NeST-GDL-BIO.01
Version 1.0
June, 2017
Status: Released

Security Guidelines for use of Biometric Technology in e-Governance Projects

Government of India
Ministry of Electronics & Information Technology
New Delhi-110003

Metadata of the Standard

S. No.	Data elements	Values
1.	**Title**	Security Guidelines for use of Biometric Technology in e-Governance Projects
2.	**Title Alternative**	Biometric guidelines
3.	**Document Identifier**	**NeST-GDL-BIO.01**
4.	**Document Version, month, year of release**	Version 1.0 June, 2017
5.	**Present Status** *(Draft/Released/Withdrawn)*	Released
6.	**Publisher**	Ministry of Electronics and Information Technology (MeitY),Government of India (GoI)
7.	**Date of Publishing**	30/06/2017
8.	**Type of Standard Document** *(Standard/ Policy/ Technical/ Specification/ Best Practice /Guideline / Framework /Procedure)*	*Guideline*
9.	**Enforcement Category** *(Mandatory / Recommended)*	*Recommended*
10.	**Creator** *(An entity primarily responsible for making the resource)*	NeST (STQC)
11.	**Contributor** *(An entity responsible for making contributions to the resource)*	**1.** MeitY **2.** UIDAI
12.	**Brief Description**	Security Guidelines for use of Biometric Technology in e-Governance Projects
13.	**Target Audience** *(Who would be referring / using the Std)*	Developers and users of e-governance applications/ systems which are using biometrics
14.	**Owner of approved Standard**	MeitY, New Delhi
15.	**Subject** (Major Area of Standardization)	e-Governance Standards

16.	**Subject. Category** (Sub Area within major area)	Biometric guidelines
17.	**Coverage. Spatial**	INDIA
18.	**Format** *(PDF/A at the time of release of final Standard)*	PDF
19.	**Language** *(To be translated in other Indian languages later)*	English
20.	**Copyrights**	MeitY, New Delhi
21.	**Source** *(Reference to the resource from which present resource is derived)*	ISO/IEC 24745, ISO/IEC 19792, ISO/IEC 24714, ISO/IEC 24760, aadhaar_registered_devices_1_5.pdf, aadhaar_authentication_api_1_6.pdf
22.	**Relation** *(Relation with other e-Governance standards notified by MeitY)*	None

Table of Contents

1. Introduction......6

2. Purpose......8

3. Scope......8

4. References......9

5. Abbreviations & Acronyms......10

6. Commonly Used Terms & Their Definitions......11

7. Biometric systems......14

7.1. Introduction to biometric systems...... 14

7.2. Biometric system operations...... 15

7.3. Biometric references and identity references...... 21

7.4. Biometric systems and identity management systems...... 22

8. Security aspects of a biometric system......23

8.1. Security requirements for biometric systems to protect biometric information...... 23

8.2. Security threats and countermeasures in biometric systems...... 25

8.3. Security of data records containing biometric information...... 27

9. Biometric application models and security......30

9.1 Biometric application models...... 30

9.2 Security in each biometric application model...... 30

9.2.1 Model A – Store on server and compare on server...... 30

9.2.2 Model F – Store on token and compare on token...... 31

10. Procedural vulnerabilities around the enrolment process......33

10.1 Leakage and alteration of biometric data...... 33

10.2 Application binding...... 33

11. Conformance Assessment/ Security Evaluation:......34

11.1 Testing security-relevant error rates...... 34

11.2 Vendor test and evaluation of vendor test...... 34

11.3 Vulnerability assessment...... 35

11.4 Biometric system threats overview...... 35

12. Recommendations:......36

12.1 Biometric Enrolment Security...... 36

12.2 Biometric Authentication Security...... 37

12.3 Authentication System Features...... 38

12.4 Offline Authentication Security Requirements...... 38

12.5 Process, Audits & Legal Provisions...... 38

1. Introduction

The Government of India has launched the Digital India programme with the vision to transform India into a digitally empowered society and knowledge economy. Under this flagship umbrella programme, various Mission Mode Projects are being implemented. e-Governance services for public including citizens and businesses in healthcare, education, agriculture, financial inclusion, banking, insurance, transportation etc. sectors are envisaged under Digital India, e-Kranti. For successful implementation of e-Governance projects, Standards play an important role by ensuring interoperability, security, reusability, openness, risk reduction and cost effectiveness.

The Aadhaar (TARGETED DELIVERY OF FINANCIAL AND OTHER SUBSIDIES, BENEFITS AND SERVICES) BILL, ACT to provide for, as a good governance, efficient, transparent, and targeted delivery of subsidies, benefits and services, the expenditure for which is incurred from the Consolidated Fund of India, to individuals residing in India through assigning of unique identity numbers to such individuals and for matters connected therewith or incidental thereto. The Aadhaar Act was published in the gazette notification on March 26, 2016.

In the Aadhaar system, every resident shall be entitled to obtain an Aadhaar number by submitting his identity reference (containing demographic information) and biometric reference by undergoing the process of enrolment.

The enrolling agency or the entity shall, at the time of enrolment, inform the individual undergoing enrolment of the following details in such manner as may be specified by Enrolment regulations of Aadhaar / Biometric System Provider, namely:—

(*a*) the manner in which the information shall be used;

(*b*) the nature of recipients with whom the information is intended to be shared during authentication; and

(*c*) the existence of a right to access information, the procedure for making requests for such access, and details of the person or department in-charge to whom such requests can be made.

On receipt of the identity reference containing demographic information and biometric reference details, the Aadhaar System issues an Aadhaar number to such individual, after verifying the information.

The Central Government or, as the case may be, the State Government may, for the purpose of establishing identity of an individual require that such individual undergo authentication, or furnish proof of possession of Aadhaar number or in the case of an individual to whom no Aadhaar number has been assigned, such individual makes an application for enrolment. Provided that if an Aadhaar number is not assigned to an individual, the individual shall be offered alternate and viable means of identification for delivery of the subsidy, benefit or service.

Any service provider or a requesting entity shall unless otherwise provided in the Aadhaar Act, obtain the consent of an individual before collecting his identity information or biometric information for the purposes of authentication ensure that the identity information or biometric information of an individual is only used for submission to the Central Identities Data Repository (CIDR) (the Aadhaar identity/biometric storage system) for authentication.

The consent information needs to be obtained as an

(a) acknowledgement from the resident regarding the entity's intimation about the purpose of authentication and his /her willingness to use Aadhaar identity information for authentication;

(b) data sharing part – for UIDAI to share identity information of Aadhaar number holder (excluding core biometric information) so that the requesting entity can subsequently use the Aadhaar number holder identity information for meeting its service needs.

Some of the e-Governance application such as e-Pramaan, e-sign, digital locker and banking are using UIDAI biometrics-based authentication services. Many other future applications will also be using this authentication mechanism. Since these applications are based on biometrics technologies, in order to provide e-Governance services in a secure manner, there is a need to secure all aspects of biometrics including the hardware, software and network components of the ecosystem based on global best practices.

This document provides guidelines to secure biometric systems including other components of the ecosystem.

2. Purpose

To develop comprehensive guidelines, recommended practices and defining the information security management process for all aspects of biometrics including the hardware, software and network components of the ecosystem based on global best practices. Scope would also cover suggested mechanism for conformance assessment.

3. Scope

The scope covers guidance for the protection of biometric information under various requirements for confidentiality, integrity and availability during storage, processing and transmission. These guidelines are meant for secure operations, processing, transmission, and storage of biometric information in e-governance applications/ systems.

This can also be used for specifying the requirements for preparing a RFP for developing a biometric-enabled system.

Scope also covers suggested mechanism for conformance assessment.

4. References

[1] THE AADHAAR (TARGETED DELIVERY OF FINANCIAL AND OTHER SUBSIDIES, BENEFITS AND SERVICES) ACT, 2016

[2] ITU-TX.1086,Tele-biometricsprotectionprocedures— Part1: A guideline to technical and managerial counter measures for biometric data security

[3] ISO 19092:2008, Financial services — Biometrics — Security framework

[4] ISO/IEC 19785-4, Information technology — Common Biometric Exchange Formats Framework — Part 4: Security block format specifications

[5] ISO/IEC 9796 (all parts), Information technology — Security techniques — Digital signature schemes giving message recovery

[6] ISO/IEC 9797 (all parts), Information technology — Security techniques — Message Authentication Codes (MACs)

[7] ISO/IEC 10116: Information technology — Security techniques — Modes of operation for an n-bit block cipher

[8] ISO/IEC 14888 (all parts), Information technology — Security techniques — Digital signatures with appendix

[9] ISO/IEC 18033-2:2006, Information technology — Security techniques — Encryption algorithms — Part 2: Asymmetric ciphers

[10] ISO/IEC 18033-3:2005, Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers2)

[11] ISO/IEC 18033-4:2005, Information technology — Security techniques — Encryption algorithms — Part 4: Stream ciphers

[12] ISO/IEC 19772, Information technology — Security techniques — Authenticated encryption

[13] ISO/IEC JTC1 /SC 37 Standing Document 11 (SD11).

