INTERNATIONAL STANDARD

ISO/IEC 24761

First edition
2009-05-15

Information technology — Security techniques — Authentication context for biometrics

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

Reference number
ISO/IEC 24761:2009(E)

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

COPYRIGHT PROTECTED DOCUMENT

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 iv
Introduction v
1 Scope 1
2 Normative references 1
3 Terms and definitions 1
4 Abbreviated terms 5
5 Model and framework of ACBio 6
5.1 Biometric enrolment and verification process model and Biometric Processing Unit (BPU) 6
5.2 Framework for use of ACBio 8
5.2.1 Preparation for use of ACBio 8
5.2.2 Biometric verification and ACBio 10
5.2.3 Validation of biometric verification process using ACBio 11
6 ACBio instance 11
6.1 BPU information block 15
6.2 Biometric process block 15
6.3 BRT certificate information 16
7 Definition of components in BPUInformationBlock 17
7.1 BPU certificate 17
7.2 BPUReportInformation 17
7.2.1 BPUFunctionReport 18
7.2.2 BPUSecurityReport 21
8 BRT certificate 21
8.1 BRTCContentInformation 22
8.2 Format Owner and Format Type values 23
Annex A (normative) ASN.1 module for ACBio 24
Annex B (informative) Implementation examples 30
Bibliography 50

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.

ISO/IEC 24761 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

Introduction

A biometric verification process executed at a remote site is exposed to many risks: falsified reference templates, forged raw data, unreliable biometric devices, etc. How can the validator check whether a biometric verification process carried out in a remote site is trustworthy? This International Standard gives a mechanism to cope with this problem.

In general, reliability of the result of a biometric verification process is dependent both on the security level of the process executed and on the functional performance level of the biometric devices used. If devices offering a better functional performance level are used, the result will be more reliable. If the devices are not secure or the process has been executed in an unsecure 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 devices used or about the process(es) executed at a remote site. Obtaining trusted information, such as the functional performance level of the biometric devices used, the security level of the remote system, and also knowing that the processes in the system were executed securely, the validator can make a better decision on how much trust can be placed on the result of the biometric verification.

This International Standard provides a solution to the above problem by sending information about the devices used and the processes executed at the remote site to the validator.

In general, the biometric enrolment process consists of the following subprocesses: data capture, intermediate signal processing, final signal processing (or feature extraction), and storage. (This is true in general, but there are many variants possible.)

In general, the biometric verification process consists of data capture, intermediate signal processing, final signal processing, retrieval from storage, comparison, and decision. (This is true in general, but there are many variants possible.)

Usually, subprocesses are executed in one or more biometric processing units (BPUs), each of which has its own uniform security level. Several subprocesses are involved in the biometric verification process, but the security of the retrieval subprocess from storage is also dependent on the subprocesses involved in the biometric enrolment process.

This International Standard is designed to be applied to this model of biometric verification processes, which is an extension of the biometric system model defined in ISO 19092, but is also applicable to other biometric verification process models.

This International Standard defines a data format for security data generated by BPUs, such as a sensor, smartcard, or comparison device, to provide certified information about the BPU to help the validator to determine the reliability of the result of the biometric verification process.

This International Standard is based on the Public Key Infrastructure (PKI) technology and PKIX (see ISO/IEC 9594-8 | ITU-T Recommendation X.509 and RFC 3852). This International Standard uses a digital signature as the base for trust and non-repudiation. This International Standard requires input and output information to be hashed, and subsequently digitally signed with other data such as a challenge from the validator, and the evaluation result of the BPU actions.

This International Standard recognizes that privacy requirements concerned with the storage of biometric elements have to respond to and 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 template used for comparison.

An ACBio instance is a report that is encoded using the XML Encoding Rules (XER) or the Basic Encoding Rules (BER) of ASN.1 [see ISO/IEC 8824 (All parts) | ITU-T Recommendations X.680-683 and ISO/IEC 8825-4 | ITU-T Recommendation X.693], commonly supported by cryptographic tool kit vendors. The syntax is algorithm independent and supports provision of data integrity and data origin authentication. The cryptographic algorithms specified by ISO/IEC JTC 1/SC 27 are recommended, though any algorithm appropriate for use by a given community may be used.

