Standard Operating Procedure - Verifying Relationship

OB.3.C

**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](#_Toc177261800)

[2. Definitions and Abbreviations 3](#_Toc177261801)

[3. Application 3](#_Toc177261802)

[3.1 Ownership and Stakeholders 3](#_Toc177261803)

[3.1.1 Digital Identity Service Providers (DISPs) 3](#_Toc177261804)

[3.1.2 IT and Security Teams 3](#_Toc177261805)

[3.1.3 Compliance and Legal Departments 4](#_Toc177261806)

[3.2 Users and Beneficiaries 4](#_Toc177261807)

[3.2.1 General Public 4](#_Toc177261808)

[3.1.2 Government Agencies 4](#_Toc177261809)

[3.1.3 Private Sector Companies 4](#_Toc177261810)

[4. Prerequisites 4](#_Toc177261811)

[4.1 Assumptions and Constraints 5](#_Toc177261812)

[4.1.1 Assumptions 5](#_Toc177261813)

[4.1.2 Constraints 5](#_Toc177261814)

[5. Process & Procedures 5](#_Toc177261815)

[5.1. Initiation of POR Verification: 5](#_Toc177261816)

[5.2. Verification of Applicant and Relationship Details: 5](#_Toc177261817)

[5.3. Authentication Using OTP: 5](#_Toc177261818)

[5.4. Contacting Issuing Authorities: 5](#_Toc177261819)

[5.5. Data Security and Encryption: 5](#_Toc177261820)

[5.6. Handling Verification Outcomes: 5](#_Toc177261821)

[5.7. Logging and Documentation: 6](#_Toc177261822)

[5.8. Security Measures 6](#_Toc177261823)

[6. Visualisation 7](#_Toc177261824)

# 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