SOP-The Binding (Credentialing) of Authenticators to the DID Subscriber Account and The Maintenance of Bound-Authenticator Data

|  |  |
| --- | --- |
| SOP #: | C.2 |
| Version: | 1.0 |
| Author(s): | Al Tariq Sheik |

# PURPOSE:

The primary purpose of these processes and procedures are to ensure the security and integrity of the subscriber's identity account. The guidelines require the administrator to maintain accurate records of all authenticators associated with the account and to monitor and control authentication attempts. When issuing new credentials that bind a new authenticator to the subscriber's account after enrollment, the administrator must require the subscriber to authenticate at the same or higher assurance level than the new authenticator's usage level. By following these procedures, the administrator can maintain the trustworthiness of the digital identity system and ensure that only authorized individuals are granted access to the subscriber's identity account.

# SCOPE:

These guidelines must be followed for the duration of the digital identity account. Records must be retained for existing and previously bound authenticators. The scope of this SOP pertains to administrators responsible for managing DID systems and the procedures they must follow to ensure the security and integrity of the system. The guidelines include maintaining information to monitor and control authentication attempts and requiring subscribers to authenticate at the same or higher assurance level than the new authenticator's usage level when issuing new credentials. These procedures are intended to maintain the trustworthiness of the digital identity system.

# 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.

**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.

**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.

# PROCESSES AND PROCEDURES:

*A. Admin records authentication attempts (3 fail attempts):*

1. Claimant attempts to authenticate a DID’s credentials.
2. Authentication is either successful or fails.
3. Admin timestamp/indexes authentication attempts and outcomes.
4. Admin commits data to server “in SIA” (?).
5. Admin maintain records by backing up data.
6. Admin maintain records/data by auditing security (due diligence).
7. Entitlement Verification Post-Authentication:

* Upon successful authentication, verify and log any entitlements that are automatically granted based on the DID’s policy or specific criteria. Document the policy criteria met and the entitlements granted, including a timestamp and index.

1. Manual Entitlement Assignment Record:

* For entitlements assigned manually by an administrator post-authentication success, maintain a detailed record including the justification for the entitlement, the administrator responsible, and the timestamp of the assignment.

*B.* *Record and maintain authentication attempts*:

1. The claimant enters credentials and authenticator.
2. Authentication process is triggered, and the administrator receives notice of authentication attempt.
3. If authentication fails, the administrator notifies the Claimant that the authenticator needs to be corrected.
4. The administrator commits a receipt of the failed authentication attempt with timestamp and index to the server in SIA.
5. The administrator system counts each authentication attempt and the outcome – the success of fail.
6. If the claimant fails to complete authentication 3 consecutive times successfully, the account becomes temporarily locked for a period of 3 hours.
7. AC System Log Specifications:

* Ensure the AC system log is detailed and structured to clearly distinguish between denied and granted access requests. For each entry, log the user ID, authentication attempt time, outcome (granted or denied), and specific reasons for denial where applicable.

1. Entitlements Tracking Integration:

* Incorporate a process to track and log entitlements that are impacted by authentication outcomes, such as entitlements that require periodic re-authentication or are contingent on authentication attempt patterns.

# SOP APPENDICES:

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