[14] ISO/IEC TR 24714-1, Information technology — Biometrics — Jurisdictional and societal considerations for commercial applications — Part 1: General guidance

[15] ISO/IEC 24761, Information technology — Security techniques — Authentication context for biometrics

[16] ISO/IEC 7816-4:2005, Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange

[17] ITU-T X.1088, Tele-biometrics digital key framework (TDK) — A framework for biometric digital key generation and protection

[18] ISO/IEC 24787, Information technology — Identification cards — On-card biometric comparison

[19] ISO/IEC 19792, Information technology — Security techniques — Security evaluation of biometrics

[20] ISO/IEC 24760-1, Information technology — Security techniques — A framework for identity management

[21] ISO/IEC 29100, Information technology — Security techniques — Privacy framework

[22] ISO/IEC JTC 1/SC 37 Standing Document 2 — Harmonized Biometric Vocabulary

[23] Aadhaar Security Policy & Framework for UIDAI Authentication Version 1.0 (uidai.gov.in/images/authentication/d3_4_security_policy_framework_v1.pdf)

5. Abbreviations & Acronyms

AFIS	Automated Fingerprint Identification Systems
BR	Biometric Reference
BIR	Biometric Information Record
CI	Common Identifier
CIDR	Central Identities Data Repository
OCC	On-Card Comparison
DBBR	Database containing Biometric Reference
DBIR	Database containing Identity Reference
FAR	False Acceptance Rate
FRR	False Reject Rate
FMR	False Match Rate
FNMR	False Non Match Rate
IdMS	Identity Management System
IR	Identity Reference
MAC	Message Authentication Code
PDA	Personal Digital Assistant
PII	Personal Identifiable Information
USB	Universal Serial Bus
UIDAI	Unique Identification Authority of India

6. Commonly Used Terms & Their Definitions

For the purposes of this document, the following terms and definitions apply.

6.1. Authentication:

Process of establishing an understood level of confidence that a specific entity or claimed identity is genuine

6.2. Biometrics –the automated recognition of individuals based on their behavioural and physiological characteristics – has come of age, and includes recognition technologies based on fingerprint image, iris image, facial image, voice patterns, gait, palm print, veins pattern etc. The cost of biometric techniques has been decreasing while their reliability has been increasing, which makes biometric systems effective as an authentication mechanism.

6.3. Biometric characteristic

Physiological or behavioural characteristic of an individual that can be detected and from which distinguishing, repeatable biometric features can be extracted for the purpose of automated recognition of individuals

6.4. Biometric data

Biometric sample, biometric feature, biometric model, biometric property, other description data for the original biometric characteristics, or aggregation of above data

6.5. Biometric data subject

Individual whose biometric reference is within the biometric system (citizen/ resident?)

6.6. Biometric feature

Numbers or labels extracted from biometric samples and used for comparison

6.7. Biometric information privacy

Right to control the collection, transfer, use, storage, archiving, and disposal of one's own biometric information throughout its lifecycle.

6.8. Biometric model

Stored function (dependent on the biometric data subject) generated from a biometric feature or features

6.9. Biometric property

Descriptive attributes of the biometric data subject estimated or derived from the biometric sample by automated means

6.10. Biometric reference BR

One or more stored biometric samples, biometric templates or biometric models attributed to a biometric data subject and used for comparison

6.11. Biometric sample

Analog or digital representation of biometric characteristics obtained from a biometric capture device or biometric capture subsystem prior to biometric feature extraction

6.12. Biometric system

System for the purpose of the automated recognition of individuals based on their behavioural and physiological characteristics

6.13. Biometric template

Set of stored biometric features comparable directly to probe biometric features

6.14. Claim

Assertion of identity

6.15. Claimant

Individual making a claim of identity

6.16. Common identifier

Identifier for correlating identity references and biometric references in physically or logically separated databases

6.17. Central Identities Data Repository (CIDR)**:**

A centralized database or storage system in one or more locations containing all Aadhaar numbers issued along with the corresponding demographic and biometric information

6.18. False Acceptance Rate (FAR):

FAR is defined as the ratio of the number of false accepts to the number of impostor authentication attempts.

6.19. False Match Rate (FMR): The probability that the system incorrectly matches the input pattern to a non-matching biometric template in the database.

6.20. False Non Match Rate (FNMR): The probability that the system fails to detect a match between the input pattern and a matching biometric template in the database.

6.21. False Reject Rate (FRR):

FRR is defined as the ratio of the number of false rejects to the number of genuine Authentication attempts

6.22. Identification

Biometrics process of performing a biometric search against an enrolment database to find and return the identity reference attributable to a single individual

6.23. Identifier

Oneormoreattributesthatuniquelycharacterizeanentityinaspecificdomain

6.24. Identity

Set of properties or characteristics of an entity that can be used to describe its state, appearance or other qualities

6.25. Identity management system IdMS

System controlling entity identity information throughout the information lifecycle in one domain

6.26. Identity reference IR

Non-biometric attribute that is an identifier with a value that remains the same for the duration of the existence of the entity in a domain

6.27. Personally identifiable information PII

Any information

- that identifies or can be used to identify, contact, or locate the person to whom such information pertains,
- from which identification or contact information of an individual person can be derived, or
- that is or might be directly or indirectly linked to a natural person

6.28. Secure channel

Communication channel providing the confidentiality and authenticity of exchanged messages

6.29. Token

Physical device storing biometric reference and in some cases performing on-board biometric comparison

6.30. Verification

Biometrics process of confirming a claim that an individual who is the subject of a biometric capture process   is the source of a claimed identity reference

7. Biometric systems

7.1. Introduction to biometric systems

Biometric systems perform automated recognition of individuals based on one or more physiological and/ or behavioural characteristics.

Physiological characteristics include but are not limited to:

- fingerprint,
- face,
- iris,
- hand geometry,
- hand/ finger vein,
- retina,
- DNA,
- palmprint

Behavioural characteristics include but are not limited to:

- signature,
- gait
- voice

The following are desirable properties of biometric characteristics that lead to good subject discrimination and reliable recognition performance:

- Universality: Every individual should have the characteristic;
- Uniqueness: Every individual should have a distinguishable characteristic;
- Permanence: The characteristics should not show variance with time, example variance over time;
- Collectability: The characteristics should be easily collected from the subjects; and
- Repeatability: The characteristics should be sufficiently distinct and repeatable to achieve successful recognition of the subject.

From an application point of view, following additional properties should be taken into account:

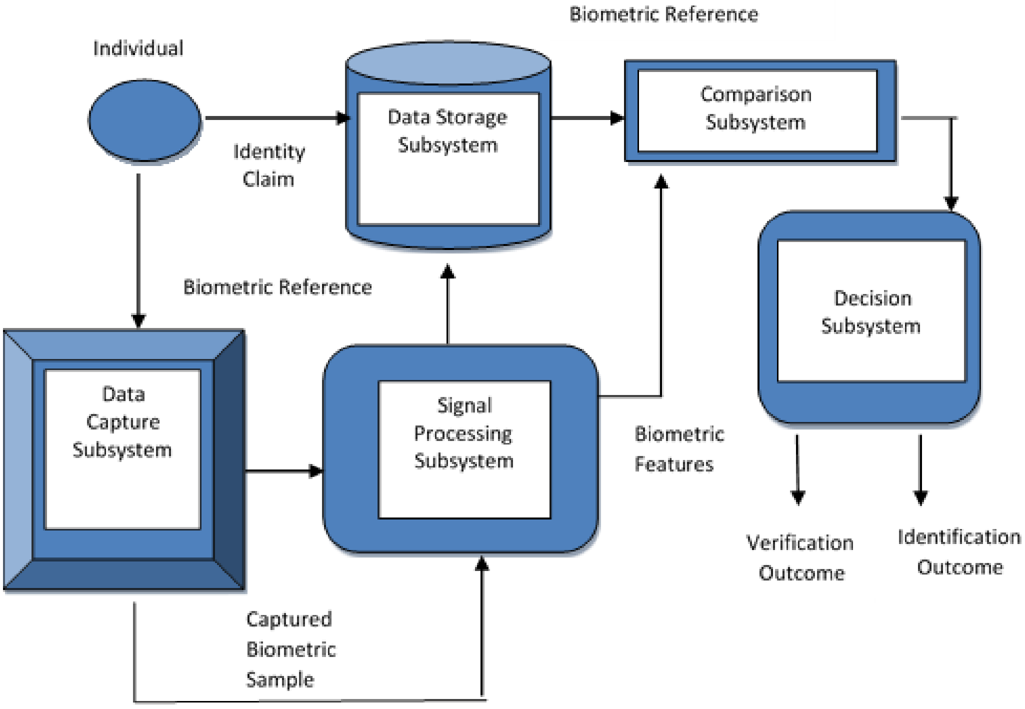
- Performance, which mainly refers to the success rate in recognizing individuals;
- Acceptability, which represents the level of willingness by the subject/ citizen to use the biometric system; and
- Spoof resistance, which indicates how difficult it is to use a replica of the biometric characteristic to circumvent the biometric system.

For verifying and/ or identifying an individual, a biometric system processes one or more probe samples for comparison against stored biometric reference(s). The biometric reference could be a biometric sample (e.g. an image representing the biometric characteristic) or a set of biometric features (i.e. a template that is derived from the image) or it could be a biometric model composed from the features.

These features are fingerprints, iris scans and photograph and other attributes as specified in the Aadhaar Act and as per regulations as and when notified.

7.2. Biometric system operations

Figure 1 — Authentication operation of a biometric system



The authentication operation of a biometric system is depicted in Figure 1, to highlight the processing of the identity reference.

The biometric system usually consists of five subsystems.

