INTERNATIONAL STANDARD

ISO/IEC 24745

Second edition
2022-02

Information security, cybersecurity and privacy protection — Biometric information protection

Securité de l'information, cybersécurité et protection de la vie privée — Protection des informations biométriques

Reference number
ISO/IEC 24745:2022(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see patents.iec.ch).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

This second edition cancels and replaces the first edition (ISO/IEC 24745:2011), which has been technically revised.

The main changes compared to the previous edition are as follows:

- correction of terms;
- removal of non-compliant requirements related to jurisdictions;
- clarification of various explanations;
- improvements on the requirements for protection of biometric information, with more explicit enforcement of irreversibility and unlinkability;
- addition of relevant references to ISO/IEC 30136:2018;
- introduction of new application models based on recent technologies;
- addition of examples in annexes.

Any feedback or questions on this document should be directed to the user’s national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Introduction

As the Internet becomes a more pervasive part of daily life, various services are being provided via the Internet, e.g. Internet banking, remote healthcare. In order to provide these services in a secure manner, the need for authentication mechanisms between subjects and the service being provided becomes even more critical. Some of the authentication mechanisms already developed include token-based schemes, personal identification and transaction numbers (PIN/TAN), digital signature schemes based on public key cryptosystems, and authentication schemes using biometric techniques.

Biometrics, the automated recognition of individuals based on their behavioural and physiological characteristics, includes recognition technologies based on, e.g. fingerprint image, voice patterns, iris image and facial image. The cost of biometric techniques has been decreasing while their reliability has been increasing, and both are now acceptable and viable for use as an authentication mechanism.

Biometric authentication introduces a potential discrepancy between privacy and authentication assurance. On the one hand, biometric characteristics are ideally an unchanging property associated with and distinct to an individual. This binding of the credential to the individual provides strong assurance of authentication. On the other hand, this strong binding also underlies the privacy concerns surrounding the use of biometrics, such as unlawful processing of biometric data, and poses challenges to the security of biometric systems to prevent or to be resilient to the compromise of biometric references (BRs). The usual solution to the compromise of an authentication credential (to change the password or issue a new token) is not generally available for biometric authentication because biometric characteristics, being either intrinsic physiological properties or behavioural traits of individuals, are difficult or impossible to change. At most, another finger or eye instance can be enrolled, but the choices are usually limited. Therefore, appropriate countermeasures to safeguard the security of a biometric system and the privacy of biometric data subjects are essential.

Biometric systems usually bind a BR with other personally identifiable information (PII) for authenticating individuals. In this case, the binding is needed to assure the security of the data record containing biometric information. The increasing linkage of BRs with other PII and the sharing of biometric information across legal jurisdictions make it extremely difficult for organizations to assure the protection of biometric information and to achieve compliance with various privacy regulations.

Information security, cybersecurity and privacy protection — Biometric information protection

1 Scope

This document covers the protection of biometric information under various requirements for confidentiality, integrity and renewability/revocability during storage and transfer. It also provides requirements and recommendations for the secure and privacy-compliant management and processing of biometric information.

This document specifies the following:

— analysis of the threats to and countermeasures inherent to biometrics and biometric system application models;

— security requirements for securely binding between a biometric reference (BR) and an identity reference (IR);

— biometric system application models with different scenarios for the storage and comparison of BRs;

— guidance on the protection of an individual's privacy during the processing of biometric information.

This document does not include general management issues related to physical security, environmental security and key management for cryptographic techniques.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 30136, *Information technology — Performance testing of biometric template protection schemes*

3 Terms and definitions

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

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
authentication
provision of assurance in the *identity* (3.22) of an individual

[SOURCE: ISO/IEC 29115:2013, 3.2, modified — "entity" replaced by "individual".]

3.2
auxiliary data
AD
subject-dependent data that are part of a *renewable biometric reference* (3.34) and may be required to reconstruct *pseudonymous identifiers* (3.29) during verification, or for verification in general

Note 1 to entry: If *auxiliary data* are part of a *renewable biometric reference*, it is not necessarily stored in the same place as the corresponding *pseudonymous identifiers*.

Note 2 to entry: *Auxiliary data* may contain data elements for *diversification* (3.19).

Note 3 to entry: *Auxiliary data* are not the element for comparison during biometric reference verification.

Note 4 to entry: *Auxiliary data* are generated by the *biometric system* (3.13) during enrolment.

EXAMPLE Secret number combined with biometric data using, for example, a helper data approach, fuzzy commitment scheme or fuzzy vault. See Table C.1 for concrete examples of *pseudonymous identifier* (PI) (3.29) and AD.

3.3
biometric authentication
authentication (3.1) where *biometric verification* (3.16) or *biometric identification* (3.8) is applied and the *identity* (3.22) is linked to the *biometric reference* (3.11)

3.4
biometric characteristic
biological and behavioural characteristic of an individual from which distinguishing, repeatable *biometric features* (3.7) can be extracted for the purpose of biometric recognition

[SOURCE: ISO/IEC 2382-37:2017, 3.1.2, modified — The EXAMPLE was removed.]

3.5
biometric data
biometric sample (3.12) or aggregation of biometric samples at any stage of processing, e.g. *biometric reference* (3.11), biometric probe, *biometric feature* (3.7) or biometric property

Note 1 to entry: As defined in ISO/IEC 2382-37:2017, 3.3.15, biometric property is a descriptive attribute of the *biometric data* (3.5) subject estimated or derived from the *biometric sample* (3.12) by automated means.

[SOURCE: ISO/IEC 2382-37:2017, 3.3.6, modified — Note 1 to entry was removed and replaced by a new Note 1 to entry.]

3.6
biometric data subject
subject
individual whose individualized *biometric data* (3.5) is within the *biometric system* (3.13)

[SOURCE: ISO/IEC 2382-37:2017, 3.7.5, modified — Note 1 to entry was removed.]

3.7
biometric feature
numbers or labels extracted from *biometric samples* (3.12) and used for comparison

[SOURCE: ISO/IEC 2382-37:2017, 3.3.11, modified — Notes 1 to 5 to entry were removed.]

3.8
biometric identification
process of searching against a biometric enrolment database to find and return the *biometric reference* (3.11) *identifier(s)* (3.21) attributable to a single individual

[SOURCE: ISO/IEC 2382-37:2017, 3.8.2, modified — Note 1 to entry was removed.]

3.9
biometric information
information conveyed or represented by *biometric data* (3.5)

Note 1 to entry: Biometric data include for instance data derived or transformed from biometric data which are handled in connection with biometric data within a *biometric system* (3.13).

3.10
biometric model
stored function generated from *biometric data* (3.5)

EXAMPLE Examples of biometric models could be a Hidden Markov Model, Gaussian Mixture Model or an Artificial Neural Network.

[SOURCE: ISO/IEC 2382-37:2017, 3.3.13, modified — Notes 1 to 3 to entry were removed.]

3.11
biometric reference
BR
one or more stored *biometric samples* (3.12), *biometric templates* (3.14) or *biometric models* (3.10) attributed to a *biometric data subject* (3.6) and used as the object of biometric comparison

EXAMPLE Face image stored digitally on a passport, fingerprint minutiae template on a National ID card or Gaussian Mixture Model for speaker recognition, in a database.

Note 1 to entry: A *biometric reference* that can be renewed is referred to as a *renewable biometric reference* (3.34).

Note 2 to entry: BR can be used as a factor in multi-factor authentication, that is, something a person is.

[SOURCE: ISO/IEC 2382-37:2017, 3.3.16, modified — Notes 1 and 2 to entry were removed and replaced by new Notes 1 and 2 to entry.]

3.12
biometric sample
analog or digital representation of *biometric characteristics* (3.4) prior to *biometric feature* (3.7) extraction

[SOURCE: ISO/IEC 2382-37:2017, 3.3.21, modified — The EXAMPLE was removed.]

3.13
biometric system
system for the purpose of the biometric recognition of individuals based on their behavioural and biological characteristics

[SOURCE: ISO/IEC 2382-37:2017, 3.2.3, modified — Note 1 to entry was removed.]

3.14
biometric template
set of stored *biometric features* (3.7) comparable directly to probe biometric features

[SOURCE: ISO/IEC 2382-37:2017, 3.3.22, modified — The EXAMPLE and Notes 1 and 2 to entry were removed.]

3.15
biometric template protection
protection of *biometric references* (3.11) under various requirements for secrecy, *irreversibility* (3.26), and *renewability* (3.33) during storage and transfer

Note 1 to entry: A *biometric template protection* scheme is one example of *biometric information* (3.9) protection scheme.

[SOURCE: ISO/IEC 30136:2018, 3.3, modified — Added Note 1 to entry.]

3.16
biometric verification
process of confirming a biometric *claim* (3.17) through biometric comparison

[SOURCE: ISO/IEC 2382-37:2017, 3.8.3, modified — Note 1 to entry was removed.]

3.17
claim
assertion of *identity* (3.22)

3.18
common identifier
CI
identifier (3.21) for correlating *identity references* (3.24) and *biometric references* (3.11) in physically or logically separated databases

3.19
diversification
deliberate creation of multiple, unlinkable, transformed *biometric references* (3.11) from one or more *biometric samples* (3.12) obtained from one subject for the purposes of security and privacy enhancement

Note 1 to entry: *Renewability* (3.33) is provided by performing *diversification* for *biometric reference*(s).

3.20
generative biometric data
biometric data (3.5) (sample(s) or features) used as primary input to the *biometric template protection* (3.15) scheme

[SOURCE: ISO/IEC 30136:2018, 3.4]

3.21
identifier
one or more attributes that uniquely characterize an individual in a specific domain

EXAMPLE The name of a club with a club-membership number, a health insurance card number together with the name of the insurance company, an IP address, and a universal unique identifier.

3.22
identity
set of properties or characteristics of an individual that can be used to describe its state, appearance or other qualities

3.23
identity management system
IdMS
system controlling individual identity information throughout the information lifecycle in one domain

3.24
identity reference
IR
non-biometric attribute that is an *identifier* (3.21) with a value that remains the same for the duration of the existence of the individual in a domain

3.25
IR claimant
identity reference claimant
individual making an *identity reference* (3.24) *claim* (3.17)

Note 1 to entry: *Claims* can be verified in a number of ways, some of which may be based on biometrics.

3.26
irreversibility
property of a transform that creates a *biometric reference* (3.11) from *generative biometric data* (3.20) such that knowledge of the transformed biometric reference cannot be used to determine any information about the generative biometric data

[SOURCE: ISO/IEC 30136:2018, 3.5, modified — Note 1 to entry was removed.]

3.27
personally identifiable information
PII
any information that a) can be used to identify the PII principal to whom such information relates, or b) is or might be directly or indirectly linked to a PII principal

[SOURCE: ISO/IEC 29100:2011, 2.9, modified — Note 1 to entry was removed.]

3.28
privacy compromise
event in which an adversary discovers part of the *generative biometric data* (3.20) of an individual enrolled in the database of a *biometric verification* (3.16) or identification system

[SOURCE: ISO/IEC 30136:2018, 3.6, modified — Note 1 to entry was removed.]

3.29
pseudonymous identifier
PI
part of a *renewable biometric reference* (3.34) that represents an individual or data subject within a domain by means of a protected *identity* (3.22) that can be verified by means of a captured *biometric sample* (3.12) and the *auxiliary data* (3.2) (if any)

Note 1 to entry: A *pseudonymous identifier* should not contain any information that allows retrieval of the original *biometric sample*, the original *biometric features* (3.7), or the true identity of its owner.

Note 2 to entry: The *pseudonymous identifier* has no meaning outside the service domain.

Note 3 to entry: Encrypted *biometric data* (3.5) with a cipher that allows retrieval of the plain-text data before comparison is not a *pseudonymous identifier*.

Note 4 to entry: A *pseudonymous identifier* may be the element for comparison during *biometric reference* verification.

Note 5 to entry: See Table C.1 for examples of PI and *auxiliary data* (AD) (3.2).

3.30
pseudonymous identifier comparator
PIC
system, process or algorithm that compares the *pseudonymous identifier* (3.29) generated during enrolment by the *pseudonymous identifier encoder* (3.31) and the *pseudonymous identifier* reconstructed during verification by the *pseudonymous identifier recoder* (3.32), and returns a similarity score representing the similarity between the two

[SOURCE: ISO/IEC 30136:2018, 3.8]

3.31
pseudonymous identifier encoder
PIE
system, process or algorithm that generates a *renewable biometric reference* (3.34) consisting of a *pseudonymous identifier* (3.29) and possibly *auxiliary data* (3.2) based on a *biometric reference*

3.32
pseudonymous identifier recoder
PIR
system, process or algorithm that reconstructs a *pseudonymous identifier* (3.29) based on the provided *auxiliary data* (3.2) and the extracted features

[SOURCE: ISO/IEC 30136:2018, 3.9]

3.33
renewability
property of a transform or process to create multiple, unlinkable transformed *biometric references* (3.11) derived from one or more *biometric samples* (3.12) obtained from the same data subject and which can be used to recognize the individual while not revealing information about the original reference

3.34
renewable biometric reference
RBR
renewable *identifier* (3.21) that represents an individual or data subject within a domain by means of a protected binary *identity* (3.22) (re)constructed from the captured *biometric sample* (3.12), and fulfilling *irreversibility* (3.26) requirements

Note 1 to entry: A *renewable biometric reference* fulfilling *irreversibility* requirement provides additional security property.

Note 2 to entry: An example of a *renewable biometric reference* is a *pseudonymous identifier* (3.29) and additional data elements required for *biometric verification* (3.16) or identification such as *auxiliary data* (3.2).

3.35
revocability
ability to prevent future successful verification of a specific *biometric reference* (3.11) and the corresponding *identity reference* (3.24)

Note 1 to entry: Rejection of a subject may occur on the grounds of its appearance on a revocation list.

3.36
secure channel
communication channel providing the confidentiality and authenticity of exchanged messages

3.37
token
physical device storing *biometric reference* (3.11) and in some cases performing on-board biometric comparison

EXAMPLE Smart card, USB memory stick or RFID chip in e-passport.

3.38
unlinkability
property of two or more *biometric references* (3.11) that they cannot be linked to each other or to the subject(s) from whom they were derived

4 Abbreviated terms

AD	auxiliary data
AFIS	automated fingerprint identification systems
BR	biometric reference
CI	common identifier

DB_{BR}	database containing biometric reference (BR)
DB_{IR}	database containing identity reference (IR)
E_{BR}	encrypted biometric reference (BR)
E_{IR}	encrypted identity reference (IR)
IdMS	identity management system
IR	identity reference
MAC	message authentication code
OCC	on-card comparison
PI	pseudonymous identifier
PIC	pseudonymous identifier comparator
PIE	pseudonymous identifier encoder
PII	personally identifiable information
PIR	pseudonymous identifier recoder
RBR	renewable biometric reference
RFID	radio frequency identification
TTP	trusted third party
USB	universal serial bus
$\xrightarrow{X}$	An arrow represents either a simple information flow of data *x* or initiation of an interactive protocol whose exchanged data may depend on the whole or a part of *x*. *x* may be encrypted when a secure messaging system such as ISO/IEC 7816-4 is used. The interactive protocol may not transfer any information on *x* when, for example, a zero-knowledge technique is used.

5 Biometric systems

5.1 General

Biometric systems perform the automated recognition of individuals based on one or more biological (physical properties of the body such as fingerprints) and/or behavioural (functions of the body, such as walking) characteristics.

Physiological characteristics include but are not limited to:

- fingerprint;
- face;
- iris;
- hand geometry;
- hand/finger vein;

- DNA.

Behavioural characteristics include but are not limited to:

- signature;
- keystroke dynamics;
- gait;
- voice.

The following are desirable properties of biometric characteristics that lead to good subject discrimination and reliable recognition performance[26]:

- universality: every individual should have the characteristic;
- uniqueness: every individual should have a distinguishable characteristic;
- permanence: the characteristics should not show variance over time;
- collectability: the characteristics should be easily collectable from the subjects;
- repeatability: the property of the minimization of variations of a subject's captured biometric data allowing successful recognition over time.

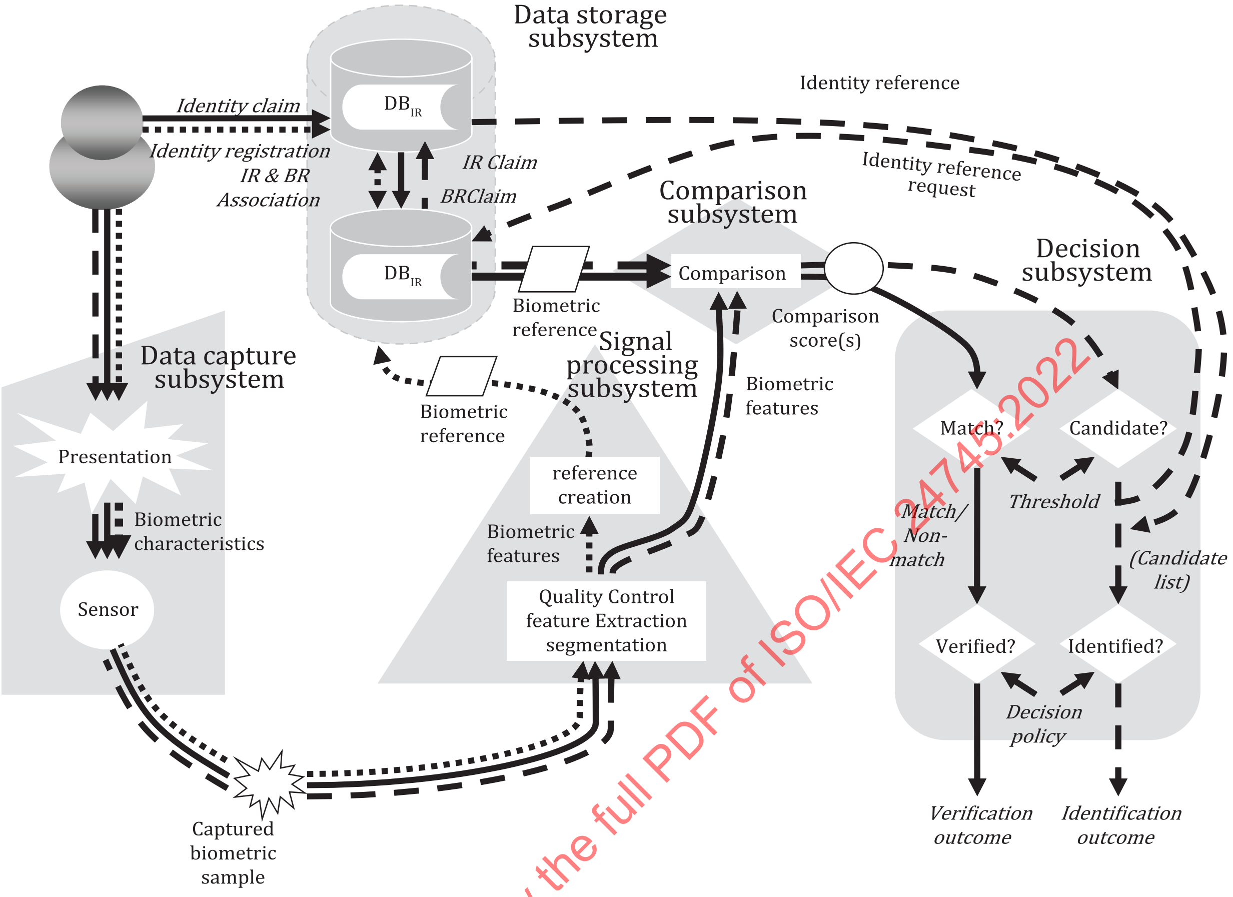
From an application point of view, the following additional properties should also be taken into account:

- performance, which mainly refers to the success rate in recognizing individuals;
- acceptability, which represents the level of willingness by the subject to use the biometric system;
- robustness against presentation attacks, 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) (BRs). The BR can 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 can be a biometric model composed from the features.

