|  |  |  |
| --- | --- | --- |
| **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 - EXPIRY AND RENEWAL OF AUTHENTICATORS (OTP, TOKEN VALIDITY)

LM.4.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](#_Toc177314918)

[2. Definitions and Abbreviations 3](#_Toc177314919)

[3. Application 3](#_Toc177314920)

[3.1 Ownership and Stakeholders 3](#_Toc177314921)

[3.1.1 Digital Identity Service Providers (DISPs) 3](#_Toc177314922)

[3.1.2 IT and Security Teams 3](#_Toc177314923)

[3.1.3 Compliance and Legal Departments 3](#_Toc177314924)

[3.2 Users and Beneficiaries 3](#_Toc177314925)

[3.2.1 General Public 3](#_Toc177314926)

[3.2.2 Government Agencies 4](#_Toc177314927)

[3.2.3 Private Sector Companies 4](#_Toc177314928)

[4. Prerequisites 4](#_Toc177314929)

[4.1 Assumptions 4](#_Toc177314930)

[4.2 Constraints 4](#_Toc177314931)

[5. Process Flow - Process and Procedures 4](#_Toc177314932)

[5.1. Initiate Authenticator Expiry Check: 4](#_Toc177314933)

[5.2. Monitor Authenticator Expiry: 4](#_Toc177314934)

[5.3. Notification and Renewal Process Initiation: 5](#_Toc177314935)

[5.4. Generate New Authenticators: 5](#_Toc177314936)

[5.5. Confirm Renewal and Update System: 5](#_Toc177314937)

[5.6. Error and Exception Handling: 5](#_Toc177314938)

[5.7. Deactivation of Authenticators: 6](#_Toc177314939)

[5.8. Logging and Termination: 6](#_Toc177314940)

[6. Visualisation 7](#_Toc177314941)

[7. Rationalisation 8](#_Toc177314942)

[8. References 9](#_Toc177314943)

# 1. Purpose

This SOP specifies the standardised procedure for renewing or expiring One-Time Passwords (OTPs) and tokens. It ensures secure and accurate processing through proper verification, documentation, 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 expiry and renewal process.
* **Responsibilities**: Ensure secure and compliant renewal of authenticators.

### 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 renewing their expired OTPs and tokens.
* **Usage**: Provide updated identity verification for secure account management.

### 3.2.2 Government Agencies

* **Users**: Agencies requiring verified and updated identities for services.
* **Usage**: Utilise verified identity information for secure service delivery.

### 3.2.3 Private Sector Companies

* **Users**: Businesses requiring updated identity verification.
* **Usage**: Use secured identities for compliance and verification purposes.

# 4. Prerequisites

## 4.1 Assumptions

* Subscribers have access to required documents and authentication methods.
* Administrators are trained to handle the expiry and renewal process securely.
* Technological infrastructure meets current security standards.

## 4.2 Constraints

* The renewal 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. Initiate Authenticator Expiry Check:**

* **Private Network Systems (Server) Action:**
  + The process begins with the system setting up expiry dates for various authenticators like OTP (One-Time Password), FTP (File Transfer Protocol), and tokens. The system continuously monitors these expiry dates.
* **Output:** Expiry dates are set, and the system is prepared to handle authentication expiry events.

## **5.2. Monitor Authenticator Expiry:**

* **Private Network Systems (Server) Action:**
  + The server tracks the status of each authenticator. If an authenticator reaches its expiry date, it triggers an expiry event.
  + Authenticator expiry is set for specific durations (e.g., 60 seconds for OTP, 30 days for tokens).
* **Output:** Expiry event triggered for expired authenticators.

## **5.3. Notification and Renewal Process Initiation:**

* **Verifier/Administrator Action:**
  + Upon detecting an expired authenticator, the system sends a notification to the relevant party (subscriber, claimant, or verifier) indicating the expiry.
  + The administrator initiates the process to generate a new authenticator, which could include a new token or OTP.
* **Output:** Expiry notifications are sent, and renewal processes are initiated.