This International Standard uses BPU certificates, issued by a BPU certification organization (a trusted third party that issues certificates concerning the security of the BPU) and biometric reference template (BRT) certificates, issued by a BRT certification organization that issues certificates concerned with the production and retention of a biometric reference template in a database or on a smart-card.

The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) draw attention to the fact that it is claimed that compliance with this document may involve the use of a patent concerning the ACBio instance given in Clauses 5, 6, 7, and 8.

ISO and IEC take no position concerning the evidence, validity and scope of this patent right.

The holder of this patent right has assured the ISO and IEC that he/she is willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statement of the holder of this patent right is registered with ISO and IEC. Information may be obtained from:

Toshiba Corporation, Toshiba Solutions Corporation,
1-1, Shibaura 1-chome, Minato-ku,
Tokyo 105-8001, Japan

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights other than those identified above. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Information technology — Security techniques — Authentication context for biometrics

1 Scope

This International Standard 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 verification process executed at a remote site. This International Standard allows any ACBio instance to accompany any data item that is involved in any biometric process related to verification and enrolment. The specification of ACBio is applicable not only to single modal biometric verification but also to multimodal fusion.

This International Standard specifies the cryptographic syntax of an ACBio instance. The cryptographic syntax of an ACBio instance is based on an abstract Cryptographic Message Syntax (CMS) schema whose concrete values can be represented using either a compact binary encoding or a human-readable XML encoding.

This International Standard 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 referenced documents are indispensable for the application 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 8824 (all parts) | ITU-T Recommendations X.680-683, *Information technology — Abstract Syntax Notation One (ASN.1)*

ISO/IEC 8825-4 | ITU-T Recommendation X.693, *Information technology — ASN.1 encoding rules: XML Encoding Rules (XER)*

ISO/IEC 9594-2 | ITU-T Recommendation X.501, *Information technology — Open Systems Interconnection — The Directory: Models*

ISO/IEC 9594-8 | ITU-T Recommendation X.509, *Information technology — Open Systems Interconnection — The Directory: Public-key and attribute certificate frameworks*

ISO/IEC 19785-1, *Information technology — Common Biometric Exchange Formats Framework — Part 1: Data element specification*

ISO/IEC 19785-3, *Information technology — Common Biometric Exchange Formats Framework — Part 3: Patron format specifications*

RFC 3852, *Cryptographic Message Syntaxt (CMS), July 2004*

3 Terms and definitions

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

3.1
ACBio instance
report generated by a biometric processing unit (BPU) compliant to this International Standard to show the validity of the result of one or more subprocesses executed in the BPU

3.2
authentication context for biometrics
ACBio
International Standard that specifies the form and encoding of ACBio instances

3.3
biometric
pertaining to the field of biometrics

3.4
biometric processing unit
BPU
entity that executes one or more subprocesses that perform a biometric verification at a uniform level of security

NOTE A sensor, a smart card, and a comparison device are examples of BPUs.

3.5
biometric processing unit certificate
BPU certificate
X.509 certificate that is issued to a BPU by a certification organization which enables the validator to determine the reliability of the BPU

3.6
biometric processing unit certification organization
BPU certification organization
organization which issues BPU certificates

3.7
biometric processing unit function report
BPU function report
report on the function of the BPU, which contains the evaluation results on each function in the BPU

3.8
biometric processing unit IO Index
BPU IO Index
integer assigned to each biometric data stream between BPUs by the subject, such as software, which utilizes the function of the BPU so that the validator can reconstruct the data flow among BPUs

3.9
biometric processing unit report
BPU report
report on a BPU, which consists of a BPU function report and a BPU security report

3.10
biometric processing unit security report
BPU security report
report on the security level of a BPU, which contains an evaluation result of the security level of the BPU

3.11
biometric sample
information obtained from a biometric sensor, either directly or after further processing

NOTE See also **raw biometric sample** (3.33), **intermediate biometric sample** (3.26), and **processed biometric sample** (3.31).

3.12
biometric reference template
biometric sample or combination of biometric samples that has been stored as a reference for future comparison

NOTE See also **raw biometric reference template** (3.34), **intermediate biometric reference template** (3.27), and **processed biometric reference template** (3.32).

