STANDARD OPERATING PROCEDURE DELIVERY OF DIGITAL ID & FTP CREDENTIALS TO SUBSCRIBER

OB.4.C - 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](#_Toc177309952)

[2. Definitions and Abbreviations 3](#_Toc177309953)

[3 Application 3](#_Toc177309954)

[3.1 Ownership and Stakeholders 3](#_Toc177309955)

[3.1.1 Digital Identity Service Providers (DISPs) 3](#_Toc177309956)

[3.1.2 IT and Security Teams 3](#_Toc177309957)

[3.1.3 Compliance and Legal Departments 3](#_Toc177309958)

[3.2 Users and Beneficiaries 4](#_Toc177309959)

[3.2.1 General Public 4](#_Toc177309960)

[3.1.2 Government Agencies 4](#_Toc177309961)

[3.1.3 Private Sector Companies 4](#_Toc177309962)

[4. Prerequisites 4](#_Toc177309963)

[4.1 Assumptions 4](#_Toc177309964)

[4.2 Constraints 4](#_Toc177309965)

[5. Process & Procedures 4](#_Toc177309966)

[5.1 Notification of Application Status 4](#_Toc177309967)

[5.2 Printing and Sending Physical ID and FTP 4](#_Toc177309968)

[5.3 Tracking and Delivery 4](#_Toc177309969)

[5.4 Receiving and Verifying Delivery 5](#_Toc177309970)

[6. Visualisation 6](#_Toc177309971)

[7. Rationalisation 7](#_Toc177309972)

[8. References 8](#_Toc177309973)

# 1. Purpose

This SOP outlines the standardized procedure for the delivery of Digital Identity (DID) and First Time Password (FTP) credentials to subscribers. It ensures secure and accurate delivery through proper verification and tracking mechanisms.

# 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

**2FA**: Two-Factor Authentication

**API**: Application Programming Interface

**HTTPS**: Hyper Text Transfer Protocol Secure

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

**IDS**: Intrusion Detection System

**IPS**: Intrusion Prevention System

# 3 Application

## 3.1 Ownership and Stakeholders

### 3.1.1 Digital Identity Service Providers (DISPs)

* **Ownership**: Oversee the delivery process.
* **Responsibilities**: Ensure secure and compliant delivery of credentials.

### 3.1.2 IT and Security Teams

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

### 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 receiving DID and FTP credentials.
* **Usage**: Use credentials to access digital identity services.

### 3.1.2 Government Agencies

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

### 3.1.3 Private Sector Companies

* **Users**: Businesses requiring verified identities.
* **Usage**: Use secured identities for compliance and verification purposes.

# 4. Prerequisites

## 4.1 Assumptions

* Administrators are trained to handle the delivery process securely.
* Technological infrastructure meets current security standards.
* Postal services are reliable and secure.

## 4.2 Constraints

* Delivery process may be affected by postal delays or system downtimes.
* Secure devices and internet access are required for administrators.

# 5. Process & Procedures

## **5.1 Notification of Application Status**

* **Action**: The administrator notifies all application statuses.
* **Output**: Application status notifications sent to users.

## **5.2 Printing and Sending Physical ID and FTP**

* **Action**:
  + Print the physical ID card with photo and attributes.
  + Print a letter with UIN and FTP in a sealed envelope.
  + Send the physical copy of DID and FTP via postal service.
* **Output**: Physical ID card and FTP credentials are securely printed and sent.

## **5.3 Tracking and Delivery**

* **Public Network Systems (Client)**
  + **Action**: Mask and encrypt tracking number.
  + **Output**: Tracking number is securely sent to the server.
* **Private Network Systems (Server)**
  + **Action**:
    - Generate tracking number.
    - Store tracking number in the user's account.
    - Notify user of tracking details.
  + **Output**: Tracking details generated and stored, user notified.
* **Postal Service Provider**
  + **Action**:
    - Receive sealed letters from the administrator.
    - Register post and generate tracking number.
  + **Output**: Letters registered and tracking number generated.

## **5.4 Receiving and Verifying Delivery**

* **Action**:
  + User receives the notification of delivery status.
  + User receives the physical ID and FTP.
  + User shows original proof of identity (POI) and signs the acknowledgment of receipt.
* **Output**: Delivery confirmed and identity verified.

# 6. Visualisation

A screenshot of a diagram

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

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **OB.4.C DELIVERY OF DIGITAL ID & FTP CREDENTIALS TO SUBSCRIBER** | | | | | |
| Step | Description | Action | Systems Involved | Security Measures | Standards and References |
| 1 | Start Process | User initiates the delivery process online | User Device, Public Network | Secure HTTPS Connection | ISO 27001 Information Security Management, eIDAS Trust Services |
| 2 | Authenticate User | User logs in and authenticates | Authentication Server | Two-Factor Authentication | ISO 27001 Access Control, NIST SP 800-63 Digital Identity Guidelines |
| 3 | Submit Application for ID and FTP | User submits application | DID Portal | Data input validation | ISO 27001 Data Protection, GDPR Compliance for Data Handling |
| 4 | Print Physical ID Card and Letter | Physical ID card and letter with credentials printed | Printing System | Data confidentiality, Secure printing | ISO 27001 Data Integrity, FATF Digital Identity Guidelines |
| 5 | Send Physical Copy Via Post | Mail physical ID and credentials | Postal System | Secure packaging and mailing | ISO 27001 Communications Security, Sing Pass Notification System |
| 6 | Track Delivery | Monitor and track delivery status | Tracking System | Real-time tracking, Data encryption | ISO 27001 Cryptography, NIST SP 800-53 Security and Privacy Controls |
| 7 | Deliver to User | Physical delivery of ID and credentials | Postal Service, User's Address | Authentication of receipt, Signature required | ISO 27001 Physical Security, eIDAS Trust Services |
| 8 | Notify User of Delivery Status | Notify user of successful/unsuccessful delivery | Notification System | Secure notification delivery | ISO 27001 Communications Security, GDPR Compliance for Notification Security |
| 9 | Error and Exception Handling | Manage errors and exceptions during delivery | Security System | Error logging and response handling | ISO 27001 Event Management, NIST SP 800-61 Incident Response |
| 10 | Log Process | Log all actions related to the delivery process | Security Logs | Audit trails, logging | ISO 27001 Secure Audit Logging, FATF Digital Identity Guidelines |
| 11 | End Process | Finalize the delivery process | System | Secure session termination | ISO 27001 Event Management |

# 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].