SOP- The Creation and Management of a Suitable Authenticator with Ownership Factor - OTPs

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

# PURPOSE

Authenticators based on "something you have" can include cryptographic keys stored in hardware or software controlled by the subscriber, a One-Time Password (OTP) generated by a hardware device or software OTP generator installed on a digital device such as a mobile phone.

These authenticators ensure secure and effective use of the DID system throughout the entire identity lifecycle, from enrolment to revocation, providing the reliable and accurate identification of the subscriber, preventing unauthorized access, and protecting sensitive personal information. Incorporating these authenticators into the system gives subscribers confidence in their personal information's security and the reliability of their system access.

# SCOPE

This SOP provides guidelines for generating and authenticating a Subscriber's credentials using an OTP for security and authentication purposes. To initiate the process, a Claimant must supply the Unique Identity Number (UIN) of an existing account. The procedures outlined in this SOP aim to ensure that the authentication process is secure and reliable, protecting sensitive personal information and preventing unauthorized access to Subscriber accounts.

# 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.

**Unique Identity Number (UIN)** – A unique number that is assigned to subscribers and is used to identity a Digital Identity account.

**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.

**Enrolment** – The process in which an Applicant becomes an online account holder, a Subscriber

**Revocation** – The process in which a Digital Identity account is removed.

# PROCESS AND PROCEDURE

A. OTP is generated:

1. The subscriber submits their UIN to the admin.
2. The administrator receives the UIN and checks if it exists in the database.
3. If the UIN is not found, the admin sends a notification to the subscriber stating that the UIN is incorrect.
4. If the UIN is found, an OTP is generated by the admin.
5. Logging OTP Requests:

* Whenever an OTP is generated, log the request details, including the UIN, timestamp, and the method of OTP delivery (e.g., SMS or email). This log should be secure and only accessible to administrators for auditing purposes.

1. Notification of OTP Generation:

* Upon successful generation of an OTP, send an automated notification to the subscriber’s registered contact method, informing them that an OTP has been generated for their account. Include information on what actions to take if they did not request this OTP.

B. Subscriber authenticates credentials with OTP:

1. The administrator sends an OTP to the subscriber's registered phone number or email.
2. The subscriber receives the OTP and enters it into the portal.
3. The administrator receives the OTP from the subscriber.
4. The administrator verifies the OTP by matching it to the generated OTP.
5. Logging OTP Authentication Attempts:

* Log all OTP authentication attempts, including the timestamp, whether the attempt was successful or not, method of OTP delivery and the source of the attempt if available (e.g., IP address).

1. If there is no match, the admin sends a notification of the failure to the subscriber.
2. Real-Time Alerts for Failed Attempts:

* Implement a system to alert subscribers in real-time of failed OTP authentication attempts, include detailed reasoning in the log, such as "OTP mismatch" or "OTP expired. This alert should advise them of the steps to take if they suspect unauthorized activity on their account.

1. If there is a match, the admin sends a confirmation notification to the subscriber via text.
2. User Access to Authentication Logs:

* Provide subscribers with a secure method to view a log of OTP authentication attempts. This feature should be accessible through the subscriber’s account portal, enabling them to monitor authorized and unauthorized access attempts.

# SOP APPENDICES

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