SOP-The Issuing and Recording of Credentials, Authenticators and Amendments to The Personal Attributes of a DID Subscriber

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

1. PURPOSE

Issuing and Recording in the context of DID lifecycle management refers to the critical function of handling and maintaining the account holder's information throughout the account's lifecycle. It encompasses the crucial responsibility of administrators to ensure that all the data associated with the DID account is stored securely and is readily accessible to perform any necessary due diligence. The management of DID account holder information is a continuous process that involves handling a wide range of personal attributes and authenticators. It is essential to note that the account holder may need to make changes to their personal information or authenticators during the lifecycle of their DID account. Administrators must adhere to Issuing and Recording SOPs to manage these changes and appropriately maintain records.

The first instance of Issuing and Recording is when the administrator issues a unique credential to the account holder (subscriber), which is linked to all personal identity attributes in the DID system. As personal identity attributes may change, an SOP has been designed to handle the authorization and recording of these amendments. Additionally, in certain circumstances, the authenticator that was bound to a DID account may also change. In such cases, the administrator is required to retain records of all bound authenticators (current and previous).

2. SCOPE

These guidelines cover the issuance, recording, and maintenance of credentials and associated data in a Subscriber Identity Account (SIA), changes to authenticators, and changes to the personal attributes of a subscriber. These guidelines should remain in place for the duration on the digital identity account. It should be noted that while the subscriber typically possesses the credential, the administrator may also have possession. The subscriber always possesses the authenticator, which is utilized to claim identity when engaging with a relying party. It is assumed that the user is a subscriber, having been validated, verified and enrolled.

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.
Identity Lifecycle Management – The overarching function undertaken primarily by Admin to maintain Digital Identity account data for security and due diligence.
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.

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

4. PROCESSES AND PROCEDURES

A. Issue a unique credential to the subscriber that is linked to their identity information:

i. Admin pulls the subscriber's account attributes and preferences.
ii. Admin generates a Unique Verified Identity to be issued to the subscriber with a known SIA reference receipt number.
iii. Admin sends an OTP to the subscriber via phone or email.
iv. The user receives the OTP from the administrator.
v. The user submits the OTP via the portal.
vi. The administrator confirms or rejects the OTP.
vii. If rejected, the administrator sends the subscriber a notification of failed authentication.
viii. The administrator binds the subscriber's Unique Verified Identity with SIA if confirmed.

B. Record the credential and associated enrollment data in the SIA throughout the credential's lifecycle:

i. Subscriber logs into the digital identity portal using their credentials and authenticator.
ii. The administrator follows Authentication processes (See SOP B.1, B.2, B.3).
iii. If authentication is successful, the administrator grants the Subscriber access to their attribute editing module.
iv. Subscriber saves and submits changes to their attributes in the digital identity portal.
v. A receipt of changes made, timestamped and indexed, is created and sent to the administrator.
vi. The administrator reviews changes made within 10 working days.
vii. The administrator may repeat Authentication processes (See SOP B.1, B.2, B.3) to assist in review.
viii. If the review of changes made is successful, the administrator commits indexed/timestamped data to server.
ix. If the review of changes made is unsuccessful, the administrator notifies the Subscriber by email or phone and rejects the changes.
x. The outcome of the review of changes is recorded in SIA.

C. Maintain a record of all authenticators that are, or have been, associated with the identity account of each subscriber:

i. The authenticator bound to a digital identity is compromised, expires, or is edited by the Subscriber.
ii. The administrator authenticates the Subscriber via an alternative, secondary authentication technique (See SOP B.1).
iii. Subscriber submits a secondary authenticator to the administrator.
iv. If secondary authentication is successful, the administrator grants Subscriber access to authenticator editing module.

v. Subscriber submits a change to the authenticator (See SOP B.1).

vi. A timestamped and index receipt containing the new Authenticator is sent to the administrator.

vii. The administrator commits the authenticator with timestamp and index to the server for SIA.

viii. If the secondary authentication fails, the administrator will notify the Subscriber by email or phone.

ix. The administrator backups data daily.

5. SOP APPENDICES:

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