INTERNATIONAL STANDARD

ISO/IEC 24745

First edition
2011-06-15

Information technology — Security techniques — Biometric information protection

Technologies de l'information — Techniques de sécurité — Protection des informations biométriques

Reference number
ISO/IEC 24745:2011(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

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.

ISO/IEC 24745 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

Introduction

As the Internet becomes a more pervasive part of daily life, various services are being provided via the Internet, such as Internet banking, remote healthcare, etc. 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 – has come of age, and includes recognition technologies based on fingerprint image, voice patterns, iris image, facial image, and the like. 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 person 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 the compromise of biometric references. 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 could be enrolled, but the choices are usually limited. Therefore, appropriate countermeasures to safeguard the security of a biometric system and the privacy of data subjects are essential.

Biometric systems usually bind a biometric reference 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 biometric references 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 technology — Security techniques — Biometric information protection

1 Scope

This International Standard provides guidance for the protection of biometric information under various requirements for confidentiality, integrity and renewability/revocability during storage and transfer. Additionally, this International Standard provides requirements and guidelines for the secure and privacy-compliant management and processing of biometric information.

This International Standard specifies the following:

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

— security requirements for securely binding between a biometric reference and an identity reference;

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

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

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

2 Terms and definitions

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

2.1
authentication
process of establishing an understood level of confidence that a specific entity or claimed identity is genuine

NOTE 1 Authentication includes the process of ascertaining an understood level of confidence of the truth of a claimed identity before the entity can be registered and recognized in a domain.

NOTE 2 Although this definition is generic, its use within this International Standard is limited to the biometric authentication of human subjects.

[ISO 19092:2008]

2.2
auxiliary data
AD
subject-dependent data that is part of a renewable biometric reference and may be required to reconstruct pseudonymous identifiers during verification, or for verification in general

NOTE 1 If auxiliary data is part of a renewable biometric reference, it is not necessarily stored in the same place as the corresponding pseudonymous identifiers.

NOTE 2 Auxiliary data may contain data elements for diversification (i.e. diversification data).

NOTE 3 Auxiliary data is not the element for comparison during biometric reference verification.

NOTE 4 Auxiliary data are generated by the biometric system during enrolment.

EXAMPLE Secret number encrypted by a key derived from a biometric sample using a helper data approach, fuzzy commitment scheme, or fuzzy vault. See Annex D, Table D.1 for concrete examples of PI and AD.

2.3
biometric characteristic
physiological or behavioural characteristic of an individual that can be detected and from which distinguishing, repeatable biometric features can be extracted for the purpose of automated recognition of individuals

[ISO/IEC JTC 1/SC 37 SD2 (v.11)]

2.4
biometric data
biometric sample, biometric feature, biometric model, biometric property, other description data for the original biometric characteristics, or aggregation of above data

[ISO/IEC JTC 1/SC 37 SD2 (v.11)]

2.5
biometric data subject
subject
individual whose biometric reference is within the biometric system

2.6
biometric feature
numbers or labels extracted from biometric samples and used for comparison

[ISO/IEC JTC 1/SC 37 SD2 (v.11)]

2.7
biometric information privacy
right to control the collection, transfer, use, storage, archiving, disposal and renewal of one's own biometric information throughout its lifecycle

2.8
biometric model
stored function (dependent on the biometric data subject) generated from a biometric feature or features

NOTE Comparison applies the stored function to the biometric features of a probe biometric sample to give a comparison score.

EXAMPLE Examples of stored functions include Hidden Markov Models, Gaussian Mixture Models or Artificial Neural Networks.

[ISO/IEC JTC 1/SC 37 SD2 (v.11)]

2.9
biometric property
descriptive attributes of the biometric data subject estimated or derived from the biometric sample by automated means

EXAMPLE Fingerprints can be classified by the biometric properties of ridge-flow (i.e. arch, whorl, and loop types); face images can be used for estimating age or gender.

[ISO/IEC JTC 1/SC 37 SD2 (v.11)]

2.10
biometric reference
BR
one or more stored biometric samples, biometric templates or biometric models attributed to a biometric data subject and used for comparison

NOTE A biometric reference that can be renewed is referred to as a renewable biometric reference.

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

[ISO/IEC JTC 1/SC 37 SD2 (v.11)]

2.11
biometric sample
analog or digital representation of biometric characteristics obtained from a biometric capture device or biometric capture subsystem prior to biometric feature extraction

[ISO/IEC JTC 1/SC 37 SD2 (v.11)]

2.12
biometric system
system for the purpose of the automated recognition of individuals based on their behavioural and physiological characteristics

2.13
biometric template
set of stored biometric features comparable directly to probe biometric features

2.14
claim
assertion of identity

2.15
claimant
individual making a claim of identity

NOTE Claims can be verified in a number of ways, some of which may be based on biometrics.

2.16
common identifier
identifier for correlating identity references and biometric references in physically or logically separated databases

2.17
diversification
deliberate creation of multiple, independent, transformed biometric references from one or more biometric samples obtained from one data subject for the purposes of security and privacy enhancement

2.18
identification
⟨biometrics⟩ process of performing a biometric search against an enrolment database to find and return the identity reference attributable to a single individual

2.19
identifier
one or more attributes that uniquely characterize an entity in a specific domain

EXAMPLES 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.

2.20
identity
set of properties or characteristics of an entity that can be used to describe its state, appearance or other qualities

2.21
identity management system
IdMS
system controlling entity identity information throughout the information lifecycle in one domain

2.22
identity reference
IR
non-biometric attribute that is an identifier with a value that remains the same for the duration of the existence of the entity in a domain

2.23
irreversibility
property of a transform that creates a biometric reference from a biometric sample(s) or features such that knowledge of the transformed biometric reference cannot be used to determine any information about the generating biometric sample(s) or features

2.24
personally identifiable information
PII
any information

— that identifies or can be used to identify, contact, or locate the person to whom such information pertains,

— from which identification or contact information of an individual person can be derived, or

— that is or might be directly or indirectly linked to a natural person

[ISO/IEC 29100:—[1)]]

2.25
pseudonymous identifier
PI
part of a renewable biometric reference that represents an individual or data subject within a certain domain by means of a protected identity that can be verified by means of a captured biometric sample and the auxiliary data (if any)

NOTE 1 A pseudonymous identifier does not contain any information that allows retrieval of the original biometric sample, the original biometric features, or the true identity of its owner.

NOTE 2 The pseudonymous identifier has no meaning outside the service domain.

NOTE 3 Encrypted biometric data with a cipher that allows retrieval of the plain-text data is not a pseudonymous identifier.

NOTE 4 A pseudonymous identifier is the element for comparison during biometric reference verification.

NOTE 5 See Annex D, Table D.1 for examples of PI and AD.

1) To be published.

2.26
pseudonymous identifier encoder
PIE
system, process or algorithm that generates a renewable biometric reference consisting of a pseudonymous identifier (PI) and possibly auxiliary data (AD) based on a biometric sample or biometric template

2.27
renewability
property of a transform or process to create multiple, independent transformed biometric references derived from one or more biometric samples obtained from the same data subject and which can be used to recognize the individual while not revealing information about the original reference

2.28
renewable biometric reference
revocable or renewable identifier that represents an individual or data subject within a certain domain by means of a protected binary identity (re)constructed from the captured biometric sample

NOTE A renewable biometric reference consists of a pseudonymous identifier and additional optional data elements required for biometric verification or identification such as auxiliary data.

2.29
revocability
ability to prevent future successful verification of a specific biometric reference and the corresponding identity reference

NOTE Rejection of an entity may occur on the grounds of its appearance on a revocation list.

2.30
secure channel
communication channel providing the confidentiality and authenticity of exchanged messages

2.31
token
physical device storing biometric reference and in some cases performing on-board biometric comparison

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

2.32
unlinkability
property of two or more biometric references that they cannot be linked to each other or to the subject(s) from which they were derived

2.33
verification
〈biometrics〉 process of confirming a claim that an individual who is the subject of a biometric capture process is the source of a claimed identity reference

3 Abbreviated terms

AD Auxiliary Data

AFIS Automated Fingerprint Identification Systems

BR Biometric Reference

BIR Biometric Information Record

CI Common Identifier

OCC	On-Card Comparison
DB_{BR}	Database containing Biometric Reference
DB_{IR}	Database containing Identity Reference
IdMS	Identity Management System
IR	Identity Reference
MAC	Message Authentication Code
PDA	Personal Digital Assistant
PET	Privacy Enhancing Technology
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
UUID	Universal Unique Identifier
$\xrightarrow{x}$	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*.

NOTE 1 *x* may be encrypted when a secure messaging system such as ISO/IEC 7816-4 is used.
NOTE 2 The interactive protocol may not transfer any information on *x* when, for example, a zero-knowledge technique is used.

4 Biometric systems

4.1 Introduction to biometric systems

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

Physiological characteristics include but are not limited to:

— fingerprint,
— face,
— iris,
— hand geometry,
— hand/finger vein,
— retina,

— DNA, and

— palm print,

and behavioural characteristics include but are not limited to:

— signature,

— gait, and

— voice.

The following are desirable properties of biometric characteristics that lead to good subject discrimination and reliable recognition performance [4]:

— universality: Every individual should have the characteristic;

— uniqueness: Every individual should have a distinguishable characteristic;

— permanence: The characteristics should not show variance with time, e.g. variance over time;

— collectability: The characteristics should be easily collected from the subjects; and

— repeatability: The characteristics should be sufficiently distinct and repeatable to achieve successful recognition of the subject.

From an application point of view, 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; and

— spoof resistance, which indicates how difficult it is to use a replica of the biometric characteristic to circumvent the biometric system.

