|  |  |  |
| --- | --- | --- |
| **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 ONLINE BIOMETRICS DATA

LM.1.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](#_Toc177314587)

[2. Definitions and Abbreviations 3](#_Toc177314588)

[3. Application 3](#_Toc177314589)

[3.1 Ownership and Stakeholders 3](#_Toc177314590)

[3.1.1 Digital Identity Service Providers (DISPs) 3](#_Toc177314591)

[3.1.2 IT and Security Teams 3](#_Toc177314592)

[3.1.3 Compliance and Legal Departments 3](#_Toc177314593)

[3.2 Users and Beneficiaries 3](#_Toc177314594)

[3.2.1 General Public 3](#_Toc177314595)

[3.2.2 Government Agencies 4](#_Toc177314596)

[3.2.3 Private Sector Companies 4](#_Toc177314597)

[4. Prerequisites 4](#_Toc177314598)

[4.1 Assumptions 4](#_Toc177314599)

[4.2 Constraints 4](#_Toc177314600)

[5. Process Flow - Process and Procedures 4](#_Toc177314601)

[5.1. Initiating the Update Process: 4](#_Toc177314602)

[5.2. Navigating to Biometric Update Request: 4](#_Toc177314603)

[5.3. Filling the Update Request Form: 5](#_Toc177314604)

[5.4. Confirming the Update Request: 5](#_Toc177314605)

[5.5. System Validation and Security Measures: 5](#_Toc177314606)

[5.6. Error Handling and Notifications: 5](#_Toc177314607)

[5.7. Logging and Audit Trail: 6](#_Toc177314608)

[6. Visualisation 7](#_Toc177314609)

[7. Rationalisation 8](#_Toc177314610)

[8. References 9](#_Toc177314611)

# 1. Purpose

This SOP outlines the standardized procedure for users to update their biometric data online within the Digital Identity (DID) system. It ensures secure and accurate updates through proper verification, encryption, and error handling.

# 2. Definitions and Abbreviations

**DID**: Digital Identity

**KM**: Key Manager

**HSM**: Hardware Security Module

**CA**: Certificate Authority

**IDA**: ID Authentication Database

**AC**: Access Control

**OTP**: One-Time Password

**2FA**: Two-Factor Authentication

**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**: Utilize 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 their DID accounts and required 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 Update Process:**

* **Claimant/Subscriber Action:**
  + The claimant begins by visiting the DID portal online.
  + They must ensure their DID account is active (reference: OL.A).
  + The claimant logs in using their username and password (AU.1.B) and performs multi-factor authentication using OTP (AU.2.C) or a memorable secret (AU.1.D).
* **Output:** Successful login to the DID portal.

## **5.2. Navigating to Biometric Update Request:**

* **Claimant/Subscriber Action:**
  + From the homepage, the claimant navigates to Settings -> Account Details -> Request for Biometric Update.
  + If the claimant is below 16 years old, they are redirected to return to the homepage and proceed offline.
* **Output:** Access to biometric update options.

## **5.3. Filling the Update Request Form:**

* **Claimant/Subscriber Action:**
  + The claimant selects the type of biometric data to update, choosing from:
    - Fingerprint
    - Iris
    - Facial
  + They fill out the update form and provide a reason for the update.
* **Output:** Completed biometric update request form.

## **5.4. Confirming the Update Request:**

* **Claimant/Subscriber Action:**
  + The claimant confirms their intent to proceed with the biometric update.
  + If confirmed, the claimant receives a notification of successful biometric update request.
* **System Action:**
  + Acknowledgment for the biometric update is downloaded.
  + The claimant is instructed to proceed offline for biometric data collection.
* **Output:** Biometric update request confirmation and acknowledgment.

## **5.5. System Validation and Security Measures:**

* **System Action (Public Network Systems - Client):**
  + The system masks and encrypts any changes to contact details.
  + Users are warned about the immediate deactivation of authentication for selected biometric types.
* **System Action (Private Network Systems - Server):**
  + The system verifies authentication success using password, 2FA, or other methods.
  + Counters are reset to handle retries.
  + If the selected biometrics already exist, the system marks the status as pending.
  + The relevant biometric authenticators are deactivated to maintain security.
* **Output:** Secure handling and storage of biometric update status.

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

* **System Action:**
  + The system uses exception and error handling procedures to manage any issues.
  + Notification generators alert the claimant to the status of their biometric update request.
  + If errors occur during authentication or if the process encounters more than three retries, the system terminates the process and locks the UIN account for 24 hours to prevent unauthorized access.
* **Output:** Error notifications and account security measures.

## **5.7. Logging and Audit Trail:**

* **System Action (Server):**
  + The system logs all update attempts, successful updates, and failures in secure logs.
  + Logs include timestamps, claimant actions, and any issues encountered.
  + This provides a comprehensive audit trail for compliance and review.
* **Output:** Complete and secure audit trail for biometric data updates.

# 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

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **LM.1.C UPDATE ONLINE BIOMETRICS DATA** | | | | | |
| **Step** | **Description** | **Action** | **Systems Involved** | **Security Measures** | **Standards and References** |
| 1 | Start Online Process | User logs into the portal | User Device, Public Network | Secure HTTPS Connection | ISO 27001 Information Security Management, eIDAS Trust Services |
| 2 | Account Authentication | User authenticates via password and OTP | Authentication Server | Two-Factor Authentication | ISO 27001 Access Control, NIST SP 800-63 Digital Identity Guidelines |
| 3 | Navigate to Update Biometrics | User selects biometric update option | User Device, Web Server | Secure Session Management | ISO 27001 Data Protection, eIDAS Electronic Identification |
| 4 | Fill Online Form for Biometric Update | User fills out the form specifying biometric data | User Device, Web Server | Data Input Validation | ISO 27001 Data Integrity, GDPR Compliance for Biometric Data |
| 5 | Submit Biometric Update Request | User submits the request for biometric update | User Device, Web Server, Database server | Encryption, Secure Data Transmission | ISO 27001 Cryptography, FATF Digital Identity Guidelines |
| 6 | Confirm Biometric Update | User confirms to proceed with the update | User Device, Web Server | Confirmation Protocol, User Consent | GDPR Consent Requirements, ISO 27001 User Access Management |
| 7 | Biometric Data Encryption and Storage | Encrypt and store the new biometric data | Database Server | Data Encryption, Secure Storage | ISO 27001 Cryptography, Emirates ID Data Security Standards |
| 8 | Notification of Update Initiation | User receives notification about update initiation | User Device, Notification System | Secure Notification Delivery | ISO 27001 Communications Security, Sing Pass Notification System |
| 9 | Biometric Data Verification Pending | Status set to pending until verification | Database Server | Status Tracking, Data Integrity | NIST SP 800-63 Digital Identity Guidelines, Estonia ID Secure Channel Communication |
| 10 | Log Update Process | System logs the update process and status | Security System | Logging, Audit Trails | ISO 27001 Secure Audit Logging, NIST SP 800-53 Security and Privacy Controls |
| 11 | End Process | User ends the session or the system logs out | User Device, Web Server | Secure Session Termination | 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].