|  |  |  |
| --- | --- | --- |
| **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 - OBTAINING CLAIMANT CONSENT

AU.3.A - 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](#_Toc177313087)

[2. Definitions and Abbreviations 3](#_Toc177313088)

[3. Application 3](#_Toc177313089)

[3.1 Ownership and Stakeholders 3](#_Toc177313090)

[3.1.1 Digital Identity Service Providers (DISPs) 3](#_Toc177313091)

[3.1.2 IT and Security Teams 3](#_Toc177313092)

[3.1.3 Compliance and Legal Departments 3](#_Toc177313093)

[3.2 Users and Beneficiaries 4](#_Toc177313094)

[3.2.1 General Public 4](#_Toc177313095)

[3.2.2 Government Agencies 4](#_Toc177313096)

[3.2.3 Private Sector Companies 4](#_Toc177313097)

[4. Prerequisites 4](#_Toc177313098)

[4.1 Assumptions 4](#_Toc177313099)

[4.2 Constraints 4](#_Toc177313100)

[5. Process Flow - Process and Procedures 4](#_Toc177313101)

[5.1. Starting the Consent Process: 4](#_Toc177313102)

[5.2. Initiating Consent Request: 5](#_Toc177313103)

[5.3. Providing Consent Information: 5](#_Toc177313104)

[5.4. Gathering Explicit Consent: 5](#_Toc177313105)

[5.5. Acknowledgement and Record Keeping: 5](#_Toc177313106)

[5.6. Handling Exceptions and Errors: 6](#_Toc177313107)

[5.7. Logging and Status Update: 6](#_Toc177313108)

[6. Visualisation 7](#_Toc177313109)

[7. Rationalisation 8](#_Toc177313110)

[8. References 9](#_Toc177313111)

# 1. Purpose

This SOP outlines the standardized procedure for obtaining explicit consent from users for processing their data within the Digital Identity (DID) system. It ensures secure and compliant consent management through proper verification, documentation, 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

**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 consent obtaining process.
* **Responsibilities**: Ensure secure and compliant consent management.

### 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 providing consent for their DID accounts.
* **Usage**: Provide explicit consent for data processing.

### 3.2.2 Government Agencies

* **Users**: Agencies requiring verified identities for services.
* **Usage**: Utilize 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 are aware of the consent process and its importance.
* Administrators are trained to handle the consent process securely.
* Technological infrastructure meets current security standards.

## 4.2 Constraints

* The consent 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. Starting the Consent Process:**

* **Claimant/Subscriber Action:**
  + The claimant provides their Unique Identification Number (UIN) and demographic data.
* **Verifier Action:**
  + The verifier verifies the UIN and demographic data provided by the claimant.
  + The verifier either receives a notification if the UIN is not found or proceeds if the UIN match is found.
* **Output:** Verification of claimant's identity and demographic data.

## **5.2. Initiating Consent Request:**

* **Verifier Action:**
  + If the UIN match is found, the verifier initiates a consent request for the claimant.
* **System Action (Server):**
  + The server checks if the UIN and demographic data match the records.
  + The server resets the counter and sends a notification to proceed with the consent request.
* **Output:** Consent request is initiated.

## **5.3. Providing Consent Information:**

* **Verifier Action:**
  + The verifier provides a consent form that includes literature about biometric data processing in the claimant's preferred language.
  + The verifier orally explains the literature and offers a Q&A session to clarify any doubts or questions.
* **Claimant Action:**
  + The claimant reads the provided literature and asks any immediate questions if needed.
* **Output:** Claimant is informed about the biometric data processing.

## **5.4. Gathering Explicit Consent:**

* **Verifier Action:**
  + If the claimant has no immediate questions, the verifier requests explicit consent, which can be provided via signature or thumbprint.
* **Claimant Action:**
  + The claimant listens and participates in any additional Q&A if required.
  + Upon agreement, the claimant provides explicit consent using a signature or thumbprint.
* **Output:** Explicit consent is provided by the claimant.

## **5.5. Acknowledgement and Record Keeping:**

* **Verifier Action:**
  + Upon receiving explicit consent, the verifier provides an acknowledgment copy to the claimant.
  + The verifier scans and uploads the consent form, sending a notification of successful consent upload.
* **System Action (Server):**
  + The server checks if the scanned consent form is accepted. If accepted, the consent form details are stored in the claimant's UIN account.
  + If the form is not accepted, the verifier enters the reason and comments, and a notification of consent failure is sent.
* **Output:** Consent form is acknowledged, scanned, and stored.

## **5.6. Handling Exceptions and Errors:**

* **System Action (Server):**
  + If errors occur or data mismatches are found, the server triggers exception handling, allowing up to three retry attempts.
  + If retry limits are exceeded, the process is terminated, and the failure is logged.
* **Output:** Error handling and retries are managed, and failures are logged.

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

* **System Action (Server):**
  + The server logs all activities during the consent obtaining process, including successful consent and any failures.
  + Status updates are stored in the system logs for auditing and compliance monitoring.
* **Output:** Detailed logs and status updates are created for compliance and security monitoring.

# 6. Visualisation

A diagram of a process flow

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.3.A OBTAINING CLAIMANT CONSENT** | | | | | |
| **Step** | **Description** | **Action** | **Systems Involved** | **Security Measures** | **Standards and References** |
| 1 | Start Consent Process | User initiates the consent process offline | User Device, Verifier | Secure data handling | ISO 27001 Information Security Management, eIDAS Trust Services |
| 2 | Provide Literature and Consent Form | Provide literature on biometric data processing in an appropriate language | User Device, Public Network | Data privacy, clear communication | ISO 27001 Data Protection, GDPR for Biometric Data, Aadhaar Communication Guidelines |
| 3 | Explanation and Q&A Session | Orally explain the literature and answer questions | Verifier, User Device | Transparency, user engagement | ISO 27001 User Awareness, NIST SP 800-53 Privacy Controls |
| 4 | Obtain Explicit Consent | Request explicit consent via signature or thumbprint | User Device, Verifier | Consent verification, biometric security | ISO 27001 User Access Management, eIDAS Electronic Identification, GDPR Consent Requirements |
| 5 | Verify UIN and Demographic Data | Verify the user's UIN and demographic data | Server, Private Network | Data verification, encryption | ISO 27001 Cryptography, NIST SP 800-63 Digital Identity Guidelines |
| 6 | Store Consent Form Details | Store the consent form details in UIN account | Server, Private Network | Secure storage, data encryption and hashing | ISO 27001 Data Protection, FATF Digital Identity Guidelines, Estonia ID Secure Data Storage |
| 7 | Receive Consent Upload Successful Notification | Notify user of the successful upload of the consent form | User Device, Notification System | Secure notification delivery | ISO 27001 Communications Security, Sing Pass Notification System |
| 8 | Handle Exceptions and Errors | Manage errors in consent upload process | Server | Exception management, error logging | ISO 27001 Event Logging and Monitoring, NIST SP 800-61 Incident Response |
| 9 | Terminate or Continue Process | Terminate or reset the process based on the outcome | Server | Process termination, secure logging | ISO 27001 Access Control Policies, NIST SP 800-63 Authenticator Management |
| 10 | End Process | Log the completion and status of the process | Server | Audit logging | NIST SP 800-53 Security and Privacy Controls, ISO 27001 Secure Audit 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].