- **A biometric data capture subsystem**, which contains biometric capture devices or sensors for collecting signals from a biometric characteristic and converting them into a biometric sample such as a fingerprint image, facial image or voice recording.
- **A signal processing subsystem**, which extracts biometric features from a biometric sample with the intent of outputting numbers or labels which can be compared with those extracted from other biometric samples. Here, the biometric feature extracted in the enrolment process is stored in the data storage subsystem as a biometric reference for the identification and verification process.
- **A data storage subsystem**, which serves primarily as an enrolment database where the linking of the enrolled biometric references to the identity reference occurs. The data may contain biometric data and also non-biometric data such as the identity reference related to the subject. In practice, DBIR and DBBR are often logically or physically separated for reasons of security and privacy concerns.
- **A comparison subsystem**, which determines similarity between captured biometric samples (or derived features) and stored biometric references. In the case of the one-to-one comparison used in the verification process, a captured biometric sample is compared with a stored biometric reference from a biometric data subject to produce a comparison score.

However, in the one-to-many comparison used in the identification process, an extracted feature of a biometric data subject is compared against a set of biometric references of more than one biometric data subject to return a set of comparison scores.

— **A decision subsystem**, which determines whether captured biometric sample and the biometric reference have the same source (biometric subject), based on a comparison score(s) and a decision policy (or policies) including a threshold. In the case of the verification process, the biometric data subject may be accepted or rejected according to the comparison score. In the case of identification, a list of candidate identities that meet the decision policy is presented.

In essence, a biometric system involves 3 functional processes:

- Enrolment process: creating and storing an enrolment data record for an individual who is the subject of a biometric capture process in accordance with the enrolment policy. The subject usually presents his/her biometric characteristics to a sensor along with his/her identity reference. The captured biometric sample is processed to extract the features which are enrolled as a reference in the enrolment database with identity reference.
- Identification process: searching the enrolment database against the captured and extracted biometric features to return a candidate list. The candidate list consists of individuals whose references match with the feature in comparison subsystems and have a similarity score value higher than a predefined threshold value.
- Verification process: testing a claim that an individual who is the subject of a biometric capture process is the source of a specified biometric reference. The subject presents his/ her identity reference for a claim of identity and also their biometric characteristic (s) to the capturing device, which acquires biometric sample (s) to be used for comparison with the biometric reference linked to the identity reference for identity.

The verification process has a possibility of impacting on subject's information privacy since this process requires both biometric reference and identity reference. The identification process requires exhaustive search of enrolment database. So, this also has a possibility of impacting on subject's physical privacy. Verification is generally considered to be less privacy intrusive than identification. In Aadhaar system verification is done via online authentication having only a “yes/no” answer.

The five above mentioned subsystems represent the technical and functional blocks that capture, process, store, compare and decide on processing of biometric data. Also, other functional subsystems can be included.

Aadhaar System - Protection of Identity/Biometric Data Reference and Resident Data Privacy:

Privacy by Design: Security and privacy of resident data has been the fundamental building blocks of the Aadhaar System without compromising the utility of the national identity system. The Aadhaar enrolment coverage of about 102 crores has been achieved by the mid of the year 2016. While creating a national identity system of such as large scale, it is imperative that security and privacy of resident personal data are not afterthoughts, as they were designed into the strategy of the Aadhaar system from day-one.

The following measures are taken in the design of the Aadhaar system to address the privacy aspects:

(i) Aadhaar Numbering Scheme: Aadhaar number is a random number with no built-in intelligence or profiling information as the number is chosen based on the identification needs of the population in the next couple of centuries. In order to ensure privacy, no identity reference information such as date-of-birth, place of birth etc. are embedded in this number.

(ii) Minimal Data (with no linkage): As the Aadhaar system has the data of all the Aadhaar number holders in the country, it was essential to keep this data to a minimum to ensure identity related functions (issuance of Aadhaar and authentication) and nothing else. All the non-essential data are not to be held as per the design of Aadhaar system thereby ensuring privacy of the resident. In addition to having minimum, essential demographic data, this centralized database (CIDR) does not have any linkage to existing systems/applications that use Aadhaar. As a result, there is a set of data islands instead of a centralized model that eliminates the risk of a single system having complete information about the resident or his/her transaction history.

(iii) No Data Pooling: By design, the Aadhaar system is not intended to pool / collate resident data and so it does not become a single repository having all knowledge about residents. It has no interface/linkage to other systems (such as PAN, PDS, EPIC etc) and so this approach allows the transaction data to reside in the domain specific database systems. This way, privacy by design allows resident data to be distributed across many systems owned by different service providers or requesting entities. Any data transfer / collation across these distribution information silos are governed by the Aadhaar Act and the details of the same are covered in this section for reference.

(iv) Yes/No for Authentication: In Aadhaar system, the authentication services respond only with a "yes"/"no" answer for the Aadhaar number holder's claim of identity and no Personal Identity Information (PII) of the resident is shared from CIDR. Thus, the resident data privacy is protected as Aadhaar authentication services of UIDAI allows the service provider's application to verify the identity claims of the resident. In order to strengthen the data security, resident data privacy aspects and to comply with the provisions of the Aadhaar Act, UIDAI mandates all the requesting entities (partnered entities who are part of authentication ecosystem) to obtain an informed consent from the concerned Aadhaar number holder for every Authentication transaction.

(v) Explicit Resident Consented e-KYC: A balance between 'privacy and purpose' is critical to ensure convenience of online identity and it is balanced with the requirement to protect resident identity data. External requesting entities or service providers do not have access to Aadhaar database (CIDR). E-KYC service allows resident to authorize UIDAI to share electronic version of Aadhaar information (demographic information and photo). Resident authorization is not used for multiple transactions, instead, every time user agencies require electronic version of Aadhaar letter data for KYC purposes, resident must authorize the agency.

(vi) No Transaction History or Authentication Record contains the Purpose of Authentication: As indicated earlier on the fundamental building blocks of Aadhaar system**,** the objective of the Aadhaar design was not to keep track of specific transaction information containing the purpose of authentication viz. depositing money, obtaining pension, marking biometric attendance etc. This was consciously designed to ensure resident transaction history is not part of the central system to ensure the privacy of the resident. in accordance with the Aadhaar Act, Authentication regulations are being framed by UIDAI on resident identity data sharing and maintaining authentication records/logs for audit purposes.

Notwithstanding anything contained in any other law for the time being in force, and save as otherwise provided in this Act, the Authority (UIDAI) or any of its officers or other employees or any agency that maintains the Central Identities Data Repository shall not, whether during his service or thereafter, reveal any information stored in the Central Identities Data Repository or authentication record to anyone:

Provided that an Aadhaar number holder may request the Authority (UIDAI) to provide access to his identity information excluding his core biometric information in such manner as specified by Aadhaar Regulations, as may be notified by the Authority from time to time.

In accordance with the section 32 of Aadhaar Act, UIDAI, as an Authority shall maintain authentication records of Aadhaar number holders in such manner and for such period as specified in the Aadhaar Regulations. The Authority shall not, either by itself, or through any entity under its control, collect or keep or maintain the information about the purpose of authentication.

Resident Data Security and Data Protection in Aadhaar System: UIDAI has implemented data centre best practices and resident data in Aadhaar database and Business Intelligence (BI) data store are protected through various security measures that include **Encryption** – Ensures data is encrypted and not exposed/available for admin user or other type of user in plain text format, **Anti-Tampering** – Ensures data altering only through authorized applications and not through command line queries/scripts, **Data Partitioning** – Data is logically separated and held in multiple database systems with a random alias being the only link to ensure that there is no centralised data table where all resident data is available, and **Anonymization** of data using hashing techniques for Business Intelligence (BI) or reporting data store.

Aadhaar authentication/e-KYC services use open security standards and are intended to address transaction privacy. The record level encryption and tamper detection features ensure resident data within authentication data store is neither available to any internal user nor can it be modified by unauthorized users or applications.

Legal Provisions in the Aadhaar system for Data Sharing/Disclosure, Offences and Penalties

This section outlines the manner in which resident privacy and data sharing aspects are addressed in the Aadhaar system while ensuring compliance to the Aadhaar Act 2016.

(i) As per the clauses specified in the sub-section (1) of Section 29 of Aadhaar Act, no core biometric information collected/created from the individual would be shared with anyone for any reason whatsoever. Also, the core biometric information / reference is used only for the purpose of the generation of Aadhaar numbers and authentication.

(ii) The identity information, other than core biometric information, collected or created under the Act may be shared only in accordance with the provisions of this Act and in such a manner as specified by the regulations framed under the Aadhaar Act.

(iii) The clause (b) of sub-section (3) of Section 29 states that no identity information available with the requesting entity shall be disclosed further, except with the prior consent of the individual to whom such information relates.

(iv) No Aadhaar number or core biometric information collected or created under this Act in respect of an Aadhaar number holder shall be published, displayed or posted publicly, except for the purposes as may be specified by Aadhaar regulations.

Exceptional Scenario (a) for disclosure of Aadhaar number holder information to third parties: As specified in the Section 33 of Aadhaar Act, the disclosure of information including identity information or authentication records is not done, except in the case of an order of a court not inferior to that of a District Judge (provided that no court order under this sub-section of the Act shall be made without giving an opportunity of hearing to UIDAI, as an Authority) or in the interest of national security in pursuance of a direction of an officer not below the rank of Joint Secretary to the Government of India specially authorised in this behalf by an order of the Central Government.

