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

AU.2.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](#_Toc177313548)

[2. Definitions and Abbreviations 3](#_Toc177313549)

[3. Application 3](#_Toc177313550)

[3.1 Ownership and Stakeholders 3](#_Toc177313551)

[3.1.1 Digital Identity Service Providers (DISPs) 3](#_Toc177313552)

[3.1.2 IT and Security Teams 3](#_Toc177313553)

[3.1.3 Compliance and Legal Departments 3](#_Toc177313554)

[3.2 Users and Beneficiaries 3](#_Toc177313555)

[3.2.1 General Public 3](#_Toc177313556)

[3.2.2 Government Agencies 4](#_Toc177313557)

[3.2.3 Private Sector Companies 4](#_Toc177313558)

[4. Prerequisites 4](#_Toc177313559)

[4.1 Assumptions 4](#_Toc177313560)

[4.2 Constraints 4](#_Toc177313561)

[5. Process Flow - Process and Procedures 4](#_Toc177313562)

[5.1. Initiating the Multi-User OTP Authentication Process: 4](#_Toc177313563)

[5.2. Submitting the OTP for Authentication: 4](#_Toc177313564)

[5.3. OTP and Verifier Credentials Verification: 5](#_Toc177313565)

[5.4. OTP Validation: 5](#_Toc177313566)

[5.5. Handling OTP Expiry and Retry: 5](#_Toc177313567)

[5.6. Successful OTP Authentication: 5](#_Toc177313568)

[5.7. Error Handling and Account Locking: 5](#_Toc177313569)

[5.8. Logging and Status Update: 6](#_Toc177313570)

[5.9. Termination of Process: 6](#_Toc177313571)

[6. Visualisation 7](#_Toc177313572)

[7. Rationalisation 8](#_Toc177313573)

[8. References 9](#_Toc177313574)

# 1. Purpose

This SOP outlines the standardized procedure for multi-user One-Time Password (OTP) authentication within the Digital Identity (DID) system. It ensures secure and accurate OTP authentication 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

**HTTPS**: Hyper Text Transfer Protocol Secure

# 3. Application

## 3.1 Ownership and Stakeholders

### 3.1.1 Digital Identity Service Providers (DISPs)

* **Ownership**: Oversee the multi-user OTP authentication process.
* **Responsibilities**: Ensure secure and compliant authentication 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 using multi-user OTPs for authentication.
* **Usage**: Provide OTPs and credentials for secure authentication.

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

## 4.2 Constraints

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

* **Claimant/Subscriber Action:**
  + The claimant/subscriber initiates the authentication process online by receiving an OTP on their registered email/phone/multi-user phone.
  + For offline scenarios, the claimant receives the OTP on the same devices and prepares to submit it verbally.
* **Output:** OTP is received by the claimant for both online and offline scenarios.

## **5.2. Submitting the OTP for Authentication:**

* **Claimant/Subscriber Action:**
  + In online mode, the claimant submits the OTP to the verifier via an online interface.
  + In offline mode, the claimant submits the OTP verbally to the verifier.
* **Verifier Action:**
  + The verifier receives the 6-digit OTP along with their own verifier credentials.
* **Output:** OTP and verifier credentials are submitted for authentication.

## **5.3. OTP and Verifier Credentials Verification:**

* **System Action (Public Network Systems - Client):**
  + The client system masks and encrypts the UIN and password provided for authentication.
* **System Action (Server):**
  + The server checks if the verifier’s credentials match the records.
  + If the credentials match, the server then proceeds to verify the OTP.
* **Output:** Verification of credentials and OTP is initiated.

## **5.4. OTP Validation:**

* **System Action (Server):**
  + The server validates the 6-digit OTP against the stored OTP associated with the claimant’s UIN.
  + If the OTP matches, the authentication is deemed successful.
  + If the OTP does not match or has expired, the server initiates an error handling routine.
* **Output:** OTP is either validated successfully or fails, leading to further actions.