3.13
biometric reference template certificate
BRT certificate
certificate that is issued to a biometric reference template by a BRT certification organization and enables the validator to determine the authenticity of the biometric reference template

3.14
biometric reference template certification organization
BRT certification organization
organization which issues BRT certificates

3.15
biometric verification
application that returns true or false for a claim about the similarity of one or more biometric reference templates and one or more recognition biometric samples by making one or more comparisons

3.16
biometrics
automated recognition of individuals based on their behavioural and biological characteristics

3.17
claimant
⟨biometric verification⟩ individual who is seeking, and is the object of, biometric verification

3.18
comparison
estimation, calculation or measurement of similarity or dissimilarity between one or more recognition biometric samples and one or more biometric reference templates

3.19
comparison decision
determination of whether the recognition biometric sample(s) and biometric reference template(s) have the same biometric source, based on comparison scores, decision policies (including threshold values), and possibly other inputs to the comparison decision

3.20
comparison score
numerical value (or set of values) resulting from a comparison

3.21
control value
random number provided by a validator that is a means by which the validator can check whether an ACBio instance is generated at the validator’s request or not

3.22
enrol
collect one or more biometric samples from an individual, and subsequently construct one or more biometric reference templates which can then be used to verify or determine the individual’s identity

3.23
enrolment
process of collecting one or more biometric samples from an individual, and the subsequent construction of a biometric reference template which can then be used to verify or determine the individual's identity

3.24
enrolment organization
organization which handles enrolment and creates and stores biometric reference templates

3.25
evaluation organization
organization which evaluates biometric processing unit function or security

3.26
intermediate biometric sample
biometric sample obtained by processing a raw biometric sample, intended for further processing

3.27
intermediate biometric reference template
intermediate biometric sample or combination of intermediate biometric samples used as a biometric reference template

3.28
match
decision that the recognition biometric sample(s) and the biometric reference template are from the same individual

3.29
non-match
decision that the recognition biometric sample(s) and the biometric reference template are not from the same individual

3.30
on-card matching
performing comparison and decision making on an integrated circuit card where the biometric reference template is retained on-card in order to enhance security and privacy

NOTE The term "matching" is deprecated and replaced with the term "comparison" in ISO/IEC JTC 1/SC 37 work. But the term "on card matching" is a term heavily used in ISO/IEC JTC 1/SC 17 work. So this term is used in this International Standard.

3.31
processed biometric sample
biometric sample suitable for comparison

3.32
processed biometric reference template
processed biometric sample or combination of processed biometric samples used as a biometric reference template

3.33
raw biometric sample
biometric sample obtained directly from a biometric sensor

3.34
raw biometric reference template
raw biometric sample or combination of raw biometric samples used as a biometric reference template

3.35
subprocess
part of a biometric verification or enrolment process usually performing data capture, intermediate signal processing, final signal processing, storage, comparison, or decision

3.36
subprocess index
integer uniquely assigned to each subprocess within a biometric processing unit (BPU) by the organization providing the BPU

3.37
subprocess IO index
unique integer assigned to each data stream between subprocesses in a biometric processing unit (BPU) so that the validator can reconstruct the data flow between subprocesses in the BPU

3.38
validator
⟨biometric verification⟩ entity which makes a decision on whether the result of a biometric verification process is acceptable or not, based on the policy of the corresponding application, using one or more comparison decisions and possibly other information, supported by ACBio instances

4 Abbreviated terms

ACBio	Authentication Context for Biometrics
ASN.1	Abstract Syntax Notation One as defined in ISO/IEC 8824
BER	Basic Encoding Rules (of ASN.1)
BIR	Biometric Information Record
BPU	Biometric Processing Unit
BRT certificate	Biometric Reference Template certificate
CBEFF	Common Biometric Exchange Formats Framework as defined in ISO/IEC 19785-1
CMS	Cryptographic Message Syntax as defined in RFC 3852
IO	Input/Output
OCM	On-Card Matching
STOC	STore On Card
URI	Universal Resource Identifier
XML	eXtensible Markup Language

5 Model and framework of ACBio

5.1 Biometric enrolment and verification process model and Biometric Processing Unit (BPU)

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

a) data capture

This subprocess captures biometric information from a claimant and converts it to a raw biometric sample. The raw biometric sample is transmitted to the intermediate signal processing subprocess for further processing.

b) intermediate signal processing

This subprocess receives a raw biometric sample and transforms it into an intermediate biometric sample. The intermediate biometric sample is transmitted to another intermediate signal processing subprocess or 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 is transmitted either to the comparison subprocess (verification) or to the storage subprocess (enrolment).

d) storage

This subprocess stores one of three types of biometric reference template; raw biometric reference template ((1) in Figure 1 and Figure 2), intermediate biometric reference template ((2) in Figure 1 and Figure 2), or processed biometric reference template ((3) in Figure 1 and Figure 2). One of the three types of biometric reference template will be compared with a biometric sample for verification.

e) comparison

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

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.

