

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.1086

(11/2008)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Information and network security – Telebiometrics

**Telebiometrics protection procedures – Part 1:
A guideline to technical and managerial
countermeasures for biometric data security**

Recommendation ITU-T X.1086

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

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

Recommendation ITU-T X.1086

Telebiometrics protection procedures – Part 1: A guideline to technical and managerial countermeasures for biometric data security

Summary

Recommendation ITU-T X.1086 defines the requirements of guidelines to provide security countermeasures for the telebiometrics protection procedures. This Recommendation defines the vulnerabilities and threats in operating telebiometric systems, and proposes a general guideline for security countermeasures, from both technical and managerial perspectives, in order to establish a safe environment for the use of telebiometric systems and to protect individual privacy.

This Recommendation describes countermeasures that allow the protection of biometric devices as related to their installation, removal, and delivery. Countermeasures are proposed for the protection of biometric systems as related to their operational procedures, as well as the roles and responsibilities of personnel involved in system design. It is expected that the proposed countermeasures will ensure the security and reliability of the flow of biometric information in a telecommunications environment.

Source

Recommendation ITU-T X.1086 was approved on 13 November 2008 by ITU-T Study Group 17 (2009-2012) under Recommendation ITU-T A.8 procedures.

Keywords

Telebiometrics authentication models, telebiometrics countermeasures, telebiometrics protection guideline, telebiometrics vulnerabilities.

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 2010

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

CONTENTS

Page

1	Scope	1
2	References.....	1
3	Definitions	1
3.1	Terms defined elsewhere	1
3.2	Terms defined in this Recommendation.....	2
4	Abbreviations and acronyms	3
5	Conventions	3
6	Components and vulnerabilities of a biometric system.....	3
7	Protection of biometric input devices	6
7.1	Vulnerabilities	6
7.2	Guidelines for protection.....	7
8	Protection of the process of transmitting biometric raw data.....	7
8.1	Vulnerabilities	7
8.2	Guidelines for protection.....	7
9	Protection of the signal processing component	8
9.1	Vulnerabilities	8
9.2	Guidelines for protection.....	8
10	Protection of the process of transmitting extracted biometric templates.....	9
10.1	Vulnerabilities	9
10.2	Guidelines for protection.....	9
11	Protection of the biometric template comparison component	9
11.1	Vulnerabilities	9
11.2	Guidelines for protection.....	9
12	Protection of the storage	10
12.1	Vulnerabilities	10
12.2	Guidelines for protection.....	10
13	Protection of the process of transmitting data from the registration to the storage.....	10
13.1	Vulnerabilities	11
13.2	Guidelines for protection.....	11
14	Protection of the process of transmitting results from the comparison component	11
14.1	Vulnerabilities	11
14.2	Guidelines for protection.....	11
15	Protection of the registration	11
15.1	Vulnerability.....	12
15.2	Guideline for protection	12
16	Protection of the biometric template decision component	12
16.1	Vulnerability.....	12

	Page
16.2 Guideline for protection	12
17 Protection of the process of transmitting the stored biometric templates.....	12
17.1 Vulnerabilities	12
17.2 Guidelines for protection	12
18 Protection of the process of transmitting results from the decision component.....	13
18.1 Vulnerabilities	13
18.2 Guidelines for protection	13
Annex A – Check list for usage of telebiometric system mechanism	14
Appendix I – Check list for the application of telebiometric protection procedures.....	15
I.1 Definition of check list	15
I.2 Check list of items	15
Appendix II – Biometric verification process model.....	18
Appendix III – Comparison between vulnerabilities and threats.....	20
Appendix IV – Replay attacks on telebiometrics.....	22
IV.1 Definition of a replay attack	22
IV.2 Countermeasures for replay attack	22

.....

Recommendation ITU-T X.1086

Telebiometrics protection procedures – Part 1: A guideline to technical and managerial countermeasures for biometric data security

1 Scope

This Recommendation proposes a general guideline for security countermeasures, from both technical and managerial perspectives, that would allow for the protection of biometric information against various threats, such as hijacking, modification and illegal access, from the point of its creation to its disposal in a telecommunications environment. Also this Recommendation proposes countermeasures for the protection of biometric systems as related to their operational procedures, as well as the roles and responsibilities of personnel involved in system design. From a technical point of view, this Recommendation proposes several countermeasures to ensure data integrity, mutual authentication, and confidentiality. From a managerial perspective, this Recommendation describes countermeasures that allow for the protection of biometric devices as related to their installation, removal, and delivery.

Not in the scope of this Recommendation is defining security requirements for biometric data and biometric security algorithms.

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.1084] Recommendation ITU-T X.1084 (2008), *Telebiometrics system mechanism – Part 1: General biometric authentication protocol and system model profiles for telecommunications systems*.
- [ISO 19092] ISO 19092 (2008), *Financial services – Biometrics – Security framework*.
- [ISO/IEC 19784-1] ISO/IEC 19784-1 (2006), *Information technology – Biometric application programming interface – Part 1: BioAPI specification*.
- [ISO/IEC 19785-1] ISO/IEC 19785-1 (2006), *Information technology – Common Biometric Exchange Formats Framework – Part 1: Data element specification*.
- [ISO/IEC 19795-1] ISO/IEC 19795-1 (2006), *Information technology – Biometric performance testing and reporting – Part 1: Principles and framework*.
- [ISO/IEC 24761] ISO/IEC 24761 (2009), *Information technology – Security techniques – Authentication context for biometrics*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 biometric [ISO/IEC 19785-1]: Pertaining to the field of biometrics.