Specifically, biological biometric characteristics are very difficult to alter, so their compromise can have permanent consequences for the individual in applications in which immutability of the biometric characteristic is assumed.

5.2 Biometric system operations



Key

⋯⋯⋯⋯	enrolment
———	verification
– – –	identification

Figure 1 — Conceptual structure of a biometric system

The overall operation of a biometric system is depicted in Figure 1, which is an expanded version of the original one given in ISO/IEC TR 24741, to highlight the processing of the identity reference (IR) within the biometric system.

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 BR for the identification and verification process.
- A data storage subsystem, which serves primarily as an enrolment database where the linking of the enrolled BRs to the IR occurs. The data may contain biometric data and also non-biometric data such as the IR related to the subject. In practice, DB$_{IR}$ and DB$_{BR}$ are often logically or physically separated for reasons of security and privacy concerns. A more detailed description of binding DB$_{IR}$ with DB$_{BR}$ is given in Annex A.

- A comparison subsystem, which determines the similarity between captured biometric samples (or derived features) and stored BRs. In the case of the one-to-one comparison used in the verification process, a captured biometric sample is compared with a stored BR 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 BRs of more than one biometric data subject to return a set of comparison scores.

- A decision subsystem, which determines whether the captured biometric sample and the BR 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 may be presented to the decision policy.

These five subsystems represent the technical and functional blocks that capture, process, store, compare and decide on the processing of biometric data. In addition, other subsystems can be included, in particular a presentation attack detection subsystem[24], or the following ones as introduced in Reference [27]:

- A reference-adaptation subsystem, which modifies a reference using a new biometric feature, extracted from a successful verification or identification process. Adaptation is generally employed by biometric systems to reflect external factors and to minimize their effects on the recognition rate. It may also be used for attenuating the potential effects of reference aging. Unsupervised adaptation can be performed automatically based on a pre-determined policy. Supervised adaptation is usually invoked by the application and is based on application-specific criteria. For example, it may be called upon when the biometric comparison score is not high but other factors clearly support the asserted identity. Since a lower comparison score can cause the system to reject a genuine user, adoption of a reference-adaptation subsystem should be considered in the earliest stages of establishing the biometric system.

- An administration subsystem, which controls the overall policy, implementation and usage of the biometric system. Examples include:

  NOTE Different relevant legal, jurisdictional and societal constraints and privacy requirements can exist in different places.

  - provision of privacy relevant information to the subject during biometric processing;
  - storage and formatting of the BRs and/or biometric interchange data;
  - making of decisions on encryption and digital signature mechanisms for confidentiality and integrity of PII, including biometric data;
  - analysis of the vulnerabilities of and security attacks against the overall biometric system and implementation of proper countermeasures;
  - provisions of the final arbitration on output from decisions and/or scores;
  - setting of threshold values for the decision subsystem;
  - control of the operational environment and non-biometric data storage;
  - provisions of appropriate safeguards for the subject's biometric information privacy.

In essence, a biometric system involves three main 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 IR. The captured biometric sample is processed to extract the features which are enrolled as a reference in the enrolment database with the IR.

- Identification process: searching the enrolment database against the captured and extracted biometric features to return an identity or a candidate list depending on the decision policy. A candidate list consists of individuals whose references match with the feature in the 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 BR. The subject presents his/her IR for a claim of identity and also his/her biometric characteristic(s) to the capturing device, which acquires biometric sample(s) to be used for comparison with the BR linked to the IR for the claimed identity. The comparison score together with the decision policy determines the verification decision.

The verification process has a possibility of impacting the subject's privacy since this process requires both BR and IR. The identification process requires an exhaustive search of the enrolment database. During this process, biometric and other personal identifiable information can be lost or misused, therefore, this also has a possibility of impacting the subject's privacy. Verification is generally considered to be less privacy intrusive than identification as it impacts only one individual at a time.

5.3 Biometric references and identity references (IRs)

Each IR is an attribute, or combination of attributes, of the identity of an individual that uniquely identifies that individual in a particular domain. An IR can also be a combination of attributes of the individual.

A BR is one of many attributes belonging to an individual that can be used to recognize that individual within a domain. This document classifies identity attributes into non-biometric and biometric ones. For the sake of simplicity, the former is referred to as the IR and the latter as the BR. Some examples, not a comprehensive or definitive list, of IRs and BRs are depicted in Figure 2, where the surrounding box represents the set of attributes that can be used to identify an individual.

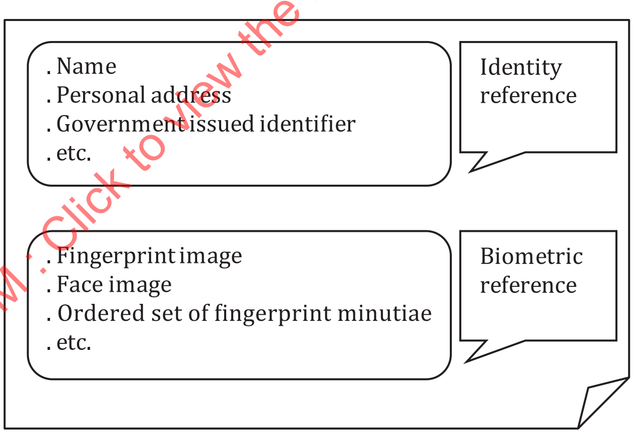


Figure 2 — Identity references and biometric references (BRs)

5.4 Biometric systems and identity management systems

The identity management system (IdMS) has an important function in any domain to avoid identity conflicts or ambiguities (for more details about IdMS, see ISO/IEC 24760-1). 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 can be in that same domain or called in from another domain. When biometrics is used to provide an authentication service, the IdMS may request authentication from the biometric system [a) in Figure 3] and the biometric system may provide the authentication result to the IdMS [b) in Figure 3].

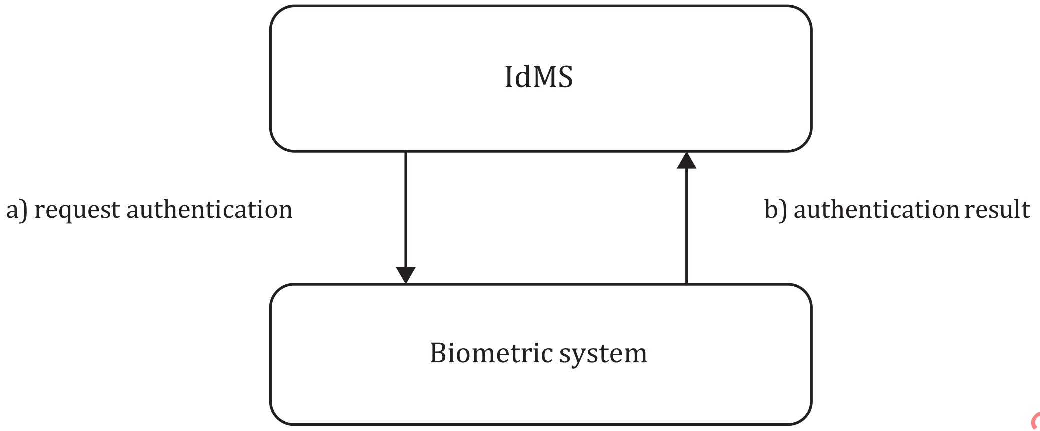


Figure 3 — Biometric system as an authentication service provider for IdMS

5.5 Personally identifiable information (PII) and privacy

Biometric data such as BRs are strongly bound to the individual subjects and when associated with linked subject identity information stored on a system can be used to identify the subject. Hence, stored biometric data are classified as personally identifiable information (PII) and have attendant privacy concerns.

The strong binding of biometric data to the individual also raises concerns that, if individuals are enrolled in multiple biometric systems using the same biometric modality, it can be possible to track the transactions of those individuals across the multiple systems by means of the BRs stored on the systems, unless precautions are taken to prevent this. This is a particular privacy concern where large systems are involved such as national identity systems which can be used by multiple government departments, but it is also a concern where biometric and identity data are inadvertently lost or intentionally shared by commercial organizations.

5.6 Societal considerations

The application of biometric systems always has a societal dimension, aspects of which can be codified in legal and regulatory requirements regarding the operation of such systems (such as those relating to the protection of personal data), while other aspects such as acceptability by subjects using these systems are very desirable and contribute to good system performance. The acceptability of a system can be influenced by religious, ethnic and cultural factors, as well as by individual psychological traits.

In all deployments of biometric systems, those individuals and organizations responsible for their operation should recognise that protection of the biometric data by appropriate security mechanisms is necessary to satisfy the legal requirements (for personal data protection), as well as to contribute to their acceptance by society and individuals.

In a similar way, designers and operators of systems using biometrics should provide information on how legal and regulatory obligations and good practice are observed in relation to the following:

- health and safety;
- accessibility, which ensures that systems are usable with a low physical and cognitive effort by as wide a population as possible, especially for physically or mentally incapacitated subjects;
- usability, which delivers systems that are effective, efficient and satisfying in use.

NOTE A more extended discussion of the societal and cross-jurisdictional considerations in commercial applications can be found in ISO/IEC TR 24714-1.

6 Security aspects of a biometric system

6.1 Security requirements for biometric systems to protect biometric information

6.1.1 Confidentiality

Confidentiality is the property that protects information against unauthorized access or disclosure. In biometric systems, a BR stored in a BR database during the enrolment process is transmitted to a comparison subsystem during the verification and identification process. During this process, the BR can be accessed by unauthorized entities and can be read or the binding to its identity information can be revealed. Unauthorized disclosure of data can 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.

NOTE Various forms of encryption algorithms, with a symmetric or asymmetric cipher, can be used for providing confidentiality of data. For more detailed information, see the ISO/IEC 18033 series.

6.1.2 Integrity

Integrity is the property of safeguarding the accuracy and completeness of assets. The integrity of a BR is critical to the assurance of overall biometric system security. The integrity of the authentication process is dependent on the integrity of the BR. If either the BR or the captured and extracted biometric feature is untrustworthy, the resulting authentication is also untrustworthy. Untrustworthy BRs or samples can 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 bona fide BR by an authorized entity (i.e. either an authorized enrolee or a system owner), without intervention of an attacker;

— modification (including substitution) of a BR of an authorized enrolee by an attacker.

Biometric systems shall employ effective data integrity protection. This can for instance be realized through integrity checking using cryptographic techniques. It is possible that integrity protection will need to be combined with other techniques (such as time stamping) to protect against the reuse of stolen biometric data and replay attacks.

NOTE 1 Various techniques, such as message authentication code (MAC) or digital signature, can be used to provide data integrity. For more detailed information, see the ISO/IEC 9796 series, the ISO/IEC 9797 series and the ISO/IEC 14888 series.

NOTE 2 Certain situations can 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 as standardized in ISO/IEC 19772.

NOTE 3 When a smart card is used for BR storage and/or comparison (Clause 8, Models B, E, F, G and H), secure messaging mechanisms according to ISO/IEC 7816-4 can be used for biometric data integrity and/or confidentiality.

6.1.3 Renewability and revocability

A major security and privacy concern for biometric systems relates to the compromise of BRs. A variety of threats can compromise a BR. For example, an attacker can unlawfully obtain a token containing a BR, or can try to gain unauthorized access by means of a fake or spoofed biometric through a false accept. In case of compromise, revocation is required to prevent the attacker from future (or continued) unauthorized access. Alternatively, a database security breach can result in unauthorized exposure of

BRs and other personal data. In case of such compromise of BRs, there is a strong need to revoke the compromised references, and to associate the legitimate data subject with a new BR.

NOTE 1 ISO/IEC 30107-1 describes the obstacles to biometric imposter presentation attacks in a biometric system. The basic requirement is that the presented attack sample resembles the compromised BR so the adoption of renewability and revocability can prevent further presentation attacks for the compromised BR.

For these, the renewability to create new differently transformed BR from the same data subject while not revealing information about biometric characteristics and the revocability to prevent future attack with the compromised BR are required for security and protecting biometric information privacy.

NOTE 2 The biometric template protection algorithms to support renewability are implemented by extracting suitable biometric features and processing the features using a template protection primitive, such as a public-key cryptosystem, an error correcting code or a secret transformation. These can have potential side effects on biometric recognition performance, so a well-designed biometric template protection system attempts to minimize the accuracy degradation. ISO/IEC 30136 covers this issue.

It is possible that a BR will need to be changed for a variety of reasons besides compromise. For example, a BR may only be valid for a specific period of time (in a manner similar to passwords). If a BR is still required at the end of that time period, the reference may be renewed, or revoked and replaced. Moreover, the diverse renewable biometric references (RBRs) generated from the same biometric characteristics support unlinkability, which can provide independent references across different applications.

6.1.4 Availability

Availability is the property that ensures that authorized parties or individuals can access the biometric information when needed. Any biometric system does not only rely on its confidentiality and integrity of authentication, but it also heavily relies on the availability of the biometric information. If the biometric information is not accessible nor available, it leaves the system useless. Denying access to any information system is a basic occurrence especially for web applications. Almost every day there are instances of a denial of service attacks, e.g. Distributed Denial of Service (DDoS) that take down websites across the globe. A biometric system is no different and can also be a victim of a relevant attack. There are also other factors such as power outages and natural disasters that pose risks to the availability of a biometric system.

NOTE DDoS is a kind of network attack that uses multiple computers that attempt to disrupt or disable systems by sending multiple service requests to consume a system's resource.

Regular backups are key to ensuring biometric information availability. Since this type of system is very critical for the PII principal, redundancy of information is an appropriate measure for maintaining availability. Also, having an off-site location ready to restore service in case anything happens to the primary data storage, heavily reduces the downtime of the system.

6.2 Security threats and countermeasures in biometric systems

6.2.1 Threats and countermeasures against biometric system components

Threats against the components of a biometric system are summarized in Table 1.

Table 1 — Threats and countermeasures of biometric subsystems

	Threats	Countermeasures
Data capture	Sensor spoofing Capture/replay of signals from sensor	— Presentation attack detection — Multimodal biometric — Challenge/response — Hardware encryption capture device

Table 1 *(continued)*

	Threats	Countermeasures
Signal processing	Unauthorized manipulation of data during processing	— Use trusted algorithm
Comparison	Manipulation of comparison scores	— Secure server and/or client — Trusted OCC
Storage	Database compromise — Unauthorized disclosure of BR/IR — Unauthorized replacement of BR/IR — Unauthorized modification of BR/IR — Unauthorized deletion of BR/IR — Distributed denial of service attack	— Revocable and renewable biometric references — Data separation — Database access control — Sign BR/RBR/IR — Encrypt BR/RBR/IR — Appropriate contingency planning and recovery procedures
Decision	Hill climbing attack	— Secure channel — Hide comparison score from subject
	Distributed denial of service	— Secure network/channel
	Threshold manipulation	— Access control to threshold setting — Threshold value protection

NOTE 1 For the secure evaluation and certification of the modular components of the biometric systems, refer to ISO/IEC 19792 for additional information.

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.

The implementation of the comparison and decision components in a certified single module constitutes an effective countermeasure against threats of comparison score manipulation. In this case, an additional countermeasure of a hiding comparison score from the subject is required to prevent a hill climbing attack.

For clarification, brief descriptions of these threats and countermeasures are provided as follows:

- Presentation attack can mean the presentation of artificial and thus non-live biometric characteristics. One countermeasure to such attack is presentation attack detection based on recognition of a subject's biological activities as signs of life or the detection and rejection of known presentation attack instruments.
- Component replacement involves the substitution of the components (e.g. comparison or decision subsystem) of the biometric system in order to control it and obtain a desired output.
- Hill climbing refers to the systematic modification of the biometric sample to obtain progressively higher comparison scores until the decision threshold has been met.
- Threshold manipulation refers to changing the threshold value of the decision subsystem such that the biometric system easily accepts an illegitimate biometric sample.
- Revocable and RBRs are created by means of diversification for different applications, organizations or companies, but are associated with the same subject. Subjects may have multiple RBRs.

- Data separation refers to the security countermeasure of logically or physically separating individual data elements (e.g. partly on a token and partly in a database, see also 8.2). Data separation can be applied to data elements such as IR, BR, PI and AD.

6.2.2 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.

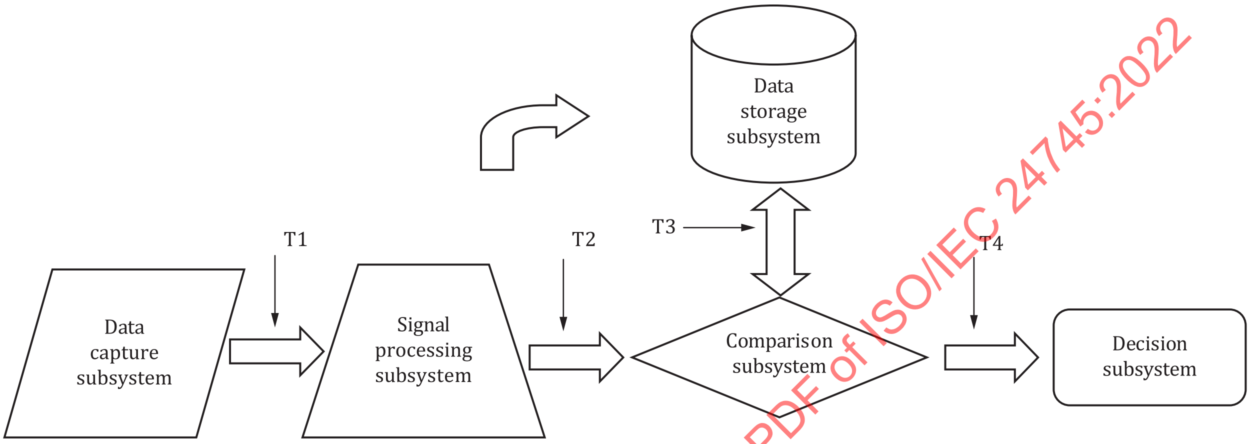


Figure 4 — Threats in the biometric system

Table 2 — Threats and countermeasures during transmission

	Data	Threats	Countermeasures
Data capture – Signal Processing (T1) Signal processing – Comparison (T2)	Biometric sample and feature	Eavesdropping	— Encrypted/secure channel
		Replay	— Challenge/response
		Brute Force	— Time out policy
Storage – Comparison (T3)	Biometric reference	Eavesdropping	— Encrypted/secure channel
		Replay	— Challenge/response
		Person 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 1 The implementation of the comparison and decision components in a certified single module constitutes an effective countermeasure against manipulation of comparison score threats.

For clarification, brief descriptions of these threats are provided as follows.

- Eavesdropping is the interception of sensitive information during its transmission between components of the biometric system.

— Person-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.

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

NOTE 2 For a more detailed description of the managerial aspect of protecting biometric systems see ITU-T X.1086, ISO 19092:2008 and ISO/IEC 19792. For telebiometric authentication using biometric hardware security module, see ISO/IEC 17922.

