INTERNATIONAL STANDARD

ISO/IEC 24761

Second edition
2019-10

Information technology — Security techniques — Authentication context for biometrics

Technologies de l'information — Techniques de sécurité — Contexte d'authentification biométrique

Reference number
ISO/IEC 24761:2019(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: 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.

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

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

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

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

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

This second edition cancels and replaces the first edition (ISO/IEC 24761:2009), which has been technically revised. It also incorporates the Technical Corrigendum ISO/IEC 24761:2009/Cor.1:2013. The main changes compared to the previous edition are as follows:

— extension of data types which reflects the progress in biometric technology for protection of biometric data such as renewable biometrics and others,

— introduction of a new biometric capability model which makes the validation of ACBio instances simpler, and

— changes to the ASN.1 module as a result of the above changes.

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

Introduction

A biometric verification process executed at a remote site is exposed to many risks, for example, falsified reference, forged captured biometric data, and unreliable biometric products, etc. How can the validator check whether a biometric verification process, carried out in a remote site, is trustworthy? This document gives a mechanism to cope with this problem.

In general, the reliability of the result of a biometric verification process is dependent both on the security of the process executed and on the functional performance of the biometric products used. If products offering a better functional performance are used, the result will be more reliable. If the products are not secure or the process has been executed in an insecure environment, then the result will not be reliable.

In the Internet environment, the validator of a biometric verification process usually does not directly know about the biometric products used or about the process(es) executed at a remote site. Authentication Context for Biometrics (ACBio) provides a solution to the above problem and mitigates security risks of biometric authentication, by sending information about the products used and the processes executed at the remote site to the validator if the biometric processing has resulted successfully.

ACBio defines data formats for evidence data generated by biometric processing units (BPUs), such as a sensor, smartcard or comparison device, which are carried in data structures called ACBio instances. ACBio specifies a trust and assurance mechanism based on digital signature technology to provide assured information about the BPU and its execution of the biometric enrolment and verification processes where the assured information about the BPU is provided as BPU report issued by the vendor of the BPU. This is based on the Public Key Infrastructure (PKI) technology and PKIX (see ISO/IEC 9594-8 and RFC 3852). An ACBio instance carries information about the biometric processing units (BPUs), biometric reference and biometric verification results that together characterise a biometric verification transaction. Assurance of the information in an ACBio instance is provided by digital certificates associated with the relevant elements of the information. These certificates are issued by trusted certification authorities in registration processes which gather evidence about the BPUs and their verification performance capabilities, and the biometric reference and the binding to a known subject. The certificates serve two purposes. Firstly, to provide assurance of the identity of the source of the biometric transaction (the BPUs) and the biometric reference, and secondly to provide assurance for the biometric verification result contained in the transaction. With all the ACBio instances sent to the validator, it can check the integrity of the data transmitted between BPUs. The real-time information of presentation attack detection is not provided with this document. The BPU report may, however, contain the assurance information of the PAD mechanism. ACBio recognizes that privacy requirements concerned with the storage of biometric data must comply with local laws and legislation on data privacy. ACBio ensures that the validator can validate the result of the biometric verification process without receiving private data, such as the biometric sample acquired from the claimant or the biometric reference used for comparison.

An ACBio instance is a report that is encoded using the Basic Encoding Rules (BER) of ASN.1 [see ISO/IEC 8824 (all parts)], commonly supported by cryptographic tool kit vendors. The syntax is algorithm independent and supports provision of data integrity and data origin authentication. In regard to cryptographic algorithms, those specified by ISO/IEC JTC 1/SC 27 are recommended, though any algorithm appropriate for use by a given community may be used.

This document reflects the progress in biometric technology for protection of biometric data such as renewable biometrics specified in ISO/IEC 24745 and others by extending the variation of biometric data types transmitted between biometric subprocesses, and in addition establishes a new biometric capability model which makes the validation of ACBio instance(s) simpler. This has resulted in some changes to the ASN.1 module which will give rise to inter-operational incompatibilities between systems implementing different versions of the ASN.1 modules.

