|  |  |  |
| --- | --- | --- |
| **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- BINDING AUTHENTICATORS TO USER IDENTIFICATION NUMBER

OB.4.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](#_Toc177311671)

[2. Definitions and Abbreviations 3](#_Toc177311672)

[3. Application 3](#_Toc177311673)

[3.1 Ownership and Stakeholders 3](#_Toc177311674)

[3.1.1 Digital Identity Service Providers (DISPs) 3](#_Toc177311675)

[3.1.2 IT and Security Teams 3](#_Toc177311676)

[3.1.3 Compliance and Legal Departments 3](#_Toc177311677)

[3.2 Users and Beneficiaries 3](#_Toc177311678)

[3.2.1 General Public 3](#_Toc177311679)

[3.1.2 Government Agencies 3](#_Toc177311680)

[3.1.3 Private Sector Companies 4](#_Toc177311681)

[4. Prerequisites 4](#_Toc177311682)

[4.1 Assumptions 4](#_Toc177311683)

[4.2 Constraints 4](#_Toc177311684)

[5 Process & Procedures 4](#_Toc177311685)

[5.1 Receive New DID Account Details 4](#_Toc177311686)

[5.2 Bind and Activate Authenticators 4](#_Toc177311687)

[5.3 Handle Notifications and Logging 4](#_Toc177311688)

[5.4 Manage Exceptions and Error Handling 4](#_Toc177311689)

[6. Visualisation 5](#_Toc177311690)

[7. Rationalisation 6](#_Toc177311691)

[8. References 6](#_Toc177311692)

# 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.

# 7. Rationalisation

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **OB.4.B BINDING AUTHENTICATORS TO USER IDENTIFICATION NUMBER** | | | | | |
| Step | Description | Action | Systems Involved | Security Measures | Standards and References |
| 1. Start Process | Begin the binding process online. | Administrator initiates the binding of authenticators to UIN. | Public Network Systems Client | Secure access and data transmission. | ISO/IEC 27001, eIDAS for digital transactions |
| 2. Bind Authenticators | Bind biometric and OTP authenticators to the user's account. | Bind phone OTP, facial biometric, fingerprint biometric, and iris biometric data to the UIN. | Public/Private Network Systems | Encryption and secure handling of biometric data and OTPs. | ISO/IEC 27001 for data security, NIST Digital Identity Guidelines |
| 3. Notify Success | Inform the user of successful binding. | Generate and send success notification upon successful binding of authenticators. | Notification Generator | Secure notification delivery. | GDPR for data protection, ISO/IEC 27001 for secure communications |
| 4. Error Handling | Manage any errors in the binding process. | Handle exceptions and errors; reset counters and retry if necessary. | Private Network Systems Server | Robust error handling and resolution mechanisms. | ISO/IEC 27001 for incident and error management |
| 5. Update and Log Status | Update the system with binding status and log the process. | Store authenticator binding status in the user's DID account and log all actions. | Private Network Systems Server, IDA | Logging for audit and compliance, secure data storage. | ISO/IEC 27001 for maintaining secure audit logs; eIDAS for reliable electronic records |

# 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].