|  |  |  |
| --- | --- | --- |
| **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 Verifying Relationship

OB.3.C - 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](#_Toc177310980)

[2. Definitions and Abbreviations 3](#_Toc177310981)

[3. Application 3](#_Toc177310982)

[3.1 Ownership and Stakeholders 3](#_Toc177310983)

[3.1.1 Digital Identity Service Providers (DISPs) 3](#_Toc177310984)

[3.1.2 IT and Security Teams 3](#_Toc177310985)

[3.1.3 Compliance and Legal Departments 4](#_Toc177310986)

[3.2 Users and Beneficiaries 4](#_Toc177310987)

[3.2.1 General Public 4](#_Toc177310988)

[3.1.2 Government Agencies 4](#_Toc177310989)

[3.1.3 Private Sector Companies 4](#_Toc177310990)

[4. Prerequisites 4](#_Toc177310991)

[4.1 Assumptions and Constraints 5](#_Toc177310992)

[4.1.1 Assumptions 5](#_Toc177310993)

[4.1.2 Constraints 5](#_Toc177310994)

[5. Process & Procedures 5](#_Toc177310995)

[5.1. Initiation of POR Verification: 5](#_Toc177310996)

[5.2. Verification of Applicant and Relationship Details: 5](#_Toc177310997)

[5.3. Authentication Using OTP: 5](#_Toc177310998)

[5.4. Contacting Issuing Authorities: 5](#_Toc177310999)

[5.5. Data Security and Encryption: 5](#_Toc177311000)

[5.6. Handling Verification Outcomes: 5](#_Toc177311001)

[5.7. Logging and Documentation: 6](#_Toc177311002)

[5.8. Security Measures 6](#_Toc177311003)

[6. Visualisation 7](#_Toc177311004)

[7. Rationalisation 8](#_Toc177311005)

[8. References 9](#_Toc177311006)

# 1. Purpose

The purpose of this SOP is to outline the standardised procedures for verifying the relationship in proof-of-relationship (POR) documents submitted during the Digital Identity (DID) account application process. This verification process ensures the authenticity and accuracy of claimed relationships between the applicant and another individual, such as a parent, guardian, or introducer. It is crucial for confirming the legitimacy of dependent applications and other relationship-based verifications.

# 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 POR documents.
* **Responsibilities:** Ensure the security, compliance, and efficiency of the POR verification process..

### 3.1.2 IT and Security Teams

* **Ownership:** Manage the technical infrastructure and security protocols involved in the verification process.
* **Responsibilities:** Maintain data security, manage encryption, and ensure the secure storage of verification data

### 3.1.3 Compliance and Legal Departments

* **Ownership:** Ensure that the POR verification process complies with legal and regulatory standards.
* **Responsibilities:** Oversee compliance checks, documentation, and regulatory adherence.

## 3.2 Users and Beneficiaries

### 3.2.1 General Public

* **Users:** Individuals submitting POR documents to verify familial or legal relationships as part of their DID account applications.
* **Usage:** Provide accurate relationship documentation for verification.

### 3.1.2 Government Agencies

* **Users:** Agencies requiring verified relationships for providing services.
* **Usage:** Utilise verified relationship information to provide secure and accurate services.

### 3.1.3 Private Sector Companies

* **Users:** Businesses needing verified relationships for customer or employee verification.
* **Usage:** Use verified relationship documents for compliance and verification purposes.

# 4. Prerequisites

This section outlines the necessary conditions and resources required before initiating the verification of relationship in POR documents. These prerequisites ensure the effective functioning and compliance of the SOP.

**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 verification processes.
* Tools for data encryption, document verification, and secure communication with issuing authorities.

**Interdependencies:**

* The process requires coordination with systems responsible for data security and identity verification. It is interdependent with other verification processes, such as proof-of-identity and proof-of-address verifications.

## 4.1 Assumptions and Constraints

### 4.1.1 Assumptions

* Administrators are trained to handle relationship verification documents and use verification systems securely.

### 4.1.2 Constraints

* The verification process may be limited by the availability of official records, system downtimes, or regulatory changes.

# 5. Process & Procedures

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

* **Action:** The administrator accesses the applicant's RID account and initiates the verification of POR documents.
* **Output:** Application and POR documents are accessed and ready for verification.

## **5.2. Verification of Applicant and Relationship Details:**

* **Action:** Verify the applicant's name and the claimed relationship (parent, guardian, introducer) as per the POR document. Authenticate the relationship type and details.
* **Output:** Verification of name and relationship type initiated.

## **5.3. Authentication Using OTP:**

* **Action:** If required, initiate OTP-based self-verification for the parent/guardian/introducer.
* **Output:** OTP authentication process completed.

## **5.4. Contacting Issuing Authorities:**

* **Action:** Contact the issuing authority to confirm the details provided in the POR document, such as document reference numbers and names.
* **Output:** Confirmation of details received from the issuing authority.

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

* **Action:** Mask and encrypt all verification data, including POR details and OTP authentication status.
* **Output:** Data securely handled and stored.

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

* **Action:** Based on the verification results, update the verification status. If the relationship details are verified, update the RID account with a verified status. If verification fails, update with a failure status and notify the applicant.
* **Output:** Verification 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 securely stored.

## **5.8. Security Measures**

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

# 6. Visualisation

A diagram of a relationship

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 Process | Initiate verification process online. | Access the account for POR validation. | Public Network Systems Client | Secure access and data transmission. | ISO/IEC 27001 for data security |
| 2. Verify Applicant Name | Confirm applicant’s name matches the relationship declaration. | Verify the names in the documents submitted match the declared relationship. | Public/Private Network Systems | Data validation for accuracy. | eIDAS for electronic identification |
| 3. Authentication Using OTP | Authenticate actions using OTP. | Send OTP to verify identity before allowing changes or confirmations. | Public/Private Network Systems | Two-factor authentication for additional security. | ISO/IEC 27001, NIST Digital Identity for authentication standards |
| 4. Verify Document Match | Check document details for consistency with declared information. | Verify that the reference number and name match across documents and databases. | Private Network Systems Server | Data integrity and validation checks. | FATF Digital Identity Guidance for document validation |
| 5. Update Verification Status | Record the outcome of the verification process. | Update the system with the POR verified or failure status. | Private Network Systems Server | Secure logging and status updates. | ISO/IEC 27001 for maintaining secure audit logs |
| 6. Notify and Conclude | End the verification process with notification. | Notify the parties involved of the verification outcome; log the process and status. | Notification Generator, IDA | Secure notification delivery and comprehensive logging. | GDPR for data protection and privacy, eIDAS for digital notification standards |

# 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].