Information technology — Security techniques — Authentication context for biometrics

1 Scope

This document defines the structure and the data elements of Authentication Context for Biometrics (ACBio), which is used for checking the validity of the result of a biometric enrolment and verification process executed at a remote site. This document allows any ACBio instance to accompany any biometric processes related to enrolment and verification. The specification of ACBio is applicable not only to single modal biometric enrolment and verification but also to multimodal fusion. The real-time information of presentation attack detection is not provided in this document. Only the assurance information of presentation attack detection (PAD) mechanism can be contained in the BPU report.

Biometric identification is out of the scope of this document.

This document specifies the cryptographic syntax of an ACBio instance. The cryptographic syntax of an ACBio instance is defined in this document applying a data structure specified in Cryptographic Message Syntax (CMS) schema whose concrete values can be represented using a compact binary encoding. This document does not define protocols to be used between entities such as BPUs, claimant, and validator. Its concern is entirely with the content and encoding of the ACBio instances for the various processing activities.

2 Normative references

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

ISO/IEC 2382-37, *Information technology — Vocabulary — Part 37: Biometrics*

ISO/IEC 9594-2, *Information Technology — Open Systems Interconnection — The Directory: Models*

ISO/IEC 9594-8, *Information technology — Open Systems Interconnection — The Directory: Public-key and attribute certificate frameworks*

ISO/IEC 24745, *Information technology — Security techniques — Biometric information protection*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 2382-37, ISO/IEC 9594-8, ISO/IEC 24745, and the following apply.

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

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

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

NOTE Terminology in this document has been updated where possible to conform to ISO/IEC 2382-37:2017. However, to maintain maximum compatibility with the terminology and type names in ASN.1 module in the first edition of this document, certain terms have been carried over from the previous edition.

3.1
ACBio instance
report generated by a BPU compliant to this document to show the validity of the execution result of one or more subprocesses executed in the BPU

3.2
biometric capability class
class of configurations for how the biometric enrolment/verification can be divided into single or multiple BPU roles

Note 1 to entry: There are four biometric capability classes defined in this document:

— all-in-one (biometric capability) class;

— sensor-and-comparator (biometric capability) class;

— storage-and-others (biometric capability) class; and

— sensor-only (biometric capability) class.

Note 2 to entry: To express each biometric capability class, "biometric capability" is usually omitted.

3.3
biometric processing unit
BPU
trusted implementation of a collection of biometric subprocesses implemented in a single physical unit

Note 1 to entry: A BPU commonly comprises biometric subprocesses that are sequential in the process flow for a biometric verification.

Note 2 to entry: Application/service requirements typically require BPU subprocesses to meet a uniform level of security assurance. In ACBio, assurance is achieved through a BPU evaluation process that is authenticated by means of an X.509 certificate embedded in an ACBio instance.

3.4
biometric processing unit certificate
BPU certificate
X.509 certificate that is issued to a BPU by a certification authority

3.5
biometric processing unit certification authority
BPU certification authority
X.509 certification authority which issues BPU certificates

3.6
biometric processing unit function report
BPU function report
report on the function of the BPU generated by the manufacturer of the BPU

3.7
biometric processing unit IO Index
BPU IO Index
integer number uniquely assigned to each biometric data stream between BPUs by the subject which utilizes the function of the BPU (e.g. a software) and used by the validator to reconstruct the data flow among BPUs

3.8
biometric processing unit report
BPU report
report on a BPU, which consists of a BPU function report and a BPU security report

3.9
biometric processing unit security report
BPU security report
report on the security of a BPU, which contains an assurance information of the security of the BPU

Note 1 to entry: The assurance information on PAD mechanism, if present in the BPU report, shall be included in the BPU security report.

3.10
biometric reference
one or more stored biometric samples, biometric templates or biometric models attributed to a biometric data subject and used as the object of biometric comparison

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

Note 1 to entry: A biometric reference may be created with implicit or explicit use of auxiliary data, such as Universal Background Models.