Provided that every direction issued under this sub-section, shall be reviewed by an Oversight Committee consisting of the Cabinet Secretary and the Secretaries to the Government of India in the Department of Legal Affairs and the Ministry of Electronics and Information Technology, before it takes effect:

Provided further that any direction issued under this sub-section shall be valid for a period of three months from the date of its issue, which may be extended for a further period of three months after the review by Oversight Committee.

Exceptional Scenario(b) for disclosure of Aadhaar number holder information: If any service provider or a requesting entity requires to disclose the identity information of the Aadhaar number holder to any another entity in the Aadhaar authentication ecosystem, then the mandated consent statement issued to the individual needs to clearly intimate the Aadhaar number holder on the aspects relating to his/her identity data disclosure (as applicable based on service provider or requesting entity's services or business needs).

During the time of authentication**,** the service provider or requesting entity shall inform the individual submitting his/her identity information for authentication before taking his/her consent, the following details w.r.t authentication, namely:-

(*a*) the nature of information that may be shared upon authentication;
(*b*) the uses to which the information received during authentication may be put by the requesting entity;
(c) alternatives to submission of identity information or biometric reference to the requesting entity.

Thus, the data sharing requirements are addressed by the requesting entity based on the scenarios explained above.
However, the core biometric information in the CIDR would not be shared even in these exceptional scenarios.

Offences and Penalties associated with impersonation and data sharing violations

Any data sharing violation or attempts relating to impersonation of Aadhaar number holder at the time of enrolment / authentication are subject to offences and penalties in accordance with the clauses specified in Chapter 7 of Aadhaar Act. Some of the penalties associated with the violations on data sharing and impersonation attempts are listed hereunder:

(a) Penalty for impersonation at the time of Enrolment (as per Section 34): Whoever impersonates or attempts to impersonate another person, whether deador alive, real or imaginary, by providing any false demographic information or biometric information, shall be punishable with imprisonment for a term which may extend to three years or with a fine which may extend to ten thousand rupees or with both.

(b) Penalty for impersonation of Aadhaar number holder by altering biometric/demographic information (as per Section 35): Whoever, with the intention of causing harm or mischief to an Aadhaar number holder, or with the intention of appropriating the identity of an Aadhaar number holder changes or attempts to change any demographic information or biometric information of an Aadhaar number holder by impersonating or attempting to impersonate another person, dead or alive, real or imaginary, shall be punishable with imprisonment for a term which mayextend to three years and shall also be liable to a fine which may extend to ten thousand rupees.

(c)Penalty for impersonation (as per Section 36 for unauthorized collection of resident information): Whoever, not being authorised to collect identity information under the provisions of this Act, by words, conduct or demean our pretends that he is authorised to do so, shall be punishable with imprisonment for a term which may extend to three years or with a fine which may extend to ten thousand rupees or, in the case of a company, with a fine which may extend to one lakh rupees or with both.

(d) Penalty for disclosing identity information (as per Section 37): Whoever, intentionally discloses, transmits, copies or otherwise disseminates any identity information collected in the course of enrolment or authentication to any person not authorized under this Act or regulations made there under or in contravention of any agreement or arrangement entered into pursuant to the provisions of this Act, shall be punishable with imprisonment for a term which may extend to three years or with a fine which may extend to ten thousand rupees or, in the case of a company, with a fine which may extend to one lakh rupees or with both.

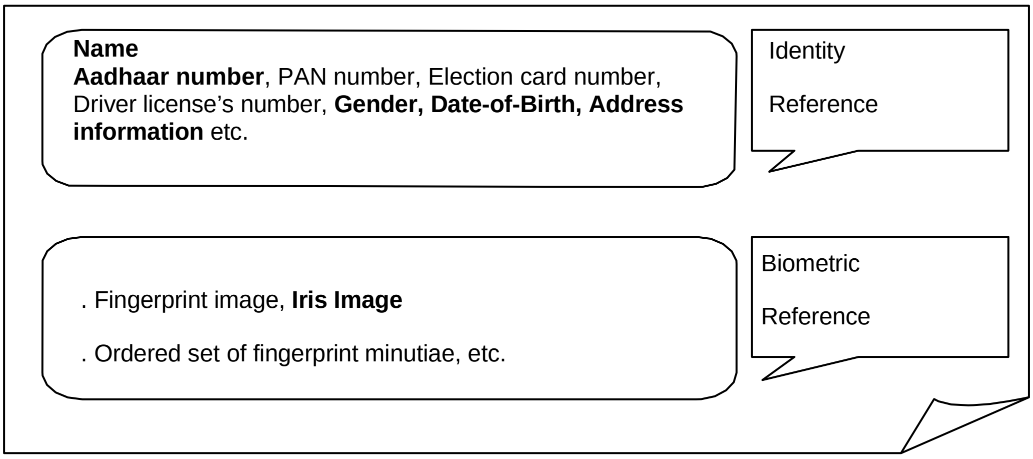
(e) Penalty for unauthorized access to the CIDR [as per Section 38(g)]: Whoever, not being authorized by the Authority, intentionally, reveals any information in contravention of sub-section (5) of Section 28, or shares, uses or displays information in contravention of Section 29 or assists any person in any of the aforementioned acts; shall be punishable with imprisonment for a term which may extend to three years and shall also be liable to a fine which shall not be less than ten lakh rupees.

7.3. Biometric references and identity references

Apersonhasoneidentifierinanyparticulardomainbutmayhaveseveralidentityreferencestoidentifythatpersonwithinthatdomain.Eachidentityreferenceis an attribute, or combination of attributes, of the identity of an entity that uniquely identifies that entity in a particular domain. An identity reference can also be a combination of attributes of the person.

A biometric reference is one of many attributes belonging to a person that can be used to recognize that person within a domain. This Standard classifies identity attributes into non-biometric and biometric ones. For the sake of simplicity, the former is referred to as the identity reference (IR) and the latter as the biometric reference (BR). Some examples, not a comprehensive or definitive list, of identity references and biometric references are depicted in Figure2. Here, the surrounding box represents the set of attributes that may be used to identify an individual.

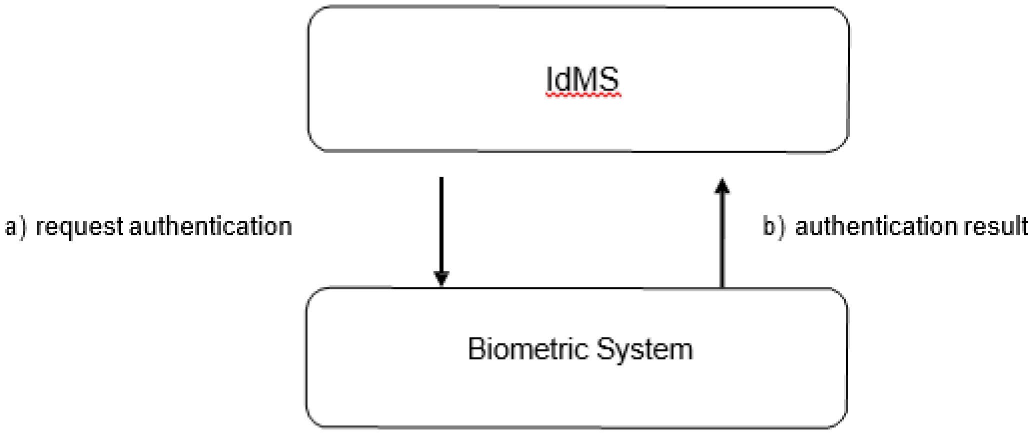
Figure 2 — Identity references and biometric references


Name
Aadhaar number, PAN number, Election card number, Driver license's number, **Gender, Date-of-Birth, Address information** etc.
Identity Reference
. Fingerprint image, **Iris Image**
. Ordered set of fingerprint minutiae, etc.
Biometric Reference

7.4. Biometric systems and identity management systems

The identity management system (IdMS) has an important role in any domain to avoid identity conflicts or ambiguities. An authentication system requires an accurate identification and verification process, within a well-defined domain, and a defined relationship with registration and enrolment processes which could be in that same domain or called in from another domain. When biometrics is used to provide an authentication service, IdMS may request authentication from the biometric system (ainFigure3) and the biometric system may provide the authentication result to IdMS (binFigure3).

Figure 3 — Biometric system as an authentication service provider for IdMS



In Aadhaar System, the basic functional process of "Identification" refers to the de-duplication of biometric data in the UIDAI database. In this de-duplication process, for each new enrolment, Aadhaar system performs a search based on the captured demographic and biometric information against all the enrolled resident data to achieve uniqueness. By having a combination of demographic and 1:1 biometric matching, the duplicate resident data can be identified including the ones corresponding to re-enrolment of same resident by different enrolment operators. Once the Biometric de-duplication is established, the applicant is issued a new Aadhaar number, as generated by the Aadhaar system.

The functional process "Verification" defined in section 7.2 correlates with the "Authentication" process in the Aadhaar system. Authentication means the process by which the Aadhaar number along with demographic information or biometric information of an individual is submitted to CIDR for its verification and such a repository verifies the correctness, or the lack thereof, on the basis of information available with it.In all forms of Authentication, the Aadhaar number of the individual is submitted so that the operation reduces to a 1:1 match. In addition, Aadhaar Authentication responds to an identity claim sent for verification, with a response "Yes"/" No" and no Personal Identity Information (PII) [including core biometric information] is returned as a part of response from the Aadhaar system except in the case of resident consented e-KYC where resident demographic details and Photograph are shared to the requesting entity that is partnered with the Authority and authorized to access itz e-KYC services.