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

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

4.2 Biometric system operations

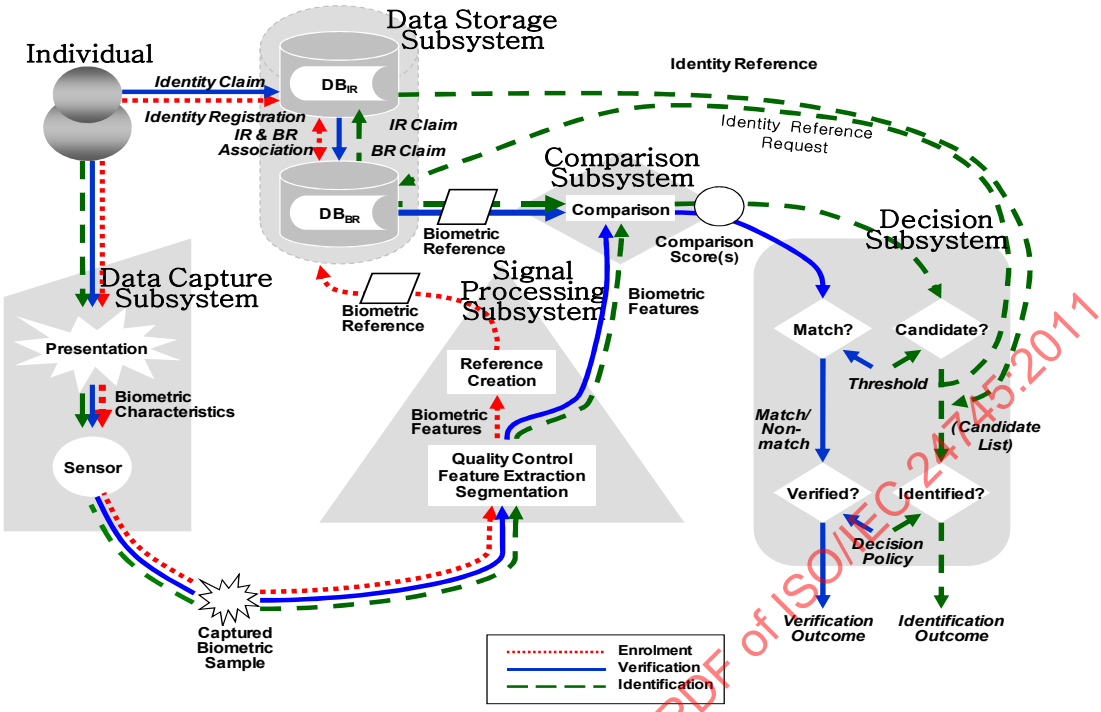


Figure 1 — Conceptual structure of a biometric system

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 SC37 SD11 [18], to highlight the processing of the identity reference.

The biometric system usually consists of five subsystems.

— A biometric data capture subsystem, which contains biometric capture devices or sensors for collecting signals from a biometric characteristic and converting them into a biometric sample such as a fingerprint image, facial image or voice recording.

— A signal processing subsystem, which extracts biometric features from a biometric sample with the intent of outputting numbers or labels which can be compared with those extracted from other biometric samples. Here, the biometric feature extracted in the enrolment process is stored in the data storage subsystem as a biometric reference for the identification and verification process.

— A data storage subsystem, which serves primarily as an enrolment database where the linking of the enrolled biometric references to the identity reference occurs. The data may contain biometric data and also non-biometric data such as the identity reference related to the subject. In practice, 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 biometric references. In the case of the one-to-one comparison used in the verification process, a captured biometric sample is compared with a stored biometric reference from a biometric data subject to produce a comparison score. However, in the one-to-many comparison used in the identification process, an extracted feature of a biometric data subject is compared against a set of biometric references of more than one biometric data subject to return a set of comparison scores.

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

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

— Identification process: searching the enrolment database against the captured and extracted biometric features to return a candidate list. The candidate list consists of individuals whose references match with the feature in 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 biometric reference. The subject presents his/her identity reference for a claim of identity and also their biometric characteristic(s) to the capturing device, which acquires biometric sample(s) to be used for comparison with the biometric reference linked to the identity reference for the claimed identity.

The verification process has a possibility of impacting on the subject's information privacy since this process requires both biometric reference and identity reference. The identification process requires exhaustive search of the enrolment database. So, this also has a possibility of impacting on the subject's physical privacy. Verification is generally considered to be less privacy intrusive than identification.

The five abovementioned subsystems represent the technical and functional blocks that capture, process, store, compare, and decide on the processing of biometric data. In addition, other functional subsystems can be included [7].

— 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 upon 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 may 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, in accordance with the relevant legal, jurisdictional and societal constraints and privacy requirements. Illustrative examples include:

  - provision of privacy relevant information to the subject during biometric processing;
  - storage and formatting of the biometric references 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; and
- provisions of appropriate safeguards for the subject's privacy.

4.3 Biometric references and identity references

A person has one identifier in any particular domain but may have several identity references to identify that person within that domain. Each identity reference is an attribute, or combination of attributes, of the identity of an entity that uniquely identifies that entity in a particular domain. An identity reference can also be a combination of attributes of the person.

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

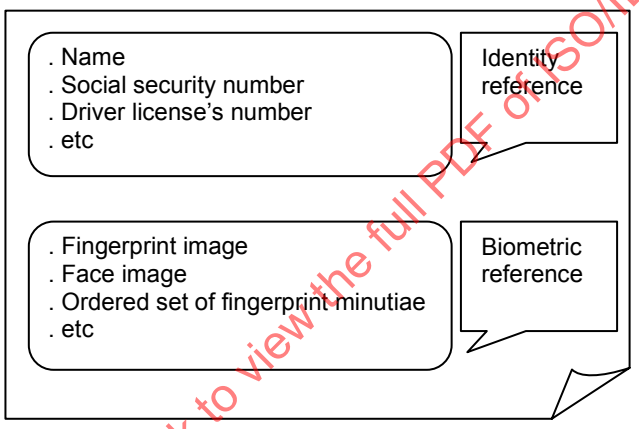


Figure 2 — Identity references and biometric references

4.4 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 could 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).

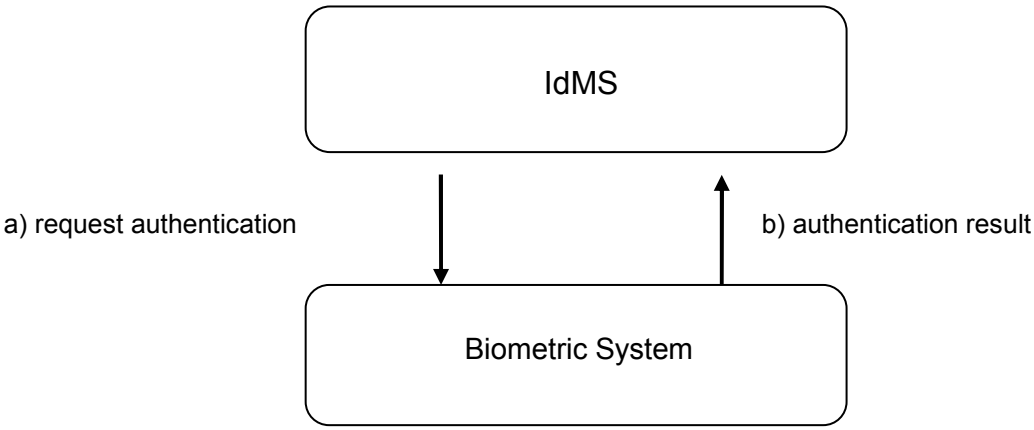


Figure 3 — Biometric system as an authentication service provider for IdMS

4.5 Personally identifiable information and universal unique identifiers

Some biometric systems use biometric samples such as facial images in e-passports to directly identify the person and others use biometric features such as the minutiae points of a fingerprint and the eigenface coefficients of a face to indirectly identify the person bound with the identity reference. This ability to be able to link biometric data to the subject makes biometric references PII.

Due to their distinctiveness, biometric references have the potential to be used as a unique universal identifier (UUID). A UUID is an identity reference which can be used to link personal information across various databases, thereby resulting in a potential threat to privacy. As such, significant concerns have been expressed about using a biometric reference as a UUID. Unless there is a clearly demonstrated need to do so, biometric references should not be used as a universal unique identifier.

The UUID becomes a potential risk to privacy in that an individual can be monitored and tracked across databases containing the corresponding PII. When the biometric reference or its binding with the identity reference is used, it could be classified as personally identifiable information that may be very important to the individual depending on the specific domain [5]. If UUID databases of biometric data are employed, consideration should given to a design that meets requirements for revocability and renewability to limit such cross-comparison, for example, though the use of diversified references as described in this International Standard.

4.6 Societal considerations

The application of biometric systems always has a societal dimension, aspects of which may be codified in legal 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 will contribute to good system performance. The acceptability of a system may be influenced by religious, ethnic and cultural factors, as well as by individual psychological traits.

In all deployments of biometric systems those persons and organisations 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 ensure that legal 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; and

— usability, which delivers systems that are effective, efficient and satisfying in use.

A more extended discussion of the societal and cross-jurisdictional considerations in commercial applications is to be found in ISO/IEC TR 24714-1 [19].

5 Security aspects of a biometric system

5.1 Security requirements for biometric systems to protect biometric information

5.1.1 Confidentiality

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

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 Annex B.1.

5.1.2 Integrity

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

— accidental corruption due to a malfunction in hardware or software;

— accidental or intentional modification of a bona fide biometric reference by an authorized entity (i.e., either an authorized enrolee or a system owner), without intervention of an attacker;

— modification (including substitution) of a biometric reference of an authorized enrolee by an attacker;

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

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 Annex B.2.

NOTE 2 Certain situations require both confidentiality and integrity. If both confidentiality and integrity protection are required, one possibility is to use both encryption and a MAC or digital signature. Another possibility is to use authenticated encryption as standardised in ISO/IEC 19772 [16].

NOTE 3 When a smart card is used for biometric reference storage and/or comparison (Clause 8, Models B, E, F, G and H), Secure Messaging mechanisms according to ISO/IEC 7816-4 [30] should be used for biometric data integrity and /or confidentiality.

5.1.3 Renewability and revocability

A major security and privacy concern for biometric systems relates to the compromise of biometric references. A variety of threats can compromise a biometric reference. For example, an attacker may unlawfully obtain a token containing a biometric reference, or may 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 may result in unauthorized exposure of biometric references and other personal data. In case of such compromise of biometric references, there is a strong need to revoke the compromised references, and to associate the legitimate data subject with a new biometric reference. It should be noted that revocation and renewal of the biometric reference do not imply renewal of the biometric characteristics of the data subject. Renewability and revocability only provide the means to resolve compromised biometric references, and not for compromised biometric characteristics.

A biometric reference may need to be changed for a variety of reasons besides compromise. For example, a biometric reference may only be valid for a specific period of time (in a manner similar to passwords). If a biometric reference is still required at the end of that time period, the reference may be renewed, or revoked and replaced.

5.2 Security threats and countermeasures in biometric systems

5.2.1 Threats and countermeasures against biometric system components

Threats against the components of a biometric system are summarized in Table 1 [8].

Table 1 — Threats and countermeasures of biometric subsystems

	Threats	Countermeasures
Data Capture	Sensor spoofing Capture/replay of signals from sensor	— Liveness detection — Multimodal biometric — Challenge/response
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	— Revocable and renewable biometric references — Data separation — Database access control — Sign BR/RBR/IR — Encrypt BR/RBR/IR
Decision	Hill climbing attack	— Secure channel — Hide comparison score from subject
	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 implementation of the Comparison and Decision components in a certified single module constitutes an effective countermeasure against threats of comparison score manipulation. Here, additional countermeasure of hiding comparison score from subject is required to prevent a hill climbing attack

NOTE 3 The threat of component replacement is applicable for all subsystems. Against this threat, using inventory control involving digitally signed components can be an effective countermeasure.

