|  |  |  |
| --- | --- | --- |
| **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.*

Standard Operating Procedure - Generation of Token (Shared Code)

AU.2.D - WITH RATIONALISATION

**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](#_Toc176259717)

[2. Definitions and Abbreviations 3](#_Toc176259718)

[3. Application 3](#_Toc176259719)

[3.1 Ownership and Stakeholders 3](#_Toc176259720)

[3.1.1 Digital Identity Service Providers (DISPs) 3](#_Toc176259721)

[3.1.2 IT and Security Teams 3](#_Toc176259722)

[3.1.3 Compliance and Legal Departments 3](#_Toc176259723)

[3.2 Users and Beneficiaries 4](#_Toc176259724)

[3.2.1 General Public 4](#_Toc176259725)

[3.2.2 Government Agencies 4](#_Toc176259726)

[3.2.3 Private Sector Companies 4](#_Toc176259727)

[4. Prerequisites 4](#_Toc176259728)

[4.1 Assumptions 4](#_Toc176259729)

[4.2 Constraints 4](#_Toc176259730)

[5. Process Flow - Process and Procedures 4](#_Toc176259731)

[5.1. Initiating Token Generation: 4](#_Toc176259732)

[5.2. Authentication Using OTP: 4](#_Toc176259733)

[5.3. OTP Verification and Token Generation: 5](#_Toc176259734)

[5.4. Storing and Displaying the Token: 5](#_Toc176259735)

[5.5. Handling Unsuccessful Authentication Attempts: 5](#_Toc176259736)

[5.6. Logging and Status Update: 5](#_Toc176259737)

[5.7. Process Termination: 6](#_Toc176259738)

[6. Resources 7](#_Toc176259739)

[6.1 Visualisation 7](#_Toc176259740)

[6.2 Rationalisation 8](#_Toc176259741)

[7. References 9](#_Toc176259742)

# 1. Purpose

This SOP outlines the standardised procedure for generating a token (shared code) within the Digital Identity (DID) system. It ensures secure and accurate token generation 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

**OTP**: One-Time Password

**HTTPS**: Hyper Text Transfer Protocol Secure

**SSL/TLS**: Secure Sockets Layer / Transport Layer Security

# 3. Application

## 3.1 Ownership and Stakeholders

### 3.1.1 Digital Identity Service Providers (DISPs)

* **Ownership**: Oversee the token generation process.
* **Responsibilities**: Ensure secure and compliant generation of 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 generating tokens for their DID accounts.
* **Usage**: Provide UIN and demographic data to receive tokens.

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

## 4.2 Constraints

* The token generation 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 Generation:**

* **Claimant/Subscriber Action:**
  + The claimant/subscriber visits the DID portal online.
  + Clicks on "Generate One-Time Token for Authentication."
  + Enters their UIN (Unique Identification Number) and demographic data as prompted by the portal.
* **Output:** Claimant's request for token generation is initiated.

## **5.2. Authentication Using OTP:**

* **System Action (Public Network Systems - Client):**
  + The client system masks and encrypts the UIN and demographic data provided by the claimant for secure verification.
* **System Action (Server):**
  + The server checks if the UIN and demographic data match the stored records.
  + If matched, the server initiates the generation of an OTP (One-Time Password) for subscriber authentication.
* **Output:** UIN and demographic data are verified, and OTP generation process begins.

## **5.3. OTP Verification and Token Generation:**

* **Claimant/Subscriber Action:**
  + The claimant authenticates using the OTP sent to their registered device (via AU.2.C).
* **System Action (Server):**
  + Upon successful OTP authentication, the server generates a temporary token for two-factor authentication.
  + The generated token includes an expiry date and time for security purposes.
* **Output:** OTP is authenticated, and a secure token is generated.

## **5.4. Storing and Displaying the Token:**

* **System Action (Server):**
  + The server stores the generated token in the UIN account using encryption, hashing, and records the expiry date and time.
  + The token is then activated as the token authenticator.
* **System Action (Public Network Systems - Client):**
  + The generated token is displayed to the claimant on the DID portal.
  + A notification containing the token details is sent to the claimant's registered email or SMS for their records.
* **Output:** Token is securely stored, activated, and displayed to the claimant.

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

* **System Action (Server):**
  + If the UIN and demographic data do not match or if OTP authentication fails, the system increments the error handling counter.
  + The system allows up to three retry attempts for authentication.
  + If the retry limit is exceeded, the system terminates the process, records the timestamp of the failed attempt, and generates a notification of the unsuccessful authentication.
* **Output:** Unsuccessful authentication attempts are logged, and the process is terminated after the allowed retry limit.

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

* **System Action (Server):**
  + The server logs all activities during the token generation and authentication process, including successful and failed attempts.
  + The status of each step is updated in the system logs for auditing and compliance.
* **Output:** Detailed logs and status updates are created for compliance and audit purposes.

## **5.7. Process Termination:**

* **System Action (Server):**
  + The process terminates upon successful token generation and activation, allowing the claimant to use the token for secure authentication.
  + If authentication fails or retry limits are exceeded, the process terminates with security measures, such as recording the failed attempt and sending out notifications.
* **Output:** Process concludes with either successful token generation or termination due to security concerns.

# 6. Visualisation

A diagram of a company

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.D Generation of Token (Shared Code)** | | | | | |
| **Step** | **Description** | **Action** | **Systems Involved** | **Security Measures** | **Standards and References** |
| 1 | Start Process | User visits DID portal and initiates token generation | User Device, Public Network | Secure portal access, HTTPS | ISO 27001 Information Security Management, eIDAS Trust Services |
| 2 | Enter UIN and Demographic Data | User inputs UIN and demographic details | User Device, Public Network | Data entry security, Encryption | ISO 27001 Data Protection, Aadhaar Secure Data Handling Guidelines |
| 3 | Authenticate Using OTP | User authenticates using OTP | User Device, Authentication Server | Two-Factor Authentication, OTP Verification | ISO 27001 Authentication Controls, NIST SP 800-63 Digital Identity Guidelines, Sing Pass OTP Security |
| 4 | Verify and Encrypt Data | Verify UIN and demographic data, encrypt for verification | Server, Private Network | Data Matching, Encryption, SSL/TLS | ISO 27001 Cryptography, FATF Digital Identity Guidelines, Emirates ID Data Security Standards |
| 5 | Generate Token | Generate a token with expiry date and time | Token Generation Server | Token generation with expiry, Hashing | NIST SP 800-63 Authentication Mechanisms, ISO 27001 Cryptography |
| 6 | Display and Send Token | Display token on user device and send via email/SMS | User Device, Notification System | Secure display and communication, Secure Notification Delivery | ISO 27001 Communications Security, Estonia ID Notification System |
| 7 | Log Process and Handle Errors | Record process steps and manage exceptions | Server, Private Network | Logging, Error handling | ISO 27001 Event Logging and Monitoring, FATF Digital Identity Error Handling |
| 8 | Terminate or Reset Process | End or reset the process based on retry count | Server | Account lockout policy, Retry limit management | ISO 27001 Access Control Policies, NIST SP 800-63 Authenticator Management |
| 9 | Notification of Success or Failure | Notify user of successful or unsuccessful authentication attempt | Notification System | Secure Notification Delivery | ISO 27001 Communications Security, eIDAS Trust Services |

# 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].