Standard Operating Procedure - REPORTING ONLINE COMPROMISED AUTHENTICATORS

LM.3.A

**Version Control**

|  |  |  |
| --- | --- | --- |
| Version | Date | Changes Made |
|  |  |  |
|  |  |  |
|  |  |  |

**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](#_Toc176729651)

[2. Definitions and Abbreviations 3](#_Toc176729652)

[3. Application 3](#_Toc176729653)

[3.1 Ownership and Stakeholders 3](#_Toc176729654)

[3.1.1 Digital Identity Service Providers (DISPs) 3](#_Toc176729655)

[3.1.2 IT and Security Teams 3](#_Toc176729656)

[3.1.3 Compliance and Legal Departments 3](#_Toc176729657)

[3.2 Users and Beneficiaries 4](#_Toc176729658)

[3.2.1 General Public 4](#_Toc176729659)

[3.2.2 Government Agencies 4](#_Toc176729660)

[3.2.3 Private Sector Companies 4](#_Toc176729661)

[4. Prerequisites 4](#_Toc176729662)

[4.1 Assumptions 4](#_Toc176729663)

[4.2 Constraints 4](#_Toc176729664)

[5. Process Flow - Process and Procedures 4](#_Toc176729665)

[5.1. Initiating the Reporting Process: 4](#_Toc176729666)

[5.2. Authentication Verification: 4](#_Toc176729667)

[5.3. Authentication Reset Options: 5](#_Toc176729668)

[5.4. Updating Contact Information: 5](#_Toc176729669)

[5.5. Administrative Review and Action: 5](#_Toc176729670)

[5.6. Security Checks and Logging: 5](#_Toc176729671)

[5.7. Notifying the User: 5](#_Toc176729672)

[5.8. Error Handling and Account Lockout: 6](#_Toc176729673)

[5.9. Final Logging and Termination: 6](#_Toc176729674)

[6. Resources 7](#_Toc176729675)

[6.1 Visualisation 7](#_Toc176729676)

[6.2 Rationalisation 8](#_Toc176729677)

[7. References 9](#_Toc176729678)

# 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.