

I n t e r n a t i o n a l T e l e c o m m u n i c a t i o n U n i o n

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1091

(04/2012)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Information and network security – Telebiometrics

A guideline for evaluating telebiometric template protection techniques

Recommendation ITU-T X.1091

ITU-T X-SERIES RECOMMENDATIONS
DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1339
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589

For further details, please refer to the list of ITU-T Recommendations.

Copyright © 2012 ITU-T. All rights reserved.

Recommendation ITU-T X.1091

A guideline for evaluating telebiometric template protection techniques

Summary

Recommendation ITU-T X.1091 describes a general guideline for testing and reporting the performance of biometric template protection techniques based on biometric cryptosystem or cancellable biometrics. This guideline specifies two reference models for evaluation, which use biometric template protection techniques in telebiometric systems. It then defines the metrics, procedures and requirements for testing and evaluating the performance of the biometric template protection techniques.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T X.1091	2012-04-13	17

Keywords

Biometric cryptosystem, biometric template protection techniques, cancellable biometrics, evaluation, telebiometrics.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at <http://www.itu.int/ITU-T/ipr/>.

© ITU 2013

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

	Page
1 Scope	1
2 References.....	1
3 Definitions	2
3.1 Terms defined elsewhere	2
3.2 Terms defined in this Recommendation.....	3
4 Abbreviations and acronyms	5
5 Conventions	5
6 Overview of protection techniques for the biometric template on telecommunication systems	5
6.1 Biometric cryptosystem mechanism.....	5
6.2 Cancellable biometrics mechanism	6
7 Reference models of protection techniques for a biometric template	7
7.1 Reference model of a biometric cryptosystem mechanism.....	7
7.2 Reference model for a cancellable biometrics mechanism	8
7.3 Specific threats for reference models	9
8 Evaluation items for biometric template protection techniques	11
8.1 Introduction	11
8.2 Evaluation items for the biometric cryptosystem mechanism.....	11
8.3 Interdependent evaluation items for the biometric cryptosystem mechanism.....	14
8.4 Evaluation items for the cancellable biometrics mechanism	16
8.5 Interdependent evaluation items for the cancellable biometrics mechanism.....	18
9 Evaluation steps of protection techniques for the biometric template.....	20
9.1 General	20
10 Requirements and procedures of protection performance testing	21
10.1 General	21
10.2 Biometric cryptosystem.....	21
10.3 Cancellable biometrics	24
Appendix I – Algorithm list of template protection techniques.....	27
Appendix II – Evaluation example for a biometric cryptosystem mechanism using a fuzzy vault scheme	29
II.1 System description (Step 1).....	29
II.2 Vendor claim (Step 2)	29
II.3 Examination of vendor claim (Step 3).....	30
II.4 Vendor test and evaluation of vendor test	32

	Page
Appendix III – Evaluation example for cancellable biometrics using correlation-based matching	40
III.1 Introduction	40
III.2 Clarification of evaluation requirements	40
III.3 Requirements of evaluation tool.....	43
III.4 Evaluation experiment.....	44
Bibliography.....	47

Introduction

Various valuable applications using password authentication are currently in general use on the open network. However, knowledge-based authentication has some shortcomings; for example, anyone can input a leaked password. Therefore, a number of other authentication methods are considered for application on the open network.

Biometrics technologies are considered as one of the methods of authentication technology. However, they reveal some vulnerability in the open network environment. Once a biometric feature is compromised, it is unable to permanently utilize a secure authentication against the replay attack because of its unique and permanent characteristics. For these reasons, attention is focused on the biometric template protection technique.

The biometric template protection technique has a specific renewal property. If a stored biometric reference has been compromised from the server, the administrator can renew the reference for a secure authentication.

Recently, various protection techniques have been proposed and the following documents have provided standard specifications to protect biometric data, based on these techniques: ISO 24745: *Biometric information protection*, ITU-T X.1088: *Telebiometrics digital key framework (TDK)* and ITU-T X.1090: *Authentication framework with one-time telebiometric templates*.

This Recommendation standardizes the guideline for evaluating protection performance of these techniques.