Note 2 to entry: The subject/object labelling in a *comparison*might be arbitrary. In some comparisons, a biometric reference might be used as the subject of the comparison with other biometric references or incoming samples and input to an algorithm for biometric comparison. For example, in a duplicate enrolment check a biometric reference will be used as the subject for comparison against all other biometric references in the database.

Note 3 to entry: A term "biometric reference template" is also used to mean biometric reference partly in this document. See NOTE at the beginning of Clause 3.

[SOURCE: ISO/IEC 2382-37:2017, 3.3.16, modified — Note 3 to entry has been added.]

3.11
biometric reference template certificate
BRT certificate
certificate that is issued to a biometric reference by a BRT certification organization and enables the validator to determine the authenticity of the biometric reference

3.12
biometric reference template certification organization
BRT certification organization
organization which issues BRT certificates

3.13
biometric subprocess
subprocess
part of an overall biometric enrolment or verification process performing a specific function

Note 1 to entry: Biometric subprocess functions is one of the following: data capture, intermediate signal processing, final signal processing, storage, comparison, and decision.

3.14
BPU role
combination of biometric functionalities provided by a BPU whose combination of functionalities is specified in this document

Note 1 to entry: A BPU role can be referenced by a name that describes the biometric functionality provided by the BPU: all BPU role, sensor BPU role, comparator-with-storage BPU role, comparator BPU role, and storage BPU role.

3.15
captured biometric reference
captured biometric sample or combination of captured biometric samples used as a biometric reference

3.16
control value
random number provided by a validator by which the validator can check whether an ACBio instance is generated at the validator's request or not

3.17
declaration expression
explicit expression of BPU function report in which information on the subprocesses and data flows are contained

3.18
enrolment organization
organization which handles enrolment and creates and stores biometric references

3.19
evaluation organization
organization which evaluates a BPU function or security

3.20
final signal processing
signal processing stage immediately preceding biometric comparison

Note 1 to entry: See NOTE at the beginning of Clause 3.

3.21
intermediate biometric reference
intermediate biometric sample or combination of intermediate biometric samples used as a biometric reference

Note 1 to entry: An intermediate biometric reference is processed through biometric final processing and then compared against a biometric sample.

3.22
intermediate signal processing
any manipulation of a biometric sample that does not produce biometric features

Note 1 to entry: In ISO/IEC 2382-37, "intermediate biometric sample processing" (ISO/IEC 2382-37:2017, 3.5.9) is defined in place of "intermediate signal processing". See NOTE at the beginning of Clause 3.

Note 2 to entry: The term "biometric feature" is defined as numbers or labels extracted from biometric samples and used for comparison in ISO/IEC 2382-37:2017, 3.3.11.

3.23
on-card biometric comparison
OCBC
performing comparison and decision making on an IC card where the biometric reference is retained on-card in order to enhance security and privacy

3.24
processed biometric reference
processed biometric sample or combination of processed biometric samples used as a biometric reference

3.25
processed biometric sample
biometric sample or biometric feature set input to an algorithm for biometric comparison to a biometric reference(s)

Note 1 to entry: ISO/IEC 2382-37, a term "biometric probe" (ISO/IEC 2382-37:2017, 3.3.14) is defined in place of "processed biometric sample". See NOTE at the beginning of Clause 3.

3.26
renewable biometric sample
biometric sample which has a property of a transform or process to create multiple, independent transformed biometric data 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 generative biometric data

Note 1 to entry: Renewablity is defined in ISO/IEC 24745:2011 as: 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. This definition is only applicable to biometric reference. The definition in this document is slightly modified from that in ISO/IEC 24745:2011 so that it can be applied to biometric sample as well as biometric reference because the biometric sample in renewable biometrics should be so transformed that it can be compared with a renewable biometric reference.

