Standard Operating Procedure - VERIFICATION: Proof of Identity

OB.3.A - WITH RATIONALISATION

|  |  |  |
| --- | --- | --- |
| **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.*

**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](#_Toc177311891)

[2. Definitions and Abbreviations 3](#_Toc177311892)

[3. Application 3](#_Toc177311893)

[3.1.Ownership and Stakeholders 3](#_Toc177311894)

[3.1.1 Digital Identity Service Providers (DISPs) 3](#_Toc177311895)

[3.1.2 IT and Security Teams 3](#_Toc177311896)

[3.1.3 Compliance and Legal Departments 3](#_Toc177311897)

[3.2 Users and Beneficiaries 4](#_Toc177311898)

[4. Prerequisites 4](#_Toc177311899)

[4.1 Assumptions and Constraints 4](#_Toc177311900)

[5. Process & Procedures 5](#_Toc177311901)

[5.1. Initiation of POI Verification: 5](#_Toc177311902)

[5.2. Verification of Name and Date of Birth: 5](#_Toc177311903)

[5.3. Verification of Photograph: 5](#_Toc177311904)

[5.4. Verification of Signature: 5](#_Toc177311905)

[5.5. Data Security and Storage: 5](#_Toc177311906)

[5.6. Handling Verification Outcomes: 5](#_Toc177311907)

[5.7. Logging and Documentation: 5](#_Toc177311908)

[5.8 Security Measures 6](#_Toc177311909)

[6. Visualisation 7](#_Toc177311910)

[7. Rationalisation 8](#_Toc177311911)

[8. References 9](#_Toc177311912)

# 1. Purpose

The purpose of this SOP is to establish a standardized procedure for the verification of proof-of-identity (POI) documents submitted during the Digital Identity (DID) account application process. This verification ensures the accuracy and authenticity of the applicant's identity details, including name, date of birth, photo, and signature. The SOP aims to provide a secure, compliant, and efficient framework for verifying identity documents, ensuring that all DID accounts are based on verified and validated identity information.

# 2. Definitions and Abbreviations

**DID**: Digital Identity

**KM**: Key Manager

**HSM**: Hardware Security Module

**CA**: Certificate Authority

**IDA**: ID Authentication Database

# 3. Application

## **3.1.Ownership and Stakeholders**

### **3.1.1 Digital Identity Service Providers (DISPs)**

* **Ownership:** Responsible for overseeing the verification process for POI documents.
* **Responsibilities:** Ensure the process is conducted securely, efficiently, and in compliance with applicable regulations.

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

* **Ownership:** Manage the technical infrastructure and security protocols used in the verification process.
* **Responsibilities:** Maintain system security, handle encryption, and manage data storage and access controls.

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

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

## **3.2 Users and Beneficiaries**

**General Public**

* **Users:** Individuals submitting POI documents as part of their DID account applications.
* **Usage:** Provide accurate and complete identity documents for verification.

**Government Agencies**

* **Users:** Agencies requiring verified identities for providing services.
* **Usage:** Utilize verified identity information to ensure secure and accurate service delivery.

**Private Sector Companies**

* **Users:** Businesses needing verified identities for customer or employee verification.
* **Usage:** Use the verified identities for compliance and security purposes.

# 4. Prerequisites

This section outlines the conditions and resources necessary before initiating the POI 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 POI documents.

**Technical Setup:**

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

**Interdependencies:**

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

## **4.1 Assumptions and Constraints**

**Assumptions**

* Administrators are trained to handle identity 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 POI Verification:**

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

## **5.2. Verification of Name and Date of Birth:**

* **Action:** Verify that the POI document contains the correct name and date of birth as provided by the applicant. Update the verification status based on the accuracy of the information.
* **Output:** Name and date of birth verified; status updated.

## **5.3. Verification of Photograph:**

* **Action:** Compare the photo on the POI document with the applicant's submitted photo for facial matching. Update the verification status.
* **Output:** Photo verification completed; status updated.

## **5.4. Verification of Signature:**

* Action: Verify the signature on the POI document against the signature provided by the applicant. Check for consistency in style and form.
* **Output:** Signature verification completed; status updated.

## **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 proceed with the application approval or reject the application. If the POI verification is successful, update the applicant's RID account with the verified 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 diagram of a work flow

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. Initiate Verification | Administrator starts the POI verification process. | Access the account for verification; initiate POI verification. | Public Network Systems Client | Secure access and data transmission. | ISO/IEC 27001 for data security; eIDAS for digital verification processes |
| 2. Verify Applicant Data | Verify the details provided by the applicant. | Check that POI matches claim; verify names and DOB; ensure format consistency. | Public/Private Network Systems | Data validation against predefined formats and standards. | ISO/IEC 27001 for data integrity; GDPR for personal data handling |
| 3. Facial Recognition Match | Use biometric data to verify identity. | Match photo with facial recognition technology; confirm identity visually. | Private Network Systems Server | Use of biometric verification to enhance security. | ISO/IEC 19794-5 for facial recognition standards; GDPR for biometric data protection |
| 4. Signature Verification | Validate signature consistency. | Verify the signature across multiple documents for consistency. | Private Network Systems Server | Signature verification to prevent fraud. | ISO/IEC 19794-7 for biometric data interchange formats |
| 5. Update Verification Status | Record the outcome of the verification process. | Update POI verification status as pending, success, or failure based on results. | Private Network Systems Server | Secure logging and status updates. | ISO/IEC 27001 for maintaining secure audit logs; eIDAS for reliable status updates |
| 6. Handle Exceptions | Manage any discrepancies or errors. | Address exceptions and errors encountered during the verification process. | Error Handling System | Robust error handling and resolution mechanisms. | ISO/IEC 27001 for incident and error 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].