## **5.5. Handling OTP Expiry and Retry:**

* **System Action (Server):**
  + If the OTP has expired, the system sends a notification to the claimant about the expiry and prompts them to request a new OTP.
  + The retry counter is reset, and the claimant can request a new OTP.
* **Claimant/Subscriber Action:**
  + The claimant requests a new OTP if the previous one has expired or if a retry is needed.
* **Output:** New OTP is requested if the previous one was invalid or expired.

## **5.6. Successful OTP Authentication:**

* **System Action (Server):**
  + Upon successful OTP verification, the server stores the verifier details and authentication success status in the UIN account with encryption and hashing.
  + The system then proceeds to a secondary factor authentication (e.g., memorable secret authentication).
* **Output:** OTP authentication is successful, and the process moves to the next authentication step.

## **5.7. Error Handling and Account Locking:**

* **System Action (Server):**
  + If the OTP authentication fails multiple times, the system increments the error handling counter.
  + After three failed attempts, the system locks the claimant’s UIN account for 24 hours to prevent unauthorized access.
  + Notifications are generated to inform the claimant and verifier of the account lock status.
* **Output:** Account is locked after multiple failed attempts, preventing further unauthorized access.

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

* **System Action (Server):**
  + The system logs all steps of the authentication process, including successful verifications and errors encountered.
  + The status is updated in the system logs for compliance and audit purposes.
* **Output:** Detailed logs are created, and status reports are generated.

## **5.9. Termination of Process:**

* **System Action (Server):**
  + The process is terminated if the OTP authentication is successful, and the claimant gains access.
  + If the account is locked due to multiple failed attempts, the process is terminated to prevent further attempts until the lock duration expires.
* **Output:** Process is either successfully completed or terminated due to security measures.

# 6. Visualisation

A diagram of a password 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.2.C Multi-User One-Time Password Authentication** | | | | | |
| **Step** | **Description** | **Action** | **Systems Involved** | **Security Measures** | **Standards and References** |
| 1 | Receive OTP | OTP received on registered email/phone | User Device, Public Network | Secure Communication Channels | ISO 27001 Information Security Management, eIDAS Trust Services |
| 2 | Submit OTP for Verification | User submits OTP to verifier online or verbally | User Device, Verifier System | Secure Data Transmission, HTTPS | ISO 27001 Access Control, NIST SP 800-63 Digital Identity Guidelines |
| 3 | Authenticate OTP | Send OTP and verifier credentials for authentication | Authentication Server | Masking & Encrypt UIN and Password | ISO 27001 Cryptography, FATF Digital Identity Guidelines |
| 4 | Verify OTP and Verifier Credentials | Check if 6-digit OTP matches and verifier credentials match | Server, Private Network | Data Matching, Secure Authentication Process | ISO 27001 User Access Management, eIDAS Electronic Identification |
| 5 | Store Authentication Details | Store verifier details and successful authentication | Server, Private Network | Encryption, Hashing | ISO 27001 Cryptography, NIST SP 800-63 Authentication Mechanisms, Aadhar Secure Data Handling Guidelines |
| 6 | Handle OTP Expiry and Retries | Manage expired OTPs and retry requests | Authentication Server | Time-out Handling, Retry Management | ISO 27001 Event Logging and Monitoring, Emirates ID Standards for Authentication Management |
| 7 | Notification of Authentication Success or Failure | Notify user of OTP authentication outcome | Notification System | Secure Notification Delivery | ISO 27001 Communications Security, Estonia ID Secure Notification Handling |
| 8 | Terminate or Reset Process | Lock UIN account for 24 hours or reset process based on retry count | Authentication Server | Account Lockout, Error Handling | ISO 27001 Access Control Policies, NIST SP 800-63 Authenticator Management |
| 9 | End Process | Log process status and conclude the authentication 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].