Brief descriptions of the aforementioned threats and countermeasures are provided below for clarification.

— Sensor spoofing means the presentation of artificial and thus non-live biometric characteristics. One countermeasure to sensor spoofing is liveness detection based on recognition of a subject's physiological activities as signs of life or the detection and rejection of known artefact types.

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

— Hill climbing is the systematic modification of the biometric sample to obtain progressively higher comparison scores until the decision threshold has been met.

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

— Revocable and renewable biometric references are created by means of diversification for different applications, organisations 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 Clause 7.2). Data separation can be applied to data elements such as IR, BR, PI and AD.

5.2.2 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.

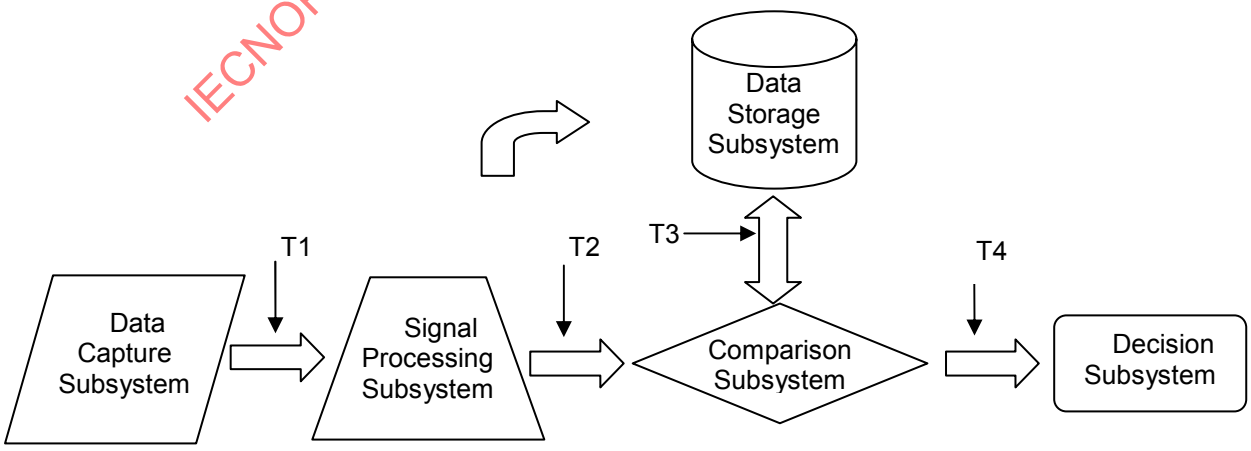


Figure 4 — Threats in the biometric system

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
		Man in the middle	— Encrypted /secure channel — Integrity check of biometric data with digital signature or MAC
		Hill climbing	— Coarse scores — Secure channel
Comparison - Decision (T4)	Comparison score	Comparison score manipulation	— Secure channel

NOTE The implementation of the Comparison and Decision components in a certified single module constitutes an effective countermeasure against manipulation of comparison score threats.

Brief descriptions of the aforementioned threats are provided below for clarification.

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

— Man-in-the-middle attacks are attacks in which an attacker can read, insert and modify the biometric data communicated between two parties without either party knowing that the established link has been compromised.

The list of countermeasures in Table 2 is not comprehensive. A risk analysis should be performed to identify threats in the context of the application. Appropriate countermeasures should be put in place which can include procedural as well as technical countermeasures. For a more detailed description of the managerial aspect of protecting biometric systems see ITU-T X.1086 [1], ISO 19092:2008 [2], and ISO/IEC 19792 [43].

5.2.3 Renewable biometric references as countermeasure technology

Renewability of biometric references is a countermeasure against storage and transmission threats. In order to permit the revocation or renewal of biometric references, the biometric reference creation process should support the process of diversification. Diversification involves the generation of multiple, independent references from the same biometric characteristics that can be used to renew a biometric reference or to provide independent references across different applications. The diversification process should be irreversible. The transformed biometric references should not be uniquely linkable.
To facilitate a common vocabulary for the implementation of renewable biometric references (RBRs) through a diversification process, and to outline the architectural aspects of renewable biometric references and the

diversification process in a technology-neutral manner, the concept of pseudonymous identifiers is used in this International Standard. In the approach described in this International Standard, renewable biometric references consist of two data elements: a pseudonymous identifier (PI) and corresponding auxiliary data (AD). Both data elements are generated during enrolment and must both be stored because both elements are required during a verification or identification process.

An overview of the architectural aspects of renewable biometric references 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 a renewable biometric reference consisting of a pseudonymous identifier (PI) and auxiliary data (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.
During verification, a feature extraction stage processes the probe biometric sample. Subsequently, a pseudonymous identifier recoder (PIR) constructs a pseudonymous identifier (PI*) based on the provided auxiliary data and the extracted features. 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 pseudonymous identifier creation and verification process, as well as its lifecycle, is provided in Annex C.

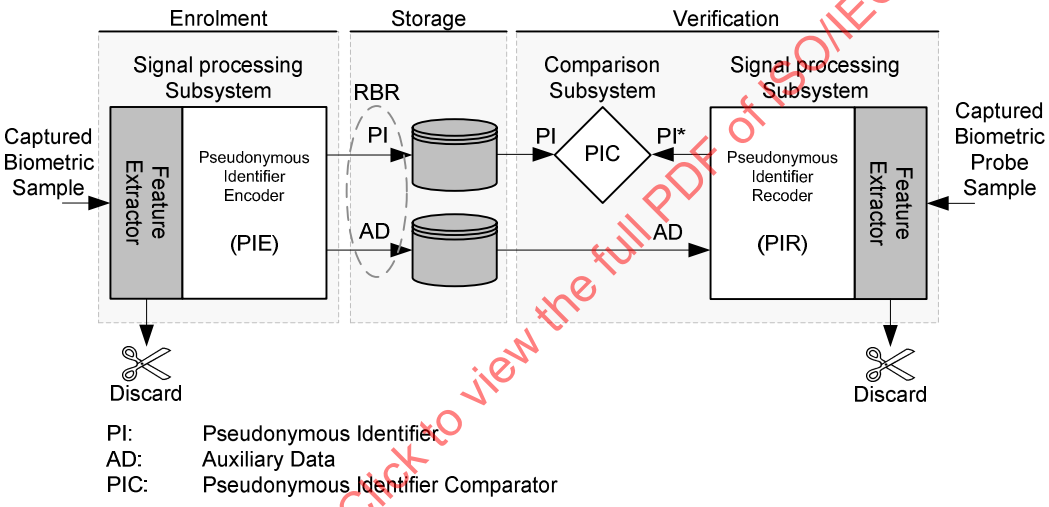


Figure 5 — Architecture for renewable biometric references

5.3 Security of data records containing biometric information

5.3.1 Security for biometric information processing in a single database

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

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

— **Scenario 2**: Raw IR and encrypted BR are stored. Neither confidentiality nor integrity is provided on IR. Confidentiality on BR is provided. A weak form of integrity may be provided on BR depending on the mode of operation of encryption. Renewability and revocability are not provided.

— **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 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 diversified BR are stored. Renewability and revocability are provided on BR, as well as limited confidentiality and integrity on BR.

— **Scenario 16**: Raw IR and diversified BR 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 diversified BR are stored. Integrity and confidentiality are provided on both IR and BR. Renewability and revocability are provided on BR.

— **Scenario 18**: Raw IR and diversified 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. Renewability and revocability are provided on BR.

— **Scenario 19**: Raw IR and encrypted, diversified BR 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

(Enc'd: encrypted, Aut'd: authenticated, AuE'd: authenticated-encrypted, Div'd: diversified, **O**: requirement, Δ: weak requirement)

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

ISO/IEC 19785 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). In ISO/IEC 19785-4, the Security Block (SB) formats are specified to keep integrity of BIRs and to encrypt/decrypt the biometric data in BIRs [3].

5.3.2 Security for biometric information processing in separated databases

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

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 DBs with a common CI are employed, the databases shall be controlled by separate operators with different cryptographic keys.

In Table 4, 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 even if only one of IR and BR is exposed. If one DB is compromised and its contents are illegally modified, the operators of two DBs should be able to detect it. Similarly, during the usage of the DBs, if a legitimate DB operator with a correct key modifies its contents, the other DB should be able to detect the modification. For these cases, more secure binding is required. Annex A provides examples of implementations of a Common Identifier (CI).

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

(Enc'd: encrypted, Aut'd: authenticated, AuE'd: authenticated-encrypted, CI: common identifier, **O**: requirement, Δ: weak requirement)

Security Requirements					Countermeasures for IR	Countermeasures for BR
Confidentiality		Integrity		Renewability		
IR	BR	IR	BR	BR		
	O		Δ		CI, Raw IR	CI, Enc'd BR
			O		CI, Raw IR	CI, Aut'd BR
	O		**O**		CI, Raw IR	CI, AuE'd BR
O		Δ			CI, Enc'd IR	CI, Raw BR
		O			CI, Aut'd IR	CI, Raw BR
O		**O**			CI, AuE'd IR	CI, Raw BR
O	**O**	Δ	Δ		CI, Enc'd IR	CI, Enc'd BR
		O	**O**		CI, Aut'd IR	CI, Aut'd BR
O	**O**	**O**	**O**		CI, AuE'd IR	CI, AuE'd BR
O	**O**	Δ	**O**		CI, Enc'd IR	CI, AuE'd BR
	O	**O**	**O**		CI, Aut'd IR	CI, AuE'd BR
O	**O**	**O**	Δ		CI, AuE'd IR	CI, Enc'd BR
O		**O**	**O**		CI, AuE'd IR	CI, Aut'd BR
	Δ			**O**	CI, PI, IR	CI, AD

	Δ	O	O	O	CI, Aut'd PI, Aut'd IR	CI, Aut'd AD
O	O	O	O	O	CI, AuE'd(PI and IR)	CI, AuE'd AD
O	O	Δ	Δ	O	CI, Enc'd(PI and IR)	CI, Enc'd AD
O	O	O	O	O	CI, Aut'd(Enc'd PI and IR)	CI, Aut'd(Enc'd AD)

6 Biometric information privacy management

6.1 Biometric information privacy threats

Since biometric data is 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 information. The use of biometric data involves several threats to privacy which must be addressed.

— Biometric data may be abused for purposes other than originally intended and consented to by the data subject.

— Biometric references may 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 may 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 biometric reference.

A more detailed description of jurisdictional and societal considerations for commercial biometric application is given in ISO/IEC TR 24714-1 [19].

