STANDARD OPERATING PROCEDURE- BINDING AUTHENTICATORS TO USER IDENTIFICATION NUMBER

OB.4.B

**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](#_Toc177282490)

[2. Definitions and Abbreviations 3](#_Toc177282491)

[3. Application 3](#_Toc177282492)

[3.1 Ownership and Stakeholders 3](#_Toc177282493)

[3.1.1 Digital Identity Service Providers (DISPs) 3](#_Toc177282494)

[3.1.2 IT and Security Teams 3](#_Toc177282495)

[3.1.3 Compliance and Legal Departments 3](#_Toc177282496)

[3.2 Users and Beneficiaries 3](#_Toc177282497)

[3.2.1 General Public 3](#_Toc177282498)

[3.1.2 Government Agencies 3](#_Toc177282499)

[3.1.3 Private Sector Companies 4](#_Toc177282500)

[4. Prerequisites 4](#_Toc177282501)

[4.1 Assumptions 4](#_Toc177282502)

[4.2 Constraints 4](#_Toc177282503)

[5 Process & Procedures 4](#_Toc177282504)

[5.1 Receive New DID Account Details 4](#_Toc177282505)

[5.2 Bind and Activate Authenticators 4](#_Toc177282506)

[5.3 Handle Notifications and Logging 4](#_Toc177282507)

[5.4 Manage Exceptions and Error Handling 4](#_Toc177282508)

[6. Resources 5](#_Toc177282509)

[6.1 Visualisation 5](#_Toc177282510)

# 1. Purpose

This SOP outlines the standardised procedure for binding authenticators to the Unique Identification Number (UIN) within the Digital Identity (DID) system. It ensures secure binding of various authenticators like OTP, facial biometric, fingerprint biometric, and iris biometric data to enhance account security and compliance.

# 2. Definitions and Abbreviations

**DID**: Digital Identity

**KM**: Key Manager

**HSM**: Hardware Security Module

**CA**: Certificate Authority

**IDA**: ID Authentication Database

**OTP**: One-Time Password

# 3. Application

## 3.1 Ownership and Stakeholders

### 3.1.1 Digital Identity Service Providers (DISPs)

* **Ownership:** Oversee the authenticator binding process.
* **Responsibilities:** Ensure secure and compliant binding of 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 whose DID accounts require authenticators.
* **Usage:** Provide biometric and OTP data for enhanced security.

### 3.1.2 Government Agencies

* **Users:** Agencies requiring enhanced security for verified identities.
* **Usage:** Utilise secured identities for service delivery.

### 3.1.3 Private Sector Companies

* **Users:** Businesses requiring high-security identity verification.
* **Usage:** Use secured identities for compliance and verification purposes.

# 4. Prerequisites

## 4.1 Assumptions

* Administrators are trained to handle the binding process securely.
* Technological infrastructure meets current security standards.
* New DID account details are accurately received and verified.

## 4.2 Constraints

* The binding process may be affected by system downtimes or regulatory changes.
* Secure devices and internet access are required for administrators.

# 5 Process & Procedures

## **5.1 Receive New DID Account Details**

* **Action**: The administrator receives new DID account details with UIN.
* **Output**: New DID account details are verified.

## **5.2 Bind and Activate Authenticators**

* **Action**: Bind and activate authenticators (e.g., email OTP, phone OTP, facial biometric, fingerprint biometric, iris biometric) to the UIN.
* **Output**: Successful binding and activation of authenticators.

## **5.3 Handle Notifications and Logging**

* **Action**: Generate and send success notifications upon successful binding of authenticators.
* **Output**: Notifications sent and process status logged in the IDA.

## **5.4 Manage Exceptions and Error Handling**

* **Action**: Handle exceptions and errors in the binding process; reset counters and retry if necessary.
* **Output**: Error handled or process terminated if retries exceed the limit.

# 6. Visualisation

A diagram of a system

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.