6.2.3 Renewable biometric references as countermeasure technology

A successful attack against storage and transmission can result in unauthorized exposure of BRs. Then, it can be possible to reverse engineer the BR to create an approximation to the biometric characteristic of the relevant subject which can be incorporated in a presentation artefact and used to impersonate the subject by means of a presentation attack. Renewability of BRs and revocability can be a countermeasure under this situation.

Similarly, the exposure of BRs during storage or transmission can enable an attacker to identify links between users across different applications and various systems. Renewability of BRs and revocability can be a measure to further improve the privacy under such an attack.

For successful renewal of RBRs, the RBR creation process should support the process of diversification. Diversification involves the generation of multiple, irreversible and unlinkable references from the same biometric characteristics that can be used to renew an RBR or to provide independent references across different applications.

NOTE 1 The ISO/IEC 30107 series presents standardization of specific presentation attack detection methods and detailed information about countermeasures in the biometric systems.

NOTE 2 ISO/IEC 30136 supports evaluation of the accuracy, secrecy and privacy of biometric template protection schemes and also gives guidance on measuring and reporting diversity and unlinkability of biometric templates

To facilitate a common vocabulary for the implementation of RBRs through a diversification process, and to outline the architectural aspects of RBRs and the diversification process in a technology-neutral manner, the concept of pseudonymous identifiers (PIs) is used in this document. In the approach described in this document, RBRs consist of two data elements: a PI and corresponding auxiliary data (AD). Both data elements are generated during enrolment and are stored because both elements are required during a verification or identification process. If an RBR renewal is required for a subject, then a new corresponding PI is generated with both a new AD and newly captured biometric sample, using the RBR creation process. The new PI and AD are given to the subject or the service provider and the previous PI and AD shall be revoked.

An example of an architectural aspect of RBRs is provided in Figure 5. An arrow in the figure represents a flow of information. During enrolment, a feature extraction stage generates biometric feature data from the captured biometric sample. Subsequently, a pseudonymous identifier encoder (PIE) generates an RBR consisting of a PI and AD. When the RBR is generated, the captured biometric sample and the extracted features can be securely disposed of. The RBR is stored on a suitable storage medium, e.g. a (smart) card or electronic database. PI and AD may be separated physically or logically from each other. The use of those specific components within the generic conceptual structure of a biometric system is illustrated in Figure 6.

During verification, a feature extraction stage processes the probe biometric sample. Subsequently, a pseudonymous identifier recoder (PIR) constructs a PI* based on the extracted features of the captured biometric verification sample and the AD component of the RBR generated during the enrolment of the subject whose identity is claimed at the verification stage. Subsequently, the comparison subsystem compares the PI generated during enrolment and PI* and returns a similarity score representing the similarity between PI and PI*. A more extensive overview of the PI creation and verification process, as well as its lifecycle, is provided in Annex B. For instance, PIR and pseudonymous identifier comparator (PIC) may be combined in a single subprocess process for direct verification from the biometric probe and the RBR.

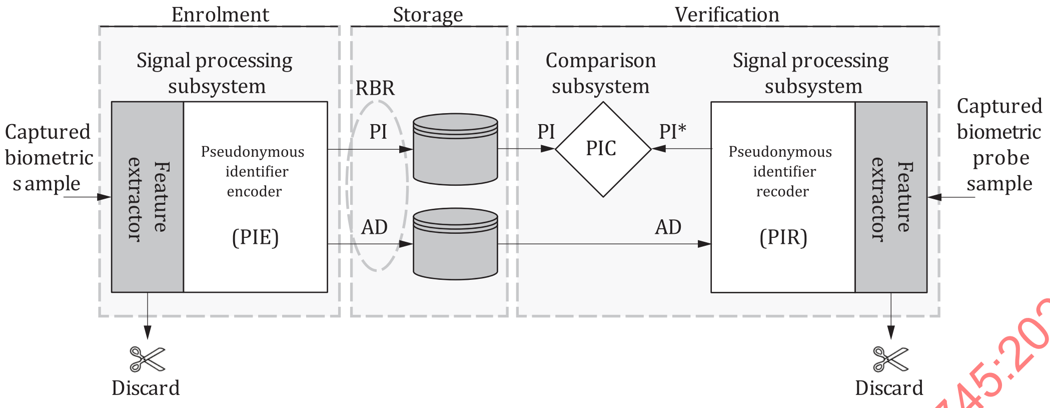
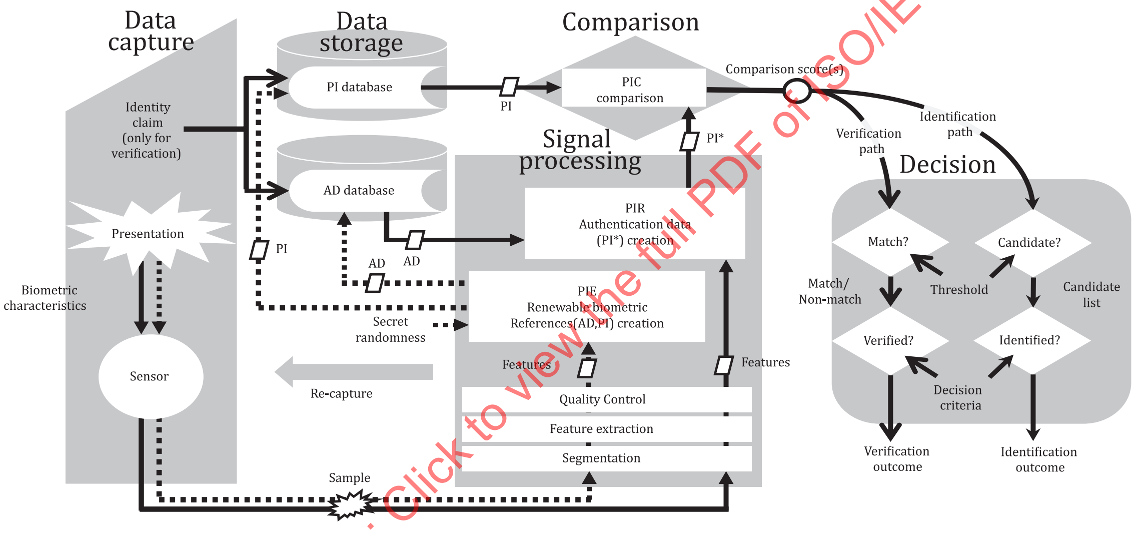

Enrolment
Storage
Verification
Signal processing subsystem
RBR
Comparison subsystem
Signal processing subsystem
Captured biometric sample
Feature extractor
Pseudonymous identifier encoder
(PIE)
PI
AD
PI
PIC
PI*
AD
Pseudonymous identifier recoder
(PIR)
Feature extractor
Captured biometric probe sample
Discard
Discard

Figure 5 — Architecture for renewable biometric references (RBRs)



Key

⋯⋯ enrolment

—— verification/identification

Figure 6 — Components of a general biometric template protection system from ISO/IEC 30136:2018

An overview of existing techniques to generate RBRs is given in Table C.1. The properties of PI and AD for a given technique are dependent on the related PIE, PIR, PIC mechanisms, e.g.:

— some techniques use PIC as an equality test with AD being a masked version of the BR, for which AD may contain some information on BR;

— some techniques use PIC as a secure comparison algorithm with AD being a random key, for which AD does not contain information on BR while PI necessary contains, at least indirectly, some information to enable the comparison.

6.3 Security of data records containing biometric information

6.3.1 Security for biometric information processing in a single database

The binding of an IR with a BR is required to perform biometric authentication operations as shown in Figure 1. Several applicable scenarios exist that can be used to describe the security of this binding, depending on the data records (e.g. IR, BR) being stored. These binding scenarios, showing the data element combinations, as well as outlining the associated security properties, are listed below. In the scenarios, the designations raw IR and raw BR refer to the plain data without additional data protection techniques and the authenticated BR denotes the signed data providing the integrity of the stored BR data.

NOTE In 6.3.1 and 6.3.2, encrypted, authenticated, authenticated-encrypted, diversified countermeasures are generic methods that can be achieved either by using encryption, authentication, authenticated encryption, diversification functions or by dedicated logical or physical means (e.g. secure execution environment or secure hardware storage).

— **Scenario 1**: Raw IR and raw BR are stored. Neither confidentiality nor integrity is provided either for IR or BR. Renewability and revocability are not provided.

— **Scenario 2**: Raw IR and encrypted BR, E_{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. Renewability and revocability are not provided if encryption is deterministic, and keys are fixed.

— **Scenario 3**: Raw IR and authenticated BR are stored. Only integrity of BR is provided.

— **Scenario 4**: Raw IR and authenticated-encrypted form of BR are stored. Both confidentiality and integrity are provided on BR.

— **Scenario 5**: 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.

— **Scenario 6**: Authenticated IR and raw BR are stored. Only integrity of IR is provided.

— **Scenario 7**: Authenticated-encrypted form of IR and raw BR are stored. Confidentiality and integrity are provided only on IR.

— **Scenario 8**: 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.

— **Scenario 9**: Raw IR and raw BR are authenticated and then stored. Integrity on both IR and BR is provided.

— **Scenario 10**: 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, E_{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.

- **Scenario 15**: Raw IR and RBR are stored. Renewability and revocability are provided on BR, as well as limited confidentiality and integrity on BR.
- **Scenario 16**: Raw IR and RBR are authenticated and then stored. Integrity on both IR and BR is provided. Renewability and revocability on BR are also provided.
- **Scenario 17**: Authenticated-encrypted forms of IR and RBR are stored. Integrity and confidentiality are provided on both IR and BR. Renewability and revocability are provided on BR.
- **Scenario 18**: Raw IR and RBR 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. Renewability and revocability are provided on BR.
- **Scenario 19**: Raw IR and encrypted, RBR are authenticated and then stored. Integrity is provided on both IR and BR. Confidentiality, renewability and revocability are provided on BR only.

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

Table 3 — Confidentiality, integrity and renewability for the data records stored in a single database

Scenario	Security and privacy requirements							Stored form of BR and IR data
	Confidentiality		Integrity		Renewability	Irreversibility	Unlinkability	
	IR	BR	IR	BR	BR			
2		0		Δ		Δ		Raw IR and enc. BR
3				0				Raw IR and aut. BR
4		0		0		Δ		Raw IR and auth.-enc. BR
5	0		Δ					Enc. IR and raw BR
6			0					Auth. IR and raw BR
7	0		0					Auth-enc. IR and raw BR
8	0	0	Δ	Δ		Δ	Δ	Enc. (IR and BR)
9			0	0				Auth. (IR and BR)
10	0	0	0	0		Δ	Δ	Auth.-enc.(IR and BR)
11	0	0	Δ	0		Δ	Δ	Enc. (IR and auth. BR)
12		0	0	0		Δ		Auth. (IR and enc. BR)
13	0	0	0	Δ		Δ	Δ	Enc. (auth. IR and BR)
14	0		0	0				Auth. (enc. IR and BR)
15					0	0		Raw IR and RBR
16		Δ	0	0	0	0		Auth. (IR and div. RBR)
17	0	0	0	0	0	0	Δ	Auth.-enc. (IR and div. RBR)
18	0	0	Δ	Δ	0	0	Δ	Enc. (IR and RBR)
19		0	0	0	0	0		Auth. (IR and enc., div. RBR)

Enc. encrypted

Auth. authenticated

Auth.-enc. authenticated-encrypted

0 satisfied

Δ partially satisfied corresponding to security Level 1 defined in ISO/IEC 19790

The ISO/IEC 19785 series specifies the common biometric exchange format framework (CBEFF) to promote interoperability of biometric-based applications and systems by specifying a standard structure for biometric information records (BIRs) for whose integrity and confidentiality the formats are specified in ISO/IEC 19785-4.

6.3.2 Security for biometric information processing in separated databases

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

A similar argument holds for storage of RBRs in the form of PI and AD. Physical or logical separation of PI and AD reduces privacy and security risks. Physical separation is desirable. If tokens are employed in a model based on distributed storage, it is advisable to store the AD on the token and PI on the client or server. If separated databases with a common CI are employed, the databases shall be controlled by separate operators with different cryptographic keys. More generally, RBR can be split via a secure splitting technique (like secret sharing approach) within different locations to reduce the privacy and security risks of one location being compromised.

In Table 4, binding scenarios employing separated databases are shown. The security requirements of confidentiality, integrity and renewability/revocability remain the same. However, the impact of a privacy compromise becomes smaller if only one of either IR and BR is exposed. If one database is compromised and its contents are illegally modified, the operators of two databases should be able to detect it. Similarly, during the usage of the databases, if a legitimate database operator with a correct key modifies its contents, the other database should be able to detect the modification. For these cases, more secure binding is required. Annex A provides examples of implementations of a CI.

Table 4 — Confidentiality, integrity and renewability for the data records stored in separated databases

Scenario	Security and privacy requirements							Stored form of IR data	Stored form of BR data
	Confidentiality		Integrity		Renewability	Irreversibility	Unlinkability		
	IR	BR	IR	BR	BR				
2		O		Δ		Δ		CI, raw IR	CI, enc. BR
3				O				CI, raw IR	CI, auth. BR
4		O		O		Δ		CI, raw IR	CI, auth.-enc. BR
5	O		Δ					CI, enc. IR	CI, raw BR
6			O					CI, auth. IR	CI, raw BR
7	O		O					CI, auth.-enc. IR	CI, raw BR
8	O	O	Δ	Δ		Δ	Δ	CI, enc. IR	CI, enc. BR
9			O	O				CI, auth. IR	CI, auth. BR
10	O	O	O	O		Δ	Δ	CI, auth.-enc. IR	CI, auth.-enc. BR
11	O	O	Δ	O		Δ	Δ	CI, enc. IR	CI, auth.-enc. BR
12		O	O	O		Δ		CI, auth. IR	CI, auth.-enc. BR
13	O	O	O	Δ		Δ	Δ	CI, auth.-enc. IR	CI, enc. BR
14	O		O	O				CI, auth.-enc. IR	CI, auth. BR
15		Δ			O	O		CI, PI, IR	CI, AD
16		Δ	O	O	O	O		CI, auth. PI, auth. IR	CI, auth. AD

Key

Enc. encrypted

Auth. authenticated

Auth.-enc. authenticated-encrypted

O satisfied

Δ partially satisfied corresponding to security Level 1 defined in ISO/IEC 19790

Table 4 *(continued)*

Scenario	Security and privacy requirements							Stored form of IR data	Stored form of BR data
	Confidentiality		Integrity		Renewability	Irreversibility	Unlinkability		
	IR	BR	IR	BR	BR				
17	0	0	0	0	0	0	Δ	CI, auth.-enc.(PI and IR)	CI, auth.-enc. AD
18	0	0	Δ	Δ	0	0	Δ	CI, enc.(PI and IR)	CI, enc. AD
19	0	0	0	0	0	0		CI, auth.(enc. PI and IR)	CI, auth.(enc. AD)

Key

Enc. encrypted

Auth. authenticated

Auth.-enc. authenticated-encrypted

0 satisfied

Δ partially satisfied corresponding to security Level 1 defined in ISO/IEC 19790

7 Biometric information privacy management

7.1 Biometric information privacy threats

Since biometric data are PII, ISO/IEC 29100, which is a general privacy framework addressing system specific issues at a high level, should be applied. It is a general framework that addresses organizational, technical, procedural and regulatory aspects of privacy for IT systems which process and store personal identifiable information. The use of biometric data involves several threats to privacy which shall be addressed:

— Biometric data can be misused for purposes other than originally intended or consented to by the data subject.

— Biometric references can allow retrieval or analysis of properties of the data subject that are not required or intended for biometric identification and verification, such as the data subject's health status or inferential medical information and ethnic background.

— Biometric references can be used to link subjects across different applications in the same database or across different databases. Privacy is related to the unlinkability of the stored BR.

NOTE A more detailed description of jurisdictional and societal considerations for commercial biometric application is given in ISO/IEC TR 24714-1.

7.2 Biometric information privacy requirements and guidelines

7.2.1 Irreversibility

To prevent the use of biometric data for any purpose other than originally intended, biometric data shall be processed by irreversible transforms before storage. Irreversibility may be obtained using the following mechanisms that can be combined:

— feature extraction algorithms which provide a measure of irreversibility by data reduction and redundancy removal, increasing the difficulty of using the extracted features to extract medical or ethnic data; see for instance [53] for an example of irreversibility measure;

— encryption using a key only known by the operator of the system and/or data subject limits unauthorized access to the biometric data;

- RBRs which limit access to the biometric characteristics of the data subject by means of irreversible transforms. An overview of transforms that produce RBRs is provided in Table C.1.

In the case of RBRs, the irreversibility shall be validated following ISO/IEC 30136.

Irreversible transforms that allow comparing biometric data without reversing the transformation should be preferred (e.g. relying on homomorphic encryption).

7.2.2 Unlinkability

The stored BRs should not be linkable across applications or databases. Unlinkability may be provided using various mechanisms that can be combined:

- encryption of BRs employing different (secret) keys or mechanisms across applications prevents linking of data subjects, provided that the secret keys are managed appropriately to avoid collusion;
- independent and unlinkable RBRs created through the process of diversification prevent linking of data subjects;
- logical or physical separation of IR and BR, or PI and AD in case of RBRs, prevents access to complete data records;
- the use of different biometric modalities, incompatible feature extraction algorithms or biometric data exchange formats across applications prevents linking of data subjects.

In case of RBRs, the unlinkability shall be validated following ISO/IEC 30136.

NOTE The use of different biometric modalities, incompatible feature extraction algorithms or data exchange formats can pose challenges for system interoperability.

7.2.3 Confidentiality

To protect BRs against access by an unauthorized entity resulting in a privacy risk, BRs shall be kept confidential. The following mechanisms may be employed to provide confidentiality:

- data separation by storing (part of the) BRs on a personal token or card instead of using centralized databases is a countermeasure to reduce privacy risks resulting from a security breach of the centralized database (e.g. when an adversary obtains illegitimate access to a centralized database and publishes its contents);
- encryption of BRs using a key only known to the operator of the IdMS and/or data subject.

NOTE The use of a token to store biometric data does not guarantee confidentiality unless the data are logically and physically protected from disclosure.

7.3 Biometric information lifecycle privacy management

7.3.1 Collection

Organizations shall obtain the consent of a subject prior to the collection of biometric information.

NOTE Different laws and regulations can exist that do not enforce consent.

When seeking the subject's consent, the organization should fully inform the subject of the following (this list is not exhaustive):

- the types and amount of biometric information to be captured;
- information about available alternative procedures in case the data subject does not want to enrol or cannot be enrolled (failure to enrol);
- the purpose of collection and the period of retention of the biometric information;

- a description of how the captured biometric information will be processed in the biometric system;
- information about the individual responsible for managing the biometric information, which includes, e.g. his/her name, organization, position, contact information.

Unauthorized collection of biometric information without justification has strong impacts on the biometric information privacy of the individual. Even if an organization had the subject's consent to create BRs, it should still only extract the minimum amount of biometric information necessary to fulfil the intended purposes. This can lessen the impact of a compromise.

7.3.2 Transfer (disclosure of information to a third party)

When transferring biometric information to other organizations, each party involved in processing of the biometric information shall agree to be bound by contract or obligation to protect such information. The transfer of biometric information shall only take place with the consent of the subject unless consent is implied by the provision of a service requested by the subject.