Recommendation ITU-T X.1091

A guideline for evaluating telebiometric template protection techniques

1 Scope

This Recommendation:

- establishes a general guideline for testing and evaluating the performance of biometric template protection techniques based on biometric cryptosystem or cancellable biometrics;
- clarifies targets of two biometric template protection mechanisms for evaluation reference models in telebiometric systems;
- clarifies evaluation items of each biometric template protection technique;
- defines the protection performance metrics for each biometric template protection technique;
- specifies requirements and procedures of evaluation methods.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

- [ITU-T X.1086] Recommendation ITU-T X.1086 (2008), *Telebiometrics protection procedures – A guideline to technical and managerial countermeasures for biometric data security*.
- [ITU-T X.1090] Recommendation ITU-T X.1090 (2011), *Authentication framework with one-time telebiometric templates*.
- [ISO 19792] ISO/IEC 19792:2009, *Information technology – Security techniques – Security evaluation of biometrics*.
<http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=51521>
- [ISO 19795-1] ISO/IEC 19795-1:2006, *Information technology – Biometric performance testing and reporting – Part 1: Principles and framework*.
<http://webstore.iec.ch/webstore/webstore.nsf/ArtNum_PK/42119?OpenDocument>
- [ISO 19795-2] ISO/IEC 19795-2:2007, *Information technology – Biometric performance testing and reporting – Part 2: Testing methodologies for technology and scenario evaluation*.
<http://webstore.iec.ch/webstore/webstore.nsf/ArtNum_PK/42120?OpenDocument>
- [ISO 19795-3] ISO/IEC TR 19795-3:2007, *Information technology – Biometric performance testing and reporting – Part 3: Modality-specific testing*.
<http://webstore.iec.ch/webstore/webstore.nsf/ArtNum_PK/41184>
- [ISO 24745] ISO/IEC 24745:2011, *Information technology – Security techniques – Biometric information protection*.
<http://www.iso.org/iso/catalogue_detail?csnumber=52946>

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 attacker [ISO 19792]: Person seeking to exploit potential vulnerabilities of a biometric system.

3.1.2 biometric (adjective) [b-ITU-T X.1084]: Of or having to do with the field of biometrics.

3.1.3 biometric data [ISO 24745]: Biometric sample or aggregation of biometric samples at any stage of processing, biometric reference, biometric probe, biometric feature or biometric property.

NOTE – Biometric data need not be attributable to a specific individual, i.e., Universal Background Models.

3.1.4 biometric reference [ISO 24745]: One or more stored biometric samples, biometric templates, or biometric models attributed to a biometric data subject and used for comparison.

3.1.5 biometric sample [ISO 24745]: Analogue or digital representation of biometric characteristics prior to biometric features being extracted and obtained from a biometric capture device or biometric capture subsystem.

3.1.6 biometrics (noun) [b-ITU-T X.1084]: An automated recognition of individuals based on their behavioural and biological characteristics.

3.1.7 challenge response [b-ITU-T X.1124]: A method of protecting against replay attack. For example, if entity A wants to obtain a new message from entity B, it can first send a challenge in the form of a nonce (e.g., a cryptographic value that is used only once) to B. A then receives a response from B, based on the nonce that proves B was the intended recipient.

3.1.8 evaluator [ISO 19792]: Person or party responsible for performing a security evaluation of a biometric product.

3.1.9 false match rate (FMR) [ISO 19795-1]: Proportion of zero-effort impostor attempt samples falsely declared to match the compared non-self template.

NOTE – The measured/observed false match rate is distinct from the predicted/expected false match rate (the former may be used to estimate the latter).

3.1.10 false non-match rate (FNMR) [ISO 19795-1]: Proportion of genuine attempt falsely declared not to match the template of the same characteristic from the same user supplying the sample.

NOTE – The measured/observed false non-match rate is distinct from the predicted/expected false non-match rate (the former may be used to estimate the latter).

3.1.11 key [b-ITU-T X.800]: A sequence of symbols that controls the operations of encipherment and decipherment.