3.27
role expression
implicit expression of BPU function report for BPU which has a BPU role

3.28
subprocess index
integer uniquely assigned to each subprocess within a BPU by the manufacturer of the BPU

3.29
subprocess IO index
unique integer assigned to each data stream between subprocesses in a BPU so that the validator can reconstruct the data flow between subprocesses in the BPU

3.30
validator
<of biometric verification> entity which makes a decision on whether the result of a biometric verification process is acceptable or not, based on the policy, using one or more comparison decisions and possibly other information, supported by ACBio instances

4 Symbols and abbreviated terms

ACBio	Authentication Context for Biometrics
ASN.1	Abstract Syntax Notation One as defined in the ISO/IEC 8824 series
BER	Basic Encoding Rules (of ASN.1)
BIR	Biometric Information Record
BRT	Biometric Reference Template
CBEFF	Common Biometric Exchange Formats Framework as defined in ISO/IEC 19785-1
CMS	Cryptographic Message Syntax as defined in RFC 3852 and RFC 5911
FAR	False Acceptance Rate
FRR	False Rejection Rate
PAD	Presentation Attack Detection

PKI Public Key Infrastructure

STOC Store On Card

URI Uniform Resource Identifier

5 Model and framework of ACBio

5.1 Biometric enrolment and verification process model and Biometric Processing Unit

This document defines the structure and the data elements of Authentication Context for Biometrics (ACBio), which is used for checking the validity of the result of a biometric enrolment and verification process executed at a remote site. An ACBio instance shall be accompanied witha biometric data output processesed by a BPU for biometric enrolment and verification.

ACBio's design is based on the following biometric subprocesses:

a) data capture: this subprocess captures biometric information from a claimant and converts it to a captured biometric sample. The captured biometric sample is transmitted to the intermediate signal processing subprocess for further processing;

b) intermediate signal processing: this subprocess receives a captured biometric sample and transforms it into an intermediate biometric sample. The intermediate biometric sample is transmitted to the final signal processing subprocess for further processing;

c) final signal processing: this subprocess receives an intermediate biometric sample and transforms it into a processed biometric sample. The processed biometric sample through the final signal processing is transmitted either to the comparison subprocess (for verification) or to the storage subprocess (for enrolment as the biometric reference). There is a variation of the output of the final signal processing, a renewable biometric sample;

d) storage: this subprocess stores one of three types of biometric reference; captured biometric reference (Key item 1 in Figure 1 and Figure 2), intermediate biometric reference (Key item 2 in Figure 1 and Figure 2), or processed biometric reference (Key item 3 in Figure 1 and Figure 2). One of the three types of biometric reference will be compared with a biometric sample for verification. As in c), there is a variation for processed biometric reference, renewable biometric reference;

e) comparison: this subprocess receives a biometric sample, which is acquired originally from a claimant, and can be further processed or not, and a biometric reference. This subprocess compares the biometric sample and the processed biometric reference, and calculates the similarity, which is called a comparison score. The comparison score is transmitted to the decision subprocess.

NOTE The processing of comparing a renewable biometric sample with a renewable biometric reference is different from that of comparing a processed biometric sample with a processed biometric reference. However, they are not distinguished in this document. They are distinguished only by the data input into the subprocess. If a BPU A executes the comparision subprocess and another BPU B executes the final signal processing subprocess or the storage subprocess, the BPU B does not know whether the BPU A can process the data submitted from the BPU B. In the ACBio framework, only the application system knows the compatibility of the data exchanged between the BPUs through the negotiation between them in advance. See B.1.2.5 for details.

f) decision: this subprocess receives a comparison score from the comparison subprocess, evaluates the score under rules determined by the security policy in use, decides the validity of the claimant's identity, and outputs the comparison decision, match or non-match, which is sent to the validator.

Besides the above six subprocesses biometric products generally have PAD mechanism. Figure 1 shows a general model of biometric verification including PAD mechanism. However, PAD is not discussed further in this document because it is dealt with only in the assurance information in the BPU report in this document. For more details of PAD, see ISO/IEC 30107-1.