6.2 Biometric information privacy requirements and guidelines

6.2.1 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 often provide a form of irreversibility by data reduction and redundancy removal, increasing the difficulty of using the extracted features to extract medical or ethnic data;

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

— pseudonymous identifiers provide a means to limit access to the biometric characteristics of the data subject by means of irreversible transforms. An overview of transforms that produce pseudonymous identifiers is provided in Annex D, Table D.1.

6.2.2 Unlinkability

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

— if the plain-text biometric references are linkable, encryption of biometric references 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 pseudonymous identifiers 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.

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

6.2.3 Confidentiality

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

— data separation by storing (part of the) biometric references 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 (for example when an adversary obtains illegitimate access to a centralized database and publishes its contents);

— encryption of biometric references using a key only known to the operator of the identity management system and/or data subject.

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

6.3 Regulatory and policy requirements

As PII, the collection, transfer, use, storage and disposal of biometric reference is governed by various laws and regulations, including privacy and data protection. All deployments of biometric technology shall be implemented in accordance with all applicable laws and regulations.

6.4 Biometric information lifecycle privacy management

6.4.1 Collection

Organizations shall obtain the consent of a subject prior to the collection of biometric information, unless applicable laws and regulations define otherwise. When seeking the subject's consent, the organization should fully inform the subject of following (note that 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; and

— information about the person responsible for managing the biometric information, which includes his/her name, organization, position, contact information, etc.

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

6.4.2 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, or if it is required by law.

Before seeking the consent of the subject, the organization should provide the following (note that 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; and

— 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 is required, unless otherwise allowed by law. Cross-border transfers are especially common in operating biometric systems including border control and electronic passports, etc. For this reason, it is important that more care is taken with respect to the privacy of the transferred biometric information which might be processed by a third party.

6.4.3 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, unless otherwise specified by law. 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.

6.4.4 Storage

Biometric information is usually stored in a data storage subsystem, as depicted in Figure 1, which may, however, be distributed. In order to satisfy privacy requirements, it may 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 biometric reference and also its related IR. To trace illegal distribution and misuse of the biometric samples, biometric watermarking schemes as described in Annex E could be adopted. Unless it is absolutely necessary, storing acquired biometric samples which can be classified as a PII shall be avoided.

6.4.5 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 is 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 information.

6.4.6 Disposal

The organization or third party to which the biometric information is disclosed shall securely dispose of the biometric information of the subject when (note that 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 is identified and securely disposed of, particularly in cases of distributed storage. The system security/privacy policy shall specify the biometric and other personal information that is to be included in the inventory of data for disposal. This shall include archive and backup data (see previous clauses for further details). The policy shall also describe suitable procedures and safeguards to ensure the complete and secure disposal of the data.

6.5 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, unless applicable laws, regulations or the terms and conditions of the services define otherwise. The biometric system owner shall provide appropriate means for the subject to make such a request and remove the corresponding biometric information from the biometric system.

— 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 biometric references 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.

7 Biometric system application models and security

7.1 Biometric system application models

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

Table 5 — Application model of a biometric system

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

The locations can be described as follows.

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

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

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

NOTE The biometric sensor connected to a client via an interface and 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 International Standard considers them as a part of the client.

In the following, models A to F describe different topologies for the locations of the various subsystems. Security requirements will be one factor that determines whether normal or renewable biometric references should be used. Models G and H on the other hand only apply to renewable biometric references (RBRs) because these models employ the concept of data separation of PI and AD 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 only applicable to a verification process.

7.2 Security in each biometric application model

7.2.1 Model A – Store on server and compare on server

In this model, biometric references are stored on a server and it is required that the extracted biometric data be transferred to the server for comparison, as shown in Figure 6 (for BRs) and Figure 7 (for RBRs). The subject's biometric reference and the corresponding identity reference are associated as part of the registration/enrolment process.

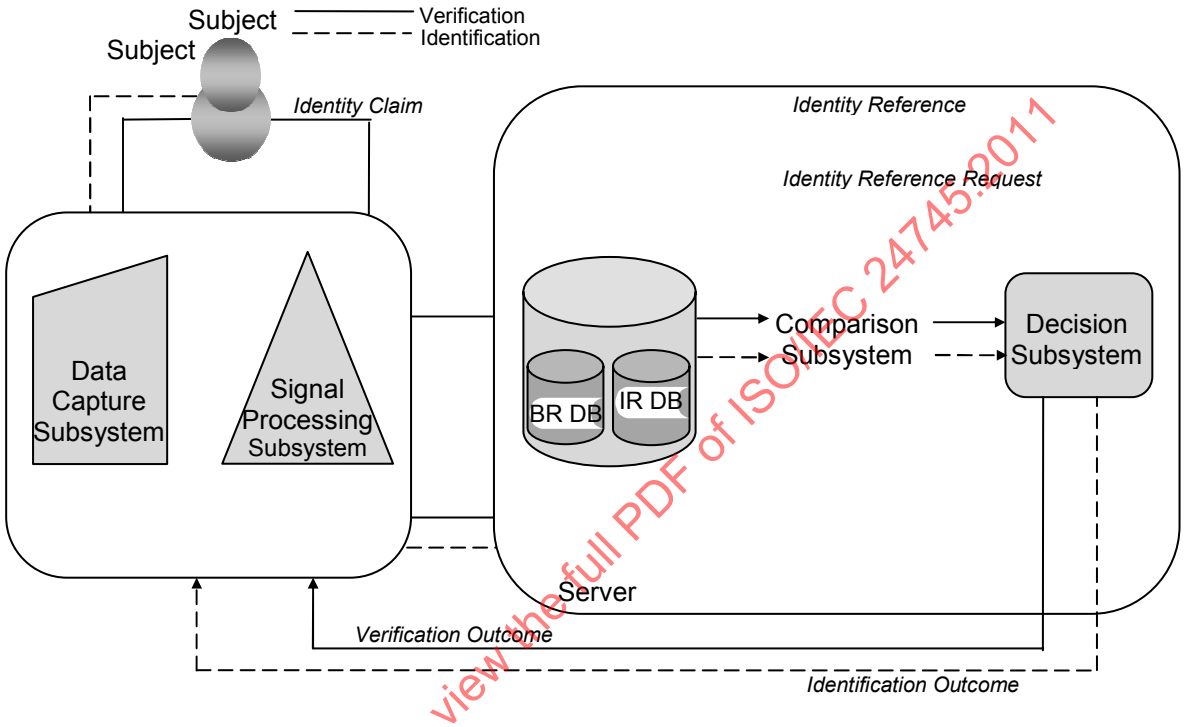


Figure 6 — Model A: store on server and compare on server using BRs

This model requires that the server trusts the data captured from the client. This model can be used for identification and also for verification. Since the sensitive PII (i.e., the biometric reference and identity reference) is handled by the server, reliable database security and network security are required. A large-sized commercial automated fingerprint identification system (AFIS) is usually implemented according to this model. From a privacy point of view, this model is usually not recommended unless renewable biometric references as exemplified by Figure 7 are employed because of the sensitive PII that is otherwise collected in a centralized database.

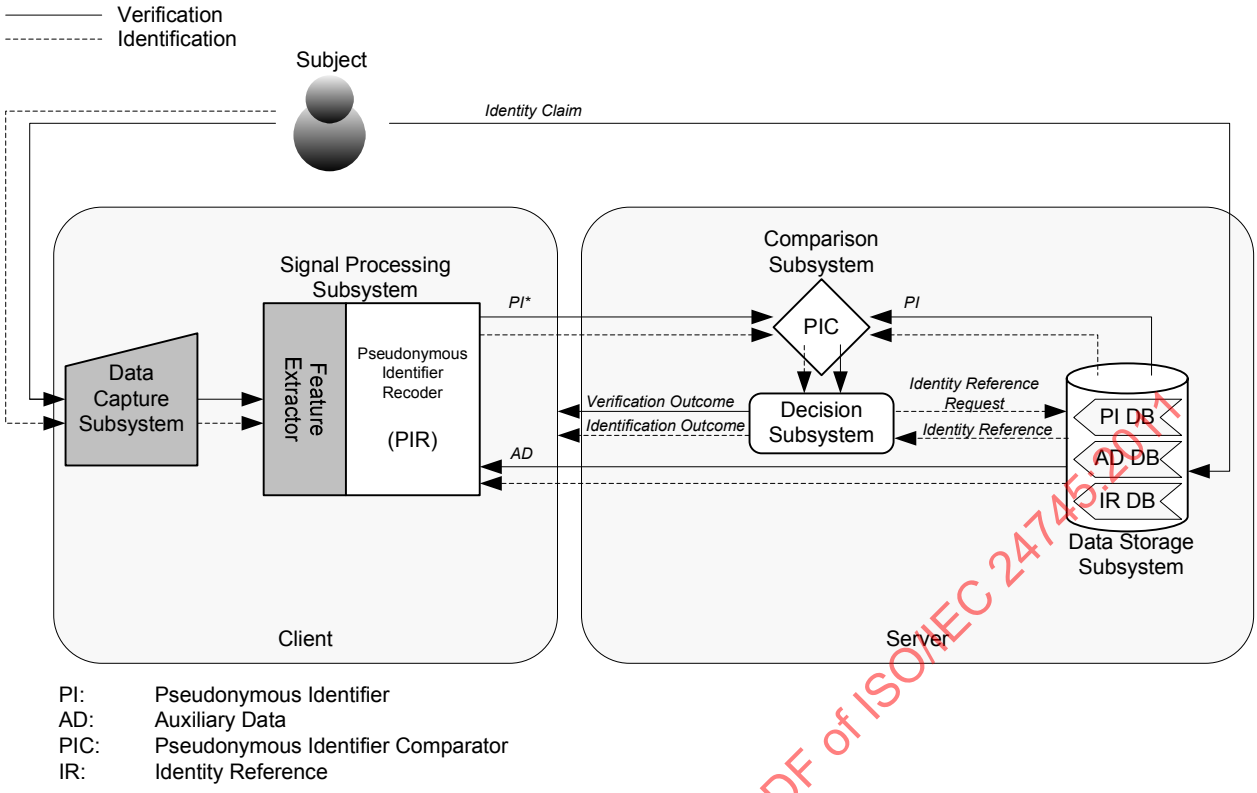


Figure 7 — Model A: store on server and compare on server using RBRs

7.2.2 Model B – Store on token and compare on server

In this model, a token is used for storing biometric references and it is required that the captured biometric data be transferred to the server for comparison, as shown in Figures 8 and 9. The biometric subject associates his/her biometric reference with the identity reference at the token during the enrolment process. A subject who wants to assert his/her identity should have the token and connect it with the client, and also submit his/her biometric characteristic(s). Then the client sends both the stored biometric reference 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.

