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

*Trustworthy Digital Identity Group*

*Bill & Melinda Gates Foundation*

STANDARD OPERATING PROCEDURE CREATING NEW DIGITAL ID ACCOUNT

OB.4.A - WITH RATIONALISATION

**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](#_Toc176723917)

[2. Definitions and Abbreviations 3](#_Toc176723918)

[3. Application 3](#_Toc176723919)

[3.1 Ownership and Stakeholders 3](#_Toc176723920)

[3.1.1 Digital Identity Service Providers (DISPs) 3](#_Toc176723921)

[3.1.2 IT and Security Teams 3](#_Toc176723922)

[3.1.3 Compliance and Legal Departments 3](#_Toc176723923)

[3.2 Users and Beneficiaries 4](#_Toc176723924)

[3.2.1 General Public 4](#_Toc176723925)

[3.1.2 Government Agencies 4](#_Toc176723926)

[3.1.3 Private Sector Companies 4](#_Toc176723927)

[4. Prerequisites 4](#_Toc176723928)

[4.1 Assumptions and Constraints 4](#_Toc176723929)

[4.1.1 Assumptions 4](#_Toc176723930)

[4.1.2 Constraints 4](#_Toc176723931)

[5. Process & Procedures 4](#_Toc176723932)

[5.1 Receive Request and Verify Identity Proofing 4](#_Toc176723933)

[5.2 Initiate UIN Generation and Binding 4](#_Toc176723934)

[5.3 Process Client and Server Side Actions 4](#_Toc176723935)

[5.4 Handle Notifications and Logging 5](#_Toc176723936)

[5.5 Manage Exceptions and Error Handling 5](#_Toc176723937)

[5.6 Security Measures 5](#_Toc176723938)

[6. Resources 6](#_Toc176723939)

[6.1 Visualisation 6](#_Toc176723940)

[6.2 Rationalisation 7](#_Toc176723941)

[7. References 8](#_Toc176723942)

# 1. Purpose

This SOP outlines the standardised procedure for creating a new Digital Identity (DID) account. It ensures all stages of identity proofing are completed accurately and securely, from the initial request to the final account creation.

# 2. Definitions and Abbreviations

**DID**: Digital Identity

**KM**: Key Manager

**HSM**: Hardware Security Module

**CA**: Certificate Authority

**IDA**: ID Authentication Database

**SSL/TLS**: Secure Sockets Layer / Transport Layer Security

**IDS**: Intrusion Detection System

**IPS**: Intrusion Prevention System

# 3. Application

## 3.1 Ownership and Stakeholders

### 3.1.1 Digital Identity Service Providers (DISPs)

* **Ownership:** Oversee the account creation process.
* **Responsibilities:** Ensure secure and compliant account creation.

### 3.1.2 IT and Security Teams

* **Ownership:** Manage technical infrastructure and security protocols.
* **Responsibilities:** Maintain system security and data encryption.

### 3.1.3 Compliance and Legal Departments

* **Ownership:** Ensure legal and regulatory compliance.
* **Responsibilities:** Oversee compliance checks and documentation.

## 3.2 Users and Beneficiaries

### 3.2.1 General Public

* **Users:** Individuals applying for DID accounts.
* **Usage:** Submit applications and documents for identity verification.

### 3.1.2 Government Agencies

* **Users:** Agencies requiring verified identities for services.
* **Usage:** Utilise verified identity information for secure service delivery.

### 3.1.3 Private Sector Companies

* **Users:** Businesses needing verified identities.
* **Usage:** Use verified identities for compliance and security purposes.

# 4. Prerequisites

## 4.1 Assumptions and Constraints

### 4.1.1 Assumptions

* Administrators are trained to handle account creation securely.
* Technological infrastructure meets current security standards.

### 4.1.2 Constraints

* Account creation process may be affected by system downtimes or regulatory changes.
* Applicant must have completed all stages of identity proofing.
* Access to secure devices and internet is required for administrators.

# 5. Process & Procedures

## 5.1 Receive Request and Verify Identity Proofing

* **Action**: The administrator receives a request for a new DID account.
* **Output**: Verify that all stages of identity proofing are completed.

## 5.2 Initiate UIN Generation and Binding

* **Action**: Initiate UIN generation and bind applicant attributes from RID to UIN account.
* **Output**: UIN is generated and bound to the applicant’s RID.

## 5.3 Process Client and Server Side Actions

* **Public Network Systems (Client)**
  + **Action**: Mask and encrypt the RID number and applicant details.
  + **Output**: Encrypted details are sent to the server securely.
* **Private Network Systems (Server)**
  + **Action**:
    - Generate UIN for the applicant if onboarding, validation, and verification are successful.
    - Store applicant information in the UIN account with encryption and hashing.
    - Bind the UIN to the DID account details.
  + **Output**: Successfully created DID account details.

## 5.4 Handle Notifications and Logging

* **Action**:
  + Generate and send notifications for account creation status.
  + Log the process and status in the IDA.
* **Output**:
  + Notifications sent to the applicant.
  + Process status logged securely.

## 5.5 Manage Exceptions and Error Handling

* **Action**:
  + If binding fails, handle exceptions and increment the retry counter.
  + If the retry count exceeds three, terminate the process with an error message.
* **Output**:
  + Error handled appropriately or process terminated if retries exceed limit.

## **5.6 Security Measures**

* **Encryption and Hashing**: All sensitive data is encrypted and hashed.
* **Network Security**: Use of SSL/TLS, firewalls, IDS, and IPS to secure communications.
* **Data Masking**: Applicant details and RID numbers are masked and encrypted.

# 6. Visualisation

A screenshot of a computer

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.