SOP-The Validation of an Applicant’s Identity

|  |  |
| --- | --- |
| SOP #: | A.2 |
| Version: | 1.0 |
| Author(s): | Al Tariq Sheik |

# PURPOSE

The purpose of the validation process is to ensure the authenticity and accuracy of evidence by comparing it against reliable sources. This is essential to confirm that the information matches with independent and dependable data/records. An example of this process is when the admin checks physical identity evidence, such as a driver's license or passport, for any alterations, and verifies that the identification numbers follow standard formats, and the physical and digital security features are valid and intact. Additionally, the admin may query relevant sources to confirm that the information matches. The validation process is crucial to ensure that the evidence provided by the applicant is genuine and can be trusted for making important decisions, such as granting access or privileges.

# SCOPE

This SOP applies to applicants who are 18 years old and above and those who are applying in-person through their parent or guardian. The SOP focuses on the validation of documents submitted by the applicant. It is assumed that the applicant has provided all necessary Minimum Supporting Documents (MSD), such as birth certificates, passports, and driving licenses, for the administrators to validate. The scope of this document is limited to the validation process for MSD submitted by the applicant and does not cover other aspects of identity verification or enrollment.

# DEFINITIONS

**Digital Identity (DID)** – An online personal identity system.

**Standard Operating Procedure (SOP)** – The functions, processes and procedures that should be followed by Applicants, Subscribers, Claimants and Admin.

**Minimum Support Documents (MSD)** – The fundamental documents that can be used to validate and verify an identity, such as birth certificates, driver’s licenses and passports.

**Applicant** – A person who applies for a Digital Identity.

**Admin/Administration** – The staff of the Digital Identity provider, who conducts Onboarding and Identity Lifecycle Management.

**Validation** – The process in which Admin ascertain if the Applicant possesses the identity that they claim.

# PROCESS AND PROCEDURE

A. *The administrator validates the Minimum Supporting Documents.*

1. The administrator validates the Minimum Supporting Documents, for example, the driving license through a public record.
2. The administrator uses the last 8 characters of the driving license number and the 8-character alphanumeric share code.
3. The administrator checks the public record for the applicant's name, date of birth, and the validity of the document. The validation status is updated to either "approve" or "reject" based on the findings.
4. Enhancement for Pseudo-anonymisation:

* Post-validation, identifiable data such as the applicant's name and date of birth used during the check are pseudo-anonymised in the system. This includes replacing direct identifiers with unique codes or identifiers not directly linked to the applicant's personal details.

1. Audit Logging:

* Each validation step and its outcome are logged in a secure, immutable audit trail.
* The log includes details such as the document type, validation method, administrator ID, timestamp, and validation outcome.
* The audit log maintains a reference to the pseudo-identifiers, ensuring the log itself adheres to privacy principles while retaining the integrity and purpose of the audit trail.

B. *If the application is rejected during the validation round, the following steps are taken:*

1. The administrator updates the validation status to "reject".
2. The system sends a notice of the status change to the applicant.
3. The administrator records the applicant's attempt.
4. Rejection Auditing:

* Document the reasons for rejection in the audit log, including any discrepancies found during the validation process.
* Record actions taken by the administrator post-rejection, such as advising the applicant on rectifying issues or additional steps required for re-application.

1. Application of Pseudo-anonymisation in Rejection Process:

* In cases of rejection, ensure that any personal data used to determine the rejection is pseudo-anonymised in subsequent processing or storage. This includes communications to the applicant where identifiable information is minimized and secured.

C. *If the applicant is approved during the validation round, the following steps are taken:*

1. The administrator updates the validation status to "approve".
2. The registration attributes are sent for verification. Please refer to SOP A.3 for the relevant processes and procedures.
3. Approval Auditing:

* Log the approval decision, including the verified attributes and the verification method used.
* Ensure the log captures any conditional approvals or additional checks required before finalizing the registration.

1. Pseudo-anonymisation Post-Approval:

* Upon approval, personal data involved in the validation process, especially that which is stored or logged for auditing purposes, is pseudo-anonymised. This ensures that ongoing processing or analysis maintains the applicant's privacy.
* Details such as verified attributes are associated with pseudo-identifiers in the system to maintain a link to the applicant's digital identity without exposing personal data.

# SOP APPENDICES:

|  |  |  |  |
| --- | --- | --- | --- |
| Revision History: | Version | Effective Date | Description |
|  | 1.0 | 18-04-2023 | First Approval |