|  |  |  |
| --- | --- | --- |
| **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 - PERMANENT ACCOUNT DELETION (BY CHOICE)

LM.5.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](#_Toc177314873)

[2. Definitions and Abbreviations 3](#_Toc177314874)

[3. Application 3](#_Toc177314875)

[3.1 Ownership and Stakeholders 3](#_Toc177314876)

[3.1.1 Digital Identity Service Providers (DISPs) 3](#_Toc177314877)

[3.1.2 IT and Security Teams 3](#_Toc177314878)

[3.1.3 Compliance and Legal Departments 3](#_Toc177314879)

[3.2 Users and Beneficiaries 3](#_Toc177314880)

[3.2.1 General Public 3](#_Toc177314881)

[3.2.2 Government Agencies 4](#_Toc177314882)

[3.2.3 Private Sector Companies 4](#_Toc177314883)

[4. Prerequisites 4](#_Toc177314884)

[4.1 Assumptions 4](#_Toc177314885)

[4.2 Constraints 4](#_Toc177314886)

[5. Process Flow - Process and Procedures 4](#_Toc177314887)

[5.1. Account Deletion Request Initiation: 4](#_Toc177314888)

[5.2. Verification of Identity: 4](#_Toc177314889)

[5.3. Submit Account Deletion Request Form: 5](#_Toc177314890)

[5.4. Administrator Review: 5](#_Toc177314891)

[5.5. Account Deletion Process Initiation: 5](#_Toc177314892)

[5.6. Authentication Verification: 5](#_Toc177314893)

[5.7. Revoke Authentication and Delete Data: 5](#_Toc177314894)

[5.8. Notification and Confirmation: 5](#_Toc177314895)

[5.9. Error Handling and Termination: 6](#_Toc177314896)

[6. Visualisation 7](#_Toc177314897)

[7. Rationalisation 8](#_Toc177314898)

[8. References 9](#_Toc177314899)

# 1. Purpose

This SOP details the process for users to permanently delete their digital ID account by choice. It ensures secure and thorough 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

**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 deletion process.
* **Responsibilities**: Ensure secure and compliant deletion of 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 wishing to delete their digital ID account.
* **Usage**: Provide authentication and verification for secure account deletion.

### 3.2.2 Government Agencies

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

### 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 deletion process securely.
* Technological infrastructure meets current security standards.

## 4.2 Constraints

* The deletion 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 Deletion Request Initiation:**

* **Claimant/Subscriber Action:**
  + The process begins with the user visiting the DID portal online or offline. They log in using their UIN (Unique Identification Number) and password.
  + The user navigates to the settings menu, selects "Account", then "Request to Forget Account", and confirms the irreversible account deletion.
* **Output:** Account deletion request initiated.

## **5.2. Verification of Identity:**

* **Claimant/Subscriber Action:**
  + For online requests, users authenticate using one of the following methods: OTP (One-Time Password), PIN, or Memorable Secret. For offline requests, users may authenticate using biometrics such as fingerprint, iris scan, or facial recognition.
* **Output:** Identity verified through selected authentication method.

## **5.3. Submit Account Deletion Request Form:**

* **Claimant/Subscriber Action:**
  + The user fills out a form with UIN, name, DOB (Date of Birth), and address details. This form is either submitted online or taken to a DID/3rd party center for offline processing.
* **Output:** Completed account deletion request form submitted.

## **5.4. Administrator Review:**

* **Administrator Action:**
  + The administrator receives the account deletion request form. They check for the subscriber's account and ensure the request is valid. They explain the deletion process to the subscriber if done offline.
* **Output:** Account deletion request reviewed and validated.

## **5.5. Account Deletion Process Initiation:**

* **Administrator Action:**
  + Upon validation, the administrator initiates the account deletion process. A form is printed with UIN and subscriber details to document the request.
* **Output:** Account deletion process initiated, and request documented.

## **5.6. Authentication Verification:**

* **Private Network Systems (Server) Action:**
  + The server checks if the UIN and details match. If authentication is successful, the server proceeds with the deletion.
* **Output:** Successful authentication and verification of details.

## **5.7. Revoke Authentication and Delete Data:**

* **Private Network Systems (Server) Action:**
  + The system revokes authentication, deactivates authenticators, and deletes all UIN account stored information from the database. This includes removing any access credentials and personal data linked to the account.
* **Output:** Account authentication revoked, authenticators deactivated, and data deleted.

## **5.8. Notification and Confirmation:**

* **Public Network Systems (Client) Action:**
  + Notifications are generated and sent to confirm the deletion. The system logs the process and status. An acknowledgment of account deletion is sent to the registered address of the subscriber.
* **Output:** Deletion confirmation sent, and process status logged.

## **5.9. Error Handling and Termination:**

* **Private Network Systems (Server) Action:**
  + If any issues arise during the process, error handling protocols are activated. The process may terminate if errors are unresolved, with a notification sent to the user indicating the request rejection.
* **Output:** Errors managed, process terminated if needed, and request rejection notification sent.

# 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.5.B PERMANENT ACCOUNT DELETION (BY CHOICE)** | | | | | |
| **Step** | **Description** | **Action** | **Systems Involved** | **Security Measures** | **Standards and References** |
| 1 | Start Process | User initiates account deletion online or offline | User Device, Public Network | Secure HTTPS Connection | ISO 27001 Information Security Management, eIDAS Trust Services |
| 2 | User Authentication | User logs in and authenticates | Authentication Server | Multi-factor authentication | ISO 27001 Access Control, NIST SP 800-63 Digital Identity Guidelines |
| 3 | Confirm Account Deletion | User confirms the irreversible deletion of account | User Device, Server | Consent verification, Secure session management | GDPR Consent Requirements, ISO 27001 User Access Management |
| 4 | Mask & Encrypt Data | Encrypt and mask UIN and authentication details | Server | Data encryption and masking | ISO 27001 Cryptography, Emirates ID Data Security Standards |
| 5 | Notify User | Notify user of the deletion process initiation | Notification System | Secure notification delivery | ISO 27001 Communications Security, Sing Pass Notification System |
| 6 | Deactivate Authenticators | Deactivate user authenticators and credentials | Authentication System | Immediate deactivation of access | ISO 27001 User Access Management, FATF Digital Identity Guidelines |
| 7 | Delete Account Information | Permanently delete account information | Database | Secure data deletion | ISO 27001 Data Protection, NIST SP 800-88 Guidelines for Media Sanitisation |
| 8 | Log Process | Log all actions related to account deletion | Security System | Audit trails, logging | ISO 27001 Secure Audit Logging, NIST SP 800-53 Security and Privacy Controls |
| 9 | End Process | Finalise the account deletion process | System | Secure session termination | ISO 27001 Information Security Management |
| 10 | Send Acknowledgement | Acknowledge account deletion to user's address | Mail System | Secure document handling | ISO 27001 Physical Security, GDPR Compliance for Data Handling |
| 11 | Terminate Process | Lock user account if needed | Authentication System | Account lockout, Error handling | 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].