): 6](#_Toc177285142)

[5.9. OTP Verification: 6](#_Toc177285143)

[5.10. Handling Authentication Outcomes: 6](#_Toc177285144)

[5.11. Logging and Status Update: 6](#_Toc177285145)

[5.12. Termination of Process: 6](#_Toc177285146)

[6. Visualisation 8](#_Toc177285147)

# 1. Purpose

This SOP outlines the standardized procedure for generating a One-Time Password (OTP) within the Digital Identity (DID) system. It ensures secure and accurate OTP generation 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 OTP generation process.
* **Responsibilities**: Ensure secure and compliant generation of OTPs.

### 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 generating OTPs for their DID accounts.
* **Usage**: Provide UIN and demographic data to receive OTPs.

### 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

* Subscribers have received their DID and FTP credentials.
* Administrators are trained to handle the OTP generation process securely.
* Technological infrastructure meets current security standards.

## 4.2 Constraints

* The OTP generation process may be affected by system downtimes or regulatory changes.

# 5. Process Flow - Process and Procedures

## **5.1. Start and Access Portal:**

* **Claimant/Subscriber Action:**
  + The claimant/subscriber initiates the process by visiting the Digital Identity (DID) portal login page.
* **Output:** The claimant accesses the login page to begin the OTP generation process.

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

* **System Action:**
  + The system prompts the claimant to log in using their username and password.
* **Claimant/Subscriber Action:**
  + The claimant enters their username and password.
* **System Action (Server):**
  + The server masks and encrypts the entered username and password for secure transmission.
  + The server validates the credentials against the stored records.
* **Output:** Password authentication is validated. If successful, proceed to the next step.

## **5.3. Provide UIN and Demographic Data:**

* **System Action:**
  + The system requests the claimant to provide their Unique Identification Number (UIN) and demographic data.
* **Claimant/Subscriber Action:**
  + The claimant provides their UIN and demographic details as required.
* **Output:** UIN and demographic data are provided for verification.

## **5.4. Request Authentication via Secure Link:**

* **Verifier Action:**
  + The verifier, either online or offline, requests authentication by sending a secure link to the claimant.
* **Output:** Secure authentication link is sent.

## **5.5. Verification of UIN and Demographic Data:**

* **System Action (Server):**
  + The server verifies the provided UIN and demographic data against the stored records.
  + If the UIN and demographic data match, the server proceeds to the next step.
* **Output:** UIN and demographic data are verified. If matched, proceed to OTP generation.

## **5.6. OTP Generation:**

* **System Action (Server):**
  + Upon successful verification, the server generates a 6-digit OTP.
  + The OTP is set with a 60-second timeout for validity.
  + The OTP is securely stored using encryption, hashing, and timestamping for future verification.
* **Output:** OTP is generated and stored securely.

## **5.7. OTP Delivery:**

* **System Action:**
  + The system sends the generated OTP to the claimant’s registered email, phone, or a multiuser's phone, depending on the claimant's registration preferences.
* **Output:** OTP is delivered to the claimant via the specified communication channel.

## **5.8. OTP Resend Request (if applicable):**

* **Claimant/Subscriber Action:**
  + If the OTP is not received, the claimant may request to resend the OTP.
* **System Action:**
  + The system generates and sends a new OTP upon request.
* **Output:** New OTP is generated and sent.

## **5.9. OTP Verification:**

* **Claimant/Subscriber Action:**
  + The claimant enters the received OTP into the system for verification.
* **System Action (Server):**
  + The server compares the entered OTP with the stored OTP.
  + If the OTP matches, the process is authenticated successfully.
  + If the OTP does not match, an error handling routine is initiated.
* **Output:** OTP is verified. If it matches, authentication is successful.

## **5.10. Handling Authentication Outcomes:**

* **System Action (Server):**
  + If the OTP matches, a success notification is generated and sent to the claimant.
  + If the OTP does not match, the system increments the retry counter.
  + If the retry count reaches three attempts, the system locks the UIN account for 24 hours to prevent unauthorized access.
* **Output:** Notification of authentication success or failure is generated and sent.

## **5.11. Logging and Status Update:**

* **System Action (Server):**
  + The system logs the details of the OTP generation and authentication process, including outcomes and any errors encountered.
  + The status of the process is updated in the system for compliance and audit purposes.
* **Output:** Process completion is logged, and status is updated.

## **5.12. Termination of Process:**

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

# 6. Visualisation

A screenshot of a computer screen

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.