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 |

# 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).

# 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.

# 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.

# PROCESSES AND PROCEDURES

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

1. Admin retrieves the subscriber's account attributes and preferences to ensure data use aligns with the stated purposes.
2. Admin generates a Unique Verified Identity to be issued to the subscriber with a known SIA reference receipt number.
3. Admin sends an OTP to the subscriber via phone or email for authentication.
4. The subscriber receives and submits the OTP via the portal, verifying their identity.
5. The administrator confirms the OTP and proceeds to bind the subscriber's Unique Verified Identity with SIA, ensuring the purpose of data collection and any subsequent changes are documented.

* Upon Unique Verified Identity issuance, the admin informs the subscriber about the specific purposes for which their identity information will be used and any potential future changes via email or the digital identity portal.

1. If OTP verification fails, the admin notifies the subscriber of the failed authentication attempt and advises on the next steps.
2. Documentation of Entitlements at Issuance:

* Upon successful issuance of the Unique Verified Identity, document any entitlements granted to the subscriber as part of this process. Clearly specify whether these entitlements are based on automated policies or were requested manually, including the rationale and approval process for each.

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

1. Subscriber logs into the digital identity portal using their credentials and authenticator, with all access logged and monitored for compliance and security.
2. The administrator follows Authentication processes (See SOP B.1, B.2, B.3).
3. If authentication is successful, the administrator grants the Subscriber access to their attribute editing module.
4. Subscriber saves and submits changes to their attributes in the digital identity portal.
5. A receipt of changes made, timestamped and indexed, is created and sent to the administrator.
6. The administrator reviews changes made within 10 working days.
7. The administrator may repeat Authentication processes (See SOP B.1, B.2, B.3) to assist in review.
8. If the review of changes made is successful, the administrator commits indexed/timestamped data to server, documenting the purpose of each data collection and any changes to it..
9. If the review of changes made is unsuccessful, the administrator notifies the Subscriber by email or phone and rejects the changes with specific reason.
10. The outcome of the review of changes is recorded in SIA.
11. The admin communicates any changes in data collection purposes to the subscriber through the digital identity portal, ensuring ongoing consent and understanding.
12. Entitlements Tracking via Granted Policies and Manual Requests:

* For entitlements granted through automated policies, create a log entry specifying the policy criteria met and the entitlements granted, along with a timestamp and index.
* For entitlements granted through manual requests, document the request, approval process, and the administrator responsible for granting the entitlement, ensuring each step is timestamped and indexed.

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

1. The authenticator bound to a digital identity is compromised, expires, or is edited by the Subscriber.
2. The administrator authenticates the Subscriber via an alternative, secondary authentication technique (See SOP B.1).
3. Subscriber submits a secondary authenticator to the administrator.
4. If secondary authentication is successful, the administrator grants Subscriber access to authenticator editing module.
5. Subscriber submits a change to the authenticator (See SOP B.1).
6. A timestamped and index receipt containing the new Authenticator is sent to the administrator.
7. The administrator commits the authenticator with timestamp and index to the server for SIA.
8. If the secondary authentication fails, the administrator will notify the Subscriber by email or phone.
9. The administrator backups data daily to ensure the integrity and availability of all records, including documentation of data collection purposes and any changes.
10. Integration of Entitlements Management with Authenticators:

* When authenticators are issued, modified, or revoked, assess any impact on subscriber entitlements. Update the entitlements log to reflect changes due to these actions, ensuring a clear link between authenticators and the entitlements they enable.

# SOP APPENDICES:

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