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

1. 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.

2. 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 These events include when the associated identity is no longer valid due to fraudulent activity or death, at the subscriber's request, or when administrators determine that the subscriber is no longer eligible.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.

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.
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.

4. PROCESSES AND PROCEDURES

A. Subscriber dies:

i. The Guardian/Next of Kin notifies Admin of Subscriber death and supplies proof within n days via reporting portal.
ii. The administrator receives revocation request and legal documentation, e.g., death certificate.
iii. The administrator sends receipt of request and documents to Guardian/Next of Kin.
iv. 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).
v. If successful, the administrator revokes the digital identity of the Subscriber.
vi. If unsuccessful, the administrator notifies the Guardian/Next of Kin/Subscriber of outcome, and the digital identity account remains open but is locked.
vii. The request and the outcome of authentication are committed to server (SIA).

B. Digital identity activity is found to be fraudulent:

i. The administrator implements fraud-detection on ID accounts.
ii. The administrator validates fraudulent activity detected on account.
iii. The administrator terminates ID of fraud.

C. Subscribers request the termination of their ID:

i. Subscriber submits a request for termination of digital identity and provides proof of identity documentation via the reporting portal to the administrator.
ii. The administrator receives the revocation request and proof of identity documentation and acknowledges receipt to the Subscriber.
iii. 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).
iv. If the identity proofing process is successful, the administrator revokes the digital identity of the Subscriber and notifies them of the successful revocation.
v. If the identity proofing process is unsuccessful, the administrator notifies the Subscriber of the outcome, and the digital identity account remains open.
vi. The request for termination and the outcome of authentication are recorded on the server (SIA) for audit purposes.

5. SOP APPENDICES

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