8. Security aspects of a biometric system

8.1. Security requirements for biometric systems to protect biometric information

8.1.1 Confidentiality

Confidentiality is the property that protects information against unauthorized access or disclosure. In biometric systems, a biometric reference stored in a biometric reference database during the enrolment process is transmitted to a comparison subsystem during the verification and identification process. During this process, the biometric reference may be accessed by unauthorized entities and may be read or the binding to its identity information may be revealed. Unauthorized disclosure of data may cause critical privacy threats since biometrics are sensitive. The confidentiality of stored and transmitted biometric data can be obtained from access control mechanisms and various forms of encryption techniques

Implementation of Data Confidentiality using Encryption in Aadhaar system: The Aadhaar authentication service entails the usage of open data format in XML and widely used protocol such as HTTP. The Personal Identity Data (PID) consisting of resident demographic and biometric information (IR as well as BR) is formed as part of every authentication request XML as per Authentication API specifications. For every transaction, the PID is encrypted with a unique, dynamic, base-64 encoded session key using AES-256 symmetric algorithm (AES/PCB/PKCS7Padding). This session key, is in turn, encrypted with 2048 bit UIDAI public key using asymmetric algorithm (RSA/ECB/PKCS1 Padding).

8.1.2 Integrity

Integrity is the property of safeguarding the accuracy and completeness of assets. The integrity of a biometric reference is critical to the assurance of overall biometric system security. The integrity of the authentication process is dependent on the integrity of the biometric reference. If either the biometric reference or the captured and extracted biometric feature is untrustworthy, the resulting authentication will also be untrustworthy. Untrustworthy biometric references or samples could occur for one or more of the following reasons:

- accidental corruption due to a malfunction in hardware or software;
- accidental or intentional modification of a bonafide biometric reference by an authorized entity (i.e.,either an authorized enrollee or a system owner), without intervention of an attacker;
- modification (including substitution) of a biometric reference of an authorized enrollee by an attacker;

Biometric systems shall employ effective data integrity protection. This could be realized through access control mechanisms preventing unauthorized access to biometric data or by integrity checking using cryptographic techniques. Integrity protection may need to be combined with other techniques (such as time stamping) to protect against the reuse of stolen biometric data and replay attacks.

NOTE1 Various techniques, such as Message Authentication Code (MAC) or digital signature, can be used to provide data integrity.

NOTE2 Certain situations require both confidentiality and integrity. If both confidentiality and integrity protection are required, one possibility is to use both encryption and a MAC or digital signature. Another possibility is to use authenticated encryption.

NOTE3 When a smart card is used for biometric reference storage and/ or comparison, Secure Messaging mechanisms should be used for biometric data integrity and/ or confidentiality.

Usage of HMAC in Authentication for Data Integrity in Aadhaar System: Every Aadhaar authentication request consists of the formation of input data in the form of Personal Identity Data (PID) in accordance with the specifications prescribed by UIDAI through Authentication API. After forming the PID for authentication request (XML), the SHA-256 is computed for the PID XML string and it is encrypted using session key generated for every authentication transaction. Then, it is followed with encoding using Base 64 encoder. On receiving the request, the Aadhaar authentication server decodes and decrypts the PID information. Then, it computes the SHA-256 hash of PID. The value of the HMAC element is also decrypted and decoded and it is compared against the Hash of the PID extracted from the authentication request. If there is a match, then the integrity of the authentication request is considered to be preserved.

Usage of Digital Signature for preserving Data Integrity in Aadhaar system: The requesting entities or service providers who intend to use Aadhaar authentication services of UIDAI ensure to digitally sign the authentication request XML for message integrity and non-repudiation purposes, in accordance with the Aadhaar Authentication API specifications. This feature ensures message security between the servers of the service provider/requesting entity and its client applications. The digital signing of request is based on XML digital signature algorithm as recommended by www consortium. Class-II or Class-III digital certificates are recommended for Aadhaar Authentication/e-KYC transactions. UIDAI validates the digital signature of the requesting entity that by checking whether the digital signature is issued by one of the valid certification authority. If this is valid, then it checks X.509 certificate to see if the requesting entity / organisation name matches with the partner entity name available in the Aadhaar system. If it matches, the server proceeds with the API logic. After processing, the authentication response is digitally signed by UIDAI and sent back to the service provider/requesting entity. This ensures that message/data integrity during the entire transmission of data i.e. request as well as response.

8.1.3 Availability (as applicable in the Aadhaar System)

Data Centre (DC) replication is implemented in the Aadhaar system and the resident data is available at two of the data centres. The application servers are hosted on both these data centres for handling transaction requests (authentication/e-KYC). Thus, availability of UIDAI hosted services is ensured through a redundancy in equipment and component level. Restricted access is enabled only through the authorized entities via leased lines or MPLS connectivity to the data centres and there is no direct link given to any third party entities.

8.2. Security threats and countermeasures in biometric systems

8.2.1 Threats and countermeasures against biometric system components

Table1—Threats and countermeasures of biometric subsystems

	Threats	Countermeasures
Data Capture	Sensor spoofing Capture/ replay of signals from sensor	• Liveness detection • Multimodal biometric • Challenge/ response • Use of registered devices
Decision	Hill climbing attack	• Secure channel • Hide comparison score from subject
	Threshold manipulation	• Access control to threshold setting • Threshold value protection through digital signature and encryption

NOTE 1 The implementation of the Comparison and Decision components in a certified single module constitutes an effective countermeasure against threats of comparison score manipulation. Here, additional counter measure of hiding comparison score from subject is required to prevent a hill climbing attack.

NOTE 2 The threat of component replacement is applicable for all subsystems. Against this threat, using inventory control involving digitally signed components can be an effective countermeasure. Brief descriptions of the aforementioned threats and countermeasures are provided below for clarification.

— Sensor spoofing means the presentation of artificial and thus non-live biometric characteristics. One countermeasure to sensor spoofing is use of assisted mode of authentication using a trained/certified operator that can address the threat encountered during spoofing. The other counter measure to this is the liveness detection based on recognition of a subject's physiological activities assigns of life or the detection and rejection of known artefact types.

— Component replacement involves the substitution of the components (e.g., comparison or decision subsystem) of the biometric system so as to control it and obtain a desired output.

— Hill climbing is the systematic modification of the biometric sample to obtain progressively higher comparison scores until the decision threshold has been met. In Aadhaar system, the threshold score is not revealed.

— Threshold manipulation is changing the threshold value of the decision subsystem such that the biometric system easily accepts an illegitimate biometric sample.

— Data separation refers to the security countermeasure of logically or physically separating individual data elements.

8.2.2 Threats and countermeasures during the transmission of biometric information

The communication channels between the various components of the biometrics system can be compromised, jeopardizing the security of the overall system. This risk is especially relevant for distributed architectures. The occurrences of data transmission are shown in Figure 4 and summarized in Table 2. In Table 2, if a network intervenes between comparison and decision subsystems, the threats and their countermeasures for T1, T2, and T3 are also applicable for T4.

Figure 4 — Threats in the biometric system

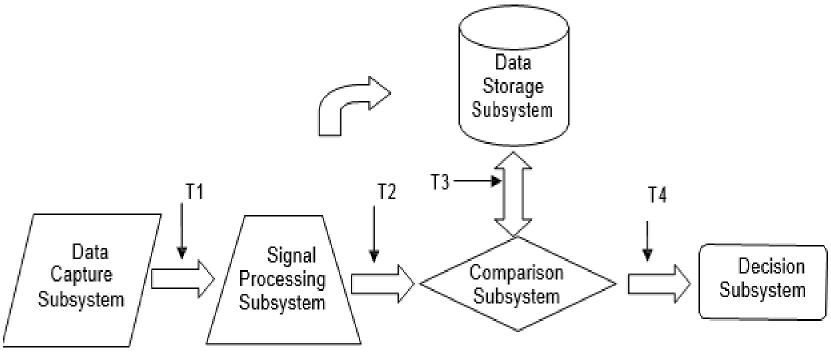


Table2—Threats and counter measures during transmission

	Data	Threats	Counter measures
Data Capture-Signal Processing(T1) Signal Processing – Comparison (T2)	Biometric sample and feature	Eavesdropping	Encrypted/ secure channel Biometric data signing within registered device
		Replay	Challenge/ response Salting and signing
		Brute Force	Time out policy
Storage - Comparison (T3)	Biometric reference	Eavesdropping	Encrypted/ secure channel
		Replay	Challenge/ response Salting and signing
		Man in the middle	Encrypted / secure channel Integrity check of biometric data with digital signature or MAC
		Hill climbing	Coarse scores Secure channel
Comparison - Decision (T4)	Comparison score	Comparison score manipulation	Secure channel

NOTE: The implementation of the Comparison and Decision components in a certified single module constitutes an effective countermeasure against manipulation of comparison score threats. Brief descriptions of the aforementioned threats are provided below for clarification.

