|  |  |  |
| --- | --- | --- |
| **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 - UPDATE OFFLINE BIOMETRICS DATA

LM.1.D - 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](#_Toc177314533)

[2. Definitions and Abbreviations 3](#_Toc177314534)

[3. Application 3](#_Toc177314535)

[3.1 Ownership and Stakeholders 3](#_Toc177314536)

[3.1.1 Digital Identity Service Providers (DISPs) 3](#_Toc177314537)

[3.1.2 IT and Security Teams 3](#_Toc177314538)

[3.1.3 Compliance and Legal Departments 3](#_Toc177314539)

[3.2 Users and Beneficiaries 3](#_Toc177314540)

[3.2.1 General Public 3](#_Toc177314541)

[3.2.2 Government Agencies 4](#_Toc177314542)

[3.2.3 Private Sector Companies 4](#_Toc177314543)

[4. Prerequisites 4](#_Toc177314544)

[4.1 Assumptions 4](#_Toc177314545)

[4.2 Constraints 4](#_Toc177314546)

[5. Process Flow - Process and Procedures 4](#_Toc177314547)

[5.1. Initiating the Offline Update Process: 4](#_Toc177314548)

[5.2. Completing the Biometric Update Form: 4](#_Toc177314549)

[5.3. Requesting Consent: 5](#_Toc177314550)

[5.4. Collection of Biometric Data: 5](#_Toc177314551)

[5.5. Acknowledgment and Notification: 5](#_Toc177314552)

[5.6. System Processing and Data Handling: 5](#_Toc177314553)

[5.7. Error Handling and Security Measures: 6](#_Toc177314554)

[5.8. Logging and Audit: 6](#_Toc177314555)

[6. Visualisation 7](#_Toc177314556)

[7. Rationalisation 8](#_Toc177314557)

[8. References 9](#_Toc177314558)

# 1. Purpose

This SOP outlines the standardised procedure for users to update their biometric data offline within the Digital Identity (DID) system. It ensures secure and accurate updates 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

**API**: Application Programming Interface

**HTTPS**: Hyper Text Transfer Protocol Secure

# 3. Application

## 3.1 Ownership and Stakeholders

### 3.1.1 Digital Identity Service Providers (DISPs)

* **Ownership**: Oversee the biometric update process.
* **Responsibilities**: Ensure secure and compliant updates to biometric data.

### 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 updating their biometric data for their DID accounts.
* **Usage**: Provide updated biometric data 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 biometric update process securely.
* Technological infrastructure meets current security standards.

## 4.2 Constraints

* The biometric update 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 Offline Update Process:**

* **Claimant/Subscriber Action:**
  + The process begins with the claimant visiting the designated DID enrollment center or the appropriate offline verification office.
  + The claimant or their representative provides the Unique Identification Number (UIN) and other necessary identity verification documents to the onsite personnel.

## **5.2. Completing the Biometric Update Form:**

* **Claimant/Subscriber Action:**
  + The claimant, with assistance if necessary, completes a biometric update form, specifying which biometric data (fingerprint, iris, facial) needs to be updated.
  + The claimant must state the reason for updating the biometric data to ensure accurate processing.
* **Parent/Guardian/Introducer Action (if applicable):**
  + If the claimant is underage or requires assistance, a parent, guardian, or authorised introducer helps complete the form.
  + They also provide their UIN and consent to act on behalf of the claimant.

## **5.3. Requesting Consent:**

* **Claimant/Subscriber Action:**
  + The claimant provides explicit consent for collecting and processing their biometric data.
  + Consent must be documented, either through a signed form or a biometric scan acknowledging consent.
* **Output:** Consent form filled and signed or biometric consent captured.

## **5.4. Collection of Biometric Data:**

* **Administrator Action:**
  + The administrator receives the completed biometric update form and verifies the claimant's details.
  + The required biometric data (fingerprint, iris, facial) is then collected using the appropriate biometric capture devices.
* **Output:** Biometric data successfully collected.

