|  |  |  |
| --- | --- | --- |
| **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 CREATING NEW DIGITAL ID ACCOUNT

OB.4.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](#_Toc177311721)

[2. Definitions and Abbreviations 3](#_Toc177311722)

[3. Application 3](#_Toc177311723)

[3.1 Ownership and Stakeholders 3](#_Toc177311724)

[3.1.1 Digital Identity Service Providers (DISPs) 3](#_Toc177311725)

[3.1.2 IT and Security Teams 3](#_Toc177311726)

[3.1.3 Compliance and Legal Departments 3](#_Toc177311727)

[3.2 Users and Beneficiaries 3](#_Toc177311728)

[3.2.1 General Public 3](#_Toc177311729)

[3.1.2 Government Agencies 3](#_Toc177311730)

[3.1.3 Private Sector Companies 4](#_Toc177311731)

[4. Prerequisites 4](#_Toc177311732)

[4.1 Assumptions and Constraints 4](#_Toc177311733)

[4.1.1 Assumptions 4](#_Toc177311734)

[4.1.2 Constraints 4](#_Toc177311735)

[5. Process & Procedures 4](#_Toc177311736)

[5.1 Receive Request and Verify Identity Proofing 4](#_Toc177311737)

[5.2 Initiate UIN Generation and Binding 4](#_Toc177311738)

[5.3 Process Client and Server Side Actions 4](#_Toc177311739)

[5.4 Handle Notifications and Logging 4](#_Toc177311740)

[5.5 Manage Exceptions and Error Handling 5](#_Toc177311741)

[5.6 Security Measures 5](#_Toc177311742)

[6. Visualisation 6](#_Toc177311743)

[7. Rationalisation 7](#_Toc177311744)

[8. References 8](#_Toc177311745)

# 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.

# 7. Rationalisation

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| OB.4.A CREATING NEW DIGITAL ID ACCOUNT | | | | | |
| Step | Description | Action | Systems Involved | Security Measures | Standards and References |
| 1. Start Process | Initiate creation of a new digital ID account online. | Admin receives request for new ID and verifies all stages of identity proofing are completed. | Public Network Systems Client | Secure data handling and transmission. | ISO/IEC 27001 for data security; eIDAS for digital identification processes |
| 2. Generate UIN | Begin generation of a Unique Identification Number. | Initiate UIN generation linked to the applicant's RID. | Public Network Systems Server | Secure generation of unique identifiers. | NIST Digital Identity Guidelines for unique identification management |
| 3. Encrypt RID and UIN | Secure applicant’s RID and newly generated UIN. | Mask and encrypt RID and UIN details before transmission or storage. | Public/Private Network Systems | Encryption to ensure data confidentiality. | ISO/IEC 27001 for encryption; GDPR for data protection |
| 4. Bind Attributes | Link applicant’s attributes from their account to the UIN. | Bind and encrypt DID account details with the UIN. | Private Network Systems Server | Secure attribute binding and encryption. | Aadhar for biometric data handling; ISO/IEC 27001 for secure data management |
| 5. Store and Secure Information | Finalise the creation and secure storage of the digital ID account. | Store all applicant information linked to the UIN securely with encryption and hashing. | Private Network Systems Server, IDA | Use of encryption and hashing to secure data. | ISO/IEC 27001 for secure data storage; Estonia ID, Emirates ID for secure ID management practices |
| 6. Notify Applicant | Confirm creation of the digital ID account or notify of issues. | Generate and send notifications of account creation success or failure. | Notification Generator | Secure notification delivery systems. | SingPass for notification systems; ISO/IEC 27001 for secure communications |

# 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].