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

OB.4.C

**Version Control**

|  |  |  |
| --- | --- | --- |
| Version | Date | Changes Made |
|  |  |  |
|  |  |  |
|  |  |  |

**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](#_Toc177261622)

[2. Definitions and Abbreviations 3](#_Toc177261623)

[3 Application 3](#_Toc177261624)

[3.1 Ownership and Stakeholders 3](#_Toc177261625)

[3.1.1 Digital Identity Service Providers (DISPs) 3](#_Toc177261626)

[3.1.2 IT and Security Teams 3](#_Toc177261627)

[3.1.3 Compliance and Legal Departments 3](#_Toc177261628)

[3.2 Users and Beneficiaries 4](#_Toc177261629)

[3.2.1 General Public 4](#_Toc177261630)

[3.1.2 Government Agencies 4](#_Toc177261631)

[3.1.3 Private Sector Companies 4](#_Toc177261632)

[4. Prerequisites 4](#_Toc177261633)

[4.1 Assumptions 4](#_Toc177261634)

[4.2 Constraints 4](#_Toc177261635)

[5. Process & Procedures 4](#_Toc177261636)

[5.1 Notification of Application Status 4](#_Toc177261637)

[5.2 Printing and Sending Physical ID and FTP 4](#_Toc177261638)

[5.3 Tracking and Delivery 4](#_Toc177261639)

[5.4 Receiving and Verifying Delivery 5](#_Toc177261640)

[6. Visualisation 6](#_Toc177261641)

# 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.