3.1.12 one-way function [b-ITU-T X.509]: A (mathematical) function f which is easy to compute, but which for a general value y in the range, it is computationally difficult to find a value x in the domain such that $f(x) = y$. There may be a few values y for which finding x is not computationally difficult.

3.1.13 renewability [ISO 24745]: Generic ability to allow the creation of multiple, independent transformed biometric references from one or more biometric samples obtained from the same data subject for the purposes of enhancing security and privacy.

3.1.14 revocability [ISO 24745]: Ability to prevent future successful verification of a specific biometric reference and the corresponding identity reference.

3.1.15 user [ISO 19792]: Person interacting with a biometric system.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 Biometric cryptosystem mechanisms

3.2.1.1 biometric cryptosystem mechanism: A mechanism for authentication with a conventional cryptographic protocol using a cryptographic key generated from secret data. The secret data are extracted from helper data that are created from the biometric reference of the user.

3.2.1.2 helper data: Information that depends on biometric reference that enables the restoration of keys in a biometric cryptosystem. If a key is exposed, it can be cancelled and renewed.

NOTE – Synonyms are auxiliary data (AD) in [ISO 24745], help data and other information and data.

3.2.1.3 key control: A part of the key output process that is a method of enabling only a genuine user to create and restore the key.

NOTE 1 – Key generation: a type of key control that is a method of generating helper data by transforming concealment by using biometric reference and a cryptographic key. Only a genuine user can generate a valid key.

NOTE 2 – Key hiding, key release: a type of key control that is a method of generating helper data by encrypting the cryptographic key using a biometric reference. Only a genuine user can decrypt the key.

3.2.1.4 key output: A process to extract a cryptographic key from a biometric feature after fluctuations have been eliminated. The extraction of the key is classified into key generation and key hiding.

3.2.1.5 key regeneration: A function to regenerate a key by modifying helper data.

3.2.1.6 key restoring: A situation where a concealed key is restored from helper data by attackers or through unintended procedures.

3.2.1.7 secret sharing: A method of dividing a key into a number of segmentations and restoring it by assembling the segmentations.

3.2.1.8 verification function: A function to verify the validity of a cryptosystem mechanism by decrypting data created by the cryptosystem mechanism using a verification key.

3.2.1.9 verification key: A key used for verification. A public key in a PKI system is felled into a verification key.

3.2.2 Cancellable biometrics mechanisms

3.2.2.1 cancellable biometrics mechanism: Authentication mechanisms whose matching process utilizes transformed biometric data by using a secret parameter. Renewing the secret parameter can disable a cancellable template.

NOTE – There are similar terms such as "revocable" and "renewable"; however, these terms imply the meaning of a mechanism for protecting templates including biometric cryptosystems. Therefore, "cancellable", which does not imply the meaning of a mechanism for biometric cryptosystems will be used in this Recommendation.

3.2.2.2 cancellable template: Enrolled data in a server that are used for a cancellable biometrics mechanism.

3.2.2.3 cancellable transformation: A function to transform biometric data by using a secret parameter in a cancellable biometrics mechanism.

3.2.2.4 comparison function: A function to compare similarity between a registered cancellable template and transformed biometric data during a verification process.

3.2.2.5 comparison score: A similarity value by comparing a registered cancellable template and transformed biometric data through a comparison function.

3.2.2.6 secret parameter: A parameter to be used in a transformation function to conceal biometric data for a cancellable biometrics mechanism. This parameter should be kept secret from servers and third parties.

3.2.2.7 secret parameter generation function: A function to generate a secret parameter. A general cipher function such as a pseudo-random generator and a symmetry cipher function can be used for this function.

3.2.2.8 transformed biometric sample: Data that are generated by a transformation function using captured biometric data from a sensor in an authentication process.

3.2.3 Evaluation process

3.2.3.1 diversity: The variety of transformed biometric samples generated from a single biometric sample in the cancellable biometrics mechanism. Transformed biometric samples should not match other transformed biometric samples generated from the same biometric sample.

3.2.3.2 restoring rate: The proportion of samples of attacker attempts to be restored from concealed biometric data or a concealed key.

NOTE 1 – Key restoring rate includes both imposter trials and genuine trials.

