|  |  |  |
| --- | --- | --- |
| **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 ONLINE COMPROMISED AUTHENTICATORS

LM.3.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](#_Toc177314769)

[2. Definitions and Abbreviations 3](#_Toc177314770)

[3. Application 3](#_Toc177314771)

[3.1 Ownership and Stakeholders 3](#_Toc177314772)

[3.1.1 Digital Identity Service Providers (DISPs) 3](#_Toc177314773)

[3.1.2 IT and Security Teams 3](#_Toc177314774)

[3.1.3 Compliance and Legal Departments 3](#_Toc177314775)

[3.2 Users and Beneficiaries 3](#_Toc177314776)

[3.2.1 General Public 3](#_Toc177314777)

[3.2.2 Government Agencies 4](#_Toc177314778)

[3.2.3 Private Sector Companies 4](#_Toc177314779)

[4. Prerequisites 4](#_Toc177314780)

[4.1 Assumptions 4](#_Toc177314781)

[4.2 Constraints 4](#_Toc177314782)

[5. Process Flow - Process and Procedures 4](#_Toc177314783)

[5.1. Initiating the Reporting Process: 4](#_Toc177314784)

[5.2. Authentication Verification: 4](#_Toc177314785)

[5.3. Authentication Reset Options: 5](#_Toc177314786)

[5.4. Updating Contact Information: 5](#_Toc177314787)

[5.5. Administrative Review and Action: 5](#_Toc177314788)

[5.6. Security Checks and Logging: 5](#_Toc177314789)

[5.7. Notifying the User: 5](#_Toc177314790)

[5.8. Error Handling and Account Lockout: 6](#_Toc177314791)

[5.9. Final Logging and Termination: 6](#_Toc177314792)

[6. Visualisation 7](#_Toc177314793)

[7. Rationalisation 8](#_Toc177314794)

[8. References 9](#_Toc177314795)

# 1. Purpose

This SOP outlines the standardized procedure for users to report compromised authenticators online 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

**HTTPS**: Hyper Text Transfer Protocol Secure

# 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**: 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 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 begins by receiving an authentication notification, potentially indicating suspicious activity. They visit the DID portal to report the compromised authenticator.
* **Output:** System records the initial report of a compromised authenticator.

## **5.2. Authentication Verification:**

* **Claimant/Subscriber Action:**
  + The user logs into the DID portal using recognized authenticators such as password, OTP, memorable secret, or token.
  + If login fails or if the user does not recognize the activity, they proceed to reset their authenticators.
* **Output:** Successful login or initiation of the authenticator reset process.

## **5.3. Authentication Reset Options:**

* **Claimant/Subscriber Action:**
  + Depending on the compromised method, users can reset passwords, update OTP, or create new memorable secrets. If biometric authenticator is compromised, the process moves offline.
* **Output:** The system initiates the selected reset process and deactivates compromised authenticators.

## **5.4. Updating Contact Information:**

* **Claimant/Subscriber Action:**
  + Users update their contact details (email, phone) if necessary to ensure future security alerts and authenticator updates are communicated correctly.
* **Output:** System stores updated contact details and confirms the update with the user.

## **5.5. Administrative Review and Action:**

* **Administrator Action:**
  + Administrators receive notification of the compromised authenticator report and validate the user's identity and the authenticity of the report.
  + If necessary, the administrator generates a new temporary password (TTP) and deactivates compromised authenticators to prevent unauthorized access.
* **Output:** Administrator's actions are recorded, and TTP is provided to the user.

## **5.6. Security Checks and Logging:**

* **System Action:**
  + The system conducts security checks, encrypts authentication data, and verifies the user's identity against stored data.
  + It logs all actions and events for audit purposes, ensuring transparency and traceability.
* **Output:** Authentication status is updated, and logs are created.

## **5.7. Notifying the User:**

* **System Action:**
  + Once the new authenticators are set, the system notifies the user through their registered contact method (email/SMS) of the successful update.
  + **Output:** User receives notification confirming the new authenticator settings.

## **5.8. Error Handling and Account Lockout:**

* **System Action:**
  + If authentication fails multiple times, the system triggers error handling protocols and locks the user's account for a specified period to prevent further unauthorized access.
* **Output:** Error notifications are generated, and the account status is updated as needed.

## **5.9. Final Logging and Termination:**

* **System Action:**
  + All processes and updates are logged. The system ensures that all compromised authenticators are deactivated and that the user's account is secure.
* **Output:** Final status of the account is logged, and the process is terminated with the account secured.

# 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.3.A REPORTING ONLINE COMPROMISED AUTHENTICATORS** | | | | | |
| **Step** | **Description** | **Action** | **Systems Involved** | **Security Measures** | **Standards and References** |
| 1 | Start Process | User initiates the report online | User Device, Public Network | Secure HTTPS Connection | ISO 27001 Information Security Management, eIDAS Trust Services |
| 2 | Authenticate User | User logs in using password and OTP | Authentication Server | Two-Factor Authentication | ISO 27001 Access Control, NIST SP 800-63 Digital Identity Guidelines |
| 3 | Notify Loss of Authenticator | User reports the compromised authenticator | Web Server | Secure Session Management | ISO 27001 Data Protection, eIDAS Electronic Identification |
| 4 | Deactivate Compromised Authenticator | System deactivates the authenticator | Server | Immediate deactivation of access | ISO 27001 User Access Management, FATF Digital Identity Guidelines |
| 5 | Generate New Authentication Details | System generates new password or OTP | Server | Secure password generation and transmission | ISO 27001 Cryptography, NIST SP 800-63 Authentication Mechanisms |
| 6 | Update Contact Details | User updates email or phone number if necessary | Web Server | Data Encryption, Verification of user input | GDPR Compliance, ISO 27001 Data Protection |
| 7 | Encrypt and Store New Authenticators | New authentication details encrypted and stored | Database | Data Encryption, Secure storage | ISO 27001 Cryptography, Emirates ID Data Security Standards |
| 8 | Notify User of Changes | User receives notification of changes | User Device, Notification System | Secure Notification Delivery | ISO 27001 Communications Security, Sing Pass Notification System |
| 9 | Reactivate Account | User's account is reactivated with new details | Server | Account reactivation protocol | ISO 27001 Authentication Controls, Aadhaar Secure Authentication Practices |
| 10 | Log Process | Log all actions related to the security incident | Security System | Logging, Audit Trails | ISO 27001 Secure Audit Logging, NIST SP 800-53 Security and Privacy Controls |
| 11 | End Process | Finalize the reporting and updating process | Server | Secure session termination | ISO 27001 Information Security Management |
| 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 |

# 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].