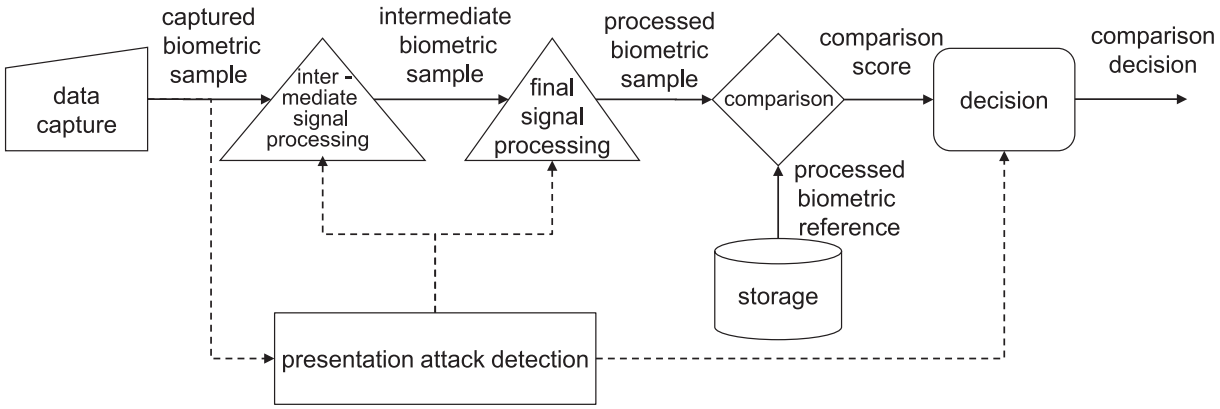


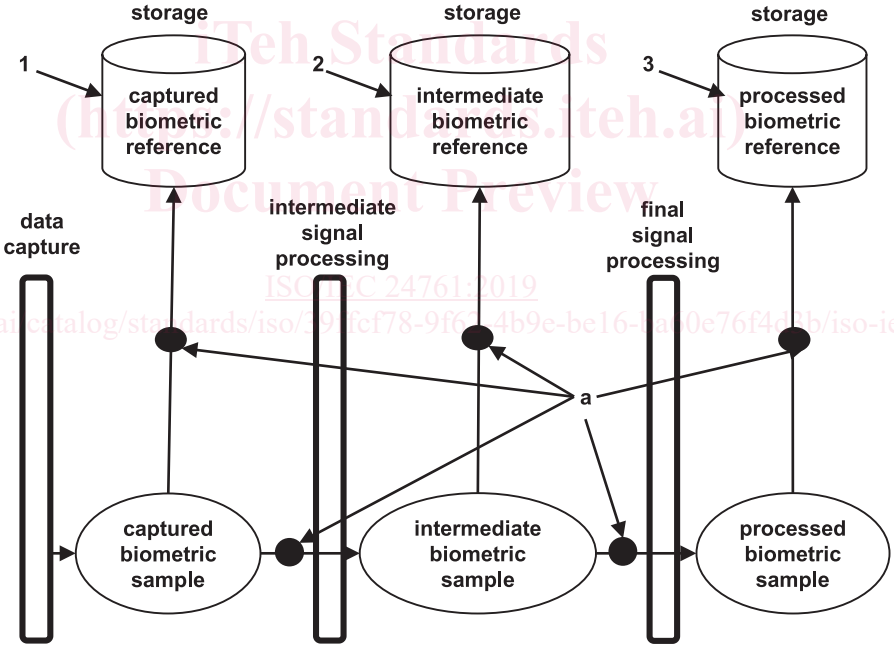
Figure 1 — General model of biometric verification including PAD mechanism

Figure 2 shows three cases of biometric enrolment process where the storage subprocess stores:

1) captured biometric samples,

2) intermediate biometric samples, and

3) processed biometric samples.



