SOP-The Verification of an Applicant's Identity

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

1. 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.

2. 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.

3. 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.

4. PROCEDURE:

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

i. The administrator records the applicant attributes from Minimum Supporting Document (MSD)
ii. 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.
iii. The administrator checks the applicant attributes.

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

i. The administrator sends an OTP (one-time password) to the applicant via postal mail.
ii. The applicant uses the digital identity portal to self-verify their identity, using their registration ID and the OTP received.
iii. The administrator updates the verified status of the application to 'Approved', if successful.
iv. The administrator forwards the application to the 'Enrolment and Binding' stage. (See SOP A.5)

C. *If application attributes are not verifiable*:

i. The administrator update verified status of application to ‘Rejected’.
ii. The system sends a notice of the status change to the applicant.
iii. The administrator records the application attempt.

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

5. SOP APPENDICES:

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