NOTE 1 Different laws and regulations can exist that can limit the consent requirement.

Before seeking the consent of the subject, the organization should provide the following (this list is not exhaustive):

- relevant information about the third party to which the biometric information is to be transferred;
- the contents and amount of biometric information to be transferred;
- the entity that makes the transfer;
- the purpose for the transfer and the period of retention of the transferred biometric information.

From the subject's point of view, transferring biometric information to a third party is essentially the same as presenting the biometric information directly to the third party. Accordingly, the consent of the subject shall be obtained.

NOTE 2 Different laws and regulations can exist that can limit the consent requirement.

Cross-border transfers are especially common in operating biometric systems including, e.g. border control and electronic passports. For this reason, it is important that more care is taken with respect to the privacy of the transferred biometric information which can be processed by a third party.

7.3.3 Use

Use refers to access, processing, or modification of biometric information within an organization. Biometric information shall only be used with the consent of the subject.

NOTE Different laws and regulations can exist that can limit the consent requirement.

If the organization wants to use the collected biometric information for purposes other than those already specified to the subject, the organization shall obtain the consent of the subject, providing a full description of the additional purpose of use, and the period of retention of the biometric information. Function creep, or expanded use of biometric information, such as determining the subject's health or genetic inheritance, shall be avoided.

7.3.4 Storage

Biometric information is usually stored in a data storage subsystem, as depicted in Figure 1. However, a data storage subsystem may be distributed. In order to satisfy privacy requirements, it can be necessary to store the information in such a way that it can be identified as being sensitive PII. Organizations should keep the collected biometric information logically or physically separate from the subject's other PII to reduce the impact on the subject's privacy of a compromise of the combined information. Suitable protection measures, as described in Clause 6, are necessary to ensure the confidentiality and integrity of the BR and also its related IR. To trace illegal distribution and misuse of the biometric samples, data encryption and biometric watermarking schemes as described in Annex D can be adopted. Acquired biometric samples can be classified as PII, and thus storing them presents security and privacy risks. This should be avoided when possible. If stored, it shall include adequate security and privacy measures following the requirements and recommendations in Clause 7.

7.3.5 Retention

Organizations shall consider the retention period of the biometric information or when to archive it. Retaining any kind of information, whether it is biometric or not, creates risks for the organization as well as for the biometric information. It is important to consider the purpose of retaining the biometric information only for as long as it is needed. Organizations should ensure that they have concrete justifications on retaining or keeping biometric information. This helps to justify whenever the organization's retention period and processes are checked/audited.

7.3.6 Archiving and data backup

Archiving is the process of storing biometric information for long-term or permanent preservation. When the organization collects biometric information with the subject's consent, the consent may contain an expiration date to specify the period for storing the captured biometric information. Preserving archived biometric information beyond its expiration data can breach the consent condition and create a risk of privacy violation. Also access restrictions to archived biometric information shall mirror that for the equivalent operational biometric information. Data backup, although undertaken for different reasons than archiving, presents a similar threat to privacy if the backup data are not adequately protected and disposed of when expired. The system security/privacy policy shall address the secure storage and control of access to archive and backup data containing biometric and other personal identifiable information.

7.3.7 Disposal

The organization or third party to which the biometric information is disclosed shall securely dispose of the biometric information of the subject when (this list is not exhaustive):

- the purpose for the collection of the biometric information has either been achieved or is determined to no longer be necessary;
- the period of retention of the biometric information has expired;
- the subject withdraws consent for the collection of the biometric information or the use of the biometric information changes, but the subject of the biometric information does not consent to the new use.

When disposing of the stored biometric information, it is essential to ensure that all relevant related data are identified and securely disposed of, particularly in cases of distributed storage. The system security/privacy policy shall specify the biometric and other personal identifiable information that is to be included in the inventory of data for disposal. This shall include archive and backup data (see 7.3.6 for further details). The policy shall also describe suitable procedures and safeguards to ensure the complete and secure disposal of the data.

7.4 Responsibilities of a biometric system owner

The biometric system owner shall be responsible for the proper management of biometric information in order to protect the information and safeguard the rights of the subject with regard to the biometric information within the organization. To meet these obligations, the biometric system owner shall:

- Provide the subject with the means to control his/her biometric information during its lifecycle including when providing such information to third parties. This means that the biometric system owner shall obtain consent when biometric information is collected.

— Provide a mechanism for consent withdrawal. The subject can request to withdraw his/her consent from an organization or any third party that has received the biometric information whenever he/she feels that it is necessary to do so. The biometric system owner shall provide appropriate means for the subject to make such a request and remove the relevant biometric information from the biometric system unless external constraints and conditions of the services override the request.

— Provide appropriate security measures to safeguard against attacks on the confidentiality, integrity and availability of the biometric information and the associated biometric system itself.

— Ensure that information used for identification or verification decisions is complete, accurate and up to date, to the extent possible. In this case, the term "information" refers to PII generally, as well as biometric information related to a subject. Poor quality BRs can result in the system accepting an attacker, which in turn can have an impact on the subject's privacy.

— Respond to any requests made by a subject to access his/her biometric information. The subject can request that the biometric system owner allow him/her to view his/her own biometric information, to make inquiries about the details of the use of the biometric information or the transfer of the biometric information to a third party, and to insist on the correction of any errors in the information when necessary.

— Provide notice of any breaches that result in the compromise of the subject's biometric information. The biometric system owner shall notify the subject of any breach involving the theft, loss, damage, unauthorized disclosure or unauthorized modification of the subject's biometric information.

8 Biometric system application models and security

8.1 Biometric system application models

Biometric systems can be classified by considering the locations where BRs and IRs 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 BRs and IRs when they are transferred, processed or stored. Conceptually, many models exist; however, this document considers eleven application models which are currently deployed in real applications.

Table 5 — Biometric system application models

		Storage			
		Server	**Client**	**Token**	**Distributed**
Comparison	**Server**	A		B	G
	Client	C	D	E	H
	Token			F	
	Distributed	I		J	K

The platforms where biometric data can be stored are 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, mobile devices 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. Personally-owned devices including mobile devices are considered to be clients in this document.

— A token is a portable physical device capable of supporting BR 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 1 The biometric sensor connected to a client via an interface and the 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 document considers them as a part of the client.

NOTE 2 The server is controlled by a service provider and the token is controlled by a user. On the other hand, the client is controlled either by a service provider or user depending on the biometric application models. Specific constraints or recommendations, when applicable, are discussed in 8.2.

NOTE 3 In Table 5, the expression “distributed” means that:

— with respect to storage, the storage of BRs or RBRs is split among different entities (at least two among server, client and token) and that the complete information is not available within a single entity;

— with respect to comparison, the execution of the comparison involves at least two entities to obtain the verification outcome.

This is not related to the notion of distributed ledgers that are not discussed in the models described in 8.2.

In the following, models A to F describe different topologies for the locations of the various subsystems. Security and privacy requirements are one factor that determines whether normal or RBRs should be used. Models G and H, on the other hand, only apply to RBRs because these models employ the concept of data separation of PI and AD (or secure splitting of the RBR) by distributing storage across multiple storage subsystems to enhance the security and privacy of biometric systems. Due to this data separation, models G and H are first applicable to a verification process. Models I, J and K describe cases where comparison is distributed between multiple locations, in order to avoid reference and probe information being gathered in one location for comparison purposes. Models I, J and K may be applicable to both normal or RBRs, if the comparison algorithm can be distributed.

When designing a biometric system, one of the models described in 8.2 or a combination of them should be preferably followed, by taking into consideration the application constraints, the trust assumption (e.g. on the client, the token, the server), the security and privacy properties of the used BR or RBR mechanism and any related risks. When possible, among the models described in 8.2, one should choose one of the models that enforces as much as possible the security and privacy properties by design. Additionally, when designing or selecting a specific solution to implement one of those models or any other biometric system models, the effective performance, privacy and security properties shall be assessed by following ISO/IEC 30136.

NOTE 4 The models described in 8.2 are chosen for illustrating the diversity of possible architectures and are seen as guidelines for the system designer. The added value of a specific model depends on the properties of the use BR or RBR scheme. Other models than those described in 8.2 are possible.

NOTE 5 The models are described with a single server architecture. Improving further privacy protection by separating the different data used in a model is possible: separation of storage can be made with multiple servers and/or multiple storage locations as described in ISO/IEC 30136:2018, 6.4.1.

An example of selection of models based on the context of a specific use case is discussed in Annex F.

8.2 Security in each biometric application model

8.2.1 General

A general recommendation related to 8.2 is that when a system corresponds to one of the following models, the alternative using RBRs should be preferred, except possibly if the solution corresponds to an on-card comparison (OCC) case.

If the server (respectively token) is not trusted by the client, no unprotected fresh biometric information (generated from the freshly capture biometric data) shall be transmitted by the client to the server (respectively token).

If the client is not trusted by the server (respectively by the token), no unprotected biometric information shall be transmitted to the client by the server (respectively by the token).

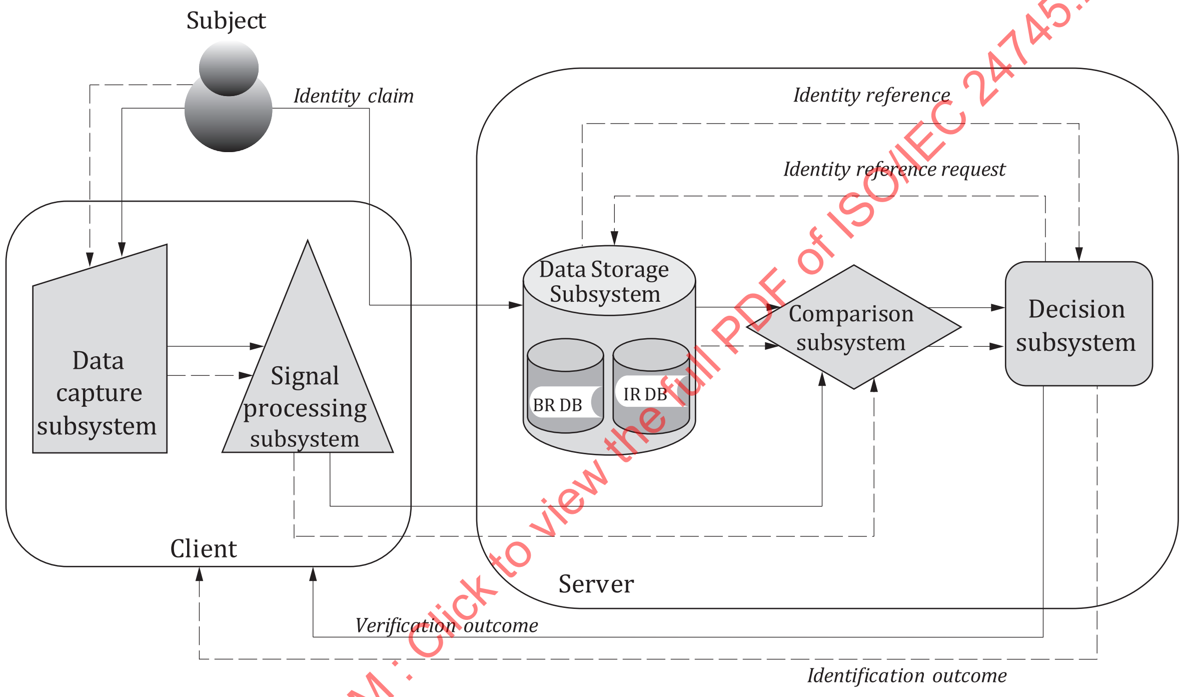
If the server is not trusted by the token, no unprotected biometric information shall be transmitted to the server by the token.

For mitigating the impact of a database breach, biometric information should be stored protected in a distributed manner.

For mitigating the risk of leaking information from transmitted data, distributed computations should be preferred.

8.2.2 Model A — Store on server and compare on server

In this model, biometric data are captured and processed on the client and then the extracted BR is transferred to the server for comparison, as shown in Figure 7 (for BRs) and Figure 8 (for RBRs). Here, biometric data capture and signal processing on the client, compare on server. The subject's BR and the corresponding IR are associated as part of the registration/enrolment process.



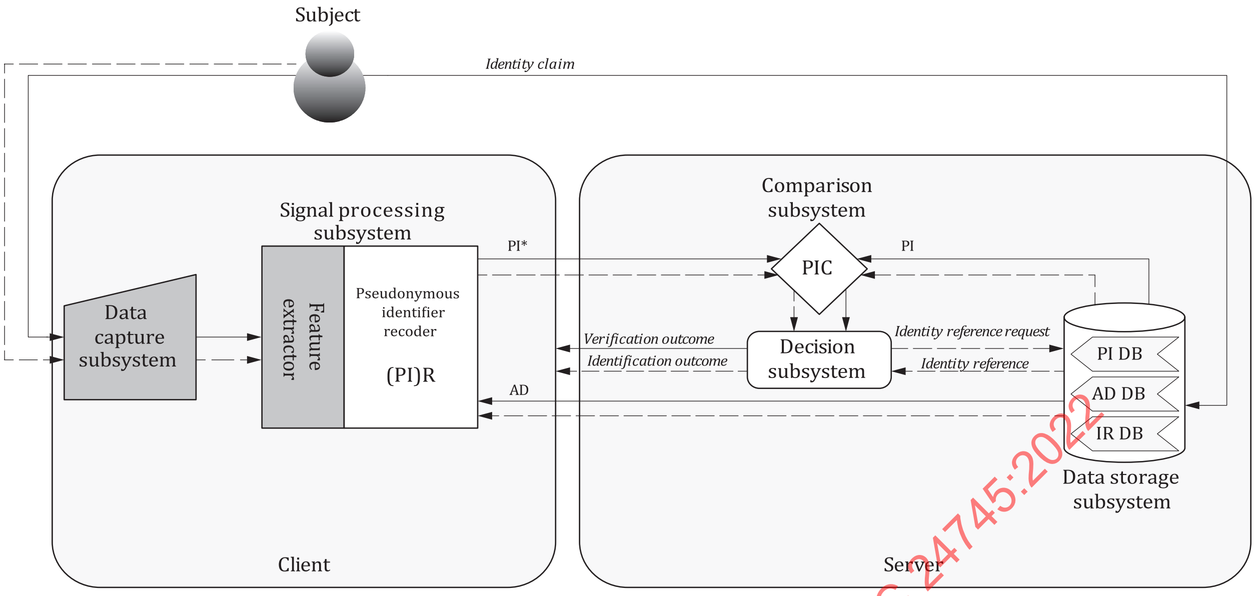
Key

——— verification

– – – identification

Figure 7 — 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 BR and IR) is handled by the server, reliable database security and network security are required. A large-sized commercial automated fingerprint identification system (AFIS) is usually implemented according to this model. From a privacy point of view, this model is usually not recommended unless RBRs as exemplified by Figure 8 are employed because of the sensitive PII that is otherwise collected in a centralized database. In Figure 8, the PIR can be implemented in the server.



Key

———	verification
– – –	identification

Figure 8 — Model A: Store on server and compare on server using RBRs

In this model, the client is controlled either by a service provider or by the user. Depending on the leakage of information from PI/PI* or AD, one option can be preferred.

8.2.3 Model B — Store on token and compare on server

In this model, a token is used for storing BRs and the captured biometric data are transferred to the server for comparison, as shown in Figure 9 and Figure 10. The biometric subject associates his/her BR with the IR at the token during the enrolment process. A subject who wants to assert his/her identity can connect a token with the client, and also submit his/her biometric characteristic(s). Then, the client sends both the stored BR and the captured biometric feature to the server for comparison.

In the case of RBRs, the PI that was generated during enrolment and then stored on the token and the PI* reconstructed during verification are sent to the server while AD is only provided to the client. This model can also be extended with storing PIs on both the token as well as the server to allow three-factor authentication. In Figure 10, the PIR can also be implemented in the server or the token.