NOTE 2 – The rate at which biometric data is restored from help information should be an evaluation target in a biometric cryptosystem mechanism. The rate at which biometric data is restored from a transformed biometric template or transformed biometric data should be an evaluation target in a cancellable biometrics mechanism.

3.2.4 General

3.2.4.1 authentication process: A process to check the validity of the claimed identity of an entity.

3.2.4.2 enrolment process: A process to create and store enrolment data for a template protection biometric mechanism.

3.2.5 Template protection techniques (commonly used)

3.2.5.1 concealment of biometric data function: A function to create helper data and a cancellable template to prevent an attacker from restoring biometric data using exposed helper data. Biometric data are transformed so that they can never be restored.

3.2.5.2 dummy information: Information that is in the same form as actual biometric data but is different from a genuine user's biometric data.

3.2.5.3 dummy information scheme: A technique to conceal the biometric data from third parties by adding a lot of dummy information.

NOTE – This is called "chaff" in a biometric encryption mechanism using a fuzzy vault scheme.

3.2.5.4 elimination of fluctuations: A technique to prevent the performance of verification from degrading due to fluctuations in the process of acquiring biometric data through biometric sensors.

3.2.5.5 error correcting code (ECC): Redundant data that are attached to biometric data to eliminate fluctuations. (In this case, the fluctuations are eliminated when the number of errors is within the permissible range.)

3.2.5.6 fluctuation: A variation in biometric samples of the same person that is determined by the capturing environment.

3.2.5.7 quantization function: A function to transform biometric data from continuous values to discrete values. The wider a quantization interval becomes in this process, the larger the quantization error will be.

3.2.5.8 secret partition: A method of storing registered information by dividing the information into several segments.

NOTE 1 – Enrolment data are helper data and act as verification keys for a biometric cryptosystem mechanism.

NOTE 2 – Enrolment data have a secret parameter and a cancellable template for a cancellable biometrics mechanism.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ECC	Error Correcting Code
FMR	False Match Rate
FNMR	False Non-Match Rate
PKI	Public Key Infrastructure

5 Conventions

This Recommendation does not require any specific conventions.

6 Overview of protection techniques for the biometric template on telecommunication systems

6.1 Biometric cryptosystem mechanism

The biometric cryptosystem uses encryption technology to dynamically generate unique encryption keys from the biometric data of each user. Similar to common encryption-based authentication techniques, a hash value of the key data is stored in the server and this hash value is used for comparison (as with password authentication), or a PKI authentication scheme can be utilized with the public key stored on the server and the generated key data can be used as a private key. In both cases, key data cannot be available on the server (i.e., biometric data are concealed), so these methods can be used as a secure method of protecting user privacy.

The basic architecture of authentication systems using the biometric cryptosystem is shown in Figure 1. The authentication mechanism in the client can be divided into two main functions: the first function generates a user's private key K_P created from the user's biometric reference, and the second function verifies the user based on cryptographic technology with the generated key.

In general, biometric data are not the same, due to various factors such as positioning, contamination (e.g., dirt and stains), ageing and environmental noise. However, it is necessary to generate a unique, stable key for each user from this non-uniform data in order to enable people to use authentication with encryption techniques. Helper data, W , that depend on biometric sample, B , are used in the process of generating the key to satisfy this requirement. The user's private key, K_P , is temporarily generated for authentication. The biometric cryptosystem mechanism is able to renew keys K_P and K_V , which correspond to key K_P by regenerating helper data W . Consequently, this mechanism will provide the specific security requirements of "renewability" in [ISO 24745].

