|  |  |  |
| --- | --- | --- |
| **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 Multi User One-Time Password

AU.2.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](#_Toc177313602)

[2. Definitions and Abbreviations 3](#_Toc177313603)

[3 Application 3](#_Toc177313604)

[3.1 Ownership and Stakeholders 3](#_Toc177313605)

[3.1.1 Digital Identity Service Providers (DISPs) 3](#_Toc177313606)

[3.1.2 IT and Security Teams 3](#_Toc177313607)

[3.1.3 Compliance and Legal Departments 3](#_Toc177313608)

[3.2 Users and Beneficiaries 4](#_Toc177313609)

[3.2.1 General Public 4](#_Toc177313610)

[3.2.2 Government Agencies 4](#_Toc177313611)

[3.2.3 Private Sector Companies 4](#_Toc177313612)

[4. Prerequisites 4](#_Toc177313613)

[4.1 Assumptions 4](#_Toc177313614)

[4.2 Constraints 4](#_Toc177313615)

[5. Process Flow - Process and Procedures 4](#_Toc177313616)

[5.1. Initiating the Multi-User OTP Creation Process: 4](#_Toc177313617)

[5.2. Form Submission and Authentication: 4](#_Toc177313618)

[5.3. Subscriber Authentication: 5](#_Toc177313619)

[5.4. Consent from Trusted Individual: 5](#_Toc177313620)

[5.5. Trusted Individual Authentication: 5](#_Toc177313621)

[5.6. Activation of Multi-User OTP Authenticator: 5](#_Toc177313622)

[5.7. Notification of OTP Creation Status: 6](#_Toc177313623)

[5.8. Error Handling and Termination: 6](#_Toc177313624)

[5.9. Logging and Status Update: 6](#_Toc177313625)

[6. Visualisation 7](#_Toc177313626)

[7. Rationalisation 8](#_Toc177313627)

[8. References 9](#_Toc177313628)

# 1. Purpose

This SOP outlines the standardised procedure for creating a Multi-User One-Time Password (OTP) within the Digital Identity (DID) system. It ensures secure and accurate OTP 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 multi-user OTP creation process.
* **Responsibilities**: Ensure secure and compliant generation of multi-user 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 creating multi-user OTPs for their DID accounts.
* **Usage**: Provide UIN and demographic data, and collaborate with trusted individuals to receive OTPs.

### 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 and trusted individuals have received their DID and FTP credentials.
* Administrators are trained to handle the multi-user OTP creation process securely.
* Technological infrastructure meets current security standards.

## 4.2 Constraints

* The OTP 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. Initiating the Multi-User OTP Creation Process:**

* **Subscriber Action:**
  + The subscriber visits the Digital Identity (DID) center to collect the application form for multi-user OTP.
  + The subscriber fills out the form with their Unique Identification Number (UIN) and demographic details, and the trusted individual's UIN and phone number.
* **Output:** Form for multi-user OTP creation is filled out with necessary details.

## **5.2. Form Submission and Authentication:**

* **Subscriber Action:**
  + The subscriber submits the completed application form.
* **System Action (Public Network Systems - Client):**
  + The system receives the multi-user OTP application form.
  + The subscriber's UIN and demographic details are entered into the system.
  + The system masks and encrypts the UIN and demographic details for authentication.
* **Output:** Application form is submitted and subscriber details are securely handled.

## **5.3. Subscriber Authentication:**

* **System Action (Server):**
  + The server verifies if the provided subscriber details match the stored records.
  + If the subscriber details match, authentication is considered successful.
  + If the details do not match, an error handling routine is initiated.
* **Output:** Subscriber authentication is performed. If successful, proceed to the next step.

## **5.4. Consent from Trusted Individual:**

* **System Action:**
  + The system requests consent from the trusted individual using the UIN provided by the subscriber.
  + The trusted individual is required to authenticate using a biometric method of their choice (e.g., fingerprint, facial recognition).
* **Trusted Individual Action:**
  + The trusted individual provides consent via biometric authentication.
* **Output:** Trusted individual's consent is requested and provided through biometric authentication.

