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

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

1. PURPOSE

To ensure that digital identity verification is both secure and accurate, it is important to establish well-defined processes and procedures for using fingerprint biometrics as an identity verification method. This includes identifying and documenting the systems and applications that will leverage fingerprint biometrics for identity verification.

In addition, it is essential to provide clear and effective communication to claimants and subscribers about these processes and how their data is collected, stored, and used. This can help promote transparency and trust in the digital identity system while ensuring that fingerprint biometrics are used in a secure and effective manner for identity verification purposes.

2. SCOPE

The purpose of this SOP is to outline the process of biometric authentication using fingerprints for. This SOP provides details on the registration and authentication procedures, as well as educating applicants and subscribers on the fingerprint registration and authentication process. Procedures are also given for acquiring permission from the subscriber to obtain and store their biometric data. The scope of this document is limited to the process of fingerprint-based biometric authentication and does not cover other biometric authentication techniques.

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.
Applicant – A person who applies for a Digital Identity.
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.
Fingerprints – A biometric dataset obtained from the fingerprint of a Subscriber, which is used for authentication purposes.

4. PROCESS AND PROCEDURE

A. Applicant education:

i. Admin provides Applicant with literature detailing how the biometric fingerprint data is captured and stored and their data rights.
ii. Admin allow the Applicant time to read literature.
iii. Admin orally explain the biometric fingerprint data literature.
iv. Admin ask Applicant to sign that they understand the procedure of capturing biometric fingerprint data and how it is stored and their data rights.

B. Obtaining Subscriber Fingerprint biometric data:

i. The admin requests the UIN and Fingerprint biometric data from the claimant.
ii. The claimant provides the UIN and Fingerprint biometric data.
iii. The admin checks if the UIN is in the database.
iv. If the UIN is not found, the admin sends a notification of incorrect UIN to the claimant.
v. If the UIN is found, the fingerprint authentication is compared to the registered fingerprint in jpeg 2000 format.
vi. If the match score is greater than the threshold of 95% for image-to-image match, the admin receives authentication success.
vii. The claimant receives a success status on SMS.

5. SOP APPENDICES

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