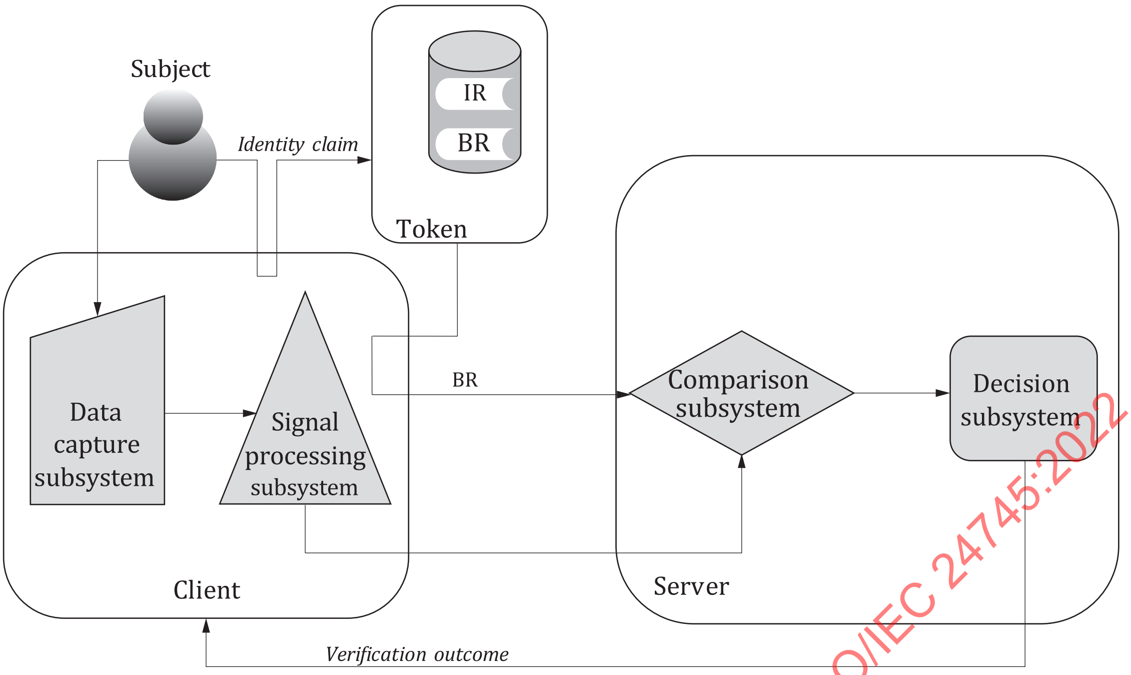


Figure 9 — Model B: Store on token and compare on server using BRs

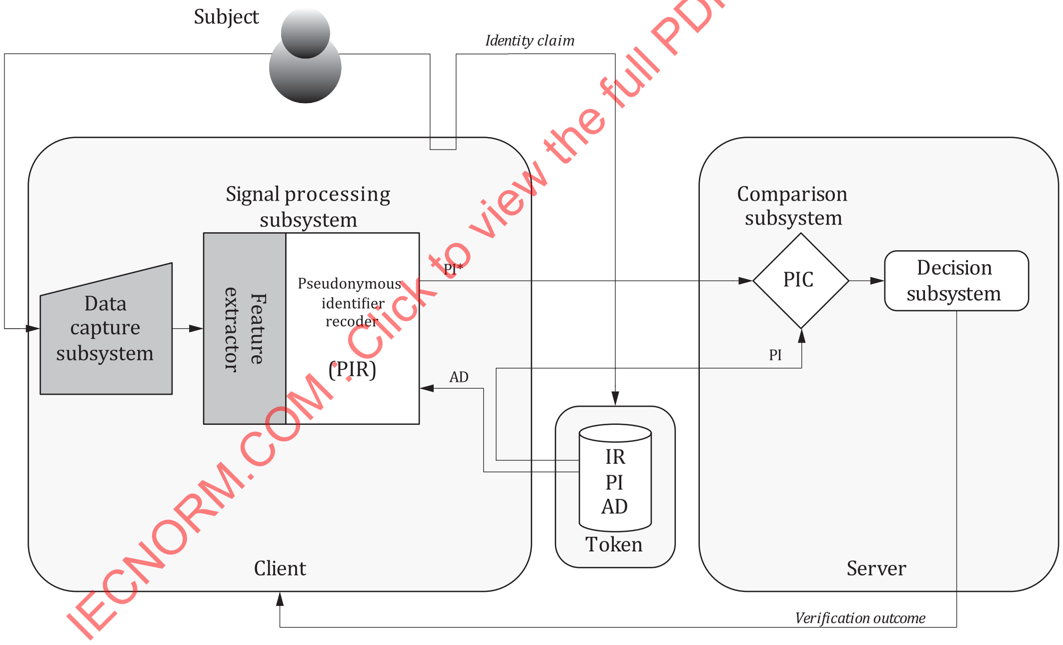


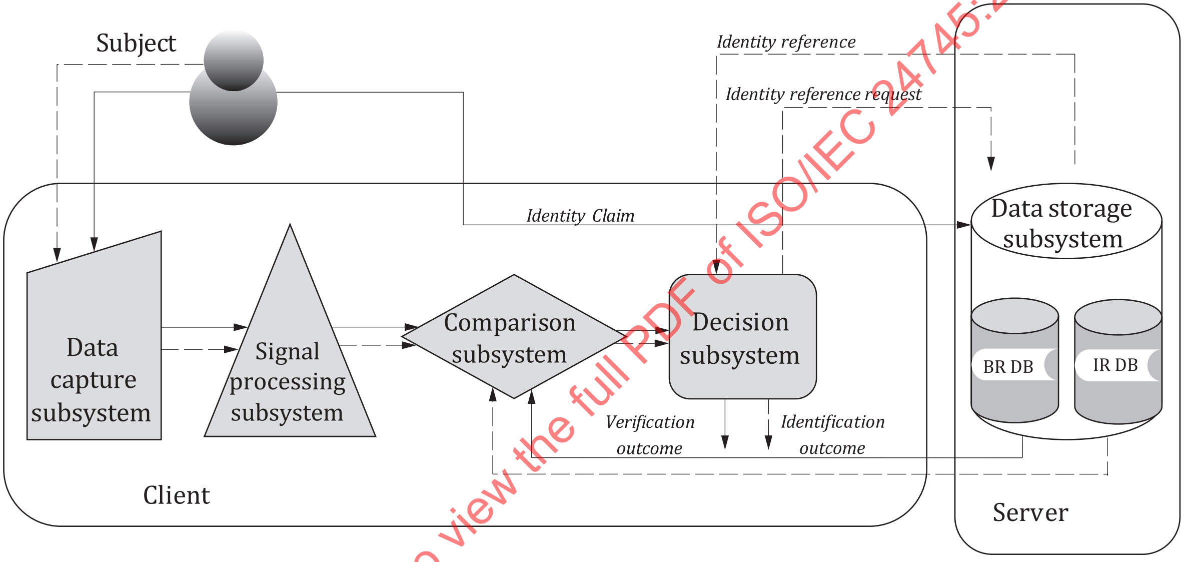
Figure 10 — Model B: Store on token and compare on server using RBRs

This model requires that the server trusts the data captured from the client. This model is usually used for verification because there is no other BR for comparison at the token except the one asserted by the individual. Since the BR is stored at the portable token, which can be securely handled by the individual, this model does not require database security. However, this model requires network security to protect the transfer of the stored BR and captured probe biometric data. This is to ensure that the server can trust that the reference data coming from the client stems from the enrolment process and was not inserted into the network immediately prior to verification. It is noted that the IR is neither transferred nor bound with the BR in the client and server. So, this model can be considered as a privacy sympathetic model.

In this model, the client is controlled either by a service provider or by the user. For the case of Figure 10, it is recommended that the client is controlled by the user to ensure additional protection of the captured biometric data.

8.2.4 Model C — Store on server and compare on client

In this model, the BRs are stored on the server and probe biometric data are extracted from the subject at the client side for the comparison process as shown in Figures 11 and 12. The biometric subject associates his/her BR with the IR at the server during the enrolment process. A subject who wants to assert his/her identity submits his/her probe biometric sample to the client and then the client requests the sending of the corresponding BR related to the asserted biometric subject. Upon request, the server sends the asserted BR to the client and finally the client executes a comparison of the captured biometric sample and the downloaded BR. For this model, the client shall be equipped with a biometric sensor and also a comparison/decision algorithm.



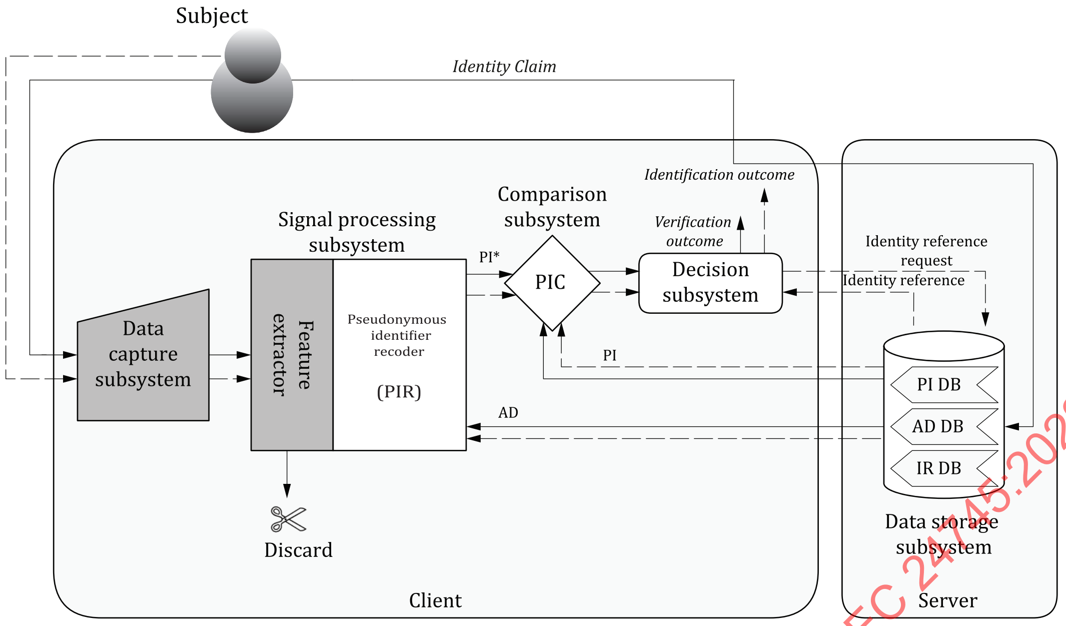
Key

______ verification

_ _ _ _ identification

Figure 11 — Model C: Store on server and compare on client using BRs

This model requires that the client trusts the data received from the server. This model can be used for identification and also verification. Since sensitive PII (i.e. BRs and IRs) are usually stored at the centralized server, reliable database security and network security are required for safeguarding the biometric subject's privacy. In Figure 12, the PIR also can be implemented in the server.



Key

——— verification

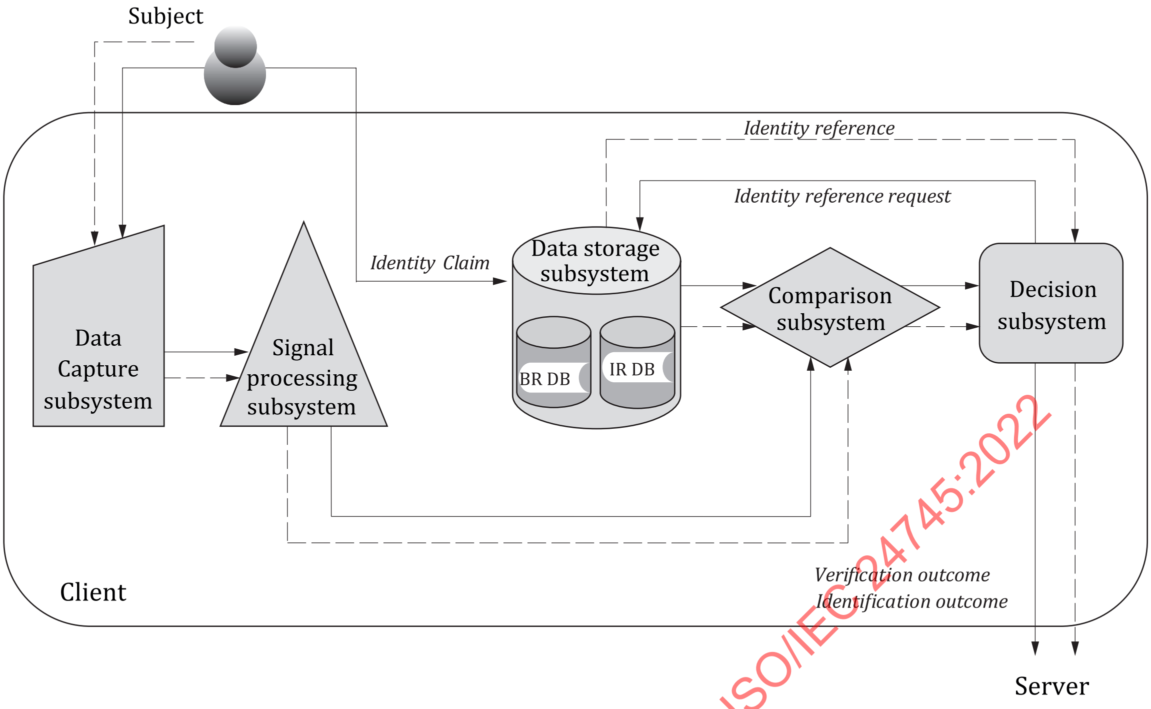
– – – – identification

Figure 12 — Model C: Store on server and compare on client using RBRs

In this model, the client is controlled either by a service provider or by the user. For the case of Figure 11, it is recommended that the client is controlled by the service provider to ensure protection of BRs. For the case of Figure 12, depending on the leakage of information from PI/PI* or AD, one option can be preferred.

8.2.5 Model D — Store on client and compare on client

In this model, the BRs are stored on the client and a probe biometric sample is extracted from the biometric subject for the comparison process which is performed on the client using BRs as shown in Figure 13 and using RBRs as shown in Figure 14. The subject associates his/her BR with the IR of the client during the enrolment process. A subject who wants to assert his/her identity submits his/her probe biometric sample to the client. To deploy this model, the client shall be equipped with a biometric sensor and a comparison/decision algorithm. This model is usually used for the authentication of subjects using devices such as personal desktop computers, laptop computers and mobile phones. In some cases, the client can operate in standalone mode for which no connection to the server is required. In other cases, the final authentication can be made by the server which confirms the verification results given by the client.

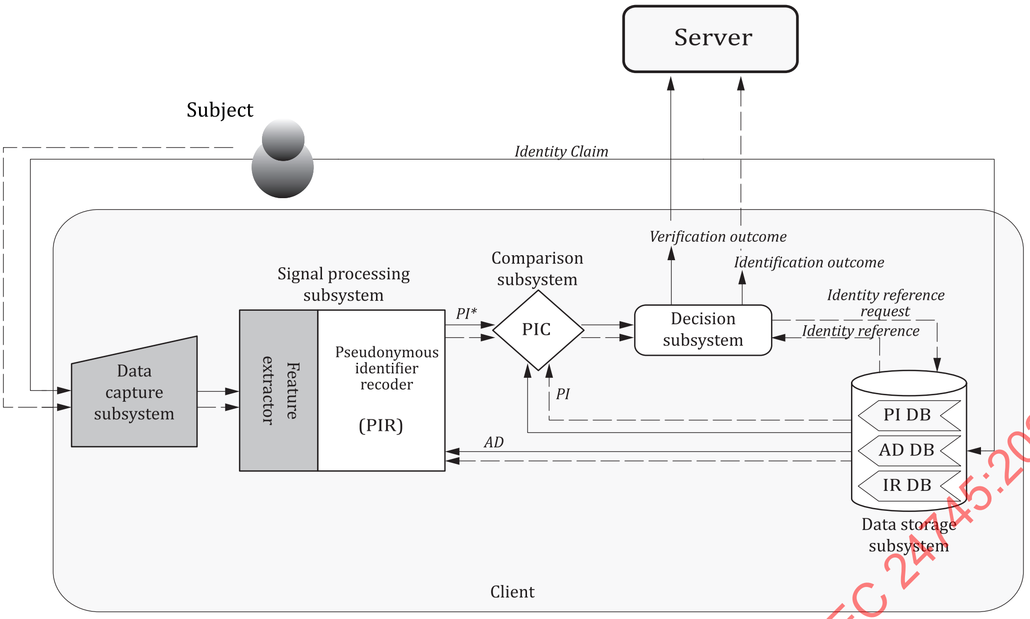


Key

———	verification
– – – –	identification

Figure 13 — Model D: Store on client and compare on client using BRs

This model can be used for both identification as well as verification. Since sensitive PII (i.e. the BR and IR) are not transferred to the server, the burden of network security can be minimized, although reliable database security is still required for the client and, hence, RBRs are recommended. In terms of privacy, this model is generally more favourable than other models using a centralized database. If the security of client is not ensured, a server-based approach is preferred.



Key

______	verification
_ _ _ _	identification

Figure 14 — Model D: Store on client and compare on client using RBRs

In this model, it is recommended that the client is controlled by the user.

NOTE This model is also applicable to the exploitation of the verification outcome directly by the client (case without any server).

8.2.6 Model E — Store on token and compare on client

In this model, the BRs are stored on the token and a probe biometric sample is extracted from the subject for the comparison process, which is performed on the client as shown in Figure 15 and Figure 16. The biometric subject associates his/her BR with the IR on the token during the enrolment process. A subject who wants to assert his/her identity presents his/her probe biometric sample to the client with the token and the BR stored therein. To deploy this model, the client shall be equipped with a biometric sensor and processing software including comparison/decision algorithm. In this case, the client can be a kiosk type, as found in public places such as an airport and public buildings for personal authentication. This model is applied at border controls using the e-passport as the token. In Figure 16, the PIR can be implemented in the token.

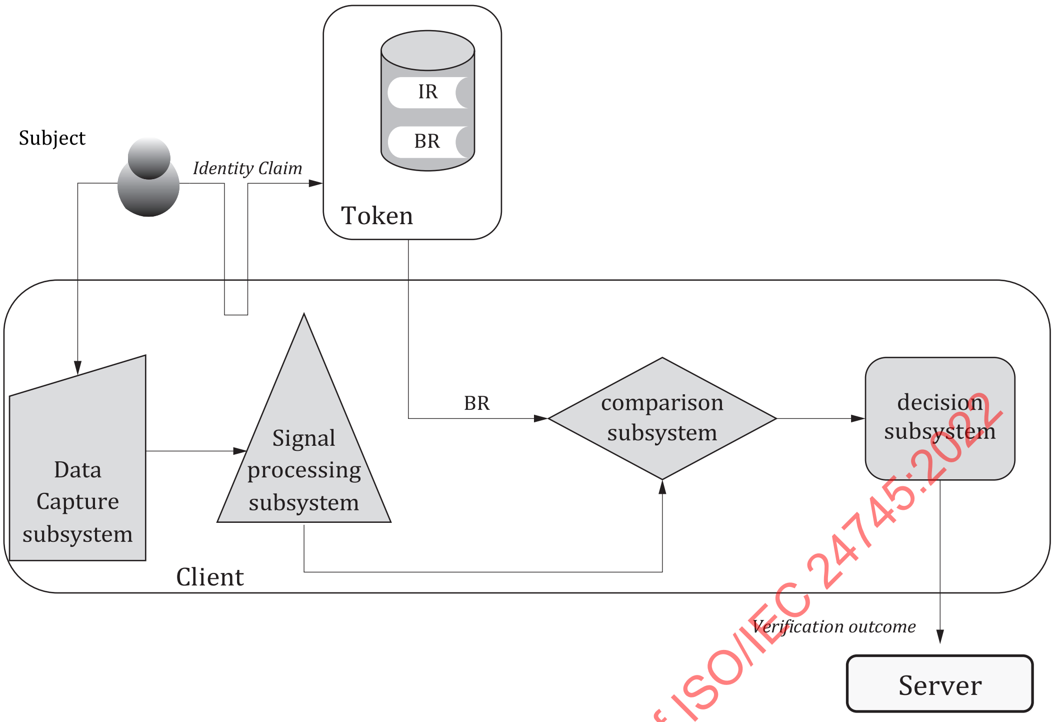


Figure 15 — Model E: Store on token and compare on client using BRs

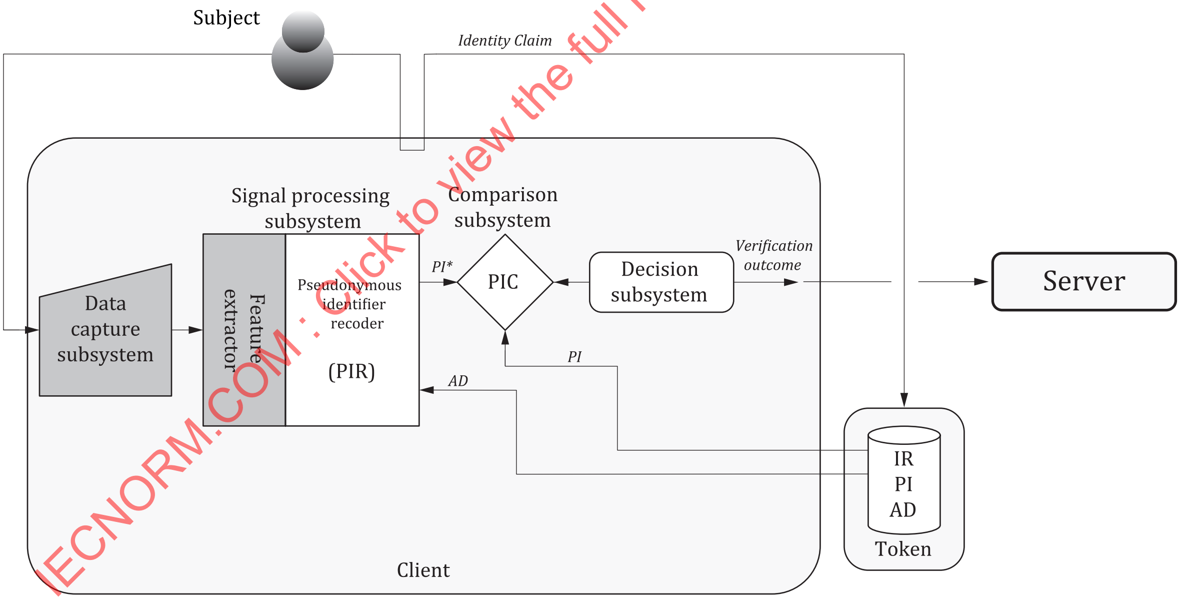


Figure 16 — Model E: Store on token and compare on client using RBRs

Biometric references and IRs can be stored on an IC chip embedded in a token. This model is usually used for verification. Since sensitive PII (i.e. the BR and IR) are not transferred to the server, the burden of network security can be minimized, although reliable database security is still required. In terms of privacy, this model is more favourable than other models using centralized storage for the biometric and IR. The command addressed to the token to read the BR and the subsequent response by the token conveying the BR data should be secured using the secure messaging mechanism according to ISO/IEC 7816-4.