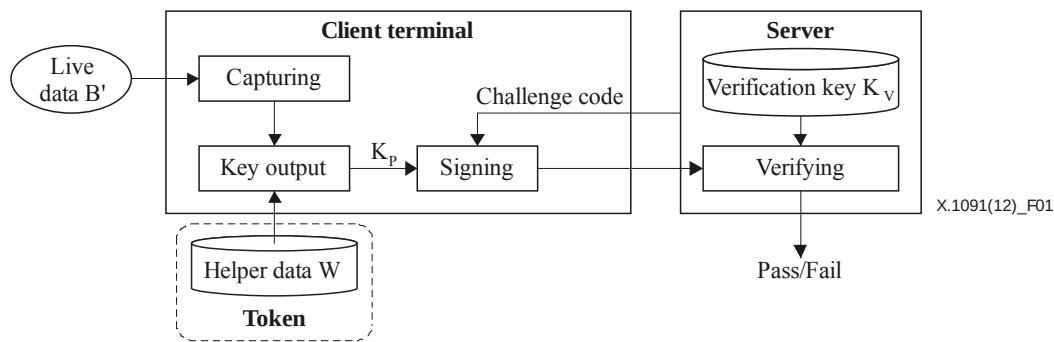


Figure 1 – Functional architecture of the biometric cryptosystem

6.2 Cancellable biometrics mechanism

Cancellable biometrics, proposed in [b-Ratha1], are a method of authentication to protect privacy in biometrics, where biometric data are transformed with a secret parameter before being registered on a server. Consequently, original biometric data are not revealed during the authentication of client/server biometric data.

The basic mechanism underlying a cancellable biometrics system is shown in Figure 2. $F_U(B')$ is obtained from biometric data B' and the transformation function F_U with parameter U which is stored in a client, or in a token. A user's biometric data B have been transformed by the same function F_U in advance in the enrolment process, and $F_U(B)$ also has been obtained. $F_U(B)$ is stored in the server database. The server calculates a score according to the similarity of B' to B by comparing $F_U(B)$ with $F_U(B')$. Where $F_U(B)$ or U is revealed, U can be replaced with U' by deleting $F_U(B)$ and re-registering $F_{U'}(B)$, and security can be retained without a user's biometric data.

However, cancellable biometrics are not effective against replay attacks if $F_U(B')$ is eavesdropped through a communication channel. A technology to protect the template that takes this into account is proposed in [b-Nagai] as an asymmetrical means of authenticating biometrics. This system uses a zero knowledge verification protocol to make it possible to authenticate a user without showing biometric data to the server.

The cancellable biometrics mechanism is able to renew parameter U and transform template $F_U(B)$ without a re-enrolment process. Therefore, this mechanism can provide the specific security requirements of "renewability" in [ISO 24745].

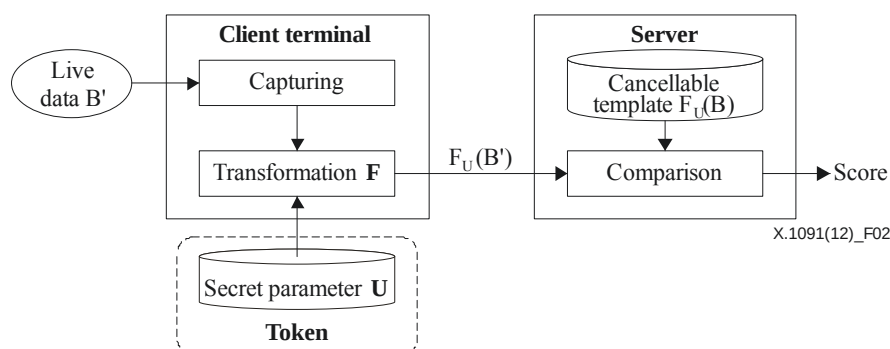


Figure 2 – Functional architecture for cancellable biometrics

7 Reference models of protection techniques for a biometric template

7.1 Reference model of a biometric cryptosystem mechanism

In this Recommendation, biometric template protection techniques are divided into two major types of telebiometric authentication systems. However, each type has some different algorithms. Hence, this Recommendation defines a reference model for each protection technique type. These reference models make it easy for an evaluator to assign functions of an intended mechanism to functional components in the model.

The following clauses describe each reference model, technical components of each protection technique type and specific threats that may arise. Figure 3 shows two fundamental reference models for the biometric cryptosystem mechanism.

