SOP-The Verification of an Applicant’s Identity

|  |  |
| --- | --- |
| SOP #: | A.3 |
| Version: | 1.0 |
| Author(s): | Al Tariq Sheik |

# PURPOSE

To ensure that a validated identity corresponds to the individual being identity-proofed, several measures can be taken. For example, service providers (SPs) can require the applicant to submit a mobile phone video or photo along with other liveness checks and compare it with the photos on the identity evidence or the photo on file in the database. To further verify that the identity evidence matches the real-person applicant, an enrolment code can be sent to the validated phone number linked to the identity. The applicant must then provide the enrolment code, confirming that they are a real person in possession and control of the validated phone number. These measures help ensure that the identity being used is legitimate and not being used fraudulently.

# SCOPE

This SOP applies to applicants who are 18 years old and above and have received a One-Time Password (OTP) by post. The SOP is designed to focus on the verification of the applicant's identity by using OTP and registration ID. It is assumed that the applicant has the necessary knowledge to access and use the identity portal for self-verification, as a Minimal Acceptable Functionality. The scope of this document is limited to the verification process for applicants who have received OTP by post and does not cover other methods 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.

**Service Provider (SP)** – Also known as Admin/administrator, the SP conducts Onboarding and Identity Lifecycle Management.

**One Time Password (OTP)** – A password that is generated by Admin and sent to the Subscriber via phone, email or post, which is used for authentication purposes.

**Verification** – The process in which Admin ascertain if the personal attributes of the Applicant are corroborated by more than one supporting document.

# PROCEDURE:

A. *The following are the steps taken by the administrator to verify applicant attributes:*

1. The administrator records the applicant attributes from Minimum Supporting Document (MSD)
2. The administrator enters the share code and the last 8 characters of the driver's license in public record portals (PLP) to validate the information.
3. The administrator checks the applicant attributes against the information obtained to confirm their validation.
4. Audit Procedure with Pseudo-anonymisation:

* Record each verification step, including the type of MSD used, share code entry, and attribute checks, in a secure and immutable audit log.
* Ensure the audit log captures the administrator ID, timestamp, and any discrepancies or issues identified during the verification process.
* Ensure audit logging to explicitly include entries for both denied and granted access requests as part of the verification process. This involves logging every attempt to access the system, whether successful or not, along with the decision (approved or rejected), using pseudo-identifiers instead of direct personal identifiers.
* Implement a procedure to pseudo-anonymise personal identifiers in the audit log post-verification. For instance, replace direct personal identifiers with unique codes that do not reveal the applicant's identity.

B. *If the applicant attributes are verifiable, the following steps are taken:*

1. The administrator sends an OTP (one-time password) to the applicant via postal mail.
2. The applicant uses the digital identity portal to self-verify their identity, using their registration ID and the OTP received.
3. The administrator updates the verified status of the application to 'Approved', if successful.
4. The administrator forwards the application to the 'Enrolment and Binding' stage. (See SOP A.5)
5. Verification Auditing with Pseudo-anonymisation:

* Log the successful verification, including the method (OTP via postal mail), the applicant's self-verification action, and the update to 'Approved' status.
* Log the granting of access, such as successful OTP verification and the approval of the applicant's identity, in the AC system log. Detail the action taken, the basis for granting access, and timestamp this activity, applying pseudo-anonymization to protect personal identifiers.
* Include details of the enrolment and binding stage initiation, ensuring a complete audit trail of the verification process.
* Incorporate pseudo-anonymisation into the verification audit log, ensuring that any personal identifiers are replaced with pseudo-identifiers or anonymized.

C. *If application attributes are not verifiable*:

1. The administrator update verified status of application to ‘Rejected’.
2. The system sends a notice of the status change to the applicant.
3. The administrator records the application attempt.
4. Rejection Auditing with Pseudo-anonymisation:

* Document the reasons for non-verification, including specific attribute discrepancies or failures in validation.
* For each denied access request, such as a failure in attribute verification or OTP mismatch, record the incident in the AC system log. Include the reason for denial, the attempted action, and the time of the attempt.
* Apply pseudo-anonymisation to the rejection audit logs, ensuring that personal data is not directly linked to the reasons for non-verification or the notification process.
* Record the notification sent to the applicant and any recommended next steps for the applicant to rectify the issue.

D. If applicant fails the self-verification process: To Be Clarified

# SOP APPENDICES:

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