## **5.4. Generate New Authenticators:**

* **Verifier/Administrator Action:**
  + The administrator verifies the request and proceeds to generate new authenticators.
  + The new OTP or token is generated securely and delivered to the subscriber or user. In the case of FTP authentication, specific protocols are followed to ensure secure delivery.
* **Public Network Systems (Client) Action:**
  + Masking and encryption techniques are applied to secure the new authenticator details during transmission.
* **Output:** New authenticators (OTP, tokens) are generated and securely delivered.

## **5.5. Confirm Renewal and Update System:**

* **Private Network Systems (Server) Action:**
  + The server verifies the successful generation and delivery of new authenticators.
  + Once verified, the system updates the status of the authenticator in the database, including new expiry dates and any relevant user details.
* **Output:** System is updated with new authenticator details, and user is notified of successful renewal.

## **5.6. Error and Exception Handling:**

* **Private Network Systems (Server) Action:**
  + If errors occur during the expiry or renewal process (e.g., failed authentication, network issues), the system logs these events and triggers appropriate error handling protocols.
  + The system may deactivate the authenticator and initiate a retry mechanism, up to three attempts.
* **Output:** Errors are logged, and retries are attempted; process may terminate if retries are exceeded.

## **5.7. Deactivation of Authenticators:**

* **Private Network Systems (Server) Action:**
  + In cases where renewal fails or is not possible, the system deactivates the expired authenticator to prevent unauthorised access.
* **Output:** Expired authenticators are deactivated, ensuring system security.

## **5.8. Logging and Termination:**

* **Private Network Systems (Server) Action:**
  + The entire process, including successful renewals and failures, is logged for auditing and monitoring purposes.
  + If the process fails after multiple retries, it is terminated, and a log entry is created to record the event.
* **Output:** All actions are logged, and the process is either completed successfully or terminated.

# 6. Visualisation

A diagram of a company

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

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **LM.4.B EXPIRY AND RENEWAL OF AUTHENTICATORS (OTP, TOKEN VALIDITY)** | | | | | |
| **Step** | **Description** | **Action** | **Systems Involved** | **Security Measures** | **Standards and References** |
| 1 | Start Process | Initiation of the OTP/token renewal or expiry | User Device, Public Network | Secure HTTPS Connection | ISO 27001 Information Security Management, eIDAS Trust Services |
| 2 | Set Expiry | Set expiration parameters for OTP/token | Server | Configuration of expiry settings | ISO 27001 Access Control, NIST SP 800-63 Digital Identity Guidelines |
| 3 | Check Expiry | Monitor authenticators for expiration | Server | Automated expiry checking | ISO 27001 Data Protection, GDPR Compliance for Data Handling |
| 4 | Deactivate Authenticator | Deactivate expired authenticators | Server | Immediate deactivation of access | ISO 27001 User Access Management, FATF Digital Identity Guidelines |
| 5 | Generate New Authenticator | Generate new OTP or token if needed | Server | Secure generation and transmission | ISO 27001 Cryptography, NIST SP 800-63 Authentication Mechanisms |
| 6 | Mask & Encrypt Authenticator Details | Secure the details of the new authenticator | Server | Data encryption and masking | ISO 27001 Cryptography, Emirates ID Data Security Standards |
| 7 | Notification of New Authenticator | Notify user of the new authenticator details | Notification System | Secure notification delivery | ISO 27001 Communications Security, Sing Pass Notification System |
| 8 | Error and Exception Handling | Manage errors and exceptions during the process | Security System | Error logging and response handling | ISO 27001 Event Management, NIST SP 800-61 Incident Response |
| 9 | Log Process | Record the renewal or expiry process | Security Logs | Audit trails, logging | ISO 27001 Secure Audit Logging, NIST SP 800-53 Security and Privacy Controls |
| 10 | End Process | Finalise the renewal or expiry process | System | Process completion logging | ISO 27001 Information Security Management |
| 11 | Terminate Process If Excessive Retries | Lock account after multiple failed authentications | Authentication System | Account lockout policy | ISO 27001 Access Control Policies, NIST SP 800-63 Authenticator Management |

# 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].