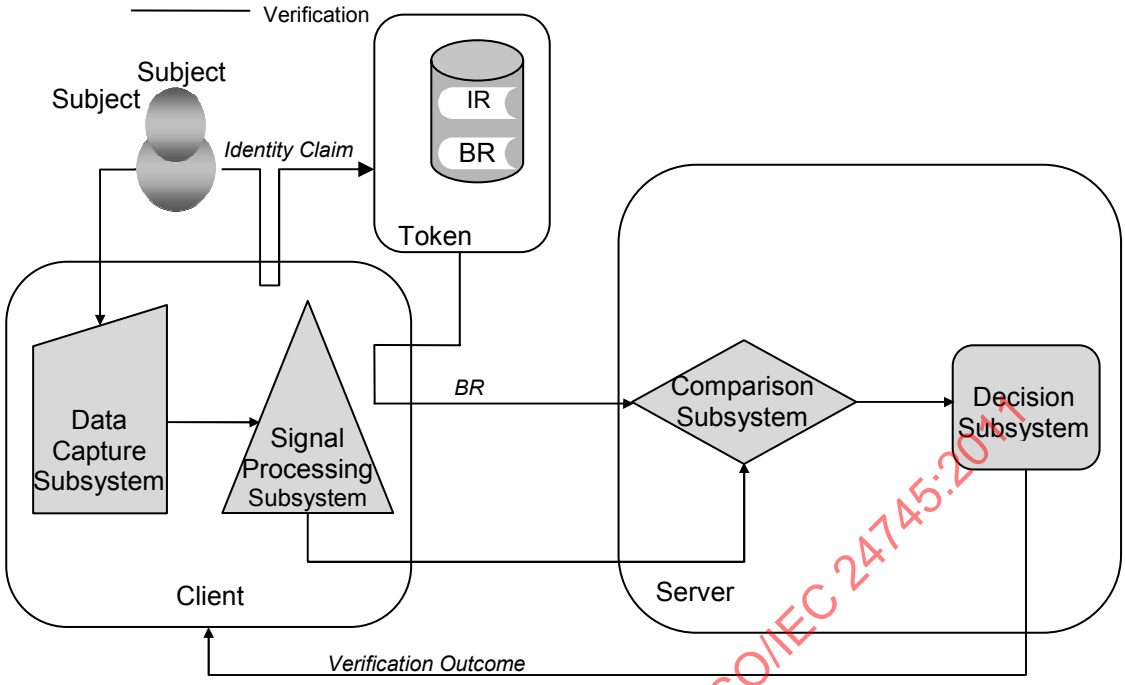
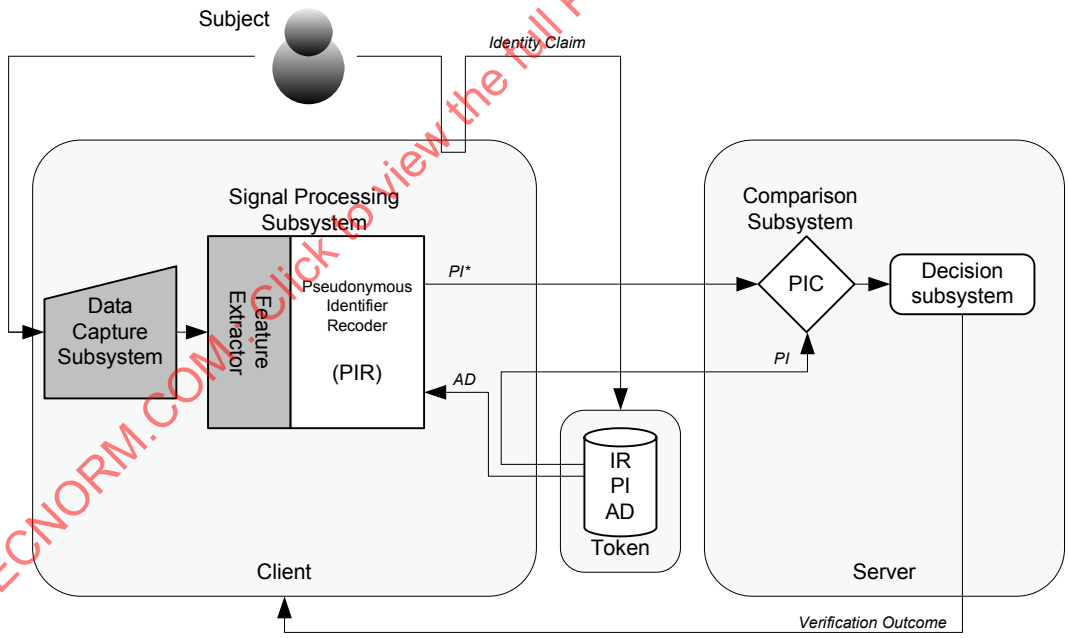


Figure 8 — Model B: Store on token and compare on server using BRs



PI: Pseudonymous Identifier
AD: Auxiliary Data
PIC: Pseudonymous Identifier Comparator
IR: Identity Reference

Figure 9 — 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 biometric reference for comparison at the token except the one asserted by individual. Since the biometric reference is stored at the portable token, which can be securely handled by the individual, this model does not require database security. This model does, however, require network security to protect the transfer of the stored biometric reference 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 identity reference is neither transferred nor bound with the biometric reference in the client and server. So, this model can be considered as a privacy sympathetic model.

7.2.3 Model C – Store on server and compare on client

In this model, the biometric references are stored on the server and probe biometric data is extracted from the subject at the client side for the comparison process as shown in Figures 10 and 11. The biometric subject associates his/her biometric reference with the identity reference 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 biometric reference related to the asserted biometric subject. Upon request, the server sends the asserted biometric reference to the client and finally the client executes a comparison of the captured biometric sample and the downloaded biometric reference. For this model, the client shall be equipped with a biometric sensor and also a comparison/decision algorithm.

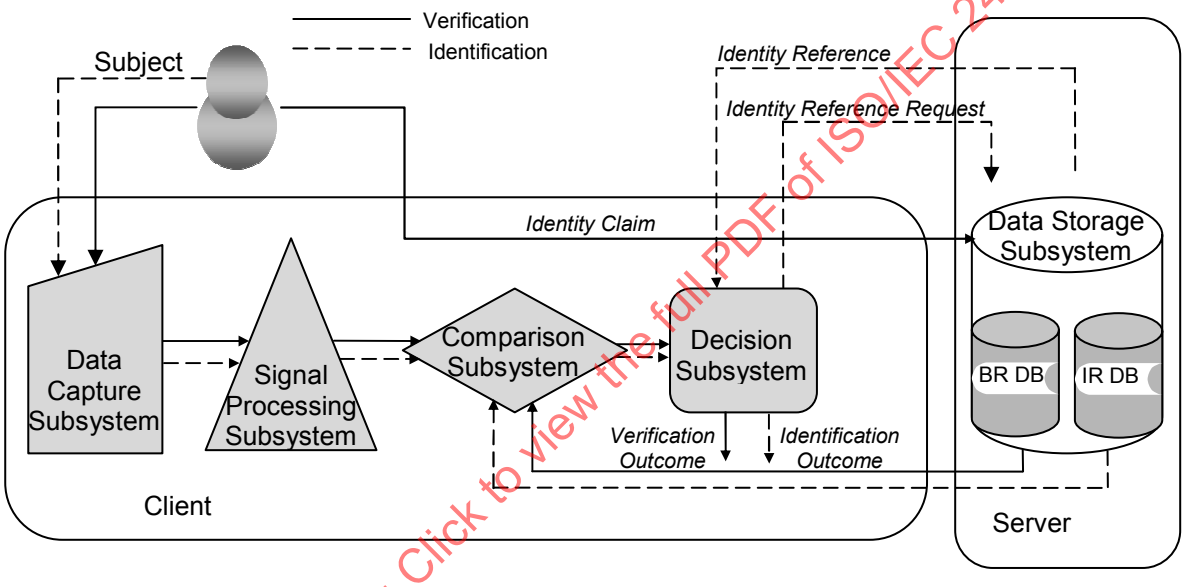


Figure 10 — Model C: Store on server and compare on client using BRs

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., biometric references and identity references) are usually stored at the centralized server, reliable database security and network security are required for safeguarding the biometric subject's privacy.

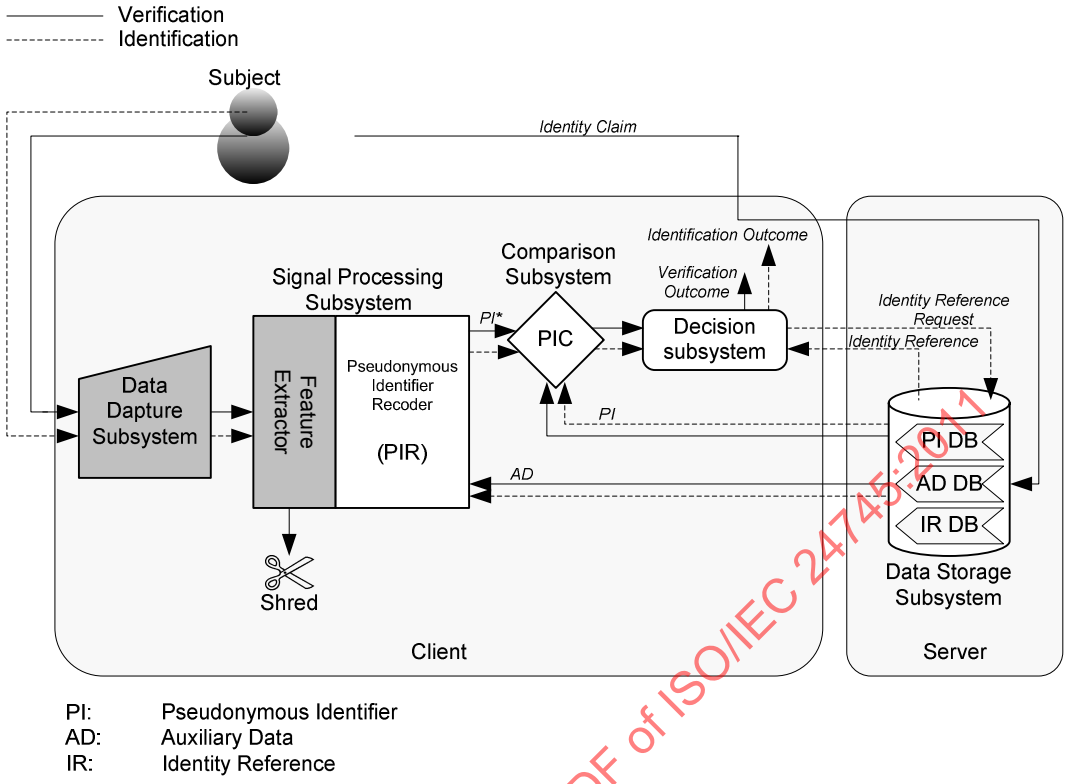


Figure 11 — Model C: Store on server and compare on client using RBRs

7.2.4 Model D – Store on client and compare on client

In this model, the biometric references 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 as shown in Figures 12 and 13. The subject associates his/her biometric reference with the identity reference at the client during the enrolment process. A subject who wants to assert his/her identity must submit his/her probe biometric sample to the client. To deploy this model, the client must 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.

