|  |  |  |
| --- | --- | --- |
| **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 (UPON DEATH)

LM.5.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](#_Toc177314642)

[2. Definitions and Abbreviations 3](#_Toc177314643)

[3. Application 3](#_Toc177314644)

[3.1 Ownership and Stakeholders 3](#_Toc177314645)

[3.1.1 Digital Identity Service Providers (DISPs) 3](#_Toc177314646)

[3.1.2 IT and Security Teams 3](#_Toc177314647)

[3.1.3 Compliance and Legal Departments 3](#_Toc177314648)

[3.2 Users and Beneficiaries 3](#_Toc177314649)

[3.2.1 General Public 3](#_Toc177314650)

[3.2.2 Government Agencies 4](#_Toc177314651)

[3.2.3 Private Sector Companies 4](#_Toc177314652)

[4. Prerequisites 4](#_Toc177314653)

[4.1 Assumptions 4](#_Toc177314654)

[4.2 Constraints 4](#_Toc177314655)

[5. Process Flow - Process and Procedures 4](#_Toc177314656)

[5.1. Initiating the Process: 4](#_Toc177314657)

[5.2. Submission of Details: 4](#_Toc177314658)

[5.3. Verification of Death Certificate: 5](#_Toc177314659)

[5.4. Account Deactivation: 5](#_Toc177314660)

[5.5. Deactivation of UIN Account and Authenticators: 5](#_Toc177314661)

[5.6. Notification and Logging: 5](#_Toc177314662)

[5.7. Error Handling and Process Termination: 5](#_Toc177314663)

[6. Visualisation 7](#_Toc177314664)

[7. Rationalisation 8](#_Toc177314665)

[8. References 9](#_Toc177314666)

# 1. Purpose

This SOP specifies the procedure for deleting a digital ID account upon the account holder’s death, ensuring secure and verified deactivation.

# 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

**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 upon death.

### 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 reporting the death of a subscriber.
* **Usage**: Provide necessary documents and authentication 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

* Informers/Next of kin have access to the 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 informers/next of kin.

# 5. Process Flow - Process and Procedures

## **5.1. Initiating the Process:**

* **Informer/Next of Kin Action:**
  + The process starts with the next of kin or designated informer obtaining a certificate of death with the necessary issuer details.
  + They can initiate the account deletion process either online by visiting the DID portal and clicking on the "Report Death" option or offline by visiting a DID/3rd party account service center.
* **Output:** Account deletion process initiated.

## **5.2. Submission of Details:**

* **Informer/Next of Kin Action:**
  + The informer provides the subscriber's details along with personal contact information.
  + They fill out a death form with the subscriber's details and attach the death certificate. This form is then submitted either online via the DID portal or offline.
* **Output:** Death form and certificate submitted.

## **5.3. Verification of Death Certificate:**

* **Administrator Action:**
  + The administrator uploads the subscriber’s details to the DID portal.
  + They verify and validate the death certificate by liaising with the appropriate issuing authority to confirm its authenticity.
* **Output:** Death certificate uploaded and validated.

## **5.4. Account Deactivation:**

* **Administrator Action:**
  + Once the death certificate is validated, the administrator receives confirmation of account deactivation. If the certificate is invalid or issues arise, a rejection notification is sent to the informer.
* **Output:** Notification of account deactivation or rejection sent.

## **5.5. Deactivation of UIN Account and Authenticators:**

* **Private Network Systems (Server) Action:**
  + The system searches for the subscriber's UIN (Unique Identification Number). If the subscriber is found, their account is deactivated along with all authenticators linked to the UIN.
  + The death certificate is securely stored in the system with encryption and hashing.
* **Output:** UIN account and authenticators deactivated; death certificate stored.

## **5.6. Notification and Logging:**

* **System Action:**
  + The system generates notifications to inform all authenticated verifiers about the deactivation of the subscriber's account.
  + The entire process and status are logged, ensuring a complete record of the actions taken.
* **Output:** Notifications sent; process and status logged.

## **5.7. Error Handling and Process Termination:**

* **System Action:**
  + If any errors or discrepancies occur during the process, exception handling protocols are activated.
  + The process may be terminated if issues cannot be resolved, with a termination process indicating a request rejection and notifying the concerned parties.
* **Output:** Errors managed, and process terminated if necessary, with a request rejection notification.

# 6. Visualisation

A screenshot of a computer screen

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.C PERMANENT ACCOUNT DELETION (UPON DEATH)** | | | | | |
| **Step** | **Description** | **Action** | **Systems Involved** | **Security Measures** | **Standards and References** |
| 1 | Start Process | Initiation of account deletion due to death | User Device, Public Network | Secure HTTPS Connection | ISO 27001 Information Security Management, eIDAS Trust Services |
| 2 | Obtain Death Certificate | Secure a death certificate with issuer details | Service Center, Issuing Authority | Document verification | ISO 27001 Data Protection, GDPR Compliance for Data Handling |
| 3 | Authenticate Request | Verify identity and validate death certificate | Authentication Server | Multi-factor authentication, Document authentication | ISO 27001 Access Control, NIST SP 800-63 Digital Identity Guidelines |
| 4 | Submit Death Notification | Report death through DID Portal | User Device, DID Portal | Secure data submission | ISO 27001 User Access Management, FATF Digital Identity Guidelines |
| 5 | Verify and Validate Certificate | Liaise with issuing authority to verify certificate | Administrative System, Database | Data integrity checks | ISO 27001 Data Integrity, eIDAS Trust Services |
| 6 | Deactivate UIN Account and Authenticators | Suspend all account activities and authenticators | Account Management System | Immediate deactivation of access | ISO 27001 User Access Management, Aadhaar Secure Authentication Practices |
| 7 | Notify Verifiers | Inform all connected verifiers of the deactivation | Notification System | Secure notification delivery | ISO 27001 Communications Security, Sing Pass Notification System |
| 8 | Store Death Certificate in Account | Encrypt and store death certificate in UIN account | Secure Database | Data encryption, Secure storage | ISO 27001 Cryptography, Emirates ID Data Security Standards |
| 9 | Log Process | Record all actions related to the account deletion | Security System | Audit trails, logging | ISO 27001 Secure Audit Logging, NIST SP 800-53 Security and Privacy Controls |
| 10 | End Process | Finalise the deletion process | System | Secure session termination | ISO 27001 Information Security Management |
| 11 | Exception and Error Handling | Manage errors and exceptions during the process | Security System | Error logging and response handling | ISO 27001 Event Management, NIST SP 800-61 Incident Response |
| 12 | Terminate Process | Lock user account permanently | Authentication System | 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].