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 |

# 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.

# 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.

# 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.

# PROCESS AND PROCEDURE

1. Applicant education:
2. Admin provides Applicant with literature detailing how the biometric fingerprint data is captured, stored, purpose of data collection and their data rights. This literature also outlines the process for subscribers to be informed about any changes in these purposes.
3. Admin allow the Applicant time to read literature.
4. Admin orally explain the biometric fingerprint data literature, emphasizing the potential for changes in data collection purposes and the process for notifying subscribers of such changes.
5. Admin ask Applicant to sign that they understand the procedure of capturing biometric fingerprint data, how it is stored, their data rights, and the process for monitoring and being informed about changes in data collection purposes.
6. Obtaining Subscriber Fingerprint biometric data:
7. The admin requests the UIN and Fingerprint biometric data from the claimant.
8. The claimant provides the UIN and Fingerprint biometric data.
9. The admin checks if the UIN is in the database.
10. If the UIN is not found, the admin sends a notification of incorrect UIN to the claimant.
11. If the UIN is found, the fingerprint authentication is compared to the registered fingerprint in jpeg 2000 format.
12. Logging Fingerprint Authentication Attempts:

* Implement a secure AC logging system that records all fingerprint authentication attempts including date, time, match score and whether the attempt was successful or not.

1. If the match score is greater than the threshold of 95% for image-to-image match, the admin receives authentication success.
2. The claimant receives a success status on SMS.

* Upon a successful fingerprint authentication, in addition to the SMS success status, include a notification that details the authentication attempt, such as the time and location (if available), and instructions on what to do if the subscriber did not initiate this access.

1. User Access to Authentication Logs:

* Provide subscribers with a secure portal where they can review a detailed log of all fingerprint authentication attempts. This portal should allow subscribers to flag any unauthorized attempts and should include instructions for securing their account if needed.

1. Real-Time Alerts for Unsuccessful Attempts:

* For any authentication attempt that fails to meet the threshold (match score), send an immediate alert to the subscriber detailing the attempt. Include a reminder of steps to take if they suspect fraudulent activity.

# SOP APPENDICES

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