|  |  |  |
| --- | --- | --- |
| **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 relationship

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](#_Toc177311938)

[2. Definitions and Abbreviations 3](#_Toc177311939)

[3. Application 3](#_Toc177311940)

[3.1 Ownership and Stakeholders 3](#_Toc177311941)

[3.1.1 Digital Identity Service Providers (DISPs) 3](#_Toc177311942)

[3.1.1 IT and Security Teams 3](#_Toc177311943)

[3.1.1 Compliance and Legal Departments 4](#_Toc177311944)

[3.2 Users and Beneficiaries 4](#_Toc177311945)

[3.2.1 General Public 4](#_Toc177311946)

[3.2.2 Government Agencies 4](#_Toc177311947)

[3.2.3 Private Sector Companies 4](#_Toc177311948)

[4. Prerequisites 4](#_Toc177311949)

[4.1 System Requirements 4](#_Toc177311950)

[4.2 Assumptions and Constraints 5](#_Toc177311951)

[4.2.1 Assumptions 5](#_Toc177311952)

[4.2.2 Constraints 5](#_Toc177311953)

[5. Process & Procedures 5](#_Toc177311954)

[5.1. Reception of Application and Initiation: 5](#_Toc177311955)

[5.2. Document Validation Initiation: 5](#_Toc177311956)

[5.3. Contact Issuing Authority: 5](#_Toc177311957)

[5.4. Confirmation of Document Validity: 5](#_Toc177311958)

[5.5. Data Security Handling: 5](#_Toc177311959)

[5.6. Validation Outcome Handling: 5](#_Toc177311960)

[5.7. Logging and Reporting: 6](#_Toc177311961)

[5.8 Security Measures 6](#_Toc177311962)

[6. Visualisation 7](#_Toc177311963)

[7. Rationalisation 8](#_Toc177311964)

[8. References 9](#_Toc177311965)

# 1. Purpose

The purpose of this SOP is to establish a standardized procedure for validating proof-of-relationship (POR) documents submitted during the Digital Identity (DID) account application process. This validation ensures that the claimed relationship between the applicant and another individual is authentic and accurately documented. The process is essential for applications that involve dependents or require verification of familial or legal relationships, ensuring compliance with legal and regulatory requirements.

# 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 validation process for proof-of-relationship documents.
* **Responsibilities:** Ensure secure and efficient management of the POR validation process.

### 3.1.1 IT and Security Teams

* **Ownership:** Manage the technical infrastructure supporting the validation processes.
* **Responsibilities:** Ensure the security and availability of systems used for POR validation.

### 3.1.1 Compliance and Legal Departments

* **Ownership:** Ensure the validation process adheres to legal and regulatory standards.
* **Responsibilities:** Oversee compliance with relevant laws and standards related to relationship verification.

## 3.2 Users and Beneficiaries

### 3.2.1 General Public

* **Users:** Individuals applying for DID accounts, especially those involving dependents or legal relationships.
* **Usage:** Submit POR documents to verify familial or legal relationships as part of the identity verification process.

### 3.2.2 Government Agencies

* **Users:** Agencies requiring verified relationships for access to services.
* **Usage:** Depend on validated POR documents to provide secure and accurate services.

### 3.2.3 Private Sector Companies

* **Users:** Businesses requiring verification of relationships for various purposes, such as insurance or benefits.
* **Usage:** Use validated POR documents for compliance and verification.

# 4. Prerequisites

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

## 4.1 System Requirements

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

**Technical Setup:**

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

**Interdependencies:**

* This SOP requires coordination with systems responsible for document scanning, encryption, and secure communications. It also depends on other processes, such as identity and address validation, to ensure comprehensive verification.

## 4.2 Assumptions and Constraints

### 4.2.1 Assumptions

* Administrators are trained to handle POR documents and use the relevant systems securely.
* The technological infrastructure is maintained to current standards and is operational.

### 4.2.2 Constraints

* The validation process may be affected by system downtimes or regulatory changes requiring adjustments in the SOP.

# 5. Process & Procedures

## 5.1. Reception of Application and Initiation:

* **Action:** The administrator receives the application along with the RID and applicant details, initiating the POR validation process.
* **Output:** Application and POR documents are received.

## 5.2. Document Validation Initiation:

* **Action:** Check if the POR is listed in the accepted documents list and initiate contact with the issuing authority for validation.
* **Output:** POR validation process started.

## 5.3. Contact Issuing Authority:

* Action: Share document details with the issuing authority to verify the authenticity of the POR.
* **Output:** Verification request sent to the issuing authority.

## 5.4. Confirmation of Document Validity:

* Action: Confirm the validity of the POR with the issuing authority and receive the application status.
* **Output:** POR validity confirmed or denied.

## 5.5. Data Security Handling:

* **Action:** Mask and encrypt POR details and validation reports.
* **Output:** Secure handling of sensitive data.

## 5.6. Validation Outcome Handling:

* Action: Based on validation results, update the RID account with the POR validation status. If validation fails, terminate the process and notify the applicant.
* Output: Application status updated; applicant notified of the outcome.

## 5.7. Logging and Reporting:

* Action: Log the validation process and outcome in the system for record-keeping.
* **Output:** Process logged and documented.

## 5.8 Security Measures

* Encryption and Hashing: All sensitive data, including POR documents and validation reports, are encrypted and securely stored.
* Network Security: Secure channels and firewalls protect data during communication with issuing authorities.

# 6. Visualisation

A diagram of a network

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 RELATIONSHIP** | | | | | |
| **Step** | **Description** | **Action** | **Systems Involved** | **Security Measures** | **Standards and References** |
| 1. Initiate POR Validation | Start the process of validating proof of relationship. | Admin starts online and receives application with POR and applicant details. | Public Network Systems Client | Secure data transmission. | ISO/IEC 27001, eIDAS |
| 2. Verify Document Acceptability | Check if POR document is on the acceptable list. | Verify if the POR is listed as an acceptable document type. | Public Network Systems Client | Data validation against approved lists. | FATF Digital Identity Guidance, NIST Digital Identity |
| 3. Encrypt and Mask Details | Secure applicant's data. | Mask and encrypt the POR and applicant details for processing. | Public Network Systems Client | Encryption and data masking to protect privacy. | ISO/IEC 27001 |
| 4. Confirm Validation with Authority | Contact issuing authority if needed. | Validate POR by contacting the issuing or third-party authority. | Private Network Systems Server | Secure communication channels. | eIDAS for cross-border verification |
| 5. Receive Validation Status | Obtain results from the validation process. | Admin receives notification of POR validation approval or rejection. | Private Network Systems Server | Notification system secure and compliant. | ISO/IEC 27001, GDPR for data protection |
| 6. Error and Exception Handling | Manage validation errors or data mismatches. | Handle exceptions and errors; retry validation if necessary. | Private Network Systems Server | Error logging and management. | ISO/IEC 27001 for incident management |
| 7. Update and Store Validation Outcome | Update database with validation outcome. | If valid, update RID account with POR approved status and store details. | IDA | Secure storage and accurate update of records. | NIST Digital Identity, Aadhar for secure data 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].