- Eavesdropping is the interception of sensitive information during its transmission between components of the biometric system.
- Man-in-the-middle attacks are attacks in which an attacker can read, insert and modify the biometric data communicated between two parties without either party knowing that the established link has been compromised.
- In Aadhaar system, the biometric data is always transmitted in encrypted format with HMAC for tamper detection.

The list of countermeasures in Table 2 is not comprehensive. A risk analysis should be performed to identify threats in the context of the application. Appropriate countermeasures should be put in place which can include procedural as well as technical countermeasures.

8.3. Security of data records containing biometric information

8.3.1 Security for biometric information processing in a single database

A logical concatenation of an identity reference (IR) with a biometric reference (BR) is required to perform biometric authentication operations as shown in Figure 1. There are a number of applicable scenarios that can be used to describe the security of this binding, depending on the data records (e.g., identity reference, biometric reference, etc.) being stored. These scenarios, showing the data element combinations, as well as outlining the associated security properties, are listed below. Only **scenario 10 is recommended** to be used for UIDAI based Authentication. The other scenarios pose risk of identity/ biometric theft.

- **Scenario1**: Raw IR and Raw BR are stored. Neither confidentiality nor integrity is provided for both IR and BR.
- **Scenario2**: Raw IR and encrypted BR are stored. Neither confidentiality nor integrity is provided on IR. Confidentiality on BR is provided. A weak form of integrity may be provided on BR depending on the mode of operation of encryption.
- **Scenario3**: Raw IR and authenticated BR are stored. Only integrity of BR is provided.
- **Scenario4**: Raw IR and authenticated-encrypted form of BR are stored. Both confidentiality and integrity are provided on BR.
- **Scenario5**: Encrypted IR and raw BR are stored. Confidentiality on IR is provided. A weak form of integrity may be provided on IR depending on the mode of operation of encryption.
- **Scenario6**: Authenticated IR and raw BR are stored. Only integrity of IR is provided.
- **Scenario7**: Authenticated-encrypted form of IR and raw BR are stored. Confidentiality and integrity are provided only on IR.
- **Scenario8**: Raw IR and raw BR are encrypted and then stored. Confidentiality on both IR and BR is provided. A weak form of integrity may be provided on both IR and BR depending on the mode of operation of encryption.

— **Scenario9** Raw IR and raw BR are authenticated and then stored. Integrity on both IR and BR is provided.

— **Scenario10** Authenticated-encrypted forms of IR and BR are stored. Confidentiality and integrity are provided on both IR and BR.

— **Scenario 11**: Raw IR and authenticated BR are encrypted and then stored. Confidentiality is provided on both IR and BR. Integrity is provided on BR. A weak form of integrity may be provided on IR depending on the mode of operation of encryption.

— **Scenario 12**: Raw IR and encrypted BR are authenticated and then stored. Integrity is provided on both IR and BR. Confidentiality is provided on BR only.

— **Scenario 13**: Authenticated IR and raw BR are encrypted and then stored. Confidentiality is provided on both IR and BR. Integrity is provided on IR. A weak form of integrity may be provided on BR depending on mode of operation of the underlying cryptographic algorithm.

— **Scenario 14**: Encrypted IR and raw BR are authenticated and then stored. Integrity is provided on both IR and BR. Confidentiality is provided on IR only.

The described scenarios and related security considerations are summarized in Table 3.

Table 3 — Confidentiality, integrity for the data records stored in a single database
(Enc'd: encrypted, Aut'd: authenticated, AuE'd: authenticated-encrypted, **O**: requirement, **Δ**: weak requirement)

Scenario	Security Requirements				
	Confidentiality		Integrity		Countermeasures
	BR	IR	IR	BR	
2		**O**		**Δ**	Raw IR and Enc'd BR
3				**O**	Raw IR and Aut'd BR
4		**O**		**O**	Raw IR and AuE'd BR
5	**O**		**Δ**		Enc'd IR and Raw BR
6			**O**		Aut'd IR and Raw BR
7	**O**		**O**		AuE'd IR and Raw BR
8	**O**	**O**	**Δ**	**Δ**	Enc'd(IR and BR)
9			**O**	**O**	Aut'd(IR and BR)
10	**O**	**O**	**O**	**O**	AuE'd(IR and BR)
11	**O**	**O**	**Δ**	**O**	Enc'd(IR and Aut'd BR)
12		**O**	**O**	**O**	Aut'd(IR and Enc'd BR)
13	**O**	**O**	**O**	**Δ**	Enc'd(Aut'd IR and BR)
14	**O**		**O**	**O**	Aut'd(Enc'd IR and BR)

8.3.2 Security for biometric information processing in separated databases

When storing IR and BR, it is recommended they be stored separately if privacy is required, because the exposure of both items leads to more serious privacy compromise. Even if IR and BR are separated into different storage areas, protection is not effective if they are controlled by same operator. For the separation to be effective, it should be controlled by different operators with their own cryptographic keys to protect their DB contents. When IR and BR are separated, there shall be a means to link them. This is achieved by a common identifier, CI.

In Table 4, scenarios employing separated databases are shown. **The security requirements of confidentiality and integrity remain the same i.e. only authenticated and encrypted - IR & BR are recommended for usage.** However, the impact of a privacy compromise becomes smaller even if only one of IR and BR is exposed. If one DB is compromised and its contents are illegally modified, the operators of two DBs should be able to detect it. Similarly, during the usage of the DBs, if a legitimate DB operator with a correct key modifies its contents, the other DB should be able to detect the modification. For these cases, more secure binding is required.

Table 4 — Confidentiality and integrity - for the data records stored in separated databases
(Enc'd:encrypted,Aut'd:authenticated,AuE'd:authenticated-encrypted,CI:commonidentifier, **O**:requirement,**Δ**:weakrequirement)

Security Requirements				Counter measures for IR	Counter measures for BR
entiality		Integrity			
IR	BR	IR	BR		
	O		Δ	CI, Raw IR	CI, Enc'd BR
			O	CI, Raw IR	CI, Aut'd BR
	O		O	CI, Raw IR	CI, AuE'd BR
O		Δ		CI, Enc'd IR	CI, Raw BR
		O		CI, Aut'd IR	CI, Raw BR
O		O		CI, AuE'd IR	CI, Raw BR
O	O	Δ	Δ	CI, Enc'd IR	CI, Enc'd BR
		O	O	CI, Aut'd IR	CI, Aut'd BR
O	O	O	O	CI, AuE'd IR	CI, AuE'd BR
O	O	Δ	O	CI, Enc'd IR	CI, AuE'd BR
	O	O	O	CI, Aut'd IR	CI, AuE'd BR
O	O	O	Δ	CI, AuE'd IR	CI, Enc'd BR
O		O	O	CI, AuE'd IR	CI, Aut'd BR

9. Biometric application models and security

9.1 Biometric application models

Biometric systems can be classified by considering the locations where biometric references and identity references are stored and where they are compared, as shown in Table 5. In terms of security, each model has certain advantages and disadvantages with regard to managing biometric references and identity references when they are transferred or stored. Conceptually, many models exist; however, this Standard considers only two types of models (A & F) which are currently deployed in real world applications.

The Aadhaar system is classified as type "A".

Table 5 — Application model of a biometric system

		Storage		
		Server	**Client**	**Token**
Comparison	**Server**	**A**		B
	Client	C	D	E
	Token			**F**

The locations can be described as follows.

— A server is a computer remotely connected with the client via the network. A "biometric authentication server" is one form of a server.

— A client is a PC or its equivalent executing a general purpose operating system which can exist in the form of a kiosk. The essential properties of a client are that it provides the front end services for a biometric system and interfaces with server and/ or token. A biometric sensor unit can be connected to or embedded in the client. PDAs and certain smart mobile phones are considered clients in this Standard.

— A token is a portable physical device capable of supporting biometric reference storage and in some cases allowing biometric comparison. Tokens for biometrics storage include USB memory sticks, e- passports and smart cards. Smart cards can integrate a Comparison-on-Card application for biometric comparison and decision.

NOTE: The biometric sensor connected to a client via an interface and embedded sensor module within a client can be considered as other locations for storage and comparison. However, clients are frequently equipped with biometric sensors. As such, this Standard considers them as a part of the client & hence controlled & secured by the client with the use of assisted mode of authentication using a trained/certified operator.

In the following, models A and F describe two topologies for the locations of the various subsystems.

