Standard Operating Procedure - TOKEN-BASED AUTHENTICATION

AU.2.E - WITH RATIONALISATION

|  |  |  |
| --- | --- | --- |
| **Version** | **Date** | **Changes Made** |
| 1.0 | 16/09/2024 |  |
|  |  |  |
|  |  |  |

*Prepared by the Trustworthy Digital Infrastructure for Identity Systems Team*

*This work was supported, in whole or in part, by the Gates Foundation [INV- 057591]. Under the grant conditions of the Foundation, a Creative Commons Attribution 4.0 Generic License has already been assigned to the Author’s Accepted Manuscript.*

**Version Control**

**Guidelines for Maintaining the SOP Version Control Table:**

* **Version**: Assign a new version number for every update. Minor changes can be denoted by incremental changes in decimal (e.g., 1.1, 1.2), while major changes can increment the whole number (e.g., 1.0 to 2.0).
* **Date**: The date when the changes were finalised.
* **Changes Made**: A brief description of the changes or updates made.

Table of Contents

[1. Purpose 3](#_Toc177313493)

[2. Definitions and Abbreviations 3](#_Toc177313494)

[3. Application 3](#_Toc177313495)

[3.1 Ownership and Stakeholders 3](#_Toc177313496)

[3.1.1 Digital Identity Service Providers (DISPs) 3](#_Toc177313497)

[3.1.2 IT and Security Teams 3](#_Toc177313498)

[3.1.3 Compliance and Legal Departments 3](#_Toc177313499)

[3.2 Users and Beneficiaries 3](#_Toc177313500)

[3.2.1 General Public 3](#_Toc177313501)

[3.2.2 Government Agencies 4](#_Toc177313502)

[3.2.3 Private Sector Companies 4](#_Toc177313503)

[4. Prerequisites 4](#_Toc177313504)

[4.1 Assumptions 4](#_Toc177313505)

[4.2 Constraints 4](#_Toc177313506)

[5. Process Flow - Process and Procedures 4](#_Toc177313507)

[5.1. Initiating Token-Based Authentication: 4](#_Toc177313508)

[5.2. Sending Token and Credentials for Authentication: 4](#_Toc177313509)

[5.3. Verifying Credentials and Token: 5](#_Toc177313510)

[5.4. Handling Successful Authentication: 5](#_Toc177313511)

[5.5. Handling Unsuccessful Authentication Attempts: 5](#_Toc177313512)

[5.6. Logging and Status Update: 5](#_Toc177313513)

[5.7. Process Termination: 6](#_Toc177313514)

[6. Visualisation 7](#_Toc177313515)

[7. Rationalisation 8](#_Toc177313516)

[8. References 9](#_Toc177313517)

# 1. Purpose

This SOP outlines the standardised procedure for token-based authentication within the Digital Identity (DID) system. It ensures secure and accurate authentication through proper verification, encryption, and error handling.

# 2. Definitions and Abbreviations

**DID**: Digital Identity

**KM**: Key Manager

**KR**: Key Revocation

**HSM**: Hardware Security Module

**CA**: Certificate Authority

**IDA**: ID Authentication Database

**AC**: Access Control

**FTP**: First Time Password

**HTTPS**: Hyper Text Transfer Protocol Secure

# 3. Application

## 3.1 Ownership and Stakeholders

### 3.1.1 Digital Identity Service Providers (DISPs)

* **Ownership**: Oversee the token-based authentication process.
* **Responsibilities**: Ensure secure and compliant authentication using tokens.

### 3.1.2 IT and Security Teams

* **Ownership**: Manage technical infrastructure and security protocols.
* **Responsibilities**: Maintain system security, data encryption, and infrastructure.

### 3.1.3 Compliance and Legal Departments

* **Ownership**: Ensure compliance with legal and regulatory standards.
* **Responsibilities**: Oversee compliance checks, documentation, and regulatory adherence.

## 3.2 Users and Beneficiaries

### 3.2.1 General Public

* **Users**: Individuals using tokens for authentication.
* **Usage**: Provide tokens and credentials for secure authentication.

### 3.2.2 Government Agencies

* **Users**: Agencies requiring verified identities for services.
* **Usage**: Utilise verified identity information for secure service delivery.

### 3.2.3 Private Sector Companies

* **Users**: Businesses requiring high-security identity verification.
* **Usage**: Use secured identities for compliance and verification purposes.

# 4. Prerequisites

## 4.1 Assumptions

* Subscribers and verifiers have received their DID and FTP credentials.
* Administrators are trained to handle the token authentication process securely.
* Technological infrastructure meets current security standards.

## 4.2 Constraints

* The token authentication process may be affected by system downtimes or regulatory changes.
* Secure devices and internet access are required for administrators and users.

# 5. Process Flow - Process and Procedures

## **5.1. Initiating Token-Based Authentication:**

* **Claimant/Subscriber Action:**
  + The claimant/subscriber provides the generated token along with their demographic data as part of the authentication process.
* **Verifier Action:**
  + The verifier initiates the authentication request by starting online and requesting a token for authentication.
* **Output:** Authentication request with token and demographic data is initiated.

## **5.2. Sending Token and Credentials for Authentication:**

* **System Action (Public Network Systems - Client):**
  + The client system sends the token, demographic details, and verifier credentials to the server for authentication.
  + These details are masked and encrypted to ensure secure transmission.
* **Output:** Secure transmission of token, demographic data, and verifier credentials to the server.