The following Figure 1 shows three biometric enrolment process models where the storage subprocess stores a raw biometric sample, an intermediate biometric sample, and a processed biometric sample.

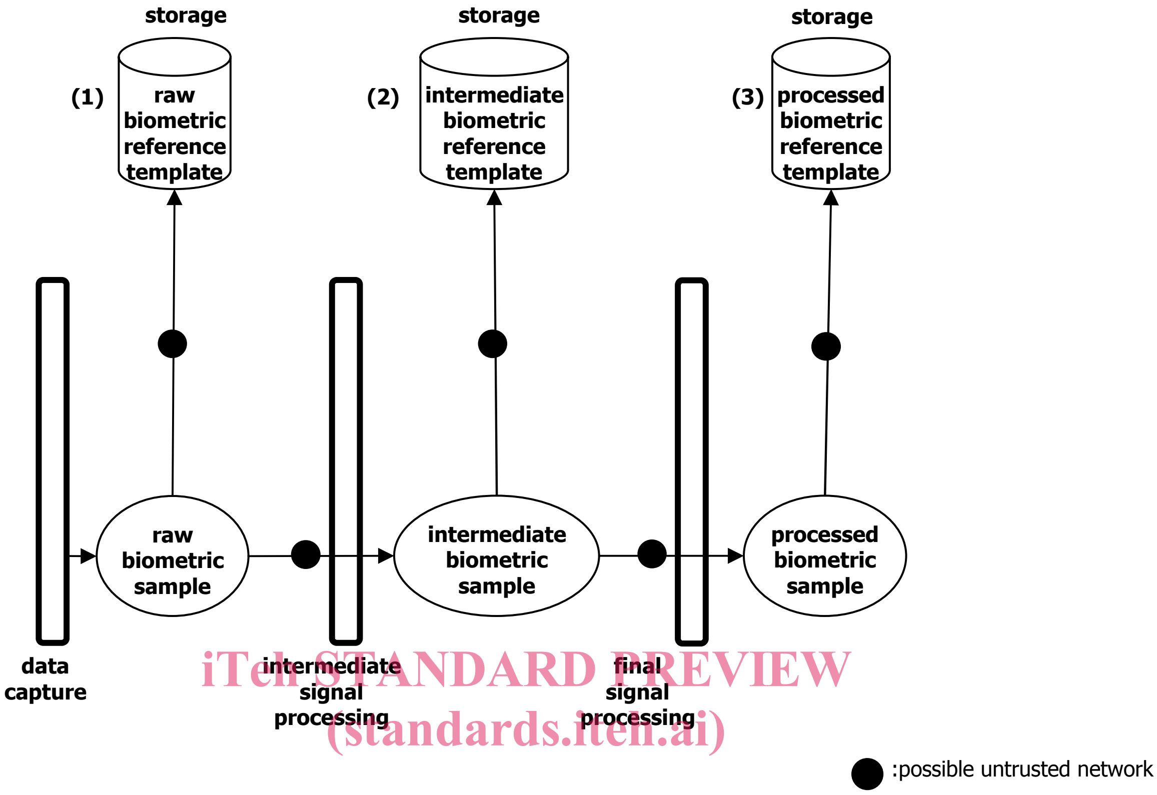
storage
storage
storage
(1)
raw biometric reference template
(2)
intermediate biometric reference template
(3)
processed biometric reference template
raw biometric sample
intermediate biometric sample
processed biometric sample
data capture
intermediate signal processing
final signal processing
● :possible untrusted network

Figure 1 — Biometric enrolment process model

The following Figure 2 shows three biometric verification process models where the storage subprocess stores a raw biometric reference template, an intermediate biometric reference template, and a processed biometric reference template.