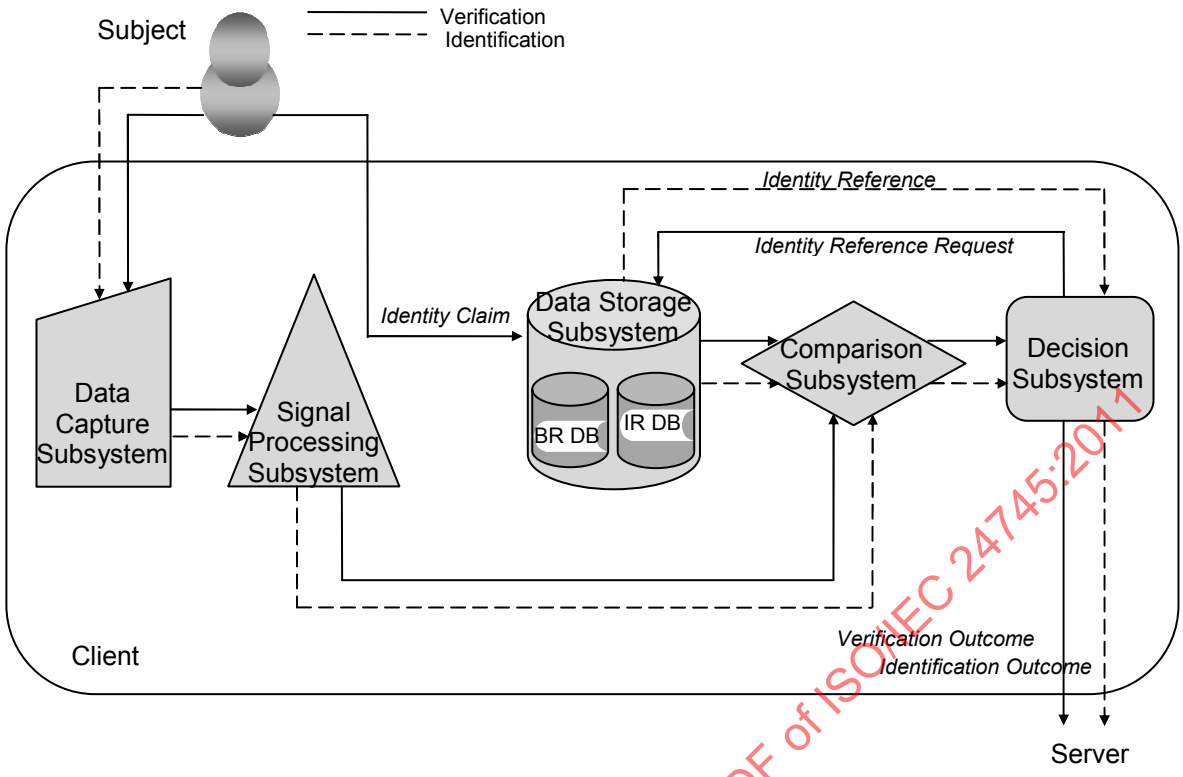
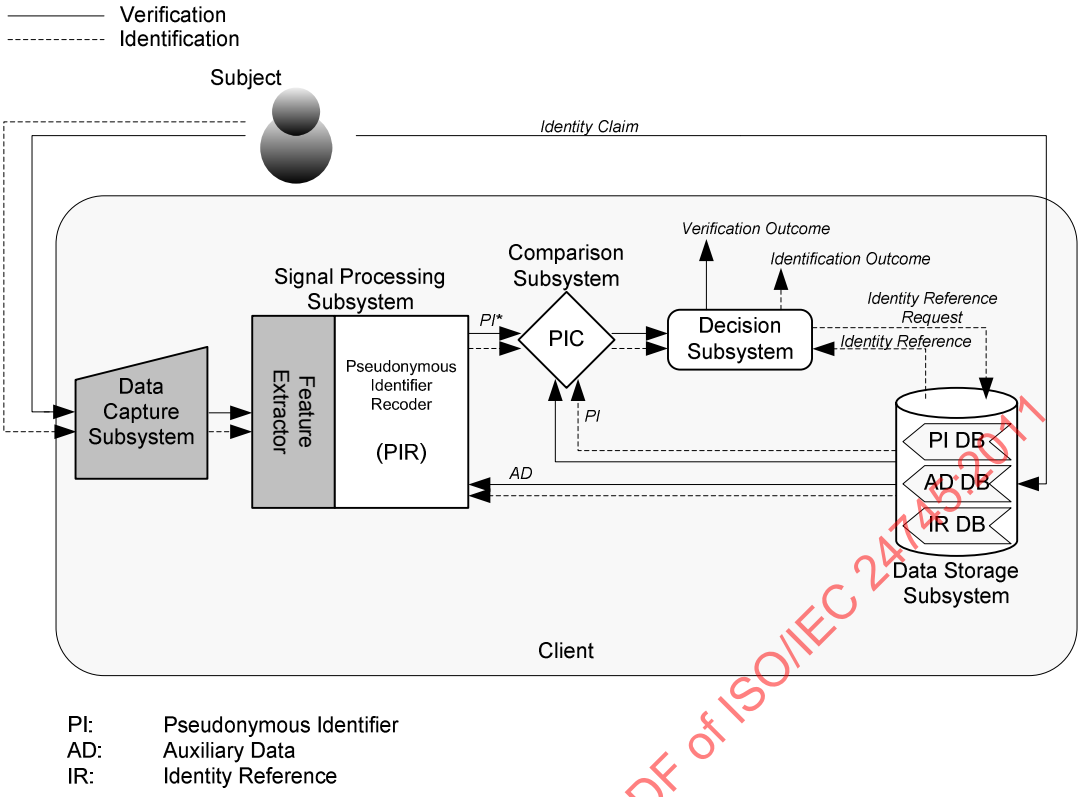


Figure 12 — Model D: Store on client and compare on client using BRs

This model can be used for both identification as well as verification. Since sensitive PII (i.e., the biometric reference and identity reference) 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 renewable biometric references are recommended. In terms of privacy, this model is more favorable than other models using a centralized database.



PI: Pseudonymous Identifier
AD: Auxiliary Data
IR: Identity Reference

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

7.2.5 Model E – Store on token and compare on client

In this model, the biometric references 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 Figures 14 and 15. The biometric subject associates his/her biometric reference with the identity reference on the token during the enrolment process. A subject who wants to assert his/her identity must present his/her probe biometric sample to the client with the token and the biometric reference stored therein. To deploy this model, the client must be equipped with a biometric sensor and processing software including comparison/decision algorithm. Here, the client can be a kiosk type, as found in public places such as airport and public buildings for personal authentication. This model is applied in border control using the e-passport as the token.

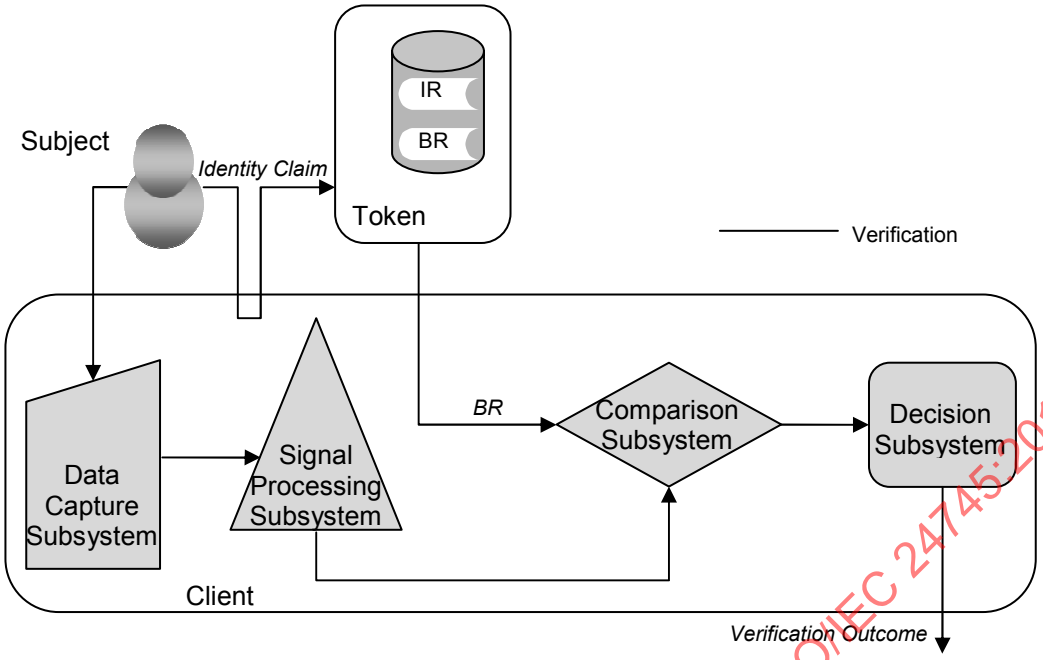
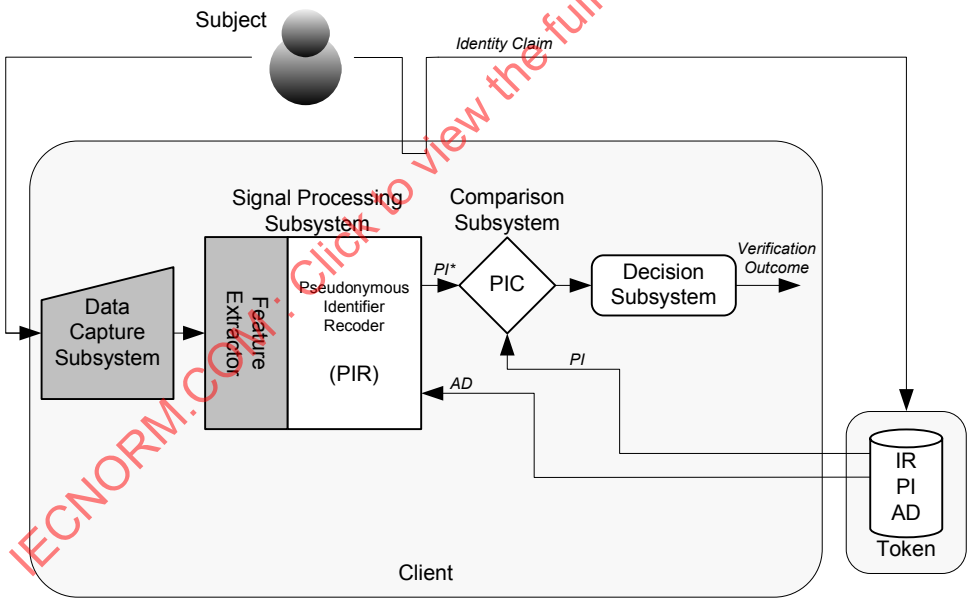


Figure 14 — Model E: Store on token and compare on client using BRs



PI: Pseudonymous Identifier
AD: Auxiliary Data
IR: Identity Reference

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

Biometric references and identity references can be stored on an IC chip embedded in a token. This model is usually used for verification. Since sensitive PII (i.e., the biometric reference and identity reference) 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 identity reference. The command addressed to the token to read the biometric reference and the subsequent response by the token conveying the biometric reference data should be secured using the Secure Messaging mechanism as per ISO/IEC 7816-4.

