|  |  |  |
| --- | --- | --- |
| **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 - BIOMETRIC AUTHENTICATION: IRIS DATA

AU.3.C - 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](#_Toc177313413)

[2. Definitions and Abbreviations 3](#_Toc177313414)

[3. Application 3](#_Toc177313415)

[3.1 Ownership and Stakeholders 3](#_Toc177313416)

[3.1.1 Digital Identity Service Providers (DISPs) 3](#_Toc177313417)

[3.1.2 IT and Security Teams 3](#_Toc177313418)

[3.1.3 Compliance and Legal Departments 3](#_Toc177313419)

[3.2 Users and Beneficiaries 4](#_Toc177313420)

[3.2.1 General Public 4](#_Toc177313421)

[3.2.2 Government Agencies 4](#_Toc177313422)

[3.2.3 Private Sector Companies 4](#_Toc177313423)

[4. Prerequisites 4](#_Toc177313424)

[4.1 Assumptions 4](#_Toc177313425)

[4.2 Constraints 4](#_Toc177313426)

[5. Process Flow - Process and Procedures 4](#_Toc177313427)

[5.1. Initiating Iris Authentication 4](#_Toc177313428)

[5.2. Verification of UIN and Demographic Data 5](#_Toc177313429)

[5.3. Iris Capture and Submission 5](#_Toc177313430)

[5.4. Iris Authentication 5](#_Toc177313431)

[5.5. Handling Exceptions and Retries 5](#_Toc177313432)

[5.6. Logging and Status Update 6](#_Toc177313433)

[6. Visualisation 7](#_Toc177313434)

[7. Rationalisation 8](#_Toc177313435)

[8. References 9](#_Toc177313436)

# 1. Purpose

This SOP outlines the standardised procedure for biometric authentication using iris data 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

**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 iris authentication process.
* **Responsibilities**: Ensure secure and compliant authentication using iris data.

### 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 iris authentication for their DID accounts.
* **Usage**: Provide iris data 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 have provided consent for biometric authentication.
* Administrators are trained to handle the iris authentication process securely.
* Technological infrastructure meets current security standards.

## 4.2 Constraints

* The iris 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 Iris Authentication**

* **Claimant/Subscriber Action:**
  + The claimant begins the process offline by providing their consent (reference: AU.3.A).
  + The claimant provides their Unique Identification Number (UIN) and demographic data to the verifier.
* **Verifier Action:**
  + The verifier requests UIN and demographic data from the claimant.
  + The verifier verifies the UIN and demographic data against the system records.
* **Output:** Initial identity verification is completed.

## **5.2. Verification of UIN and Demographic Data**

* **System Action (Client and Server):**
  + The UIN and demographic data provided by the claimant are encrypted using secure protocols (SSL/TLS) and sent for verification.
  + The server checks if the UIN and demographic data match the existing records.
  + If a match is found, a notification of successful verification status is sent. If no match is found, a failure status notification is generated.
* **Output:** Verification success or failure status is determined.

## **5.3. Iris Capture and Submission**

* **Verifier Action:**
  + Upon successful verification of UIN and demographic data, the verifier requests the claimant to provide their iris for scanning using the iris scanner.
  + The claimant positions their eye in front of the iris scanner.
* **System Action (Client):**
  + The iris scanner captures the iris image.
  + The captured iris image is encrypted for secure transmission.
* **Output:** Iris image is captured and encrypted for authentication.

## **5.4. Iris Authentication**

* **System Action (Server):**
  + The encrypted iris scan image is sent to the server for authentication.
  + The server checks if the iris scan matches the iris data stored in the claimant's UIN account with a match score threshold (≥ 95%).
  + If the iris matches, a notification of successful authentication is generated. If not, failure notifications are sent, and exception handling is initiated.
* **Output:** Iris authentication success or failure is determined.

## **5.5. Handling Exceptions and Retries**

* **System Action (Server):**
  + If the iris does not match or errors occur during scanning, the system triggers exception handling and allows up to three retry attempts.
  + If the retry count exceeds three, the process is terminated, and the claimant's UIN account is locked for 24 hours.
* **Output:** Error handling and retries are managed, and account security is enforced.

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

* **System Action (Server):**
  + All activities, including successful iris authentication and any failures, are logged in the system.
  + Status updates are stored in the system logs for auditing, compliance monitoring, and future reference.
* **Output:** Detailed logs and status updates are created for compliance and security monitoring.

# 6. Visualisation

A diagram of a flowchart

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.C BIOMETRIC AUTHENTICATION: IRIS DATA** | | | | | |
| **Step** | **Description** | **Action** | **Systems Involved** | **Security Measures** | **Standards and References** |
| 1 | Start Iris Authentication Process | User initiates the iris authentication process offline | User Device, Public Network | Ensure secure initiation of the authentication process, regardless of the mode (offline/online). | ISO 27001 Information Security Management, eIDAS Trust Services |
| 2 | Provide UIN and Demographic Data | User provides their UIN and demographic information | User Device | Data entry security | ISO 27001 Data Protection, NIST SP 800-63 Digital Identity Guidelines |
| 3 | Request Iris Scanning | User is prompted to provide an iris scan | Iris Scanner, Private Network | Biometric data collection | ISO 27001 User Access Management, GDPR for Biometric Data |
| 4 | Verify UIN and Demographic Data | Verification of UIN and demographic data | Server, Private Network | Data Matching, Secure Authentication Process | ISO 27001 Cryptography, FATF Digital Identity Guidelines |
| 5 | Iris Match Verification | Match iris scan with UIN account | Biometric System, Private Network | Biometric verification, Match score (>95%) | ISO 27001 Authentication Controls, NIST SP 800-63 Biometric Authentication Mechanisms |
| 6 | Encrypt Iris Scan Image for Authentication | Encrypt iris scan image before storage and transmission | Server, Private Network | Data encryption, Privacy preservation | ISO 27001 Cryptography, Emirates ID Data Security Standards |
| 7 | Receive Authentication Status | Notify user of iris authentication result | User Device, Notification System | Secure Notification Delivery | ISO 27001 Communications Security, Sing Pass Notification System |
| 8 | Handle Authentication Failures | Manage unsuccessful authentication attempts | Server | Error handling, Retry management | ISO 27001 Access Control Policies, NIST SP 800-61 Incident Handling |
| 9 | Terminate or Reset Process | Lock UIN account or reset process based on retries | Server | Account lockout, Process termination | ISO 27001 Access Control Policies, NIST SP 800-63 Authenticator Management |
| 10 | End Process | Log process completion and status | 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].