|  |  |  |
| --- | --- | --- |
| **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 UPDATING ONLINE: PERSONALLY IDENTIFIABLE INFORMATION

LM.1.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](#_Toc177315077)

[2. Definitions and Abbreviations 3](#_Toc177315078)

[3. Application 3](#_Toc177315079)

[3.1 Ownership and Stakeholders 3](#_Toc177315080)

[3.1.1 Digital Identity Service Providers (DISPs) 3](#_Toc177315081)

[3.1.2 IT and Security Teams 3](#_Toc177315082)

[3.1.3 Compliance and Legal Departments 3](#_Toc177315083)

[3.2 Users and Beneficiaries 4](#_Toc177315084)

[3.2.1 General Public 4](#_Toc177315085)

[3.2.2 Government Agencies 4](#_Toc177315086)

[3.2.3 Private Sector Companies 4](#_Toc177315087)

[4. Prerequisites 4](#_Toc177315088)

[4.1 Assumptions 4](#_Toc177315089)

[4.2 Constraints 4](#_Toc177315090)

[5. Process Flow - Process and Procedures 4](#_Toc177315091)

[5.1. Initiating the Update Process: 4](#_Toc177315092)

[5.2. Navigating to Account Settings: 5](#_Toc177315093)

[5.3. Updating Personal Information: 5](#_Toc177315094)

[5.4. System Actions: 5](#_Toc177315095)

[5.5. Notification and Confirmation: 5](#_Toc177315096)

[5.6. Error Handling and Security Measures: 6](#_Toc177315097)

[5.7. Logging and Audit Trail: 6](#_Toc177315098)

[6. Visualisation 7](#_Toc177315099)

[7. Rationalisation 8](#_Toc177315100)

[8. References 9](#_Toc177315101)

# 1. Purpose

This SOP outlines the standardized procedure for users to update their personally identifiable information (PII) 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

**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

**2FA**: Two-Factor Authentication

**API**: Application Programming Interface

**HTTPS**: Hyper Text Transfer Protocol Secure

**SSL/TLS**: Secure Sockets Layer / Transport Layer Security

**IDS**: Intrusion Detection System

**IPS**: Intrusion Prevention System

# 3. Application

## 3.1 Ownership and Stakeholders

### 3.1.1 Digital Identity Service Providers (DISPs)

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

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

## 4.2 Constraints

* The PII 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 starts by visiting the DID portal online.
  + They activate their DID account (reference: OL.A) if not already active.
  + They log in using their username and password (AU.1.B) and proceed with 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 Account Settings:**

* **Claimant/Subscriber Action:**
  + The claimant navigates to the account settings section from the homepage.
  + They select the option to update their personal details, such as contact information or address.
* **Output:** Access to account settings and personal information update options.

## **5.3. Updating Personal Information:**

* **Updating Address:**
  + **Action:** If updating the address, the claimant enters the new address manually and uploads any supporting documents.
  + **Verification:** The system validates the proof of address (POA) (OB.2.A) to ensure compliance and authenticity.
  + **Encryption:** Uploaded documents are masked and encrypted using HTTPS, IDS, IPS, and Honeypot to protect the information.
* **Updating Contact Information:**
  + **Action:** If updating contact information, the claimant can manually enter a new email or phone number.
  + **Multi-user OTP:** The claimant may choose to create a new multi-user OTP (AU.2.B) for added security.
  + **OTP Authentication:** The claimant receives an OTP on their new mobile number and authenticates using it (AU.2.C).
  + **Output:** Updated address or contact details.

## **5.4. System Actions:**

* **Public Network Systems (Client):**
  + The system masks and encrypts the claimant's updated information for secure processing.
  + The system validates the format and size of the uploaded documents.
* **Private Network Systems (Server):**
  + The server checks authentication success for password, 2FA, or additional authentication (AU.1.B, AU.2.C).
  + If the verification of POA fails or is incorrect, the system generates a notification and retries the verification process up to three times.
  + If verification is successful, the updated details are securely stored in the claimant’s UIN account.
* **Output:** Secure storage of updated personal information.

## **5.5. Notification and Confirmation:**

* **System Action (Client and Server):**
  + The system generates notifications for successful updates to the claimant's contact information or address.
  + If the address update is unsuccessful, the claimant is notified to return to the homepage and proceed offline.
  + If contact information updates fail, the system sends a UIN account suspension notification with further contact instructions for support.
* **Output:** Notifications sent to the claimant, confirming updates or providing instructions for failure.

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

* **System Action:**
  + If errors occur during authentication or updates, the system counts retries and provides error notifications.
  + After three unsuccessful retries, the system locks the claimant’s UIN account for 24 hours to prevent unauthorized access.
* **Output:** Account security maintained through strict error handling and retry limits.

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

* **System Action (Server):**
  + The system logs all update attempts, successful updates, and failures in secure logs for auditing purposes.
  + Logs include timestamps, IP addresses, and the nature of the updates for compliance monitoring.
* **Output:** Complete and secure audit trail for all update activities.

# 6. Visualisation

A diagram of a process

Description automatically generated with medium confidence

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.A UPDATING ONLINE: PERSONALLY IDENTIFIABLE INFORMATION** | | | | | |
| **Step** | **Description** | **Action** | **Systems Involved** | **Security Measures** | **Standards and References** |
| 1 | Start Process | User starts updating personal information | User Device, Public Network | Secure HTTPS Connection | ISO 27001 Information Security Management, eIDAS Trust Services |
| 2 | Account Authentication | User logs in using password and OTP | Authentication Server | Two-Factor Authentication (2FA) | ISO 27001 Access Control, NIST SP 800-63 Digital Identity Guidelines |
| 3 | Enter New Details | User enters new address or phone number | User Device, Web Server | Data Input Validation | ISO 27001 Data Protection, GDPR for Personal Data Handling |
| 4 | Validate Proof of Address (POA) | POA is checked to validate new address | Server, Private Network | Encryption, Secure Data Transmission | ISO 27001 Cryptography, FATF Digital Identity Guidelines |
| 5 | Encrypt and Store New Details | New details are encrypted and stored | Database Server | Data Encryption, Access Control | ISO 27001 Cryptography, Emirates ID Data Security Standards |
| 6 | Notification of Update | User receives notification of update success | User Device, Notification System | Secure Notification Delivery | ISO 27001 Communications Security, Sing Pass Notification System |
| 7 | Update Contact Details | User updates additional contact details | Web Server | Data Encryption, Secure Data Input | GDPR Compliance, eIDAS Electronic Identification |
| 8 | Authenticate Changes | Changes are authenticated via OTP | Authentication Server | OTP Verification, Secure Session | NIST SP 800-63 Authentication Mechanisms, ISO 27001 Authentication Controls |
| 9 | Verification and Error Handling | System verifies updates and handles errors | Server | Error Detection, Automated Error Handling | ISO 27001 Event Logging and Monitoring, NIST SP 800-61 Incident Response |
| 10 | Log Update Process | All actions and outcomes are logged | Server | Logging, Audit Trails | ISO 27001 Secure Audit Logging, NIST SP 800-53 Security and Privacy Controls |
| 11 | Terminate Process | Process is terminated if multiple failures | Server | 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].