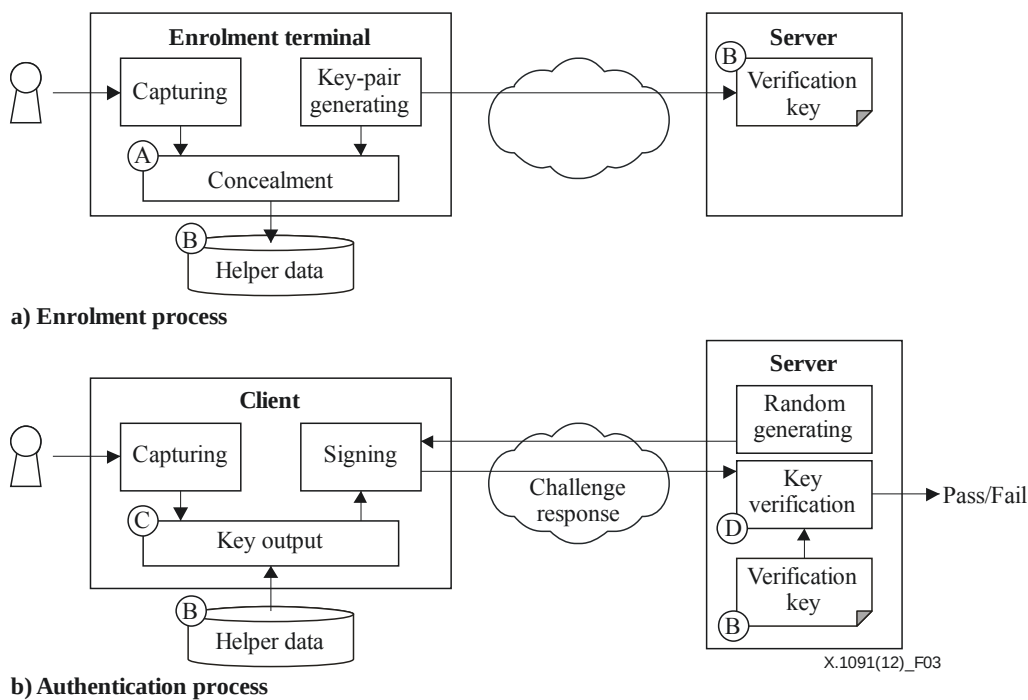


Figure 3 – Reference models for the biometric cryptosystem mechanism

The following list categorizes technical components on the biometric cryptosystem mechanism. Technical components are categorized with respect to functional components in Figure 3 (A) to (D). Technical components can be used for picking up evaluation items and interdependency items in clause 8. Depending on the target of evaluation, one or more technical components are selected for each functional component.

Technical components on the enrolment process

A) Concealment function

- 1) Secret sharing scheme: A scheme to conceal biometric data by dividing biometric data into a number of segmentations and restoring them by assembling the segmentations.
- 2) Dummy information scheme: A scheme to conceal the biometric data from third parties by adding a lot of dummy information.
- 3) One-way function scheme: A scheme to conceal the biometric data x using (mathematical) function f (it is computationally difficult to find a biometric data x in the domain such that $f(x) = y$).

B) Data management function

- 1) Secret partition scheme: A scheme that will make it difficult to restore biometric data by secure partitioning helper data.

Technical components on authentication process

C) Key output function

- a) Elimination of fluctuations
 - 1) Quantization scheme: A scheme to transform biometric data from continuous values to discrete values. The wider a quantization interval becomes in this process, the larger the quantization error will be.
 - 2) Error correcting code scheme: A scheme to attach redundant data to biometric data to eliminate fluctuations. (In this case, the fluctuations are eliminated when the number of errors is within the permissible range.)
- b) Key control
 - 1) Key generation scheme: A scheme to generate a valid key using a biometric reference.
 - 2) Key hiding scheme: A scheme to decrypt a key from helper data using a biometric reference.

D) Key verification function

A function to verify whether there is a genuine person on the server side by checking the encryption key generated in the client using a verification key.

7.2 Reference model for a cancellable biometrics mechanism

Figure 4 shows a representative reference model for the cancellable biometrics mechanism.

