Standard Operating Procedure - Validation: Proof of Identity and Proof of Address

OB.2.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](#_Toc177261981)

[2. Definitions and Abbreviations 3](#_Toc177261982)

[3. Application 3](#_Toc177261983)

[3.1 Ownership and Stakeholders 3](#_Toc177261984)

[3.1.1 Digital Identity Service Providers (DISPs) 3](#_Toc177261985)

[3.1.2 IT and Security Teams 3](#_Toc177261986)

[3.1.3 Compliance and Legal Departments 3](#_Toc177261987)

[3.2 Users and Beneficiaries 4](#_Toc177261988)

[3.2.1 General Public 4](#_Toc177261989)

[3.1.2 Government Agencies 4](#_Toc177261990)

[3.1.3 Private Sector Companies 4](#_Toc177261991)

[4. Prerequisites 4](#_Toc177261992)

[4.1 Assumptions and Constraints 4](#_Toc177261993)

[4.1.1 Assumptions 4](#_Toc177261994)

[4.1.2 Constraints 4](#_Toc177261995)

[5. Process & Procedures 5](#_Toc177261996)

[5.1 Initiation and Reception of Application: 5](#_Toc177261997)

[5.2. Document Validation Initiation: 5](#_Toc177261998)

[5.3. Contacting Issuing Authorities: 5](#_Toc177261999)

[5.4. Confirmation of Document Validity: 5](#_Toc177262000)

[5.5. Data Handling and Security: 5](#_Toc177262001)

[5.6. Validation Outcome Handling: 5](#_Toc177262002)

[5.7. Logging and Reporting: 5](#_Toc177262003)

[5.8 Security Measures 5](#_Toc177262004)

[6. Visualisation 6](#_Toc177262005)

# 1. Purpose

The purpose of this SOP is to define the standardised process for validating proof-of-identity (POI) and proof-of-address (POA) documents submitted as part of the Digital Identity (DID) account application process. It ensures that all documents are authenticated, compliant with regulatory standards, and accurately reflect the applicant's identity and residence. This SOP is designed to maintain the integrity and security of the identity verification process, providing clear guidelines for administrators and systems involved in the validation workflow.

# 2. Definitions and Abbreviations

**DID**: Digital Identity

**KM**: Key Manager

**HSM**: Hardware Security Module

**CA**: Certificate Authority

**IDA**: ID Authentication Database

**AC**: Access Control

**API**: Application Programming Interface

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

# 3. Application

## 3.1 Ownership and Stakeholders

### 3.1.1 Digital Identity Service Providers (DISPs)

* **Ownership:** Oversee the validation process for POI and POA documents.
* **Responsibilities:** Ensure the process is secure, compliant, and efficiently managed.

### 3.1.2 IT and Security Teams

* **Ownership:** Manage the technical infrastructure supporting the DID portal's validation processes.
* **Responsibilities:** Ensure the security and availability of the systems used for document verification.

### 3.1.3 Compliance and Legal Departments

* **Ownership:** Ensure the validation process complies with legal and regulatory standards.
* **Responsibilities:** Oversee adherence to relevant laws and standards, including document validation requirements.

## 3.2 Users and Beneficiaries

### 3.2.1 General Public

* **Users:** Individuals submitting applications for DID accounts.
* **Usage:** Provide required POI and POA documents for identity verification.

### 3.1.2 Government Agencies

* **Users:** Agencies requiring verified identities for access to services.
* **Usage:** Depend on validated identity documents to provide secure services.

### 3.1.3 Private Sector Companies

* **Users:** Businesses requiring verified identities for customers or employees.
* **Usage:** Use the validated documents for compliance and verification purposes.

# 4. Prerequisites

This section outlines the necessary conditions and resources before initiating the validation process for POI and POA documents. These prerequisites ensure the SOP functions effectively within the broader SOP framework.

**System Requirements:**

* Access to secure, internet-capable devices for document submission and review.

**Technical Setup:**

* Integration with the DID portal server and backend systems for data storage and validation processes.
* Tools and systems for document scanning, data encryption, and secure communication with issuing authorities.

**Interdependencies:**

* This SOP requires coordination with systems responsible for document scanning, data encryption, and secure communications. It operates in conjunction with security protocol SOPs and system maintenance SOPs to ensure compliance and integrity.

## 4.1 Assumptions and Constraints

## 4.1.1 Assumptions

* Administrators are trained to handle the validation process and use relevant systems securely.
* The technological infrastructure is operational and meets current security standards.

## 4.1.2 Constraints

* Validation may be affected by system downtimes, maintenance, or changes in regulatory requirements.

# 5. Process & Procedures

## 5.1 Initiation and Reception of Application:

* **Action:** The administrator receives the application, including the POI and POA documents and relevant applicant details.
* **Output:** Application and documents are received and ready for validation.

## 5.2. Document Validation Initiation:

* Action: Initiate the validation process by verifying the provided POI/POA against the acceptable document list and checking their completeness.
* Output: Validation process initiated, and document types confirmed.

## 5.3. Contacting Issuing Authorities:

* **Action:** Share document details (e.g., QR codes, reference numbers) with the issuing authorities for validation.
* **Output:** Request for document verification sent to issuing authorities.

## 5.4. Confirmation of Document Validity:

* **Action:** Confirm the validity of the documents with the issuing authorities and note the application status.
* **Output:** Validation status (success or failure) received and recorded.

## 5.5. Data Handling and Security:

* **Action:** Mask and encrypt POI/POA data and validation reports.
* **Output:** Data securely stored and transmitted.

## 5.6. Validation Outcome Handling:

* **Action:** Based on validation outcomes, either proceed with approval or rejection of the application. If documents are valid, update the RID account with approved status. If not, terminate the process with a rejection notification.
* **Output:** Application status updated; applicant notified.

## 5.7. Logging and Reporting:

* **Action:** Log the validation process and outcome in the system for record-keeping and auditing.
* **Output:** Process logged, and reports generated.

## 5.8 Security Measures

* **Encryption and Hashing:** Use encryption and hashing to protect applicant data during storage and transmission.
* **Network Security:** Employ SSL/TLS, firewalls, and other security protocols to safeguard communications with issuing authorities.

# 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.