SOP- The Expiration and Renewal of an Authenticator During the Lifecycle of a DID Account

SOP #:	C.4
Version:	1.0
Author(s):	Al Tariq Sheik

1. PURPOSE

An authenticator may have an expiration date if it was initially bound to a DID account with a set lifespan. It is crucial to ensure that subscribers can access their DID account after their existing their authenticator is due to expire. Therefore, there must be clear and well-defined processes and procedures in place to guarantee the timely and secure replacement of expiring authenticators.

Administrators are responsible for following these processes and procedures to ensure that subscribers can continue to use their accounts without any disruptions. It is recommended that administrators bind a new authenticator before the existing one expires, thereby ensuring uninterrupted access. Furthermore, administrators must revoke the expiring authenticator to maintain the security and integrity of the subscriber's identity account.

These procedures are designed to ensure the availability of the digital identity system for subscribers and maintain their trust and confidence in the system. By adhering to these guidelines, administrators can facilitate a smooth and seamless user experience, while also enhancing the security and reliability of the DID system.

2. SCOPE

This document outlines guidelines for administrators regarding the issuance, expiration, and replacement of authenticators in the DID system. It is assumed that administrators can issue authenticators with a limited lifespan, which become unusable for authentication after their expiration. Admin may also choose to expire an authenticator when is has been reported as compromised. To ensure the smooth and secure replacement of expiring or compromised authenticators, administrators must follow the same processes and procedures as the initial authenticator binding (as outlined in SOP A.4). Adherence to these guidelines maintains the integrity of the digital identity system, safeguards subscriber trust, and ensures a seamless and secure user experience for reliable identity verification and authentication.

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.
Subscriber Identity Account (SIA) – The unique Digital Identity account belonging to a Subscriber, in which all data (current, upcoming and historic) are contained.
Revocation – The process in which a Digital Identity account is removed.

4. PROCESSES AND PROCEDURES

A. *An issued authenticator expires:*

i. The admin issues an authenticator with a defined service life of 30 days.
ii. The authenticator and its service life are recorded in the server's SIA.
iii. The admin monitors the age of the authenticator.
iv. When the authenticator has reached 30 days of service, the admin terminates it.

B. *Admin bind new authenticator before existing authenticator expires:*

i. The administrator monitors the age of the authenticator.
ii. When the authenticator reaches 30 days old, the administrator initiates a new authenticator process.
iii. The administrator notifies the subscriber and prompts them to change their authenticator.
iv. The renewed authenticator must confirm to the initial authenticator binding process and protocol.
v. The administrator terminates the existing authenticator once 30 days have passed.

5. SOP APPENDICES

Revision History:	Version	Effective Date	Description
blank	1.0	DD-MMM-YYYY	First Approval