|  |  |  |
| --- | --- | --- |
| **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 DID ACCOUNT

LM.4.A - 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](#_Toc177314978)

[2. Definitions and Abbreviations 3](#_Toc177314979)

[3. Application 3](#_Toc177314980)

[3.1 Ownership and Stakeholders 3](#_Toc177314981)

[3.1.1 Digital Identity Service Providers (DISPs) 3](#_Toc177314982)

[3.1.2 IT and Security Teams 3](#_Toc177314983)

[3.1.3 Compliance and Legal Departments 3](#_Toc177314984)

[3.2 Users and Beneficiaries 3](#_Toc177314985)

[3.2.1 General Public 3](#_Toc177314986)

[3.2.2 Government Agencies 4](#_Toc177314987)

[3.2.3 Private Sector Companies 4](#_Toc177314988)

[4. Prerequisites 4](#_Toc177314989)

[4.1 Assumptions 4](#_Toc177314990)

[4.2 Constraints 4](#_Toc177314991)

[5. Process Flow - Process and Procedures 4](#_Toc177314992)

[5.1. Account Expiry Notification: 4](#_Toc177314993)

[5.2. Determine Eligibility for Renewal: 4](#_Toc177314994)

[5.3. Booking Appointment for Renewal: 5](#_Toc177314995)

[5.4. Visit to DID Center for Data Collection: 5](#_Toc177314996)

[5.5. Authentication and Consent: 5](#_Toc177314997)

[5.6. Data Processing and Verification: 5](#_Toc177314998)

[5.7. Account Activation and Notification: 6](#_Toc177314999)

[5.8. Logging and Termination: 6](#_Toc177315000)

[6. Visualisation 7](#_Toc177315001)

[7. Rationalisation 8](#_Toc177315002)

[8. References 9](#_Toc177315003)

# 1. Purpose

This SOP outlines the standardised procedure for the expiry and renewal of Digital Identity (DID) accounts. 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

# 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 DID accounts.

### 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 DID accounts.
* **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. Account Expiry Notification:**

* **Claimant/Subscriber Action:**
  + The process begins with the user receiving a notification regarding the upcoming expiry of their DID account. This notification prompts the user to take action to renew their account.
* **Output:** User is informed of account expiry and need for renewal.

## **5.2. Determine Eligibility for Renewal:**

* **Claimant/Subscriber Action:**
  + The user reviews the notification and checks if they meet the eligibility criteria for renewal.
  + Different scenarios are evaluated, such as age (under 16 years), visa or residence permit validity, and other criteria that might necessitate renewal.
  + If the user does not meet the criteria, the process is terminated.
* **Output:** Eligibility for renewal is determined.

## **5.3. Booking Appointment for Renewal:**

* **Claimant/Subscriber/Parent/Guardian/Introducer Action:**
  + If the user is eligible, they proceed to book an appointment at a designated DID (Digital Identity) center for biometric data collection and renewal.
  + The appointment can be booked online or via a service center. A confirmation of the appointment, along with the details, is sent to the user.
* **Output:** Appointment for renewal is scheduled, and confirmation is sent to the user.

## **5.4. Visit to DID Center for Data Collection:**

* **Claimant/Subscriber/Parent/Guardian/Introducer Action:**
  + On the appointment date, the user visits the DID center for biometric data collection.
  + The user is required to provide the necessary documents, such as UIN (Universal Identification Number), proof of address, and other supporting documents as per the notification.
* **Administrator Action:**
  + The administrator at the DID center verifies the documents and initiates the data collection process.
* **Output:** Biometric data is collected, and documentation is verified.

## **5.5. Authentication and Consent:**

* **Claimant/Subscriber Action:**
  + The user provides consent for biometric data collection and verification. This includes authentication using various methods such as fingerprint, iris scan, facial recognition, or other biometric authentications.
  + If consent is not provided, the process is terminated.
* **Output:** User consent is recorded, and biometric authentication is performed.

## **5.6. Data Processing and Verification:**

* **Network Systems Action (Client & Server):**
  + The collected biometric data is encrypted and sent to the network systems for processing.
  + The system verifies the data, checks for any discrepancies, and validates the authenticity of the biometric information.
* **Administrator Action:**
  + The administrator monitors the verification process and ensures that the data is correctly processed.
* **Output:** Biometric data is processed and verified for accuracy and authenticity.

## **5.7. Account Activation and Notification:**

* **Network Systems Action (Server):**
  + Upon successful verification, the system updates the user’s DID account status to active.
  + A notification is sent to the user confirming the activation of their DID account.
* **Claimant/Subscriber Action:**
  + The user receives a new DID card or digital confirmation of account renewal.
* **Output:** DID account is renewed and activated, and the user is notified of the successful renewal.

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

* **Network Systems Action (Server):**
  + The entire process, including each step and its outcome, is logged in the system for record-keeping and future reference.
  + If the renewal process fails or if the user is ineligible, the system terminates the process and logs the details.
* **Output:** Process is logged, and any failed attempts are recorded for audit purposes.

# 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

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **LM.4.A EXPIRY AND RENEWAL DID ACCOUNT** | | | | | |
| **Step** | **Description** | **Action** | **Systems Involved** | **Security Measures** | **Standards and References** |
| 1 | Start Process | User is notified of DID expiry | User Device, Notification System | Secure notification delivery | ISO 27001 Communications Security, eIDAS Trust Services |
| 2 | Authenticate User | User logs in for renewal process | Authentication Server | Two-Factor Authentication | ISO 27001 Access Control, NIST SP 800-63 Digital Identity Guidelines |
| 3 | Book Appointment for Re-enrollment | User books an appointment online or offline | Online Booking System, Service Center | Secure session management | ISO 27001 Data Protection, eIDAS Electronic Identification |
| 4 | Provide Consent for Biometric Collection | Consent taken for collecting biometric data | Service Center | Consent verification, Data privacy | GDPR Consent Requirements, ISO 27001 User Access Management |
| 5 | Collect New Biometrics | Biometric data collection at appointment | Biometric Collection System | Biometric data security | ISO 27001 Authentication Controls, FATF Digital Identity Guidelines |
| 6 | Authenticate Claimant for Re-enrollment | Multiple biometric authenticators used for verification | Authentication System | Multi-factor authentication | ISO 27001 Cryptography, NIST SP 800-63 Authentication Mechanisms |
| 7 | Validate Supporting Documents | Verification of provided documents | Document Verification System | Document authentication | ISO 27001 Data Integrity, eIDAS Trust Services |
| 8 | Update and Store New Biometrics to Authenticators | New biometric data encrypted and stored | Secure Database System | Data Encryption, Secure storage | ISO 27001 Cryptography, Emirates ID Data Security Standards |
| 9 | Issue New DID and FTP to Subscriber | New digital identity and FTP details provided | Distribution System | Secure distribution, Data masking | ISO 27001 Physical Security, eIDAS Trust Services |
| 10 | Activate DID Account | Activation of new DID account | Account Management System | Account activation protocol | ISO 27001 User Access Management, NIST SP 800-63 Identity Verification |
| 11 | Notify User of Successful Renewal | User receives notification of successful renewal | Notification System | Secure notification delivery | ISO 27001 Communications Security, Sing Pass Notification System |
| 12 | Log Process | Log details of the renewal process | Security System | Audit trails, logging | ISO 27001 Secure Audit Logging, NIST SP 800-53 Security and Privacy Controls |
| 13 | End Process | Process completion | System | Secure session termination | ISO 27001 Information Security 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].