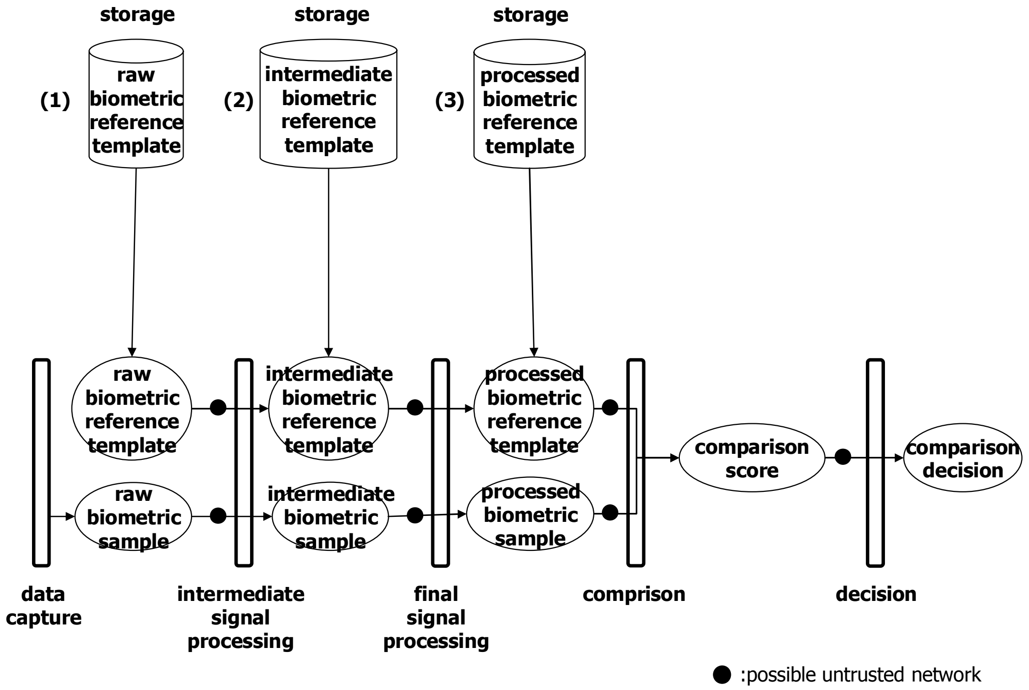
storage
storage
storage
(1)
raw biometric reference template
(2)
intermediate biometric reference template
(3)
processed biometric reference template
raw biometric reference template
intermediate biometric reference template
processed biometric reference template
raw biometric sample
intermediate biometric sample
processed biometric sample
comparison score
comparison decision
data capture
intermediate signal processing
final signal processing
comprison
decision
● :possible untrusted network

Figure 2 — Biometric verification process model

5.2 Framework for use of ACBio

ACBio gives information to the validator of a biometric verification process about the level of trust of the biometric verification process.

Subclauses 5.2.1 to 5.2.3 describe what shall be prepared in the production process of BPUs that result in a comparison and the enrolment process of BPUs that produce biometric references template, how ACBio instances are generated in these processes, and how biometric verification is validated.

5.2.1 Preparation for use of ACBio

To validate biometric verification processes with ACBio, preparation is necessary in addition to capture and storage (enrolment) of the biometric reference templates of claimants.

The series of steps in preparations for the use of ACBio is shown in Figure 3, separated into the production process, and the enrolment process, and the subsequent verification process.

