SOP-The Revocation (Termination) of a DID Account due to the Death of a Subscriber, at the Request of the Subscriber or if the DID Account is Fraudulent or Ineligible

|  |  |
| --- | --- |
| SOP #: | C.5 |
| Version: | 1.0 |
| Author(s): | Al Tariq Sheik |

# PURPOSE

To maintain the security and integrity of the DID system and DID account access, it is important to establish clear and comprehensive guidelines for administrators to promptly revoke authenticators when required. This SOP outlines the processes and procedures for revoking a DID account in the event of a subscriber’s death, a subscriber request, the DID account is found to be fraudulent or the DID account holder is no longer eligible for a DID account.

Strict adherence to these procedures is crucial to ensuring that only authorized users have access to a DID account. However, administrators must also ensure that the revocation is at the request of an appropriate party (such as a next of kin, subscriber, or administrator) to avoid any unauthorized access or misuse of the account.

By following these detailed and well-defined guidelines, administrators can maintain the trust and security of the DID accounts, mitigate any potential risks or breaches.

# SCOPE

This SOP outlines common events in which a DID account may be revoked. These events include when the associated identity is no longer valid due to fraudulent activity or death, at the subscriber's request, or when administrators determine that the subscriber is no longer eligible.

To maintain the security and integrity of the digital identity system, it is crucial to adhere to proper authentication processes and procedures in revoking authenticators, including any applicable time restrictions. By following these procedures, the system can prevent any unauthorized access or misuse of subscriber accounts and ensure that only authorized users have access to the 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.

**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.

**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.

# PROCESSES AND PROCEDURES

A. The subscriber dies:

1. The Guardian/Next of Kin notifies Admin of Subscriber death and supplies proof within n days via reporting portal.
2. The administrator receives revocation request and legal documentation, e.g., death certificate.
3. The administrator sends receipt of request and documents to Guardian/Next of Kin.
4. The administrator initiates the identity-proofing process to prove identities of Guardian/Next of Kin/Subscriber (See SOP A.2, A.2, A.3 and A.4).
5. If successful, the administrator revokes the digital identity of the Subscriber.

* Deploy secure deletion routines to ensure all data associated with the Subscriber's DID account is irreversibly destroyed.
* This includes personal information, authentication details, transaction logs, and any other data stored within the system.

1. If unsuccessful, the administrator notifies the Guardian/Next of Kin/Subscriber of outcome, and the digital identity account remains open but is locked.
2. The request and the outcome of authentication are committed to server (SIA) along with a record of the deletion procedures executed.

B. Digital identity activity is found to be fraudulent:

1. The administrator implements fraud-detection on ID accounts.
2. Upon validating fraudulent activity detected on an account, the administrator terminates the ID.
   * Initiate secure deletion routines to erase all data related to the fraudulent account from the system.
   * Ensure the deletion process is thorough, leaving no recoverable traces of the account or its activities.
3. Record the termination and deletion process details in the server (SIA) for audit and compliance purposes.

*C. Integration of Anomaly Detection for Account Security:*

1. Anomaly detection systems are deployed across the DID platform to monitor account activities continuously.
2. When anomalous behavior indicative of unauthorized access or fraud is identified:

* The system automatically flags the account and alerts administrators for immediate review.
* Account access is temporarily restricted to prevent further potentially fraudulent activities.

1. Administrators assess the alert, verifying if the anomaly suggests actual fraud or a false positive.

* For confirmed fraudulent activities, the administrator proceeds with account termination.
* Secure deletion routines are activated to completely remove all data associated with the compromised account, ensuring no information is recoverable.

1. Detailed records of the anomaly detection alert, assessment process, and any actions taken (including account termination and data deletion) are meticulously documented in the System Information Archive (SIA) for future audit and compliance verification.

D. Subscribers request the termination of their ID:

1. Subscriber submits a request for termination of digital identity and provides proof of identity documentation using the revocation form to the administrator.
2. The administrator receives the revocation request and proof of identity documentation and acknowledges receipt to the Subscriber.
3. The administrator initiates the identity-proofing process to confirm the identity of the Subscriber (refer to SOP A.2, A.2, A.3 and A.4).
4. If the identity proofing process is successful, the administrator revokes the digital identity of the Subscriber.
   * Secure deletion routines are deployed to erase all subscriber data, ensuring no residual data remains.
   * The subscriber is notified of the successful revocation and data deletion.
5. If the identity proofing process is unsuccessful, the administrator notifies the Subscriber of the outcome, and the digital identity account remains open.
6. Documentation of the request for termination, the outcome of authentication, and details of the deletion process are recorded on the server (SIA) for audit purposes.

# SOP APPENDICES

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