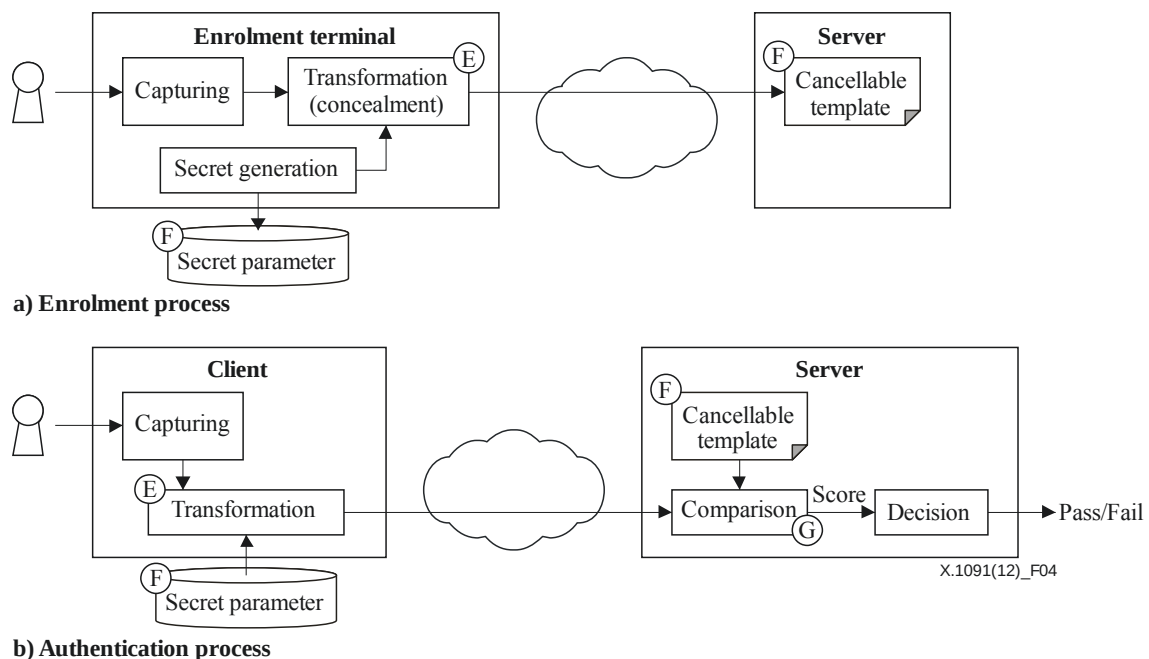


Figure 4 – Reference model for the cancellable biometrics mechanism

The following list categorizes technical components on the cancellable biometrics mechanism. Technical components are categorized with respect to functional components in Figure 4 (E) to (G). Technical components can be used for picking up evaluation items and interdependency items in clause 8. Depending on the target of evaluation, one or more technical components are selected for each functional component.

Technical components on enrolment process

E) Transformation (concealment) function

- 1) Geometrical deformation scheme: A scheme to conceal biometric data by changing the original shape of biometric data with user specific parameters. It is difficult to find a biometric datum without knowing user specific parameters.
- 2) One-way function scheme: A scheme to conceal the biometric data x using (mathematical) function f (it is computationally difficult to find a biometric data x in the domain such that $f(x) = y$).
- 3) Dummy information scheme: A scheme to conceal the biometric data from third parties by adding a lot of dummy information.

F) Data management function

- 1) Secret partition: A scheme that will make it difficult to restore biometric data by secure partitioning helper data.

Technical components on authentication process

G) Server process

- a) Elimination of fluctuations
 - 1) Quantization scheme: A scheme to transform biometric data from continuous values to discrete values. The wider a quantization interval becomes in this process, the larger the quantization error will be.
 - 2) Error correcting code scheme: A scheme to attach redundant data to biometric data to eliminate fluctuations. (In this case, the fluctuations are eliminated when the number of errors is within the permissible range.)
- b) Comparison
 - 1) Score calculation scheme: A function to verify whether there is a genuine person on the server side by checking biometric data and the cancellable template, which are both cancellable and transformed through the authentication process.

7.3 Specific threats for reference models

This Recommendation describes the evaluation items of all reference models using template protection techniques. Specific threats are able to indicate the need for evaluating the protection performance.

