SOP- The Creation and Management of a Suitable Authenticator with Ownership Factor - OTPs

SOP #:	B.2
Version:	1.0
Author(s):	Al Tariq Sheik

1. PURPOSE

Authenticators based on "something you have" can include cryptographic keys stored in hardware or software controlled by the subscriber, a One-Time Password (OTP) generated by a hardware device or software OTP generator installed on a digital device such as a mobile phone.

These authenticators ensure secure and effective use of the DID system throughout the entire identity lifecycle, from enrolment to revocation, providing the reliable and accurate identification of the subscriber, preventing unauthorized access, and protecting sensitive personal information. Incorporating these authenticators into the system gives subscribers confidence in their personal information's security and the reliability of their system access.

2. SCOPE

This SOP provides guidelines for generating and authenticating a Subscriber's credentials using an OTP for security and authentication purposes. To initiate the process, a Claimant must supply the Unique Identity Number (UIN) of an existing account. The procedures outlined in this SOP aim to ensure that the authentication process is secure and reliable, protecting sensitive personal information and preventing unauthorized access to Subscriber accounts.

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.
Subscriber – An Applicant who has passed validation and verification, and has been enrolled into the online Digital Identity system. Also, a Claimant who has passed authentication. The Digital Identity account holder.
Claimant – A person who claims to possess an identity and has not yet passed authentication.
Admin/Administration – The staff of the Digital Identity provider, who conducts Onboarding and Identity Lifecycle Management.
Unique Identity Number (UIN) – A unique number that is assigned to subscribers and is used to identity a Digital Identity account.
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.
Enrolment – The process in which an Applicant becomes an online account holder, a Subscriber
Revocation – The process in which a Digital Identity account is removed.

4. PROCESS AND PROCEDURE

A. OTP is generated:

i. The subscriber submits their UIN to the admin.
ii. The admin receives the UIN and checks if it exists in the database.
iii. If the UIN is not found, the admin sends a notification to the subscriber stating that the UIN is incorrect.
iv. If the UIN is found, an OTP is generated by the admin.
v. The OTP is sent to the registered phone of the subscriber.

B. Subscriber authenticates credentials with OTP:

i. The admin sends an OTP to the subscriber's registered phone number or email.
ii. The subscriber receives the OTP and enters it into the portal.
iii. The admin receives the OTP from the subscriber.
iv. The admin verifies the OTP by matching it to the generated OTP.
v. If there is no match, the admin sends a notification of the failure to the subscriber.
vi. If there is a match, the admin sends a confirmation notification to the subscriber via text.

5. SOP APPENDICES

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