|  |  |  |
| --- | --- | --- |
| **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 - REPORTING OFFLINE COMPROMISED AUTHENTICATORS

LM.3.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](#_Toc177314432)

[2. Definitions and Abbreviations 3](#_Toc177314433)

[3 Application 3](#_Toc177314434)

[3.1 Ownership and Stakeholders 3](#_Toc177314435)

[3.1.1 Digital Identity Service Providers (DISPs) 3](#_Toc177314436)

[3.1.2 IT and Security Teams 3](#_Toc177314437)

[3.1.3 Compliance and Legal Departments 3](#_Toc177314438)

[3.2 Users and Beneficiaries 3](#_Toc177314439)

[3.2.1 General Public 3](#_Toc177314440)

[3.2.2 Government Agencies 4](#_Toc177314441)

[3.2.3 Private Sector Companies 4](#_Toc177314442)

[4. Prerequisites 4](#_Toc177314443)

[4.1 Assumptions 4](#_Toc177314444)

[4.2 Constraints 4](#_Toc177314445)

[5. Process Flow - Process and Procedures 4](#_Toc177314446)

[5.1. Initiating the Reporting Process: 4](#_Toc177314447)

[5.2. Verification of Identity: 4](#_Toc177314448)

[5.3. Requesting Re-authentication: 5](#_Toc177314449)

[5.4. Setting New Authenticators: 5](#_Toc177314450)

[5.5. System Processing: 5](#_Toc177314451)

[5.6. Notification and Confirmation: 5](#_Toc177314452)

[5.7. Finalising and Logging: 6](#_Toc177314453)

[6. Visualisation 7](#_Toc177314454)

[7. Rationalisation 8](#_Toc177314455)

[8. References 9](#_Toc177314456)

# 1. Purpose

This SOP outlines the standardised procedure for users to report compromised authenticators offline within the Digital Identity (DID) system. It ensures secure and accurate 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

# 3 Application

## 3.1 Ownership and Stakeholders

### 3.1.1 Digital Identity Service Providers (DISPs)

* **Ownership**: Oversee the authenticator reporting process.
* **Responsibilities**: Ensure secure and compliant reporting of compromised authenticators.

### 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 compromised authenticators for their DID accounts.
* **Usage**: Provide updated identity verification 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 reporting process securely.
* Technological infrastructure meets current security standards.

## 4.2 Constraints

* The reporting 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 Reporting Process:**

* **Claimant/Subscriber Action:**
  + The user starts by receiving a notification of potential compromise or noticing unauthorised activity.
  + They proceed to report the issue by visiting a DID (Digital Identity) third-party service center.
  + If the user cannot visit, they may call the DID service provider to report the issue.
* **Output:** System receives a report of a compromised authenticator.

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

* **Administrator Action:**
  + The administrator receives the user’s Universal Identification Number (UIN), name, proof of address (POA), and other details for verification.
  + The administrator confirms the user’s identity to ensure the authenticity of the compromise report.
* **Output:** Identity verification is completed, and the user’s status is updated.

## **5.3. Requesting Re-authentication:**

* **Claimant/Subscriber Action:**
  + The user fills out a request form to reactivate the compromised authenticator.
  + Depending on the compromised method, users may authenticate using one or more of the following:
    - **Password:** The user enters their password to verify their identity.
    - **Biometric Data:** If using biometrics, the user may authenticate using fingerprint, iris, facial recognition, or OTP (One-Time Password).
    - **Memorable Secret:** The user may enter a new memorable secret for authentication purposes.
* **Output:** Re-authentication request is initiated.

## **5.4. Setting New Authenticators:**

* **Claimant/Subscriber Action:**
  + Users are prompted to enter a new password, memorable secret, or PIN as part of the re-authentication process.
  + New authenticator details are entered twice for confirmation to avoid errors.
  + The system encrypts these new authenticator details for security.
* **Output:** New authenticators are set and encrypted.

## **5.5. System Processing:**

* **System Action:**
  + The system processes the re-authentication request and checks the new details against existing records.
  + The authenticator status is updated in the system’s account records.
  + If authenticator details do not match or verification fails, the system triggers exception and error handling protocols.
* **Output:** Authenticator status is updated, and error handling is initiated if necessary.

## **5.6. Notification and Confirmation:**

* **System Action:**
  + The system generates a notification to inform the user of the status of their authenticator update (success or failure).
  + If successful, the system logs the process and status, updating the user’s account records.
* **Output:** User is notified of the authenticator update status.

## **5.7. Finalising and Logging:**

* **System Action:**
  + The system ensures all steps are logged for auditing and security purposes.
  + If multiple failed attempts occur, the system locks the user’s account for 24 hours to prevent unauthorised access.
* **Output:** Logs are finalised, and the process is terminated with account security ensured.

# 6. Visualisation

A diagram of a flowchart

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.3.B REPORTING OFFLINE COMPROMISED AUTHENTICATORS** | | | | | |
| **Step** | **Description** | **Action** | **Systems Involved** | **Security Measures** | **Standards and References** |
| 1 | Start Offline Process | User initiates the report at a service center | User, Service Center | Physical security measures | ISO 27001 Information Security Management, eIDAS Trust Services |
| 2 | Authenticate Identity | Verify user identity using alternative authenticators | Service Center | Multi-factor authentication | ISO 27001 Access Control, NIST SP 800-63 Digital Identity Guidelines |
| 3 | Fill Out Compromise Form | User fills out form detailing the compromise | Service Center | Data confidentiality measures | ISO 27001 Data Protection, GDPR for Personal Data Handling |
| 4 | Verify Form and Request Details | Service agent verifies the form and details | Service Center | Manual verification, Document authentication | ISO 27001 Data Integrity, FATF Digital Identity Guidelines |
| 5 | Deactivate Compromised Authenticator | Systematically deactivate the compromised authenticator | Database | Immediate deactivation of access | ISO 27001 User Access Management, Aadhaar Secure Authentication Practices |
| 6 | Generate New OTP | New OTP generated for user | Authentication System | Secure generation and transmission | ISO 27001 Cryptography, FATF Digital Identity Guidelines |
| 7 | Update Contact Details | Update user's contact details if necessary | Service Center | Verification of user input, Data encryption | GDPR Compliance, ISO 27001 Data Integrity |
| 8 | Encrypt and Store New Authenticators | Encrypt and store new authentication details | Database | Data Encryption, Secure storage | ISO 27001 Cryptography, Emirates ID Data Security Standards |
| 9 | Notify User of Changes | Notify user of the changes and new authenticator | User, Notification System | Secure Notification Delivery | ISO 27001 Communications Security, Sing Pass Notification System |
| 10 | Reactivate Account | Reactivate user's account with new details | Authentication System | Account reactivation protocol | ISO 27001 Authentication Controls, Estonia ID Secure Authentication Practices |
| 11 | Log Update Process | Log the entire process for auditing | Security System | Audit trails, logging | ISO 27001 Secure Audit Logging, NIST SP 800-53 Security and Privacy Controls |
| 12 | Terminate Process if Multiple Failures | Lock user account if multiple authentication failures occur | Authentication System | Account lockout, Error handling | ISO 27001 Access Control Policies, NIST SP 800-63 Authenticator Management |
| 13 | End Process | Finalise the process and log out | Service Center | Secure session termination | ISO 27001 Information Security 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].