## **5.3. Verifying Credentials and Token:**

* **System Action (Server):**
  + The server first checks if the verifier credentials match the expected credentials.
  + It then verifies if the token and demographic data provided by the claimant match the records in the database.
  + The server checks if the token is still valid and not expired.
* **Output:** Credentials and token verification process is conducted.

## **5.4. Handling Successful Authentication:**

* **System Action (Server):**
  + If the verifier credentials match, and both the token and demographic data are validated, and the token is not expired:
    - The server stores the successful token authentication status in the claimant's UIN (Unique Identification Number) account with appropriate encryption and hashing for security.
    - A notification generator sends confirmation notifications to the claimant and verifier, including the timestamp of the successful authentication.
* **Output:** Successful authentication is logged, and notifications are sent.

## **5.5. Handling Unsuccessful Authentication Attempts:**

* **System Action (Server):**
  + If the verifier credentials do not match, the token or demographic data is incorrect, or the token is expired:
    - The system increments the exception and error handling counter.
    - The system allows up to three retry attempts for authentication.
    - If retry limits are exceeded, the system terminates the process, records the timestamp of the failed attempt, and sends a notification of the unsuccessful authentication.
* **Output:** Unsuccessful authentication attempts are logged, retry attempts are tracked, and notifications are sent.

## **5.6. Logging and Status Update:**

* **System Action (Server):**
  + The server logs all activities during the token-based authentication process, including both successful and failed attempts.
  + Status updates are stored in the system logs for auditing, compliance, and monitoring.
* **Output:** Detailed logs and status updates are created for compliance and security monitoring.

## **5.7. Process Termination:**

* **System Action (Server):**
  + The process terminates after successful authentication, enabling secure access to the system or service for the claimant.
  + In case of authentication failure, the process terminates with security measures in place, such as logging the attempt and sending out failure notifications.
* **Output:** Process concludes with either successful access granted or termination due to security concerns.

# 6. Visualisation

A screenshot of a computer

Description automatically generated

Please refer to the [GitHub](https://github.com/alan-turing-institute/Standard-Operating-Procedures-for-Digital-Identity-Systems) repository for further information.

# 7. Rationalisation

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **AU.2.E TOKEN-BASED AUTHENTICATION** | | | | | |
| **Step** | **Description** | **Action** | **Systems Involved** | **Security Measures** | **Standards and References** |
| 1 | Request Token for Authentication | User initiates the authentication process | User Device, Public Network | Secure HTTPS Connection | ISO 27001 Information Security Management, eIDAS Trust Services |
| 2 | Provide Token and Demographic Data | User submits generated token and demographic data | User Device, Authentication Server | Token Verification, Secure Data Transmission | ISO 27001 Data Protection, NIST SP 800-63 Digital Identity Guidelines |
| 3 | Receive Token and Demographic Data | Server receives token and demographic details | Server, Private Network | Data Encryption, Secure Storage | ISO 27001 Cryptography, FATF Digital Identity Guidelines |
| 4 | Authenticate Token and Data | Verify if token and demographic data is validated | Authentication Server | Matching Algorithm, Token Expiry Check | ISO 27001 Access Control, Estonia ID Electronic Identification |
| 5 | Reset Counter If Token Valid | Reset retry counter if token is not expired | Authentication Server | Counter Reset, Error Handling | ISO 27001 Event Logging and Monitoring, NIST SP 800-63 Authenticator Management |
| 6 | Store Authentication Status | Record successful token authentication in UIN account | Server, Private Network | Secure Logging, Data Encryption and Hashing | ISO 27001 Cryptography, Emirates ID Data Security Standards |
| 7 | Notification of Authentication Outcome | Notify user of authentication success or failure | User Device, Notification System | Secure Notification Delivery | ISO 27001 Communications Security, Sing Pass Secure Notification Handling |
| 8 | Handle Unsuccessful Authentication Attempts | Manage retries and send notifications on failure | Authentication Server | Retry Limit Management, Notification of Failure | ISO 27001 Access Control Policies, Aadhar Secure Authentication Practices |
| 9 | Terminate Process on Excessive Failures | Lock account and record timestamp and attempt | Authentication Server | Account Lockout, Secure Timestamp Recording | ISO 27001 Access Control Policies, NIST SP 800-63 Authenticator Management |
| 10 | End Process | Log process completion and status | Authentication Server | Process Logging | NIST SP 800-63 Authenticator Management, Estonia ID Secure Logging |

# 8. References

1. NIST. Digital Identity Guidelines: Age Verification Guidance. Available at: [https://pages.nist.gov/800-63-3/].
2. eIDAS. Identity Proofing Requirements. Available at: [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L\_.2014.257.01.0073.01.ENG].
3. ISO. 27001, Secure System Access Control. Available at: [https://www.iso.org/standard/27001].
4. Aadhaar. Account Creation and Management. Available at: [https://uidai.gov.in/en/my-aadhaar/about-your-aadhaar/aadhaar-enrolment.html].
5. SingPass. Account Creation and Management. Available at: [https://www.singpass.gov.sg/home/ui/assets/pdf/Singpass\_Registration\_Guide.pdf].
6. FATF. Digital Identity Guidance: Authentication Mechanisms. Available at: [https://www.fatf-gafi.org/en/publications/Financialinclusionandnpoissues/Digital-identity-guidance.html].
7. Estonia ID. Data Protection Practices. Available at: [https://toolbox.estonia.ee/asset-page/252494-e-estonia-guide-full-brochure].
8. Emirates ID. Available at: [https://u.ae/en/information-and-services/visa-and-emirates-id/emirates-id].