Key

1 storage subprocess which stores captured biometric samples

2 storage subprocess which stores intermediate biometric samples

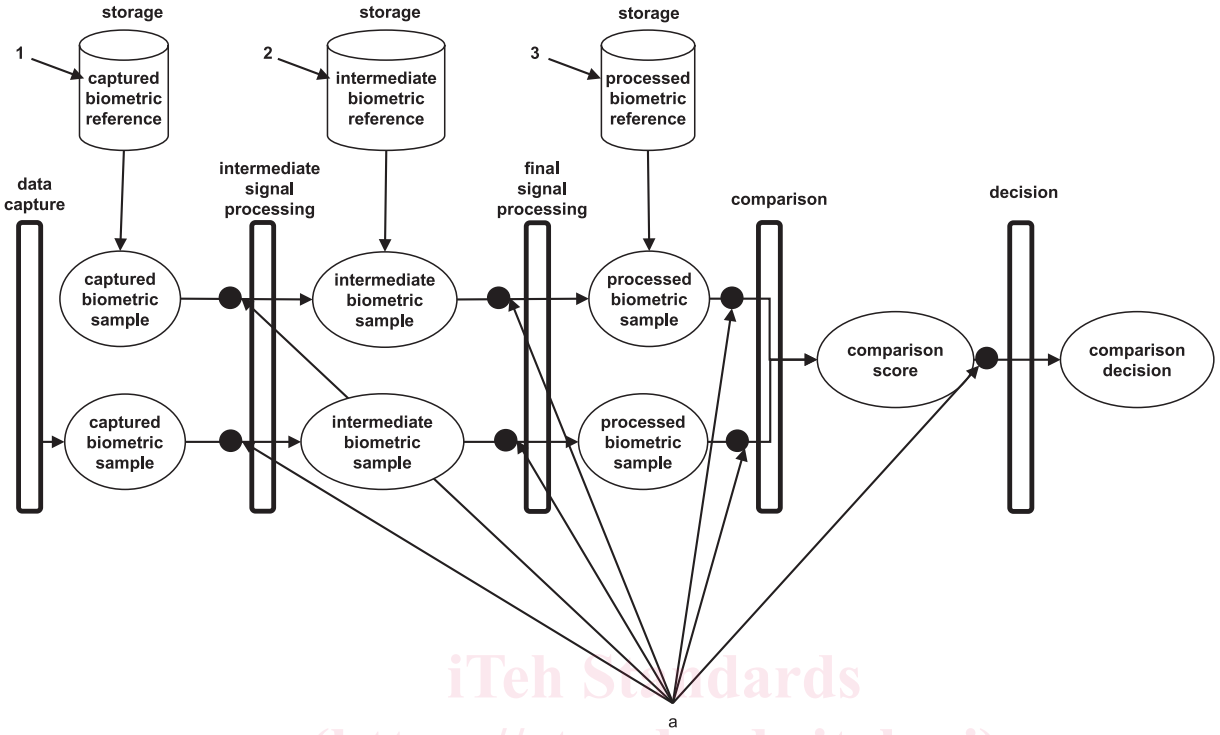
3 storage subprocess which stores processed biometric samples

[a] Possible untrusted network.

Figure 2 — Biometric enrolment process model

The small black disks with Key a in Figure 2 mean that an untrusted network may intervene at the points, i.e., a captured biometric sample, an intermediate biometric sample, and a processed biometric sample can be transferred through untrusted networks.

Figure 3 shows three cases of biometric verification process model where the storage subprocess stores a captured biometric reference, an intermediate biometric reference, and a processed biometric reference.



Key

1 storage subprocess which stores captured biometric samples

2 storage subprocess which stores intermediate biometric samples

3 storage subprocess which stores processed biometric samples

[a] Possible untrusted network.

Figure 3 — Biometric verification process model

The small black disks with Key a in Figure 3 mean the same as in Figure 2.

This document considers only biometric data flows in Figure 3 and does not consider any other non-biometric data flows such as auxiliary data in renewable biometrics.

5.2 BPU role and biometric capability class

5.2.1 Overview

When implementing biometric systems, the various biometric subprocesses that compose the system are often grouped together into components called biometric processing units (BPUs). The groupings reflect the physical and architectural details and the grouping of biometric subprocesses in the system implementation. Commonly used combinations of BPU functionalities are described and defined as BPU roles in this document. In principle, a BPU can include any grouping of biometric subprocesses but, in practice, BPUs commonly comprise biometric subprocesses that are sequential in the overall process flow for a biometric verification. BPU roles that equate to commonly used combinations of BPU functionality are defined in 5.2.2.