## **5.5. Trusted Individual Authentication:**

* **System Action (Server):**
  + The server verifies the biometric authentication provided by the trusted individual.
  + If the trusted individual's UIN and biometric data match the records, authentication is successful.
* **Output:** Trusted individual's authentication is performed. If successful, proceed to activate the multi-user OTP.

## **5.6. Activation of Multi-User OTP Authenticator:**

* **System Action (Server):**
  + Upon successful authentication of both subscriber and trusted individual, the system stores the trusted individual's phone number in the subscriber's UIN account with encryption and hashing.
  + The system binds and activates the multi-user OTP authenticator.
* **Output:** Multi-user OTP authenticator is activated, and trusted individual's phone number is securely stored.

## **5.7. Notification of OTP Creation Status:**

* **System Action:**
  + The system sends a notification to both the subscriber and the trusted individual, indicating the successful creation of the multi-user OTP authentication.
* **Output:** Notifications of successful OTP creation are sent to the subscriber and trusted individual.

## **5.8. Error Handling and Termination:**

* **System Action (Server):**
  + If there are errors during authentication, such as mismatched details or failed biometric authentication, the system initiates an error handling routine.
  + The system increments the retry counter. If the retry count exceeds three attempts, the UIN account is locked for 24 hours to prevent unauthorised access.
  + The process is terminated if errors persist.
* **Output:** Errors are handled, and the process is terminated after multiple failed attempts.

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

* **System Action (Server):**
  + The system logs the entire process, including all authentication attempts, outcomes, and errors encountered.
  + The status is updated for compliance and audit purposes.
* **Output:** Detailed logs are maintained, and status reports are generated.

# 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.2.B Creation of Multi User One-Time Password** | | | | | |
| **Step** | **Description** | **Action** | **Systems Involved** | **Security Measures** | **Standards and References** |
| 1 | Start Process | Subscriber visits DID center & collects form | Subscriber Device, Public Network | Secure Access to Forms | ISO 27001 Information Security Management, eIDAS Trust Services |
| 2 | Fill Application Form | Subscriber fills form with UIN and demographic details | Subscriber Device, Public Network | Data Entry Security | ISO 27001 Data Protection, Aadhar Guidelines on Secure Data Handling |
| 3 | Trusted Individual Consent | Trusted individual provides consent via biometric authentication | Biometric Authentication System | Biometric Data Security, Consent Verification | ISO 27001 User Access Management, eIDAS Electronic Identification, Emirates ID Biometric Standards |
| 4 | Authenticate Using Biometrics | Biometric authentication to verify identity | Biometric Scanner, Private Network | Secure Biometric Processing, Identity Verification | ISO 27001 Authentication Controls, NIST SP 800-63 Digital Identity Guidelines, Sing Pass Biometric Authentication |
| 5 | Encrypt and Mask UIN and Demographic Data | Masking and encryption for secure transmission | Server, Private Network | Data Masking, SSL/TLS Encryption | ISO 27001 Cryptography, FATF Digital Identity Guidelines |
| 6 | Generate Multi-User OTP | System generates OTP for the multi-user | OTP Generation Server | OTP Generation with Encryption and Hashing | ISO 27001 Cryptography, NIST SP 800-63 Authentication Mechanisms |
| 7 | Send OTP Notification | OTP sent to subscriber's and trusted individual's email/phone | Notification System | Secure Notification Delivery | ISO 27001 Communications Security, Estonia ID Notification System |
| 8 | Handle Authentication Errors | Manage errors and exceptions in OTP generation | Authentication Server | Error Logging and Exception Management | ISO 27001 Event Logging and Monitoring, FATF Digital Identity Error Handling |
| 9 | Retry or Terminate Process Based on Attempts | Manage retry attempts or lock account | Authentication Server | Account Lockout, Retry Limit Management | ISO 27001 Access Control Policies, NIST SP 800-63 Authenticator Management |
| 10 | End Process | Log process status and conclude the session | Authentication Server | Process Logging | NIST SP 800-63 Authenticator Management, Estonia ID Secure Logging |

# 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].