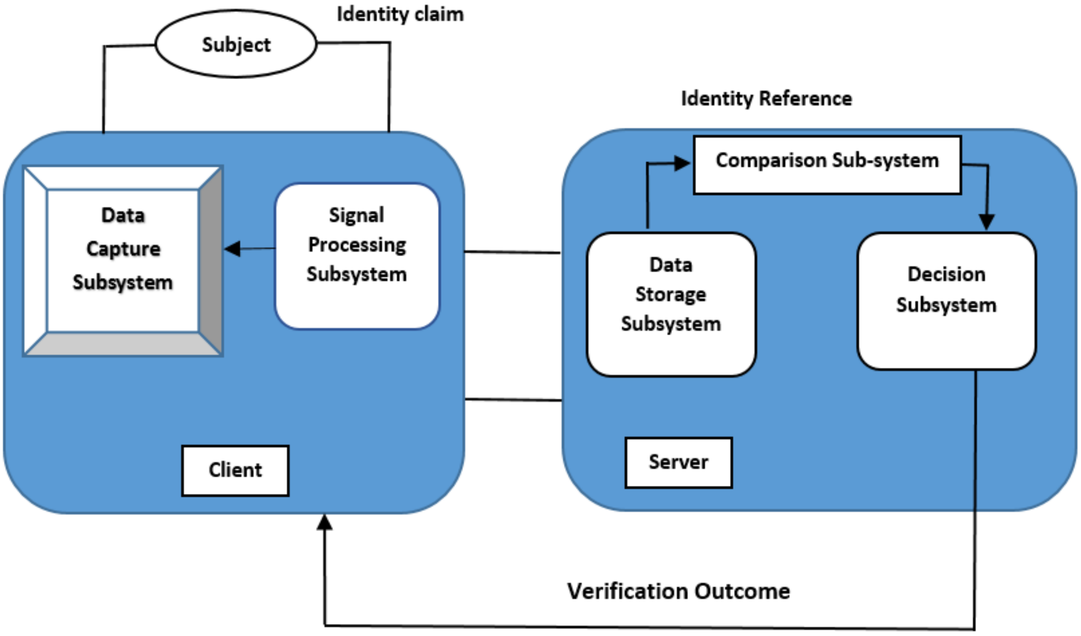
9.2 Security in each biometric application model

9.2.1 Model A – Store on server and compare on server

In this model, biometric references are stored on a server and it is required that the extracted biometric data be transferred from client to the server for comparison, as shown in Figure 5.

The subject's biometric reference and the corresponding identity reference are associated as part of the registration/ enrolment process.

Figure 5 — Model A: store on server and compare on server using BRs

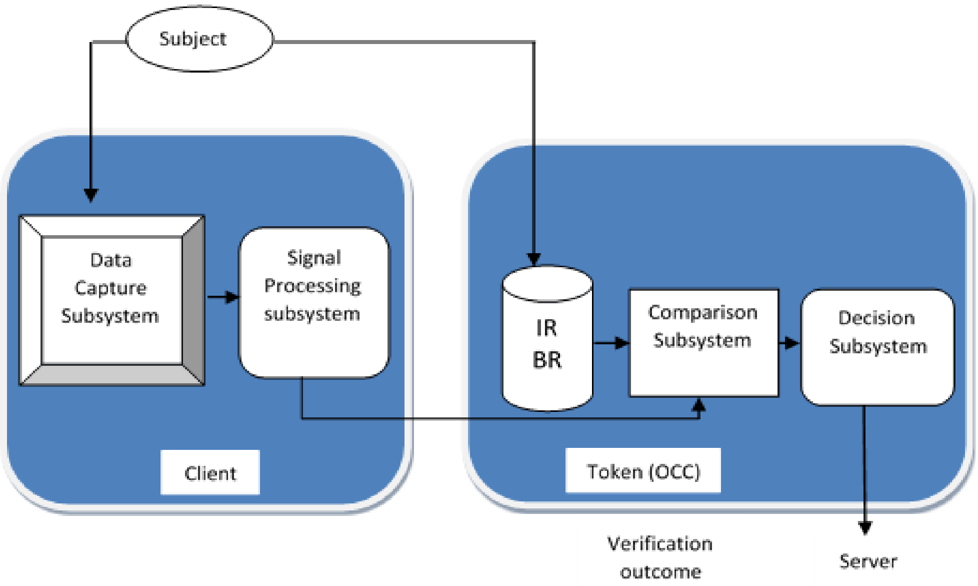


This model requires that the server trusts the data captured from the client. This model can be used for identification and also for verification. Since the sensitive PII (i.e., the biometric reference and identity reference) is handled by the server, reliable database security and network security are required. A large-sized commercial automated biometric identification system (ABIS) is usually implemented according to this model.

9.2.2 Model F – Store on token and compare on token

In this model, the biometric references are stored on the token and the probe biometric sample is extracted from the biometric subject for the comparison process, which is performed on the token as shown in Figure 6. The subject associates his/her biometric reference with the identity reference at the token during the enrolment process. A subject who wants to assert his/her identity must present his/her probe biometric sample to the client with the token. To deploy this model, the token must be equipped with a comparison/decision algorithm. Here, the client could be an automated teller machine (ATM). This model is usually applied to bank transactions using OCC.

Figure 6 — Model F: Store on token and compare on token using BRs



The token stores the BR and IR and the comparison process is also executed on the card. The token shall have self-execution ability. The command addressed to the card to start the comparison process and the subsequent response by the card conveying the result of the comparison process should be secured using the Secure Messaging mechanism as per ISO/IEC 7816-4. The client acquires a probe biometric sample and IR data and sends them to the token for the comparison process. The result of the comparison is sent to the server. Here, the token may contain the signal processing subsystem. The e-governance projects which can be mapped to this type of system are Rashtriya Swasthya Bima Yojna (RSBY) and e-Passport.

In this model, the client can be a kiosk type, as found in public places such as airports and in public buildings for personal authentication. This model can also be applied in border control settings using the e-passport (or another token) in a registered traveller application. Mostly used for offline authentication, in situations where connectivity with database server is an issue. **This model is to be used in very rare conditions where the network connectivity is not available and those projects which are using this model are advised to have a plan to migrate to Type "A" (Model).**

10. Procedural vulnerabilities around the enrolment process

There are three cases that involve potential vulnerability during the enrolment process.

An attacker could try to become enrolled into the biometrics system by inappropriate registration and enrolment using false (someone else) or bogus (invented) identity documentation. Such an attack, if successful, would allow the attacker to be recognized by the biometric system as another user in future. Aadhaar eliminates the possibility of multiple fake enrolments by following a de-duplication process. An attacker could also try to get enrolled into the biometric system with an artefact to generate a false (someone else) or bogus (invented) biometric reference. A successful attack in this case would allow the attacker to recognize by the biometric system as another user in future.

Poor quality biometric reference usually adversely affects security relevant error rates resulting in higher error rates than predicted. This will not only reduce the security assurance level of operational verifications or identifications involving poor quality references; if an attacker can identify individuals with poor quality references, they could become targets for impersonation attempts.

10.1 Leakage and alteration of biometric data

Through common IT vulnerabilities do not fall into the scope of this Standard, the possible leakage and manipulation of security-relevant data such as biometric samples, biometric references, comparison scores, threshold settings etc. is an important vulnerability to be considered during each security evaluation. In additional, it should be mentioned that while possible countermeasures for such vulnerabilities are common to IT system, the role of the information that is handled by the biometric system is specific to the biometric technology.

10.2 Application binding

Due to the fact that interoperable biometric systems are available, it may be possible that a biometric template is usable in a system other than that for which it was created.

The evaluator shall ensure that the biometric system provides mechanisms to prevent the privacy-relevant data from being used in systems outside the scope of the application context. Aadhaar system envisages only encrypted biometrics to be transmitted.

NOTE: The management, i.e. import and/ or export, of the databases may be an issue regarding the application binding. The limitation and/ or the control of the importing and exporting of databases (including backup procedures) should prevent unexpected or non-specified usages of them for applications and purposes other than their intended and specified goals. However, procedural mechanisms for application binding are out of the scope of this standard.

11. Conformance Assessment/ Security Evaluation:

Security evaluation of a biometric system can be conducted in the same manner as the security evaluation of any other IT system. This section introduces the concept of a test of security-relevant error rates in the context of a biometric system security evaluation. Statistical error rates can be measured for biometric algorithms alone (typically using pre-existing databases of biometric samples), or for systems where users provide the biometric samples directly to the sensor of the data capture component. Error rate testing of biometric algorithms is often used to compare the performance of different algorithms and to quantify changes resulting from algorithm development. Algorithm testing is of limited value in security evaluation because algorithmic errors are only one source of errors in a biometric system. It is normally necessary to conduct statistical error measurement of biometric systems using biometric samples acquired by the capture component of the system from real subjects in a scenario test. However, a statistical test of an algorithm may contribute to the necessary understanding of the biometric system that is needed to prepare the test or to find a claim about the maximum error rates of the biometric system. STQC-UIDAI device certification scheme envisages all the devices to participate in Field FRR testing, only those which meet the UIDAI's criteria are allowed to participate in the constellation.

11.1 Testing security-relevant error rates

The reason why both FAR/FMR and FRR/FNMR need to be measured is that there exists an inverse relationship between these types of error for a biometric system and it is usually possible to adjust the system to achieve any desired FAR/FNMR value if no limitation is placed on the FRR/FNMR value. For an access control application, the FAR/FMR value can be thought of as denoting the security while the FRR/FNMR value corresponds to usability. This security/usability trade-off is analogous to the case of passwords where password length and randomness (security) can be traded off against difficulty of memorizing (usability). Many password security policies are formulated by consideration of the security aspects alone, without regard to usability. This is not, however, deemed acceptable for a biometric system. The reason for this apparent inconsistency is perhaps that a usability failure for password authentication is seen as a human failure, whereas for biometric recognition it is seen as a system failure. The purpose of measuring security relevant error rates of a biometric system is to provide reliable figures upon which to establish the fundamental assurance of verification or identification decisions made by the system.

11.2 Vendor test and evaluation of vendor test

Performance testing requires significant resources. It is therefore advisable for the vendor and evaluator to agree the test methodology, protocol and report format prior to commencing the performance test, to ensure that the performance test will meet the requirements of the evaluation. In addition, the following issues shall be addressed during planning and execution of testing and shall be included in test documentation:

- The test crew shall be appropriate to the targets application,
- Any assumption made about the test scenario shall be stated and justified.
- The test environment shall be consistent with the target application,

- The security relevant error rates shall be reported and shown to be acceptable for the target application,
- Security relevant threshold value(s) and configuration parameters shall be set in accordance with vendor recommendations for the test,
- The retry counter shall be set in accordance with the vendor recommendations,
- The single attempt error rate shall be measured and reported,
- The statistical approach to the test shall be reported and justified by the vendor.