In this model, the client is controlled either by a service provider or by the user. For the case of Figure 15, it is recommended that the client is controlled by the user to ensure further protection of BR.

For the case of Figure 16, depending on the leakage of information from PI/PI* or AD, one option can be preferred.

NOTE This model is also applicable to the exploitation of the verification outcome directly by the client (case without any server).

8.2.7 Model F — Store on token and compare on token

In this model, the BRs 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 17. The subject associates his/her BR with the IR stored on the token during the enrolment process. A subject who wants to assert his/her identity presents his/her probe biometric sample to the client with the token (comparison on card, see ISO/IEC 24787). With this model the token provides the comparison and decision functionality. In this case, the client can be an automated teller machine (ATM). This model is usually applied to bank transactions using OCC.

This type of OCC model is the strongest mechanism for protecting personal identifiable information under the assumption that the token is able to provide a secure and isolated execution environment. The token stores the BR and IR and the comparison process is also executed on the card. 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 according to 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. The token can contain the signal processing subsystem. In this case, the biometric data are confined to the token and the client, and is not passed to the server

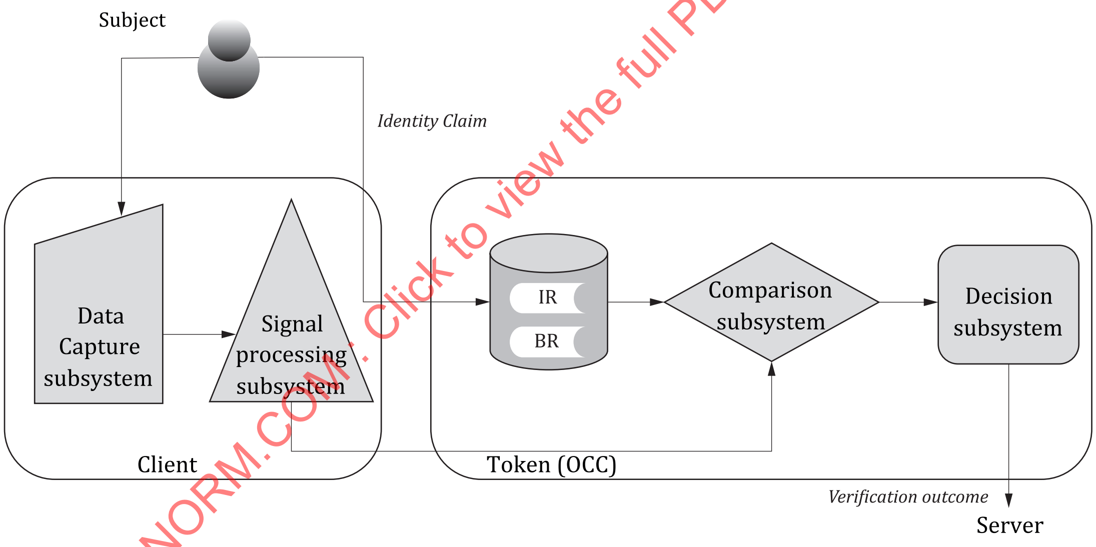


Figure 17 — Model F: Store on token and compare on token using BRs

This model limits the exposure of an individual's PII by storing the biometric and IR on the token. Furthermore, for RBRs (see Figure 18), only AD may have to be transmitted to the client while PI remains within the token. This model can, therefore, be considered as privacy-protective since the biometric information is more under the control of the subject, in particular for the full OCC model (i.e. the case where PIC and PIR are embedded in the token). However, as in some of the previous models, reliable steps shall be embedded in the client-server communication such that the server can trust that the data subject authentication is the result of a genuine comparison. Alternatively, the data capture and signal processing subsystems can also be integrated into the token. Modalities for the implementation of Model F are standardized by ISO/IEC 24787 (on-card biometric comparison). In Figure 18, the PIR can be implemented in the token. In this case, AD remains inside the token, minimizing the risk of privacy compromise.

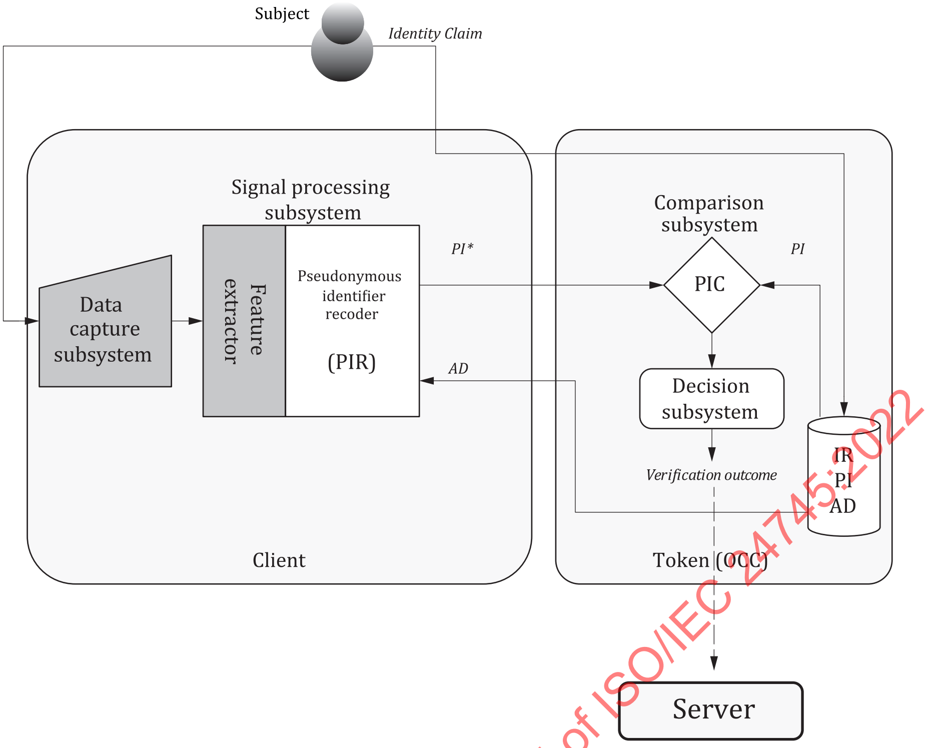


Figure 18 — Model F: Store on token and compare on token using RBRs

In this model, the client is controlled either by a service provider or by the user. For the case of Figure 18, depending on the leakage of information from AD, one option can be preferred.

NOTE This model is also applicable to the exploitation of the verification outcome directly by the client (case without any server).

8.2.8 Model G — Store distributed on token and server, compare on server

This model employs data separation through distributed storage of data elements from the RBRs. During the enrolment phase of one implementation of this model, a PI is created and stored on the server accompanied by CI. The corresponding AD, the IR and CI are stored on a token. During verification, the token publishes the AD and CI to the client (see Figure 19). The client captures probe biometric data and transforms it to a PI*. The PI* and CI are transferred to the server. The server compares PI and PI* resulting in a verification outcome.

An important advantage of this model is that the RBR is distributed between the token and the server. Verification is only possible if both the token and the server contain the correct data. This property reduces the risk of tampering with BRs since it requires tampering with the token as well as the data at the server. Furthermore, it allows revocation of BR data (PIs) on the server side without the need to access a token. A third advantage is that the subject has control over the verification process since his/her token is required.

The following variations/adaptations of this model can be applied:

- IR stored on the server instead of the token;
- storage of CI, IR, AD on the client and PI, CI on the server without the need for a token;
- storage of PI on both the token as well as on the server to allow three-factor authentication at the server side. In this implementation, the PIC receives the PI from the server storage subsystem, the PI from the token, and the PI* resulting from the PIR.

This model is especially suitable for online transaction authentication (such as e-banking, online credit card transactions and as PIN replacement or enhancement for ATMs) that employs a card or token that can store AD. To minimize the amount of information exchange between client and server, and to prevent the transmission of parts of RBR data from the server to the client, it is not recommended to store the PI on a token and the AD at the server. In Figure 19, the PIR also can be implemented in the server or token.

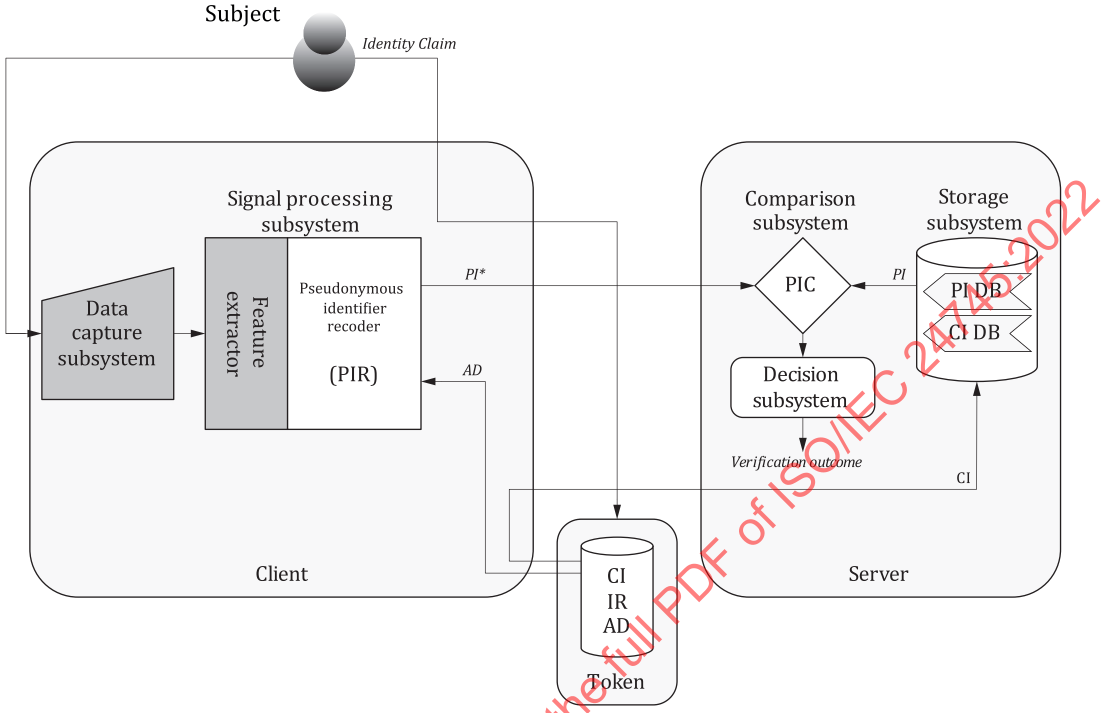


Figure 19 — Model G: Store distributed on token and server, compare on server

In this model, the client is controlled either by a service provider or by the user. For the case of Figure 19, depending on the leakage of information from AD, control by the user can be preferred.

NOTE 1 This model applies in principle only to RBRs as storage is distributed throught the separation of an RBR into PI and AD.

An example of an application relying on this model is provided in Annex E.

NOTE 2 In this model, part of the data stored in the token can be represented as memorizable secrets (e.g. AD as password as in ISO/IEC 30136:2018, 6.4.3). In that case, it can be impossible to store them and, instead, necessary to provide them as an input directly by the subject.

8.2.9 Model H — Store distributed on token and client, compare on client

In this model, the AD, IR and a CI are stored on a token and the PI and CI are stored with the client (Figure 20). During verification, the token publishes the CI and AD to the client. The client retrieves the PI corresponding to the CI from its storage subsystem and transfers the AD to the PIR, which generates a candidate PI* based on the captured biometric probe. The resulting PI* is compared to the PI that is stored with the client, and the comparison result is communicated to the decision subsystem to produce a verification outcome.

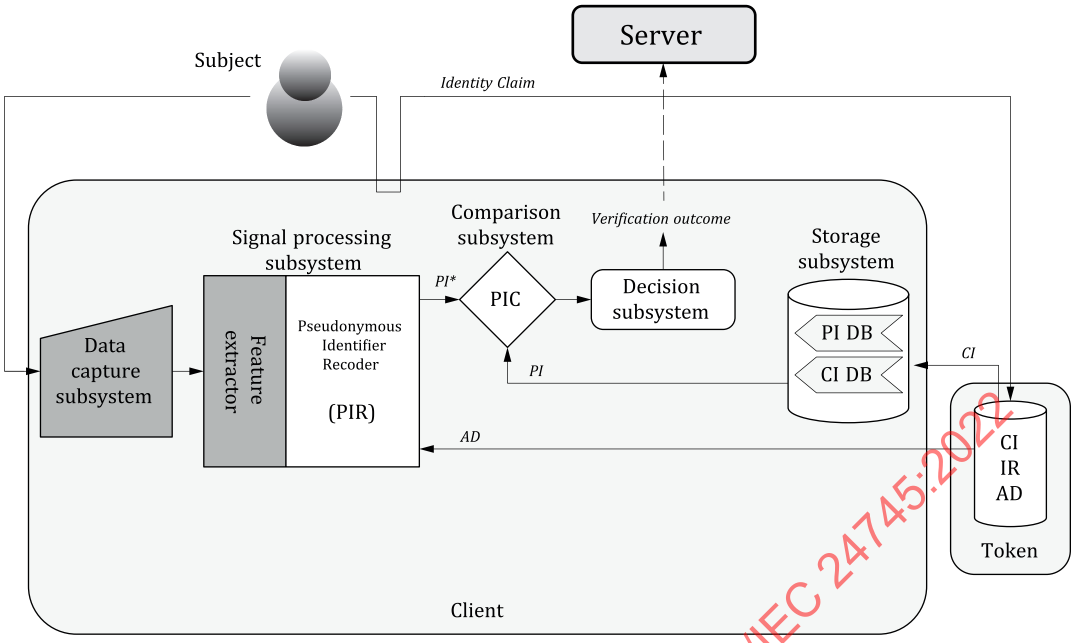


Figure 20 — Model H: Store distributed on token and client, compare on client

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.

The following modifications can be applied to this model:

— store IR on the client instead of on the token;

— store PI on the token and AD at the client.

As described in this clause, most biometric systems usually consist of a server and several remotely connected clients which are equipped with biometric capture devices. In general, the overall security level of the biometric authentication process is dependent both on the security level of the process executed and on the functional performance level of the biometric capture devices. By obtaining trusted information such as the functional performance level of the biometric devices used, and the security level of the remote system, and by determining whether the processes in the system were executed securely, the verifier of the authentication can make a better decision on the extent to which the result of the biometric verification can be trusted. For this, authentication context for biometrics (ACBio) defined in ISO/IEC 24761 can be used as a solution to the above issue by sending the information about the devices used and the process executed at a remote site to the verifier. In Figure 20, the PIR also can be implemented in the token.

In this model, the client is controlled either by a service provider or by the user. For the case of Figure 20, depending on the leakage of information from PI and AD, control by the user can be preferred.

NOTE 1 This model applies in principle only to RBRs as storage is distributed through the separation of an RBR into PI and AD.

NOTE 2 This model is also applicable to the exploitation of the verification outcome directly by the client (case without any server).

NOTE 3 In this model, part of the data stored in the token can be represented as memorisable secrets (e.g. AD as password as in ISO/IEC 30136:2018, 6.4.3). In that case, it can be impossible to store them and, instead, necessary to provide them as an input directly by the subject.

8.2.10 Model I — Store on server, compare distributed

In this model, the AD, IR, PI and a CI are stored on the server and CI is stored with the client (see Figure 21). During verification, the server and the client never share AD, IR and PI, but only CI. The server and the client execute together an interactive protocol to commonly execute PIR and PIC without ever revealing to the other party the information owned by each party (AD, IR, PI on server side, the captured biometric probe on client side). Based on this interactive protocol, the client and the server learn only the final result of PIC.

This model can be applied to various settings where online communication and local computation are sufficiently reliable, as it is generally heavier than execution without interaction.

The following modifications can be applied to this model:

- the output of the interactive execution can be available only on the server side or only on the client side;
- the interactive execution can be applied partially to PIR only and then PIC is executed locally on one side (client or server);
- the interactive execution can be applied partially to PIC only with PIR being executed locally on one side (client or server) after prior communication of the required input (AD);
- storage of PI and AD can be distributed between client and server, not only by storing PI and AD on two different places, but even by using secure secret sharing mechanisms (see ISO/IEC 19592-1).

This model is usually implemented by the use of secure multiparty computation techniques[47], [54].

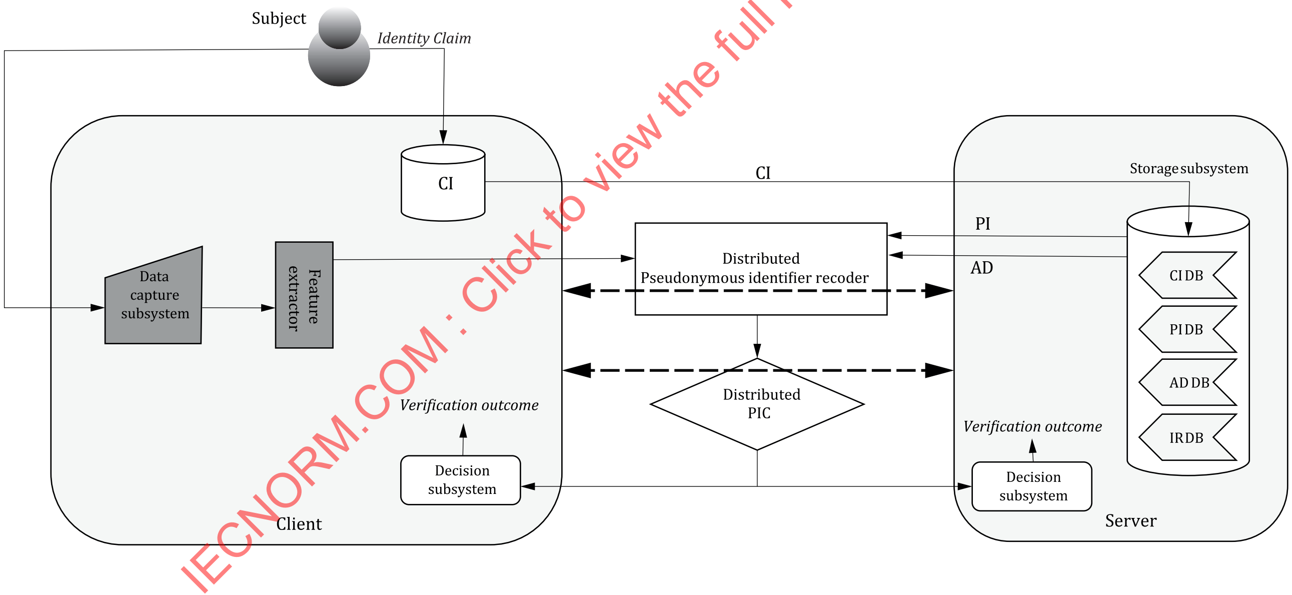


Figure 21 — Model I: Store on server, compare distributed using RBRs

The same model can be implemented with normal BRs (see Figure 22), under the condition that the comparison subsystem can be computed in a distributed manner (which is the case for comparison techniques based on simple metrics such as Hamming distance and Euclidean distance).