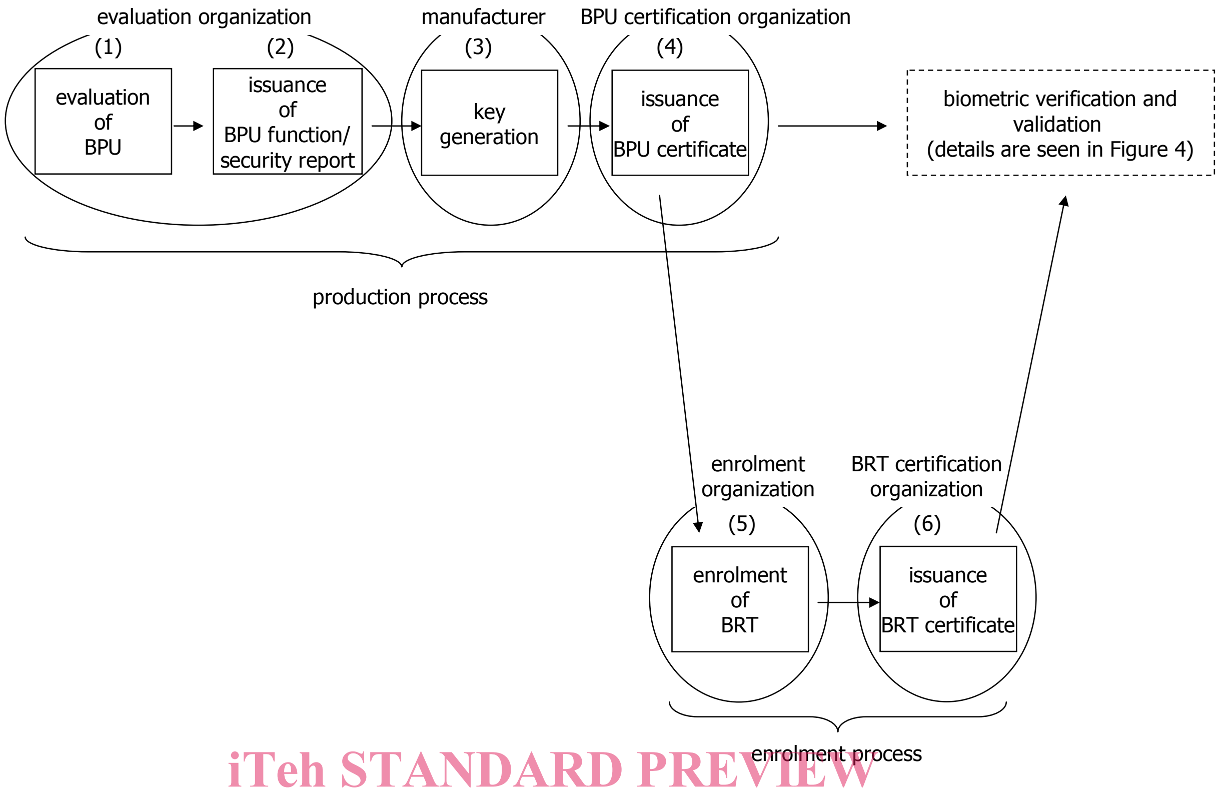
evaluation organization
(1)
(2)
evaluation of BPU
issuance of BPU function/ security report
manufacturer
(3)
key generation
BPU certification organization
(4)
issuance of BPU certificate
biometric verification and validation (details are seen in Figure 4)
production process
enrolment organization
(5)
enrolment of BRT
BRT certification organization
(6)
issuance of BRT certificate
enrolment process

Figure 3 — Preparation for use of ACBio and biometric verification execution

5.2.1.1 Preparation in the production process

The security level and functional performance level (quality) of each function in each BPU are evaluated by one or more evaluation organizations which may include the manufacturer of the product (software or hardware that forms the BPU ((1) in Figure 3).

After the evaluation, a BPU function report (See 7.2.1) and a BPU security report (See 7.2.2) are issued from the evaluation organization ((2) in Figure 2), which compose a BPU report.

Manufacturers of the products forming the BPU shall generate a key of symmetric cryptosystem or a key pair of asymmetric key cryptosystem depending on the BPU, to each BPU ((3) in Figure 3).

The key shall be certified and a BPU certificate (See 7.1) shall be issued by a BPU certification organization which may be the manufacturer of the product of the BPU ((4) in Figure 3).

The BPU report or a referrer to it, the BPU certificate or the referrer to it, and the key shall be stored in each BPU before shipping of the product of the BPU. Each BPU shall have the means to generate a digital signature or a message authentication code so that the validator can validate the integrity of the ACBio instance.

5.2.1.2 Preparation in the enrolment process

For biometric verification, a biometric reference template shall be created and enrolled in advance with an enrolment organization ((5) in Figure 3).

To use ACBio for validation of a biometric verification process, a certificate of biometric reference template called a BRT certificate (see Clause 8) shall be issued by a BRT certification organization ((6) in Figure 3).