SOP-The Creation and Management of a Suitable Authenticator with Knowledge Factor - Passwords

SOP #:	B.1
Version:	1.0
Author(s):	Al Tariq Sheik

1. PURPOSE:

Processes and procedures must be in place for events such as creating and managing passwords securely and reliably. These procedures aim to ensure that the passwords used in the digital identity system are strong, unique, and protected against unauthorized access or theft. By following these procedures, the digital identity system can protect its users' personal and sensitive data and prevent unauthorized access to their accounts. Additionally, these procedures help to ensure that users can easily manage and reset their passwords, if necessary, without compromising the security of their accounts. Listed below are some steps that can be included in a standard operating procedure for strong passwords for digital identities.

To safeguard personal and sensitive data in the DID, it is crucial to have established processes and procedures for creating and managing passwords securely and reliably. These procedures should ensure that the passwords used in the DID system are strong, unique, and protected against unauthorized access or theft. Following these procedures helps to maintain the integrity of the DID system and prevent unauthorized access to user accounts. It also ensures that users can easily manage and reset their passwords without compromising the security of their accounts.

To achieve this goal, this SOP for strong passwords should include several steps. These steps may include educating users on how to create strong passwords, requiring the use of multifactor authentication, enforcing password complexity requirements, regularly checking for compromised passwords, and resetting passwords when necessary. By following these steps, administrators can help to ensure that the digital identity system remains secure and trustworthy for its users.

2. SCOPE

The SOP for creating and managing passwords in the DID system is designed to prioritize security and reliability. It includes comprehensive guidelines for creating strong, unique passwords that will safeguard personal information and prevent unauthorized access to subscriber accounts. Procedures also covers the specific scenario in which a subscriber must use the Forgotten Password module, requiring additional security measures to ensure that the password reset process is secure and that the new password is stored safely. To enhance security, this SOP includes guidelines for the secure storage of subscriber passwords. These guidelines include measures such as password encryption and protection against unauthorized access or theft. By following these guidelines, the digital identity system can maintain the trust and confidence of its subscribers, who can rely on the security of their personal information and the accessibility of the system.

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.
Admin/Administration – The staff of the Digital Identity provider, who conducts Onboarding and Identity Lifecycle Management.
Password – A Subscriber-defined code that is known only to the Subscriber, and is used for authentication purposes.
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.
Subscribers Digital Identity System (SDIS) – The location within the Digital Identity system in which logs of Subscriber actions are made.

4. PROCESS AND PROCEDURE:

A. Establish moderate password complexity:

i. Establish an 8-character length and character mix of upper- and lower-case letters, numbers, and special characters.
ii. In passwords, prohibit the use of personal information, such as a user's name, birthdate, or address.
iii. Prohibit the reuse of previous passwords or easily guessable passwords, such as "password" or "123456".
iv. Require regular password changes, such as every 90 days.
v. Implement password management tools to help Admin store and manage their passwords securely.

B. Enhance password security measures:

i. Implement an OTP authentication for all user accounts to increase security.
ii. Use encryption standard AES-256 to protect passwords and other sensitive data.
iii. Use Argon2id (m=47104, 46 MiB, t=1, p=1) hash algorithms to store passwords securely in the database.

C. Establish a process for resetting passwords if a user forgets their password:

i. Subscriber initiates password reset request through post by sending a written request to the Administrator, providing the following information: Full Name, Registered Address, Registered Mobile Number
ii. The administrator receives the request and verifies the Subscriber's identity by validating the following information: Full Name, Registered Address, Registered Mobile Number
iii. If the Subscriber's identity is verified, the Administrator sends a One-Time Password (OTP) to the Subscriber through the post, which can be used to reset the password.
iv. Subscriber receives the OTP and logs in to the system using their registered credentials.
v. Subscriber navigates to the password reset page and inputs the OTP along with a new password.
vi. Subscriber submits the new password and OTP.
vii. The system validates the OTP and updates the Subscriber's password.
viii. The Administrator records the password reset attempt in the SDIS log.

ix. The Administrator sends an acknowledgement to the Subscriber confirming the password reset.
x. If the Subscriber's identity cannot be verified, the Administrator informs the Subscriber through post that the password reset request cannot be processed.
xi. The Administrator records the unsuccessful password reset attempt in the identity system (log).
xii. If the Subscriber faces any issues with the password reset process, they can contact the Administrator through the SDIS helpline or email for assistance.

5. SOP APPENDICES:

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