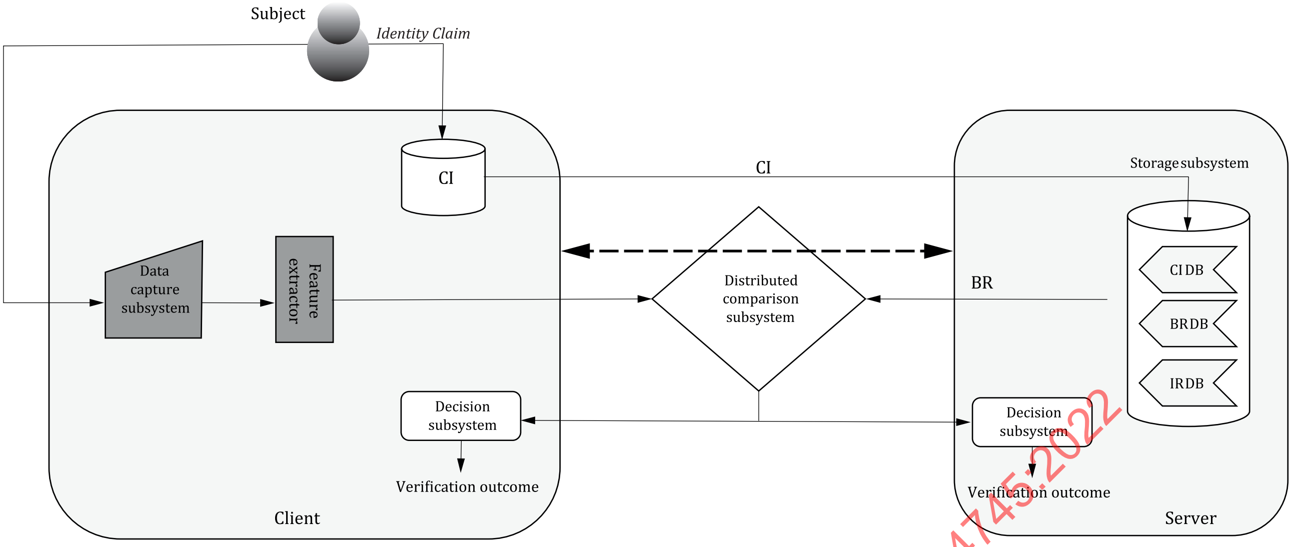


Figure 22 — Model I: Store on server, compare distributed using BRs

In this model, the client shall be controlled by the user to strengthen the security and privacy during the distributed comparison.

8.2.11 Model J — Store on token, compare distributed

In this model, the AD, IR, PI and a CI are stored on the token and CI is stored with the client (Figure 23). During verification, the token and the client never share AD, IR and PI, but only CI. The token and the client execute together an interactive protocol to commonly execute PIR and PIC without ever revealing to the other party the information owns by each party (AD, IR, PI on token side, the captured biometric probe on client side). Based on this interactive protocol, the client and the token learn only the final result of PIC.

This model can be applied to various settings where local computation is sufficiently reliable, as it is generally heavier than execution without interaction.

The following modifications can be applied to this model:

- the output of the interactive execution can be available only on token side or only on client side;
- the interactive execution can be applied partially to PIR only and then PIC is executed locally on one side (client or token);
- the interactive execution can be applied partially to PIC only with PIR being executed locally on one side (client or token) after prior communication of the required input (AD);
- distribution of execution can be between token, client and server in order to have the final result available only on server side;
- storage of PI and AD can be distributed between client and token, not only by storing PI and AD on two different places, but even by using secure secret sharing mechanisms (see ISO/IEC 19592-1).

This model is usually implemented by using secure multiparty computation techniques[47] and secure execution environment for the token.

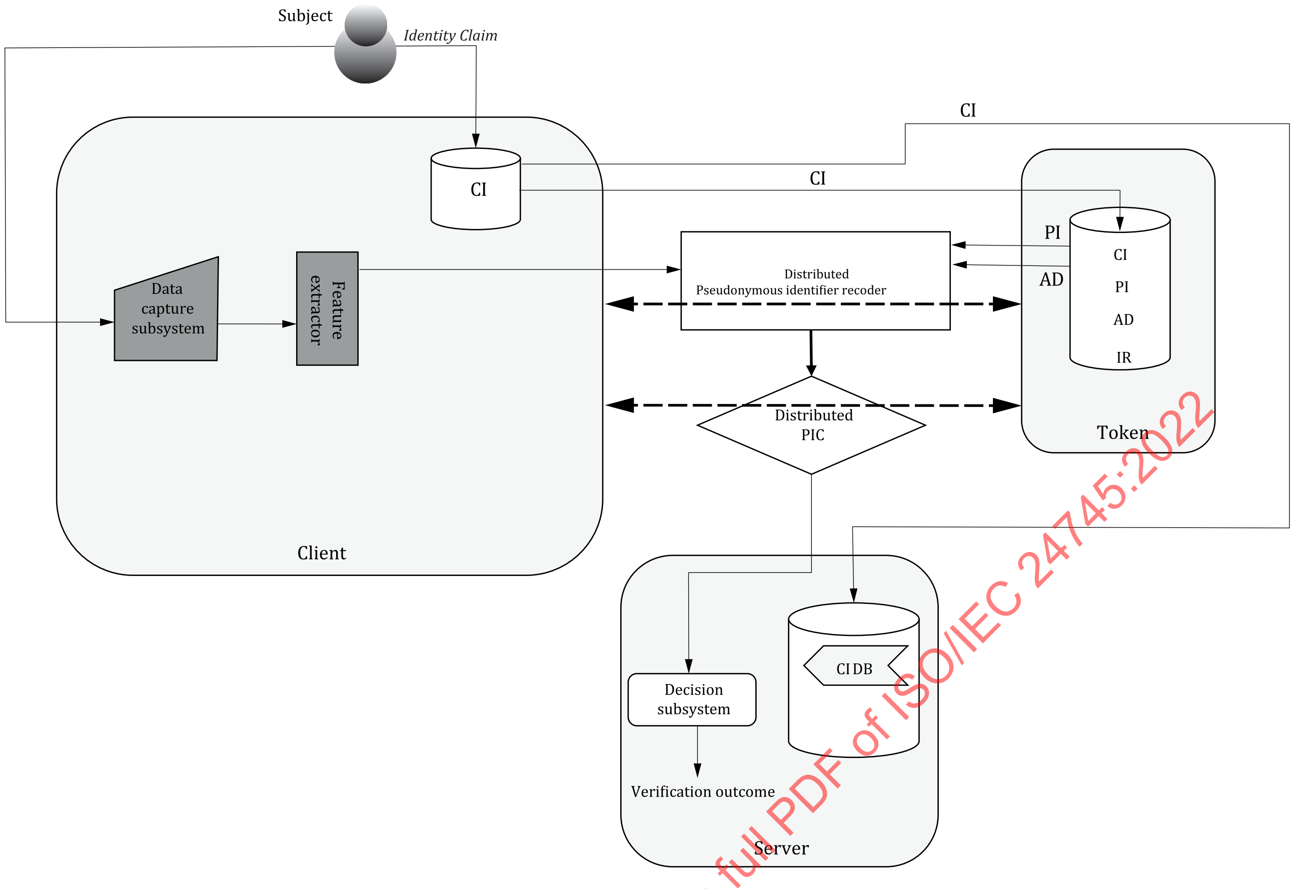


Figure 23 — Model J: Store on token, compare distributed using RBRs (variant with decision available only on server)

As for model I, the same model can be implemented with normal BRs (see Figure 24), under the condition that the comparison subsystem can be computed in a distributed manner.

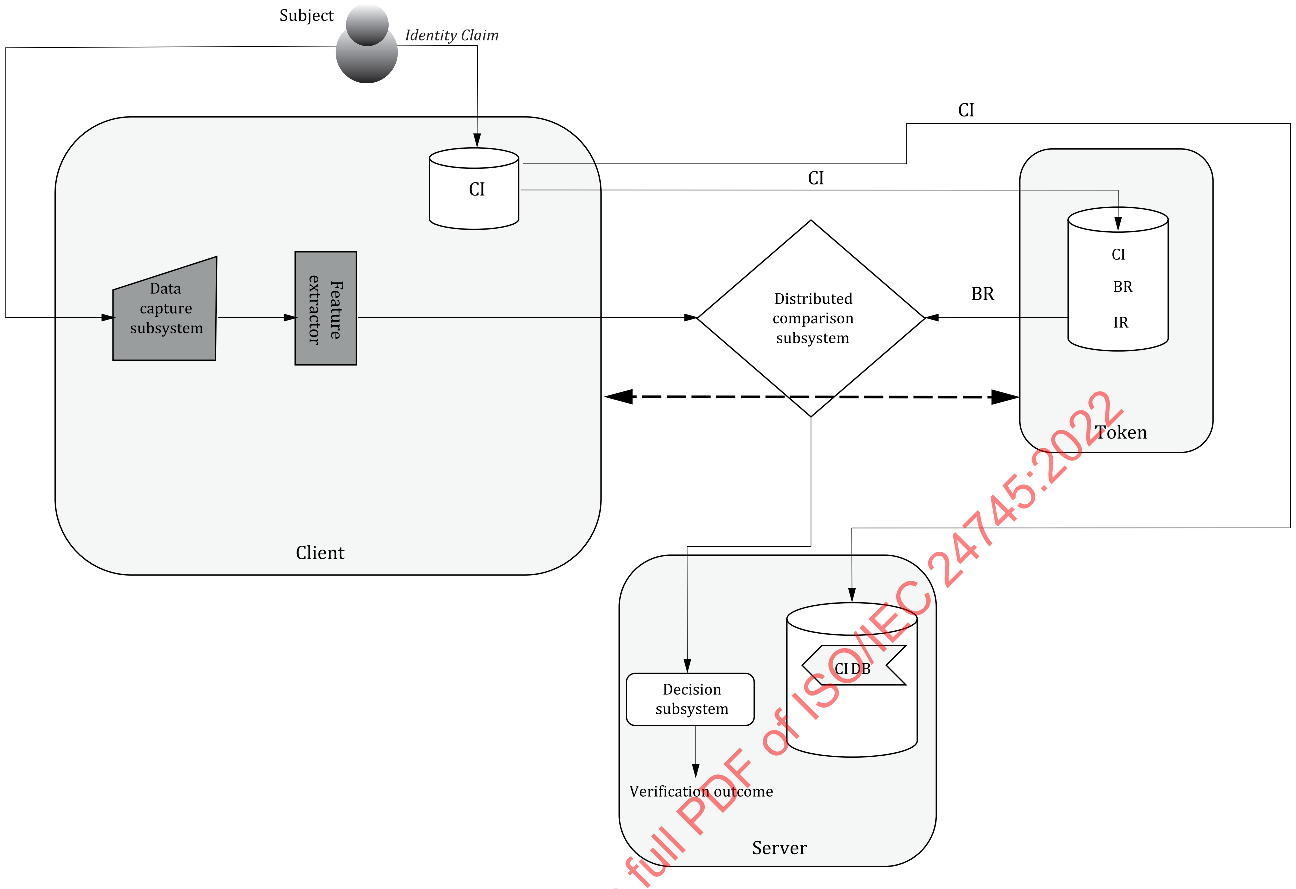


Figure 24 — Model J: Store on token, compare distributed using BRs (variant with decision available only on server)

In this model, the client is controlled either by a service provider or by the user.

NOTE This model is also applicable to the exploitation of the verification outcome directly by the client (case without any server).

8.2.12 Model K — Store distributed, compare distributed

In this model, the AD, IR, PI are distributed between client, token (if any) and server, and a CI are stored on each side (Figure 25), but AD and PI are stored in an encrypted form that allows operations without prior decryption (e.g. using homomorphic encryption, [35], [28] ISO/IEC 18033-6). During verification, PIR and PIC are executed either on client, or token or server side, directly on encrypted data. The output of PIC computed on encrypted data can lead either directly into the plain decision result, or the encrypted decision result. In the latter case, only the output may be decrypted.

In order to ensure confidentiality of the encrypted data, the owner of the decryption key related to a specific encrypted data shall be the party that does not store this encrypted data.

This model can be applied to various settings where local computation is sufficiently reliable, as it is generally heavier than execution without encrypted data.

Depending on the underlying mechanisms used to implement PIR and PIC, the following variants can be applied for this model:

- PIR and PIC can be executed on the same side (either client, or token or server);
- PIR can be executed on client (or token) side with the captured biometric probe in clear text, and PIC can be executed on server side on encrypted inputs and, when applicable, output decrypted by the client;

- PIR can be executed on server side with an encrypted version of the capture biometric probe, and PIC can be executed on client (or token) side;
- storage of PI and AD can be distributed between client, token and server, not only by storing PI and AD on two different places, but even by using secure splitting mechanisms.

This model is usually implemented by using homomorphic encryption primitives.

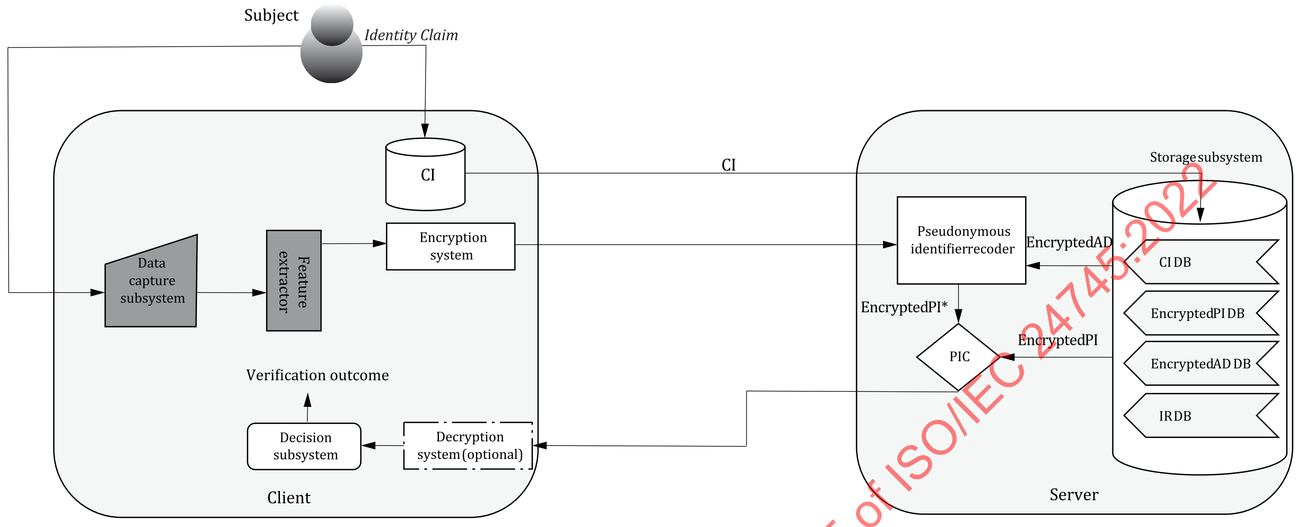


Figure 25 — Model K: Store distributed, compare distributed (variant with PIR and PIC on server side) using RBRs, decryption system being optional

The same model can be implemented with normal BRs (see Figure 26), under the condition that the comparison subsystem can be adapted to work on encrypted inputs (e.g. this is the case for Hamming distance-based comparison).

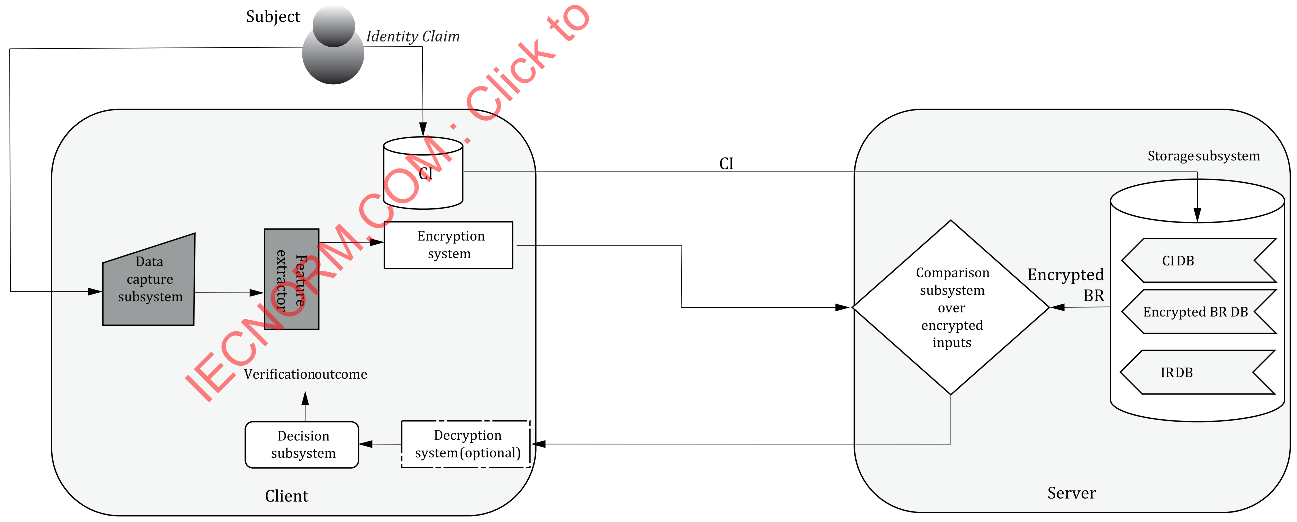


Figure 26 — Model K: Store distributed, compare distributed (variant with PIR and PIC on server side) using BRs, decryption system being optional

In this model, the client shall be controlled by the user to strengthen the security and privacy during the distributed comparison.

Annex A
(informative)

Secure binding and use of separated DB_{IR} and DB_{BR}

A.1 General

Even if two DBs are used to separate the biometric data to minimize the effect of privacy infringement, for their use, they should be bound with a common identifier (CI). However, one should not be able to extract any information about the data from the CI. If one DB is infringed and its contents are compromised, the operators of two DBs should be able to detect it. Similarly, if during the use of the DBs a legitimate DB operator with the correct key modifies its contents, the other DB should be able to detect the modification.

This annex describes examples for secure binding of a pair of IR and BR assuming separated databases for IR and BR with separated control and their usages. The database for IRs is called DB_{IR} and that for BRs is called DB_{BR}. It is assumed that DB_{IR} uses a secret key K_i, and DB_{BR} uses a secret key K_b to protect their database contents. In addition, it is assumed that the databases share two secret keys: K_{ib} for computing CI and a cryptographic check value and K_e for securing communication messages (if needed).

A.2 Secure binding between separated DB_{IR} and DB_{BR}

The communication channel between DB_{IR} and DB_{BR} is either secure or insecure, with a secure channel providing confidentiality and authenticity. In the first case (Case A), the communication channel between the two databases is assumed to be secure. In the second case (Case B), the communication channel is assumed to be insecure, but the two databases share a symmetric cipher and a common secret key K_e. The secure binding of a particular set of IR and BR is described below.