11.3 Vulnerability assessment

This sub clause focuses on the vulnerability assessment specific to biometric systems. It provides guidance for evaluations by identifying typical vulnerabilities that are common to biometric systems and describes the characteristics of a biometric system upon which these potential vulnerabilities are based. Vulnerability assessment benefits from a methodical approach. However, it also requires expertise and creative thinking on the part of the evaluator. Evaluators will therefore need to be aware of the threats, vulnerabilities and countermeasures that exist and in some cases are specific to biometric systems. Information on biometric vulnerabilities is provided in this Standard but evaluators should also seek out further information available in the literature, including public domain reports on biometric vulnerabilities appearing in magazines, academic studies and by searching the internet. Additionally, evaluators should acquire practical experience with the techniques of biometric vulnerability investigation as described in these reports. This should be regarded as necessary pre-requisite training for evaluators before conducting a vulnerability assessment as part of a biometric security evaluation under this Standard.

11.4 Biometric system threats overview

Threats against biometric systems can manifest themselves in various ways but are principally aimed at achieving one or more of the following objectives:

- **Impersonation**: A threat against a verification or identification system that is working with a positive claim where an attacker is recognized as another user that is correctly registered, thereby allowing the attacker to obtain the other user's ID.
- **Disguise**: A threat to a verification or identification system that an enrolled user might deliberately change or conceal their biometric characteristic(s) in order to avoid being recognized. This could be a particular threat to a system whose objectives include the prevention of multiple enrolments by a single individual using different identities.
- **Denial of service**: A threat to a verification system or identification system that is working with a positive claim where an attacker repeatedly causes a false rejection, which may cause a biometric system breakdown. This could be a precursor to an attack on a fall-back system that is easier to exploit than the disabled biometric system.

12. Recommendations:

Biometrics data handling is a complex task due to the sensitivity of the data. It is thus highly recommended that e-Governance applications eliminate the need to enroll, process, and store biometrics within their applications and instead take advantage of Aadhaar system. In most scenarios, customer/beneficiary identification and authentication can be done using Aadhaar and e-Governance application can build on the strengths and convenience of Aadhaar. Aadhaar system fully supports a federated authentication model where in e-Governance applications can add additional factors of authentication (such as mobile OTP, PIN, etc.) on top of Aadhaar without having to deal with biometrics.

E-Governance applications needing to capture and process biometrics should carefully evaluate the need and ensure this is necessary for their applications. In the case where the application decides to capture, process, and store biometrics, all security measures described within this section should be followed to ensure biometrics data is protected.

In the case where e-Governance application decides to take advantage of Aadhaar, agencies can eliminate the need for biometric enrolment and storage. For the purposes of authentication, agencies should follow authentication security guidelines of specified by UIDAI without having to worry about enrolment and storage of biometrics data.

12.1 Biometric Enrolment Security

The Unique Identification Authority of India (UIDAI) has been mandated for providing a unique identity (Aadhaar) number to all residents of India and also defining usages and applicability of Aadhaar for various services.

Aadhaar, from UIDAI, provides the ability to digitally establish individual unique identity and further authenticate the beneficiary during service delivery.

Biometric Capture

The following capabilities are mandated during biometric data capture during enrolment:

- The enrolment software must be written, maintained, and provided by enrolling entity to all field enrolment agencies.
- Enrolment software provided for field work ensures that only approved and authentic operators can sign-in to the enrolment software system to perform enrolment.
- Enrolment data packets (individual electronic file containing resident demographics and biometrics) should be strongly encrypted by the Enrolment Client software at the time of enrolment even before saving any data to any hard disk.
- Client software should preferably run in a secure environment such as Virtual Machine, to prevent Malware and modification to the client software
- Every enrolment record should be signed by operator ensuring traceability and non-repudiation.
- All audits during field enrolment should be captured electronically. This means every enrolment is fully traceable in terms of “who”, “when”, "where", “which agency”, “who reviewed”, “any exceptions”, "software version", "host OS info", etc.

Transmission

The following security requirements are mandate during transmission from the enrolment client to the data centre:

- Every enrolment data packet should "always" be stored and transmitted in encrypted form and is never decrypted or modified during transmission.

Data Centre

The following security requirements are mandated when processing the enrolment at a data centre:

- Data centres must be located within India.
- The data centre must be secured using multiple levels of firewalls and intrusion detection and protection systems.
- The data centre should be divided in multiple zones with highly controlled access between zones.
- Continuous vulnerability assessments should be done and all security patches should be up to date.
- Even within the data centres, biometric data should be stored in different databases without any PII.
- Biometric data should always be stored in encrypted form even within data centre kept isolated with highly controlled access.
- This biometric signature is validated at the server end before even processing the enrolment. This is to ensure only those packets from authentic and approved operators/sources are processed.

12.2 Biometric Authentication Security

Towards Aadhaar enable delivery of various services, UIDAI proposes to provide online authentication using demographic and biometric data. The purpose of Aadhaar Authentication is to enable Aadhaar-holders to prove their identity digitally and online, and for service providers to confirm the resident's identity claim in order to supply services and give access to benefits.

Aadhaar authentication is the process wherein Aadhaar number, along with other attributes (demographic/ biometrics/ OTP) is submitted to UIDAI central identities data repositories (CIDR) for verification, the CIDR verifies whether the data submitted matches the data available in CIDR and response with a "YES/NO". No personal identity information (PII) is returned as part of the response. The purpose of the authentication is to enable residents to prove their identity and service providers to confirm that the residents are "who they say they are" in order to supply services and give access to benefits.

The following security requirements are recommended for biometric authentication.

Biometric Capture

- Liveness detection - Biometric sensor implementations should preferably implement liveness detection to ensure any attempt at making fake fingers/iris etc. are prevented.
- Secure capture - The authentication system should preferably implement a secure capture process (as in Aadhaar registered devices), which prevents any stored biometrics from being used within any network.

Transmission

- Data security - Every biometric data packet should be strongly encrypted and tamper proofed from the time it is captured within the application. Agencies must use a secure transport protocol such as SSL to transmit encrypted data. Use of this double encryption scheme (data and transport) is essential to ensure no "man-in-the-middle" attack can happen and entire biometrics data is end-to-end secure.
- Network security - All transactions should be digitally signed to ensure calling agencies are authenticated for every transaction. In addition, API keys must be provided to ensure authentication of calling agencies and their access to various online services. Secure protocols such as SSL must be used to transmit data.

12.3 Authentication System Features

- Biometric locking - The authentication system should implement biometric locking feature for users to lock their biometrics from being used for authentication. System should allow people to lock their biometrics and unlock only when needed for a short period (say 20 min). This means that even if biometrics is available to a fraudster, they cannot use it for authentication since the user has securely locked his/her biometrics.
- Resident notification - The authentication system should support user notifications (email, SMS, and app notification) so that notifications are sent on every biometric authentication. This allows users to immediately flag any suspicious usage in the rare case that happens.
- Agency traceability - All transactions should be digitally signed to ensure calling agencies/applications are authenticated. In addition, API keys should be used to ensure API access. Every transaction should traceable and audited against a particular agency/application in a non-repudiable way.

  Device traceability - In the case of secure capture devices, every physical device should be identifiable and usage should be audited within the authentication system.

12.4 Offline Authentication Security Requirements

In the case of offline biometric matching systems, the following requirements are mandated:

- Any Biometrics stored must be stored on a secure element.
- Biometric captured must be securely sent to the secure element.
- No copy of biometric should be available outside the secure element post the transaction.
- Matching must be performed within the secure element.

12.5 Process, Audits & Legal Provisions

A number of nontechnical requirements are required to create a secure biometric system for e-governance applications.

- Device certification - The system needs to set up a device certification process to ensure all biometric capture devices are certified for use.
- Agency on-boarding - The system needs to set up formal on-boarding process and insists on IT audits and readiness before any agency can access production authentication.

- Audits - All agencies must perform 3rd party IT audit reports to ensure biometrics and PII data is protected securely.
- Contracts - Strong contracts must be put in place between all agencies handling biometric data to ensure clear responsibilities, accountability, and liability are defined and understood between various parties.
- IT Act - Misuse of biometrics and any misuse of PII data including biometrics attract strict legal penalties under IT Act. The system should take measures to align its implementation of the overall system to be compliant with IT Act and mandates that its partners also comply with IT Act when it comes to PII data protection.
- Aadhaar Act 2016–The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 was published in the gazette on March 26, 2016. The Act seeks to provide for, as a good governance measure, efficient, transparent, and targeted delivery of subsidies, benefits and services, the expenditure for which is incurred from the Consolidated Fund of India, to individuals residing in India through assigning of unique identity numbers to such individuals and for matters connected therewith or incidental thereto**.** As discussed in relevant portions of this document, the Aadhaar Act contains provisions for sharing, disclosure and permitted uses of information, which have implications on implementing biometric systems for e-governance using Aadhaar numbers. Collection, disclosure or use in contravention of the provisions would attract penalties under the Aadhaar Act.