## **5.5. Acknowledgment and Notification:**

* **Administrator Action:**
  + After successful collection, the claimant receives an acknowledgment confirming the receipt of their biometric data.
  + A confirmation notification is sent to the claimant’s registered contact details (email/SMS), verifying that the biometric update request has been initiated.
* **Output:** Acknowledgment and notification sent to the claimant.

## **5.6. System Processing and Data Handling:**

* **Public Network Systems (Client) Action:**
  + The system masks and encrypts the collected biometric data and claimant details for secure transmission.
  + Data is sent through secure channels (API/HTTPS) to prevent unauthorised access during transfer.
* **Private Network Systems (Server) Action:**
  + Upon receipt, the server checks if the claimant's details are in the user database.
  + The system deactivates old biometric authenticators related to the claimant to prevent misuse.
  + New biometric data is updated in the claimant's account, and the new authenticator is activated.
  + If the data matches successfully and the update is completed, a success notification is generated.

## **5.7. Error Handling and Security Measures:**

* **System Action:**
  + Exception and error handling routines are in place to manage any discrepancies or issues encountered during the process.
  + If the biometric update fails or requires more than three retries, the process is terminated, and the claimant’s account is locked for 24 hours as a security measure to prevent unauthorised access.

## **5.8. Logging and Audit:**

* **System Action:**
  + The system logs the entire update process, including user interactions, errors encountered, and final status.
  + Logs are securely stored and provide a complete audit trail to ensure transparency and compliance with regulatory standards.
* **Output:** Secure audit trail logs.

# 6. Visualisation

A diagram of a data flow

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.1.D UPDATE OFFLINE BIOMETRICS DATA** | | | | | |
| **Step** | **Description** | **Action** | **Systems Involved** | **Security Measures** | **Standards and References** |
| 1 | Start Offline Process | User initiates the update process at service center | User device, Service Center | Physical security measures | ISO 27001 Information Security Management, eIDAS Trust Services |
| 2 | Fill Out Offline Forms | User fills out forms with biometric data | User Forms | Data confidentiality measures | ISO 27001 Data Protection, GDPR for Personal Data Handling |
| 3 | Document Verification | Service center verifies provided documents | Service Center, Document Verification | Document authentication, manual verification | ISO 27001 Data Integrity, FATF Digital Identity Guidelines |
| 4 | Request Consent for Biometric Data | User consents to biometric data collection | User Consent, Service Center | Consent verification | GDPR Consent Requirements, ISO 27001 User Access Management |
| 5 | Collect Biometric Data | Biometric data (e.g., fingerprints, iris scans) collected | Service Center, Biometric Devices | Biometric data security | ISO 27001 Authentication Controls, NIST SP 800-63 Biometric Authentication Mechanisms |
| 6 | Encrypt and Store Biometric Data | Biometric data encrypted and stored | Database | Encryption, secure data storage | ISO 27001 Cryptography, Emirates ID Data Security Standards |
| 7 | Verify Biometric Data | Cross-check biometric data for accuracy | Service Center, Verification System | Data validation | ISO 27001 Data Integrity, Aadhaar Secure Authentication Practices |
| 8 | Update Biometric Data in User Account | Update user account with new biometric information | User Account Database | Secure data update | ISO 27001 Access Control, NIST SP 800-63 Digital Identity Guidelines |
| 9 | Notification of Biometric Update | Notify user of successful biometric data update | User Device, Notification System | Secure notification delivery | ISO 27001 Communications Security, Sing Pass Notification System |
| 10 | Log Update Process | Log the biometric update process | Security Logs | Audit trails, logging | ISO 27001 Secure Audit Logging, NIST SP 800-53 Security and Privacy Controls |
| 11 | Terminate Process | Process termination if errors persist | Security System | Error handling, account lockout | ISO 27001 Access Control Policies, NIST SP 800-63 Authenticator Management |
| 12 | End Process | Finalise the update process | Service Center | Process completion | ISO 27001 Information Security Management, eIDAS Trust Services |

# 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].