Case A: Secure communication channel between DB_{IR} and DB_{BR} as shown in Figure A.1

a) DB_{IR} receives an authentic IR from an identity reference (IR) claimant (individual) or from a trusted third party (TTP), encrypts *IR* using K_i to get $E_{Ki}(IR)$, and hashes *IR* to get $h(IR)$.

b) DB_{BR} receives the corresponding authentic BR from the signal processing subsystem, encrypts *BR* using K_b to get $E_{Kb}(BR)$, and hashes *BR* to get $h(BR)$.

c) DB_{IR} sends $h(IR)$ to DB_{BR}.

d) DB_{BR} receives $h(IR)$ from DB_{IR}, calculates MAC for $\{h(IR), h(BR)\}$ with shared secret key K_{ib} to get $CI = MAC_{Kib}(h(IR), h(BR))$ where *CI* will be used as a CI and as a cryptographic check value, sends $h(BR)$ to DB_{IR}, and stores $\{CI, E_{Kb}(BR)\}$.

e) DB_{IR} receives $h(BR)$ from DB_{BR}, calculates MAC for $\{h(IR), h(BR)\}$ with shared secret key K_{ib} to get $CI = MAC_{Kib}(h(IR), h(BR))$, and stores $\{CI, E_{Ki}(IR)\}$.

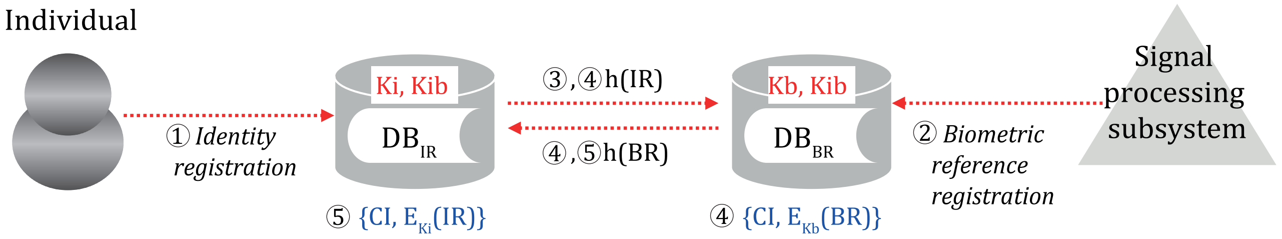


Figure A.1 — Secure binding between separated $\mathrm{DB_{IR}}$ and $\mathrm{DB_{BR}}$ (Case A)

Case B: Insecure communication channel between $\mathrm{DB_{IR}}$ and $\mathrm{DB_{BR}}$, with shared secret key $\mathrm{K_e}$

a) $\mathrm{DB_{IR}}$ receives an authentic IR from an IR claimant (individual) or from a TTP, encrypts *IR* using $\mathrm{K_i}$ to get $\mathrm{E}_{Ki}(IR)$, hashes *IR* to get h(*IR*), and encrypts {h(*IR*), $IDDB_{IR}$, N_i} using $\mathrm{K_e}$ to get E_{Ke}(h(*IR*), $IDDB_{IR}$, N_i), where *IDDB* is a unique identifier for DB and N_i is a nonce (time stamp or sequence number) generated by $\mathrm{DB_{IR}}$.

b) $\mathrm{DB_{BR}}$ receives the corresponding authentic BR from the signal processing subsystem, encrypts *BR* using $\mathrm{K_b}$ to get $\mathrm{E_{Kb}}(IR)$, and hashes *BR* to get h(*BR*).

c) $\mathrm{DB_{IR}}$ sends E_{Ke}(h(*IR*), $IDDB_{IR}$, N_i) to $\mathrm{DB_{BR}}$.

d) $\mathrm{DB_{BR}}$ receives E_{Ke}(h(*IR*), $IDDB_{IR}$, N_i) from $\mathrm{DB_{IR}}$, decrypts it to recover {h(*IR*), $IDDB_{IR}$, and N_i}, and checks $IDDB_{IR}$, and N_i (if the check fails, it stops with an error message). $\mathrm{DB_{BR}}$ calculates MAC for {h(*IR*), h(*BR*)} with shared secret key $\mathrm{K_{ib}}$ to get *CI* = MAC_{Kib}(h(*IR*), h(*BR*)) where CI will be used as a CI and as a Check value, encrypts {*CI*, h(*BR*), $IDDB_{BR}$, N_b} using $\mathrm{K_e}$ to get E_{Ke}(*CI*, h(*BR*), $IDDB_{BR}$, N_b), sends E_{Ke}(*CI*, h(*BR*), $IDDB_{BR}$, N_b) to $\mathrm{DB_{IR}}$, and stores {*CI*, $\mathrm{E}_{Kb}(BR)$}.

e) $\mathrm{DB_{IR}}$ receives E_{Ke}(*CI*, h(*BR*), $IDDB_{BR}$, N_b) from $\mathrm{DB_{BR}}$, decrypts $\mathrm{E_{Ke}}$(*CI*, h(*BR*), $IDDB_{BR}$, N_b) to recover {*CI*, h(*BR*), $IDDB_{BR}$, and N_b}, and checks $IDDB_{BR}$, and N_b (if the check fails, it stops with an error message.). $\mathrm{DB_{IR}}$ calculates MAC for {h(*IR*), h(*BR*)} with shared secret key $\mathrm{K_{ib}}$ to get *CI* = MAC_{Kib}(h(*IR*), h(*BR*)), compare it with the received *CI* (if the comparison fails, it stops with an error message), and stores {*CI*, $\mathrm{E}_{Ki}(IR)$}.

A.3 BR claim for verification

This clause describes an example of a BR claim from $\mathrm{DB_{IR}}$ to $\mathrm{DB_{BR}}$ for verification. It is assumed that the method for finding the correct $\mathrm{E_{Ki}}(IR)$ from a legitimate identity claim is given.

Case A: Secure communication channel between $\mathrm{DB_{IR}}$ and $\mathrm{DB_{BR}}$ as shown in Figure A.2

a) Upon receiving a legitimate identity claim from an IR claimant (individual) or from a TTP, $\mathrm{DB_{IR}}$ decrypts corresponding $\mathrm{E}_{Ki}(IR)$ to get *IR* and hashes *IR* to get h(*IR*), and sends {*CI*, h(*IR*)} to $\mathrm{DB_{BR}}$.

b) $\mathrm{DB_{BR}}$ receives {*CI*, h(*IR*)} from $\mathrm{DB_{IR}}$, finds $\mathrm{E}_{Kb}(BR)$ using *CI*, decrypts $\mathrm{E}_{Kb}(BR)$ to get *BR*, hashes *BR* to get h(*BR*), computes MAC_{Kib}(h(*IR*), h(*BR*)) and compares it with the received CI.

c) If they match, $\mathrm{DB_{BR}}$ sends BR securely to the comparison subsystem. If the match fails, it exits with an error message.

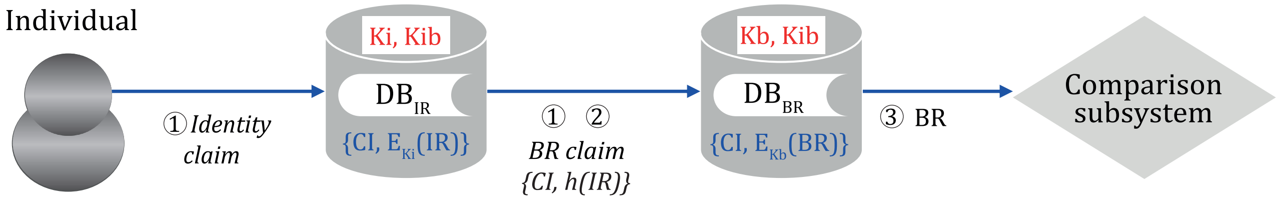


Figure A.2 — BR claim for verification (Case A)

Case B: Insecure communication channel between $\mathrm{DB_{IR}}$ and $\mathrm{DB_{BR}}$, with shared secret key $\mathrm{K_{ib}}$

a) Upon receiving a legitimate identity claim from an IR claimant (individual) or from a TTP, $\mathrm{DB_{IR}}$ decrypts corresponding $\mathrm{E}_{Ki}(IR)$ to get *IR* and hashes *IR* to get h(*IR*), encrypts {*CI*, h(*IR*), $IDDB_{IR}$, N_i} to get $\mathrm{E}_{Kib}(CI, \mathrm{h}(IR), IDDB_{IR}, N_i)$, and sends $\mathrm{E}_{Kib}(CI, \mathrm{h}(IR), IDDB_{IR}, N_i)$ to $\mathrm{DB_{BR}}$.

b) $\mathrm{DB_{BR}}$ receives $\mathrm{E}_{Kib}(CI, \mathrm{h}(IR), IDDB_{IR}, N_i)$ from $\mathrm{DB_{IR}}$, decrypts it to recover {*CI*, h(*IR*), $IDDB_{IR}$, N_i}, and checks $IDDB_{IR}$, and N_i (if the check fails, exits with an error message), finds $\mathrm{E}_{Kb}(BR)$ using *CI*, decrypts $\mathrm{E}_{Kb}(BR)$ to get *BR*, hashes *BR* to get h(*BR*), computes $\mathrm{MAC}_{Kib}(\mathrm{h}(IR), \mathrm{h}(BR))$ and compares it with received *CI*.

c) If they match, $\mathrm{DB_{BR}}$ sends *BR* securely to the comparison subsystem. If the match fails, it exits with an error message.

A.4 IR claim for identification

This clause describes an example of an IR claim from $\mathrm{DB_{BR}}$ to $\mathrm{DB_{IR}}$ for verification. It is assumed that $\mathrm{DB_{BR}}$ has already decrypted $\mathrm{E}_{Kb}(BR)$ to get *BR*, and has sent it to the comparison subsystem.

Case A: Secure communication channel between $\mathrm{DB_{IR}}$ and $\mathrm{DB_{BR}}$ as shown in Figure A.3

a) Upon receiving a legitimate identity request from the decision subsystem, $\mathrm{DB_{BR}}$ hashes *BR* to get h(*BR*), and sends {*CI*, h(*BR*)} to $\mathrm{DB_{IR}}$.

b) $\mathrm{DB_{IR}}$ receives {*CI*, h(*BR*)} from $\mathrm{DB_{BR}}$, finds $\mathrm{E}_{Ki}(IR)$ using *CI*, decrypts $\mathrm{E}_{Ki}(IR)$ to get *IR*, hashes *IR* to get h(*IR*), computes $\mathrm{MAC}_{Kib}(\mathrm{h}(IR), \mathrm{h}(BR))$, and compares it with the received *CI*.

c) If they match, $\mathrm{DB_{IR}}$ sends *IR* securely to the decision subsystem. If the match fails, it exits with an error message.

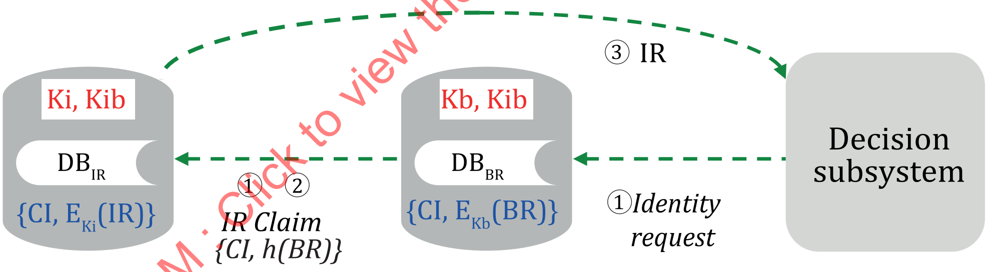


Figure A.3 — IR claim for identification (Case A)

Case B: Insecure communication channel between $\mathrm{DB_{IR}}$ and $\mathrm{DB_{BR}}$, with shared secret key Kib

a) Upon receiving a legitimate identity request from the decision subsystem, $\mathrm{DB_{BR}}$ hashes *BR* to get h(*BR*), encrypts {*CI*, h(*BR*), $IDDB_{BR}$, N_b} to get $\mathrm{E}_{Ke}(CI, \mathrm{h}(BR), IDDB_{BR}, N_b)$, where N_b is a nonce generated by $\mathrm{DB_{BR}}$, and sends $\mathrm{E}_{Ke}(CI, \mathrm{h}(BR), IDDB_{BR}, N_b)$ to $\mathrm{DB_{IR}}$.

b) $\mathrm{DB_{IR}}$ receives $\mathrm{E_{Ke}}(CI, \mathrm{h}(BR), IDDB_{BR}, N_b)$ from $\mathrm{DB_{BR}}$, decrypts it to recover {*CI*, h(*BR*), $IDDB_{BR}$, N_b}, checks $IDDB_{BR}$, and N_i (if the check fails, exits with an error message), finds $\mathrm{E}_{Ki}(IR)$ using *CI*, decrypts $\mathrm{E}_{Ki}(IR)$ to get *IR*, hashes *IR* to get h(*IR*), computes $\mathrm{MAC}_{Kib}(\mathrm{h}(IR), \mathrm{h}(BR))$, and compares it with the received *CI*.

c) If they match, $\mathrm{DB_{IR}}$ sends *IR* securely to the decision subsystem. If match fails, it exits with an error message.

Annex B
(informative)

Framework for renewable biometric references (RBRs)

B.1 Renewable biometric references (RBRs)

Renewable biometric references (RBRs) are revocable/renewable identifiers that represent an individual or data subject within a certain domain by means of a protected binary identity (re) constructed from a captured biometric sample. An RBR does not allow access to the original biometric measurement data, biometric template or true identity of its owner. Furthermore, the RBR has no meaning outside the service domain.

RBRs follow four distinct phases:

a) creation of new RBRs from biometric data during an enrolment phase;

b) operational use of the RBR as a reference to verify a claimed identity;

c) expiration of the validity of an RBR;

d) renewal or revocation of an RBR if its validity has expired or if the RBR has been compromised.

B.2 Creation and renewal

The signal processing subsystem for the RBR creation and renewal process is outlined in Figure B.1. An arrow in the figure represents a flow of information. Generally, it represents a protocol between two stages initiated by the source or the destination of the arrow. A feature extraction stage generates biometric feature data from the captured biometric sample. The features are preferably generated according to existing standards for BR data as described in the ISO/IEC 19794 series. Subsequently, a PIE generates an RBR consisting of a PI and AD. When the RBR is generated, the captured biometric sample and the extracted features can be discarded. The AD can serve one of the following purposes:

— allows the recreation of a PI associated with the captured biometric sample for comparison with the reference PI;

— allows generation of multiple independent PIs from the same individual within an application to provide renewable references;

— allows generation of independent PIs across applications to prevent database cross-comparing and linking;

— provides a means for easy BR data separation (PI and AD) to enhance security and privacy.

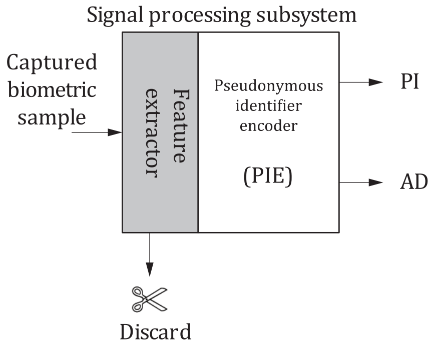

Signal processing subsystem
Captured biometric sample
Feature extractor
Pseudonymous identifier encoder
(PIE)
PI
AD
Discard

Figure B.1 — Signal processing subsystem for the generation of renewable biometric references (RBRs)

The AD can result from various approaches that provide RBRs (see Annex C for an overview). Both PI and AD are stored (either together as a combined database entry or on separate storage media/ databases), while all other captured biometric data are securely destroyed. The combination of PI and AD forms the RBR.

NOTE The renewal process is simply the re-iteration of the creation process.

B.3 Comparison

In a remote comparison scenario, the data capture and signal processing subsystems on the one hand and the comparison subsystem on the other hand are physically separated (see Figure B.2 and Figure B.3). Verification requires the following steps:

- a feature extraction stage processes the probe biometric data sample;
- a PIR generates a new PI* based on the provided AD and the extracted features;
- a comparison subsystem by means of a PI comparator (PIC) compares PI with PI* and generates a comparison score (this step and the previous step may be combined in a single step as illustrated by Figure B.3);
- a decision subsystem (not shown in Figure B.2 and Figure B.3) provides a verification outcome based on the comparison score.

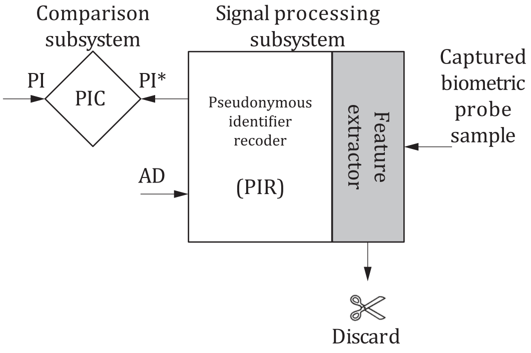

Comparison subsystem
Signal processing subsystem
PI
PIC
PI*
AD
Pseudonymous identifier recoder
(PIR)
Feature extractor
Captured biometric probe sample
Discard

Figure B.2 — Signal processing subsystem and comparison subsystem

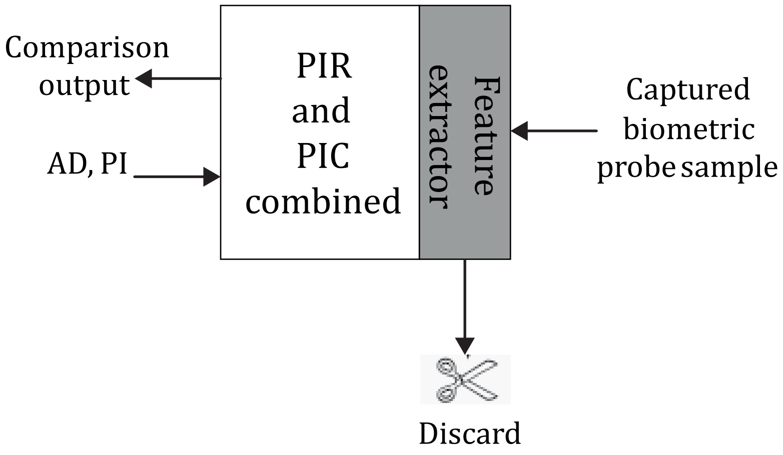


Figure B.3 — Signal processing and comparison combined

B.4 Expiration

RBRs expire for several reasons. For example, an RBR can have been issued for a limited period only or may require renewal because it was compromised. Furthermore, aging effects can impact the biometric characteristic, as is the case for the human face, which would require a renewal of the BR. Validity checks and expiration can be controlled by means of revocation lists.

B.5 Revocation

Depending on the implementation of a verification system, RBRs can be revoked by:

— deleting the RBR from a database; and/or

— removing the authorization to use an RBR.

Subsequent to revocation, re-enrolment can result in a renewed biometric reference. Depending on the deployed implementation, this can require capturing new genuine biometric samples. In other implementations, re-enrolment is based on raw biometric data, or spare RBRs that are stored in a highly secured database which is both logically as well as physically separated from the operational RBR database to allow re-enrolment without the physical presence of the data subject.

B.6 Architecture overview

The enrolment, storage and verification processes are provided in Figure B.4. The decision subsystem that is connected to the comparison subsystem is not shown in Figure B.4.