|  |  |  |
| --- | --- | --- |
| **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 - Validation: Proof of Identity and Proof of Address

OB.2.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](#_Toc177311988)

[2. Definitions and Abbreviations 3](#_Toc177311989)

[3. Application 3](#_Toc177311990)

[3.1 Ownership and Stakeholders 3](#_Toc177311991)

[3.1.1 Digital Identity Service Providers (DISPs) 3](#_Toc177311992)

[3.1.2 IT and Security Teams 3](#_Toc177311993)

[3.1.3 Compliance and Legal Departments 3](#_Toc177311994)

[3.2 Users and Beneficiaries 4](#_Toc177311995)

[3.2.1 General Public 4](#_Toc177311996)

[3.1.2 Government Agencies 4](#_Toc177311997)

[3.1.3 Private Sector Companies 4](#_Toc177311998)

[4. Prerequisites 4](#_Toc177311999)

[4.1 Assumptions and Constraints 4](#_Toc177312000)

[4.1.1 Assumptions 4](#_Toc177312001)

[4.1.2 Constraints 4](#_Toc177312002)

[5. Process & Procedures 5](#_Toc177312003)

[5.1 Initiation and Reception of Application: 5](#_Toc177312004)

[5.2. Document Validation Initiation: 5](#_Toc177312005)

[5.3. Contacting Issuing Authorities: 5](#_Toc177312006)

[5.4. Confirmation of Document Validity: 5](#_Toc177312007)

[5.5. Data Handling and Security: 5](#_Toc177312008)

[5.6. Validation Outcome Handling: 5](#_Toc177312009)

[5.7. Logging and Reporting: 5](#_Toc177312010)

[5.8 Security Measures 5](#_Toc177312011)

[6. Visualisation 6](#_Toc177312012)

[7. Rationalisation 7](#_Toc177312013)

[8. References 8](#_Toc177312014)

# 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.

# 7. Rationalisation

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **OB.2.A VALIDATION OF PROOF-OF-IDENTITY AND PROOF-OF-ADDRESS** | | | | | |
| Step | Description | Action | Systems Involved | Security Measures | Standards and References |
| 1. Start Validation Process | Administrator initiates POI and POA validation. | Start the process online; receive application with POI and POA details. | Administrator Interface, Public Network Systems Client | Secure reception and handling of personal identification documents. | ISO/IEC 27001: Secure handling of sensitive information. |
| 2. Verify Document Authenticity | Confirm the authenticity of the documents. | Verify POI/POA by contacting the issuing authority or using a third-party database. | Public Network Systems Server | Use of SSL/TLS for secure API calls; data masking and encryption. | NIST Digital Identity Guidelines: Verification of identity documents. |
| 3. Document Encryption and Masking | Securely handle document details. | Mask and encrypt POI and POA details before processing. | Public and Private Network Systems | Data encryption and masking to ensure confidentiality and integrity. | GDPR: Data protection standards for handling personal data. |
| 4. Check Document Validity | Evaluate the documents for compliance and validity. | Check if documents are not expired and meet the necessary compliance standards. | Private Network Systems Server | Validation against compliance and regulatory requirements. | eIDAS: Compliance checks for electronic identification. |
| 5. Resolve Exceptions and Errors | Manage any discrepancies or errors. | Handle exceptions or errors in document validation; retry validation if necessary. | Private Network Systems Server | Exception handling and error logging mechanisms. | ISO/IEC 27001: Incident and error management protocols. |
| 6. Update RID and Notify | Update records and notify the applicant. | Update RID account with approved status or terminate the process based on validation outcome. | Private Network Systems Server, Notification Generator | Secure update and notification procedures. | FATF Digital Identity Guidance: Ensuring transparency and accountability in notifications. |
| 7. Log Process and End | Document the validation process and conclude. | Log all actions and outcomes; securely end the process. | IDA | Comprehensive logging for audit and compliance; secure termination of the process. | ISO/IEC 27001: Logging and monitoring requirements; NIST Digital Identity: Secure process closure protocols. |

# 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].