7.2.6 Model F – Store on token and compare on token

In this model, the biometric references are stored on the token and the probe biometric sample is extracted from the biometric subject for the comparison process, which is performed on the token as shown in Figure 16. The subject associates his/her biometric reference with the identity reference at the token during the enrolment process. A subject who wants to assert his/her identity must present his/her probe biometric sample to the client with the token (comparison on card [42]). To deploy this model, the token must be equipped with a comparison/decision algorithm. Here, the client could be an automated teller machine (ATM). This model is usually applied to bank transactions using OCC.

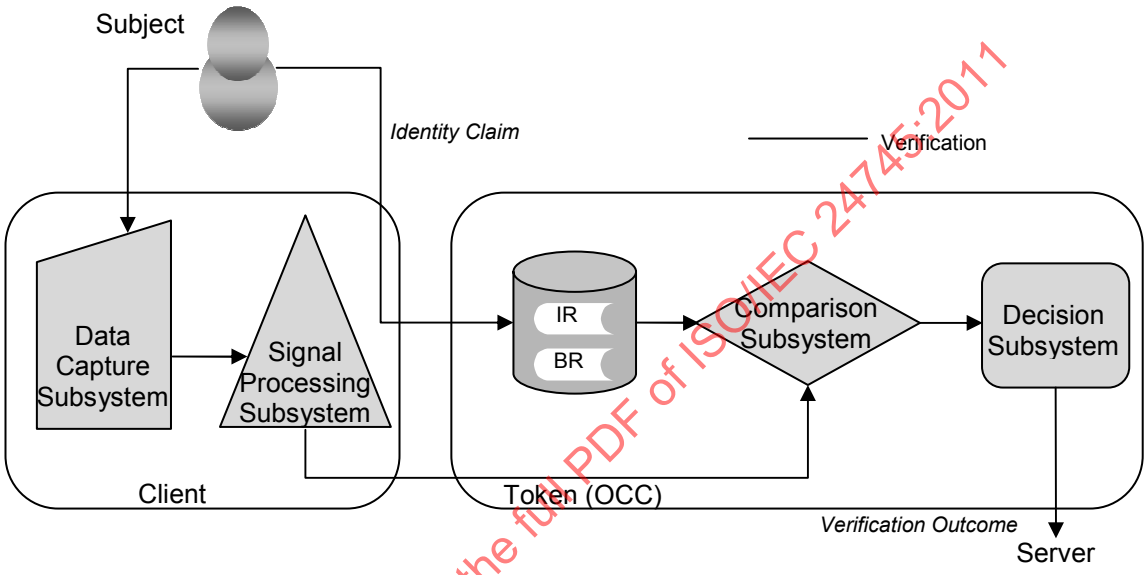


Figure 16 — Model F: Store on token and compare on token using BRs

This type of OCC model is the strongest mechanism for protecting personal information. The token stores the BR and IR and the comparison process is also executed on the card. The token shall have self-execution ability. The command addressed to the card to start the comparison process and the subsequent response by the card conveying the result of the comparison process should be secured using the Secure Messaging mechanism as per ISO/IEC 7816-4. The client acquires a probe biometric sample and IR data and sends them to the token for the comparison process. The result of the comparison is sent to the server. Here, the token may contain the signal processing subsystem. In this case, the possibility of compromising subject's biometric information can be reduced.

This model limits the exposure of an individual's PII by storing the biometric and identity reference on the token. Furthermore, for RBRs (see Figure 17), only AD has to be transmitted to the client while PI remains within the token. This model can, therefore, be considered as a privacy-protective one since the biometric information is under the control of the subject. 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 in the token. Modalities for the implementation of Model F are standardized by ISO/IEC 24787(On-Card biometric comparison).

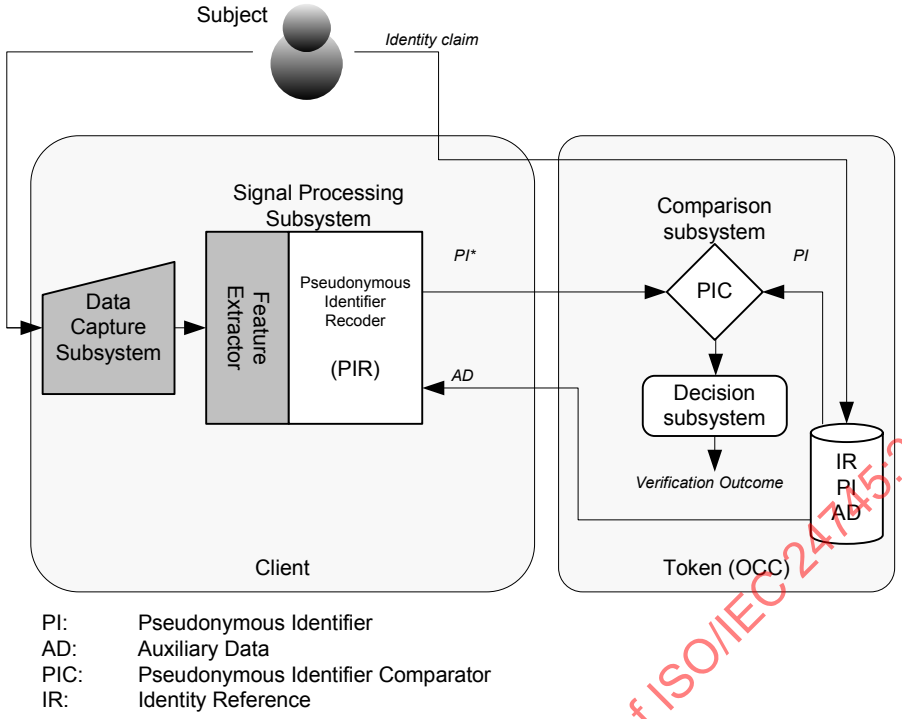


Figure 17 — Model F: Store on token and compare on token using RBRs

7.2.7 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 pseudonymous identifier is created and stored on the server accompanied by Common Identifier (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 18). 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 renewable biometric reference 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 biometric references since it requires tampering with the token as well as the data at the server. Furthermore, it allows revocation of biometric reference 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 employed:

— 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 is capable of storing auxiliary data. 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.

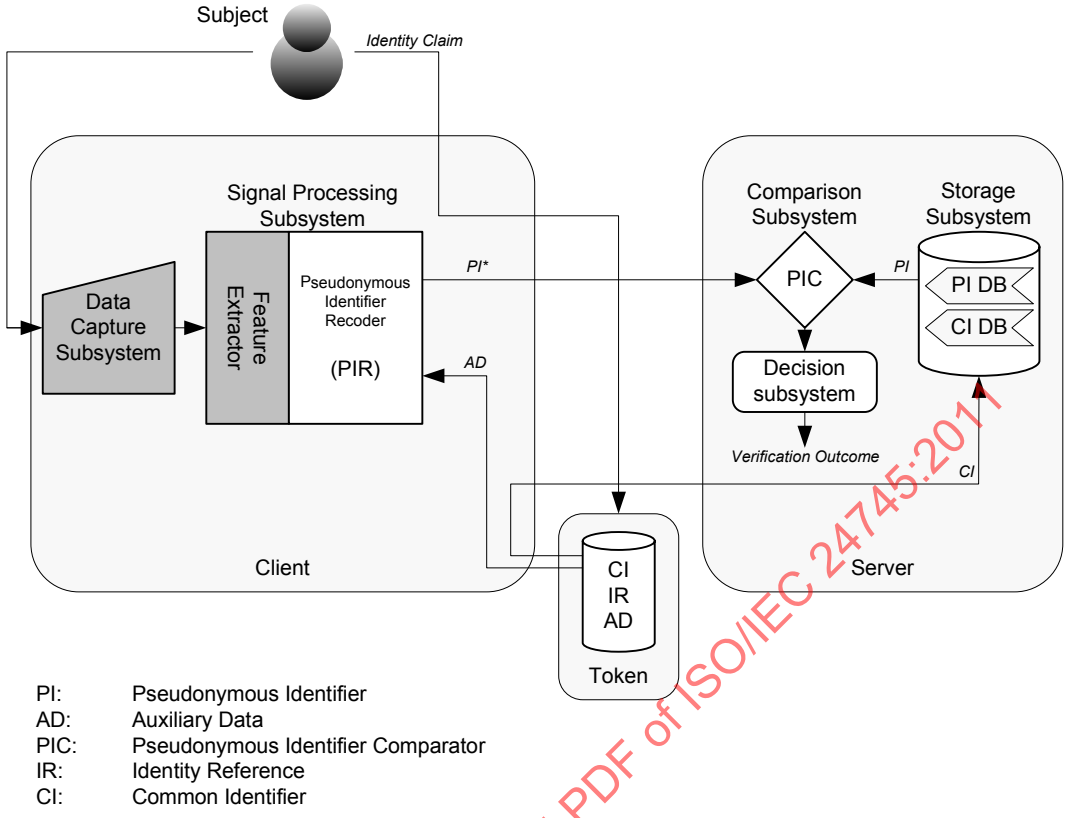
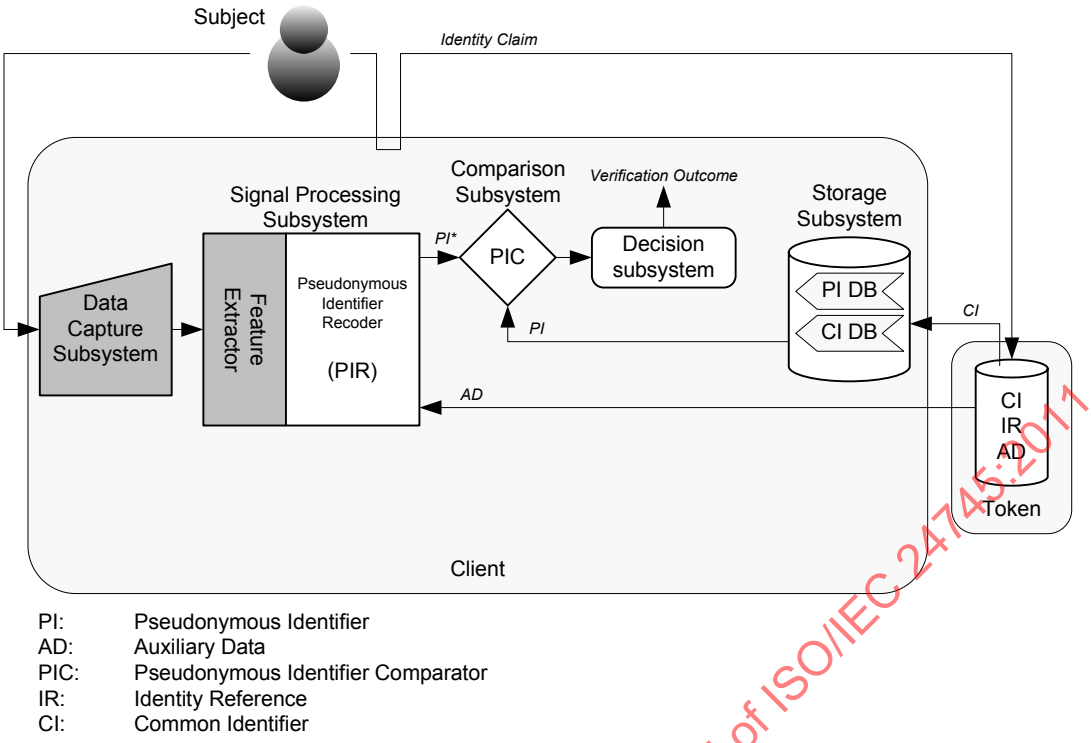


