|  |  |  |
| --- | --- | --- |
| **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 Verification – Proof of Address

OB.2.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](#_Toc177311032)

[2. Definitions and Abbreviations 3](#_Toc177311033)

[3. Application 3](#_Toc177311034)

[3.1 Ownership and Stakeholders 3](#_Toc177311035)

[3.1.1 Digital Identity Service Providers (DISPs) 3](#_Toc177311036)

[3.1.2 IT and Security Teams 4](#_Toc177311037)

[3.1.3 Compliance and Legal Departments 4](#_Toc177311038)

[3.2 Users and Beneficiaries 4](#_Toc177311039)

[4. Prerequisites 4](#_Toc177311040)

[4.1 Assumptions and Constraints 5](#_Toc177311041)

[5. Process & Procedures 5](#_Toc177311042)

[5.1. Initiation of POA Verification: 5](#_Toc177311043)

[5.2. Verification of Address Details: 5](#_Toc177311044)

[5.3. Verification of Name on POA: 5](#_Toc177311045)

[5.4. In-Person Verification (If Required): 5](#_Toc177311046)

[5.5. Data Security and Storage: 5](#_Toc177311047)

[5.6. Handling Verification Outcomes: 5](#_Toc177311048)

[5.7. Logging and Documentation: 6](#_Toc177311049)

[5.8 Security Measures 6](#_Toc177311050)

[6. Visualisation 7](#_Toc177311051)

[7. Rationalisation 8](#_Toc177311052)

[8. References 9](#_Toc177311053)

# 1. Purpose

The purpose of this SOP is to establish a standardised process for verifying proof-of-address (POA) documents submitted during the Digital Identity (DID) account application process. The verification ensures that the applicant's residential address is accurate and valid, which is crucial for service eligibility and communication. This SOP outlines the steps to verify address information, ensuring compliance with legal and regulatory standards while maintaining the security and integrity of the verification process.

# 2. Definitions and Abbreviations

**DID**: Digital Identity

**KM**: Key Manager

**KR**: Key Revocation

**HSM**: Hardware Security Module

**CA**: Certificate Authority

**IDA**: ID Authentication Database

**AC**: Access Control

**FTP**: First Time Password

**OTP**: One-Time Password

**2FA**: Two-Factor Authentication

**API**: Application Programming Interface

**HTTPS**: Hyper Text Transfer Protocol Secure

**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 verification process for proof-of-address documents.
* **Responsibilities:** Ensure the process is secure, compliant, and efficiently managed.

### **3.1.2 IT and Security Teams**

* **Ownership:** Manage the technical infrastructure and security protocols for the verification process.
* **Responsibilities:** Maintain system security, manage data encryption, and handle secure storage of POA documents.

### **3.1.3 Compliance and Legal Departments**

* **Ownership:** Ensure the verification process adheres to relevant legal and regulatory standards.
* **Responsibilities:** Oversee compliance checks, documentation, and regulatory adherence.

## **3.2 Users and Beneficiaries**

**General Public**

* **Users:** Individuals submitting POA documents as part of their DID account applications.
* **Usage:** Provide accurate residential address information for verification.

**Government Agencies**

* **Users:** Agencies requiring verified addresses for providing services.
* **Usage:** Utilise verified address information to ensure accurate service delivery and communication.

**Private Sector Companies**

* **Users:** Businesses needing verified addresses for customers or employees.
* **Usage:** Use verified addresses for compliance, security, and communication purposes.

# 4. Prerequisites

This section outlines the necessary conditions and resources before initiating the POA verification process. These prerequisites ensure the effective implementation and functioning of the SOP.

**System Requirements:**

* Access to secure, internet-capable devices for submitting and reviewing POA documents.

**Technical Setup:**

* Integration with the DID portal's server and backend systems for secure data handling and storage.
* Tools for document scanning, data encryption, and secure communication with verification authorities or third parties.

**Interdependencies:**

* Coordination with systems responsible for data encryption, secure communications, and in-person address verification, if required. The process is also dependent on other identity verification procedures for comprehensive validation.

## **4.1 Assumptions and Constraints**

**Assumptions**

* Administrators are trained to handle address documents and verification systems securely.
* The technological infrastructure is operational and meets current security standards.

**Constraints**

* The verification process may be affected by system downtimes, regulatory changes, or limitations in document quality or availability.

# 5. Process & Procedures

## **5.1. Initiation of POA Verification:**

* **Action:** The administrator accesses the application, including POA details, and begins the verification process.
* **Output:** Application and POA documents are received for verification.

## **5.2. Verification of Address Details:**

* **Action:** Verify the address details provided on the POA document against the application form and ensure the address is within an acceptable jurisdiction.
* **Output:** Address verification status updated.

## **5.3. Verification of Name on POA:**

* **Action:** Confirm the applicant's name matches the name on the POA document. If the application is for a dependent, verify the relationship and the name on the POA.
* **Output:** Name match verification status updated.

## **5.4. In-Person Verification (If Required):**

* **Action:** If necessary, initiate in-person verification of the address through officials or a third party. Receive and process the verification report.
* **Output:** In-person verification report received and processed.

## **5.5. Data Security and Storage:**

* **Action:** Mask and encrypt all verification statuses and sensitive data.
* **Output:** Data securely handled and stored.

## **5.6. Handling Verification Outcomes:**

* **Action:** Based on verification results, either approve the address or reject the application. Update the applicant's RID account with the verification status. If unsuccessful, terminate the process and notify the applicant.
* **Output:** Application status updated; applicant notified.

## **5.7. Logging and Documentation:**

* Action: Log the verification process and outcomes for record-keeping and audit purposes.
* **Output:** Verification process documented and stored securely.

## **5.8 Security Measures**

* **Encryption and Hashing:** All sensitive information is encrypted and securely stored.
* **Network Security:** Secure communication channels and firewalls are used to protect data during the verification process.

# 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.2.A VALIDATION OF PROOF-OF-IDENTITY AND PROOF-OF-ADDRESS** | | | | | |
| Step | Description | Action | Systems Involved | Security Measures | Standards and References |
| 1. Start Verification | Initiate the POA verification process. | Admin accesses the account for POA verification. | Public Network Systems Client | Secure access and data transmission. | ISO/IEC 27001, eIDAS for secure electronic identification processes |
| 2. Verify Address Details | Check address details against official records. | Verify the address by matching it with postal or government databases. | Private Network Systems Server | Data validation and integrity checks. | NIST Digital Identity Guidelines, ISO/IEC 27001 for data accuracy and integrity |
| 3. Name Match Verification | Ensure the name on POA matches with applicant's identity. | Check the consistency of the name across documents and databases. | Private Network Systems Server | Consistency checks to prevent identity fraud. | ISO/IEC 27001, FATF Digital Identity Guidance for verification practices |
| 4. Update Verification Status | Record and encrypt the outcome. | Update and encrypt the POA verification status; handle data securely. | Private Network Systems Server | Encryption and secure data handling. | GDPR for data protection, ISO/IEC 27001 for data security |
| 5. Third-Party Verification | If necessary, involve third-party services for additional verification. | Initiate third-party verification for addresses that are ambiguous or lack clarity. | External Verification Services | Secure integration with third-party services. | eIDAS for trusted verification services, ISO/IEC 27001 for third-party data handling |
| 6. Notification and Conclusion | Notify the applicant of the verification results. | Generate notifications based on the verification results; log the process. | Notification Generator, IDA | Secure notification delivery and logging of verification process. | ISO/IEC 27001 for logging and notification security, Estonia ID, Emirates ID standards for digital identity management |

# 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].