Specific threats are able to clarify the requirements for protecting the templates of target systems and are also able to clarify the reasons for which evaluation items are employed and their priorities.

This Recommendation excludes threats to a general biometric system that are already described in [ITU-T X.1086]. It should be noted that biometric systems using template protection techniques have threats and vulnerabilities. Consequently, in addition to this Recommendation, other Recommendations and standards such as [ISO 19792], [ISO 19795-1] and [ISO 19795-2] should be referred to for evaluation.

7.3.1 Specific threats for the biometric cryptosystem mechanism

The points at which the biometric cryptosystem mechanism is threatened are presented in Figure 5.

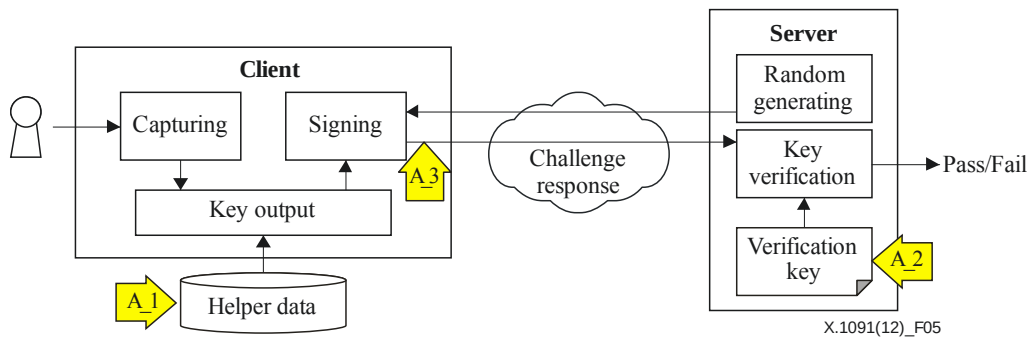


Figure 5 – Points at which the biometric cryptosystem mechanism is threatened

Threat point A_1

- Biometric data are analysed or disclosed by an attacker who has obtained leaked helper data.
- Disclosed biometric data are used for physical/electronic impersonation.
- A signing key is analysed or disclosed by an attacker who has obtained leaked helper data.
- A disclosed signing key is used for electronic impersonation.

Threat point A_2

- A signing key is analysed or disclosed by an attacker who has obtained a leaked verification key.
- A disclosed verification key is used for electronic impersonation.

Threat point A_3

- A signing key is disclosed by an attacker who has eavesdropped a challenge code (random code) and a response code (signature).
- A disclosed signing key is used for electronic impersonation.

7.3.2 Specific threats for the cancellable biometrics mechanism

The points at which the cancellable biometrics mechanism is threatened are outlined in Figure 6.

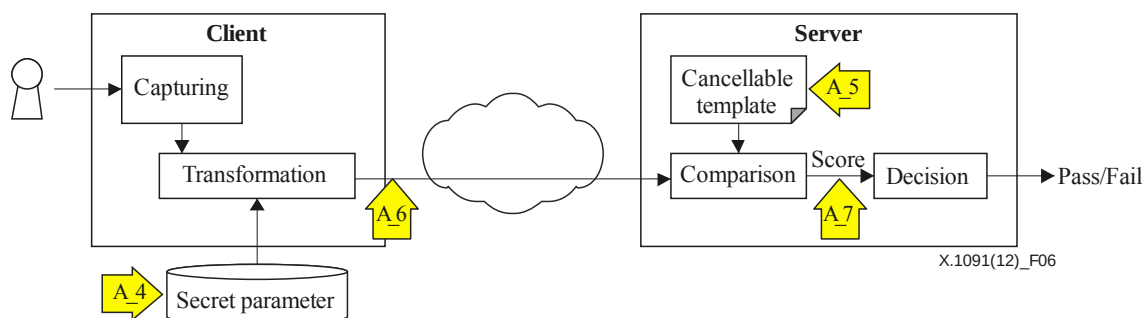


Figure 6 – Points at which the cancellable biometrics mechanism is threatened

Threat point A_4

- An impersonation by an attacker who has obtained a leaked secret parameter.