Figure 18 — Model G: Store distributed on token and server, compare on server

7.2.8 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 19). 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 pseudonymous identifier recoder (PIR), which generates a candidate pseudonymous identifier (PI*) based on the captured biometric probe sample. 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.



PI: Pseudonymous Identifier
AD: Auxiliary Data
PIC: Pseudonymous Identifier Comparator
IR: Identity Reference
CI: Common Identifier

Figure 19 — 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 employed 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 [20] 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.

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 never 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.

In this Annex, examples for secure binding of a pair of IR and BR assuming separated databases for IR and BR with separated control and their usages will be described. The database for identity references will be called DB_{IR} and that for biometric references will be 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}

a) DB_{IR} receives an authentic IR from an IR claimant (individual) or from a 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 common identifier 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 DB_{IR} and DB_{BR} (Case A)

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

a) DB_{IR} receives an authentic IR from an IR claimant (individual) or from a TTP, encrypts IR using K_i to get $E_{Ki}(IR)$, hashes IR to get h(IR), and encrypts {h(IR), $IDDB_{IR}$, N_i} using 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 DB_{IR}.

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

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

d) DB_{BR} receives $E_{Ke}(h(IR), IDDB_{IR}, N_i)$ from 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.). DB_{BR} 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 common identifier and as a Check value, encrypts {CI, h(BR), $IDDB_{BR}$, N_b} using K_e to get $E_{Ke}(CI, h(BR), IDDB_{BR}, N_b)$, sends $E_{Ke}(CI, h(BR), IDDB_{BR}, N_b)$ to DB_{IR}, and stores {CI, $E_{Kb}(BR)$}.

e) DB_{IR} receives $E_{Ke}(CI, h(BR), IDDB_{BR}, N_b)$ from DB_{BR}, decrypts $E_{Ke}(CI, h(BR), IDDB_{BR}, N_b)$ 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.). DB_{IR} calculates MAC for {h(IR), h(BR)} with shared secret key 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, $E_{Ki}(IR)$}.

A.3 BR claim for verification

In this Subclause, an example of a BR claim from DB_{IR} to DB_{BR} for verification will be described. Here, the method for finding the correct $E_{Ki}(IR)$ from a legitimate identity claim is assumed to be given.

Case A: Secure communication channel between DB_{IR} and DB_{BR}

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

b) DB_{BR} receives {CI, h(IR)} from DB_{IR}, finds $E_{Kb}(BR)$ using CI, decrypts $E_{Kb}(BR)$ 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, DB_{BR} sends BR securely to the comparison subsystem. If the match fails, it exits with an error message.

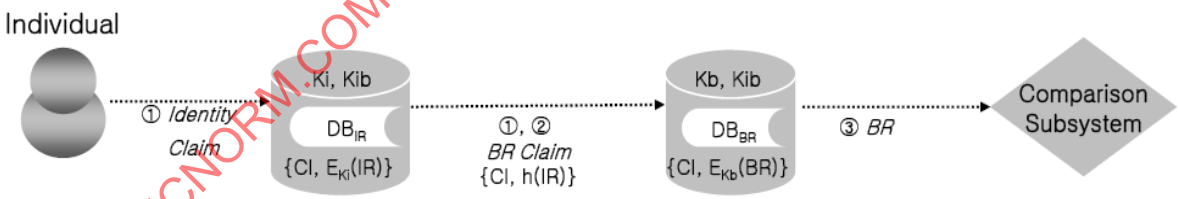


Figure A.2 — BR claim for verification (Case A)

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

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

b) DB_{BR} receives $E_{Kib}(CI, h(IR), IDDB_{IR}, Ni)$ from 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 $E_{Kb}(BR)$ using CI, decrypts $E_{Kb}(BR)$ to get BR, hashes BR to get h(BR), computes $MAC_{Kib}(h(IR), h(BR))$ and compares it with received CI.

c) If they match, 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

In this Subclause, an example of an IR claim from DB_{BR} to DB_{IR} for verification will be described. Here, it is assumed that DB_{BR} has already decrypted $E_{Kb}(BR)$ to get BR, and has sent it to the comparison subsystem.

Case A: Secure communication channel between DB_{IR} and DB_{BR}

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

b) DB_{IR} receives {CI, h(BR)} from DB_{BR}, finds $E_{Ki}(IR)$ using CI, decrypts $E_{Ki}(IR)$ to get IR, hashes IR to get h(IR), computes $MAC_{Kib}(h(IR), h(BR))$, and compares it with the received CI.

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

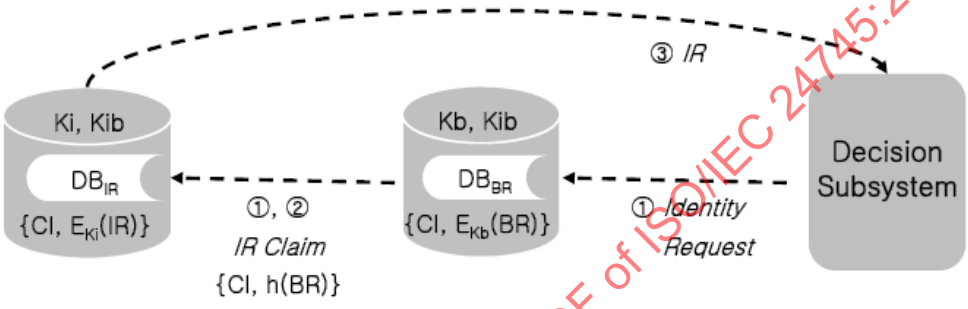


Figure A.3 — IR claim for identification (Case A)

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

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

b) DB_{IR} receives E_{Ke}(CI, h(BR), $IDDB_{BR}$, N_b)) from 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 $E_{Ki}(IR)$ using CI, decrypts $E_{Ki}(IR)$ to get IR, hashes IR to get h(IR), computes $MAC_{Kib}(h(IR), h(BR))$, and compares it with the received CI.

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

Annex B
(informative)

Cryptographic algorithms for security of biometric systems

B.1 Cryptographic algorithms providing confidentiality

To provide confidentiality of data, encryption algorithms can be used. An encryption algorithm is applied to data (often called plaintext or cleartext) to yield encrypted data (or ciphertext): this process is known as encryption. The encryption algorithm is designed in a way that the ciphertext yields no information about the plaintext except, perhaps, its length. Associated with every encryption algorithm is a corresponding decryption algorithm, which transforms ciphertext back into its original plaintext.

Ciphers work in association with a key. In a symmetric cipher, the same key is used in both the encryption and decryption algorithms. ISO/IEC 18033-3 [14] and ISO/IEC 18033-4 [15] are devoted to two different classes of symmetric ciphers: block ciphers and stream ciphers. The key used in a symmetric cipher is referred as a secret key. In an asymmetric cipher, different but related keys are used for encryption and decryption. ISO/IEC 18033-2 [13] is devoted to asymmetric ciphers. Asymmetric ciphers utilize a public encryption key and a private decryption key. For biometric data encryption, symmetric-key ciphers are used more often in practice than asymmetric ciphers.

B.2 Cryptographic algorithms providing integrity

To provide integrity of data, one can use a Message Authentication Code (MAC) algorithm or a digital signature algorithm. MAC algorithms can be used as data integrity mechanisms to verify that data has not been altered in an unauthorised manner. They can also be used as message authentication mechanisms to provide assurance that a message has been originated by an entity in possession of the secret key. There are two types of MAC: mechanisms using a block cipher (see ISO/IEC 9797-1 [10]) and mechanisms using a dedicated hash-function (see ISO/IEC 9797-2 [10]).

Digital signatures can be used in place of hand-written signatures for implementing services such as entity and message authentication. They can also be used to provide message integrity and non-repudiation. These services apply to digital messages which are strings of bits (e.g., concatenations of data elements or objects).

Most digital signature schemes are based upon a particular public-key system. This system includes a process producing pairs of keys (i.e., a private key and a public key); a process using a private key; and a process using a public key. There are two types of digital signature schemes. When the whole message or a part of the message can be recovered from the signature, the scheme is named a "digital signature scheme giving message recovery" (see ISO/IEC 9796 [9]). When the whole message has to be stored and transmitted along with the signature, the scheme is named a "digital signature scheme with appendix" (see ISO/IEC 14888 [12]).

B.3 Cryptographic algorithms providing confidentiality and integrity

To provide both confidentiality and integrity, both encryption and a MAC or signature can be used. Whilst these operations can be combined in many ways, not all combinations of such mechanisms provide the same security guarantees. As a result it is desirable to define in detail exactly how integrity and confidentiality mechanisms should be combined to provide the optimum level of security. Moreover, in some cases significant efficiency gains can be obtained by defining a single method of processing the data with the objective of providing both confidentiality and integrity protection. In ISO/IEC 19772 [16], authenticated encryption mechanisms are defined. These are methods for processing data to provide both integrity and confidentiality protection. They typically involve either a specified combination of a MAC computation and data encryption, or the use of an encryption algorithm to provide both integrity and confidentiality.