NOTE – "biometric" should never be used as a noun.

3.1.2 biometrics [ISO/IEC 19785-1]: Automated recognition of individuals based on their behavior and characteristics.

3.1.3 biometric data [ISO/IEC 19785-1]: A biometric sample at any stage of processing, biometric reference, biometric feature, or biometric property.

3.1.4 biometric product [ISO/IEC 19785-1]: A software or hardware product or a combination of software and hardware, which is assigned a biometric product identifier by a CBEFF biometric organization called the biometric product owner of the biometric product.

3.1.5 biometric sample [ISO/IEC 19785-1]: Information obtained from a biometric device, either directly or after further processing.

3.1.6 biometric system [ISO 19092]: Automated system capable of capturing, extraction, matching and returning a decision (match/ non-match).

3.1.7 biometric template [ISO/IEC 19784-1]: A biometric sample or combination of biometric samples that is suitable for storage as a reference for future comparison.

3.1.8 capture [ISO/IEC 19785-1]: Acquisition of a biometric sample.

3.1.9 enrolment [ISO 19092]: Process of collecting biometric samples from a person and the subsequent generation and storage of biometric reference templates associated with that person.

NOTE – See also initial enrolment and re-enrolment.

3.1.10 extraction (feature extraction) [ISO/IEC 19785-1]: Process of converting raw biometric data into processed biometric for use in template comparison or reference template creation.

3.1.11 identification [ISO/IEC 19795-1]: Application in which a search of the enrolled database is performed, and a candidate list of 0, 1 or more identifiers is returned.

3.1.12 registration [ISO/IEC 19785-1]: The process in which a person shall prove their identity by presenting credentials to the biometric service provider before being allowed to enroll, and assigns an electronic identifier.

3.1.13 score (scoring) [ISO/IEC 19784-1]: Value indicating the degree of similarity or correlation between a biometric sample and a biometric reference template.

3.1.14 template [ISO/IEC 19785-1]: Data, which represents the biometric measurement of an individual, used by a biometric system to execute biometric matches.

3.1.15 threshold [ISO/IEC 19785-1]: Point above which the degree of similarity between two compared templates is sufficiently high to constitute a "match", and below which the degree of similarity between two compared templates is sufficiently low to constitute a "non-match".

NOTE – Thresholds can often be adjusted at an administrative level to decrease the false match rate or to decrease the false non-match rate.

3.1.16 verification [ISO/IEC 19795-1]: Biometric measures are compared to the enrolled template for the claimed identity, and an accept or reject decision regarding the identity claim is returned.

NOTE – The claimed identity might be in the form of a name, personal identification number (PIN), swipe card, or other unique identifier provided to the system.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 biometric data auditor: An independent third-party auditing organization, or a member thereof, given the task of protecting privacy.

3.2.2 biometric data manager: A person who collects, manages, or utilizes biometric data.

3.2.3 biometric data provider: An individual who provides his or her biometric data for the purposes of personal identification.

3.2.4 biometric feature: Concise representation of information extracted from a biometric sample by applying a mathematical transformation.

3.2.5 biometric reference: One or more stored biometric samples, biometric templates, or biometric models attributed to a subject and used for comparison.

3.2.6 managerial protection countermeasures: Protection countermeasures regarding biometric data protection policies, biometric data protection organizations, outsider security, information property classification, information protection education and training, and business continuity management.

NOTE – A biometric data provider must prepare all the necessary procedures required to access and manage users' biometric data, and enforce relevant employees such that they understand and comply with them. The biometric data provider must assign a manager with the authorization to access the biometric data, and provide the ID and password to the manager when processing users' biometric information using computers. In this case, the service provider, etc., should periodically renew the respective password/s.

3.2.7 technical protection countermeasures: Human security, physical security, system development security, code control, access control, operation management, electronic transaction security, security accident administration, control of reviewing, monitoring and auditing.

NOTE – Examples are prevention of computer viruses by installing and operating a vaccine program, security countermeasures used to safely transmit personal information over a network by use of encoded algorithms, installation and operation of an access control device such as an entry blocking system, and other technical measures required to secure safety.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ASP	Application Service Provider
FAR	False Acceptance Rate
PKI	Public Key Infrastructure
TTP	Trusted Third Party
USB	Universal Serial Bus

5 Conventions

None.

6 Components and vulnerabilities of a biometric system

The first step in taking technological protection measures for biometric data is to accurately identify the target and scope that required protection. Thereafter, establishing biometric data policies is the second step. In order to be able to reflect the technological protection measures on the protection policies, technical staff who are able to entirely understand and implement the proposed policies, and decision-makers who have the authorization to execute these policies, must participate in the process and work together effectively.

When a biometric system is installed or organized including the mechanism for the protection of the biometric data, an authorized data auditor supervises the auditing process, and the audit results will be open to public in cases where the biometric system is to be used in a more complicated and extended manner than initially designed.

One or more sub-processes are executed on a biometric processing unit. And one or more biometric processing units become biometric verification processes. A biometric processing unit is the abstract concept of a security domain, such as a sensor, a smart card, a storage device, or software running on a personal computer. Appendix II describes the functions of five sub-processes in a biometric verification process model.

Figure 1 describes a biometric system through a network, illustrating how a client acquires personal information and biometric data, thereafter transmitting them to a server installed at the aforementioned biometric step.

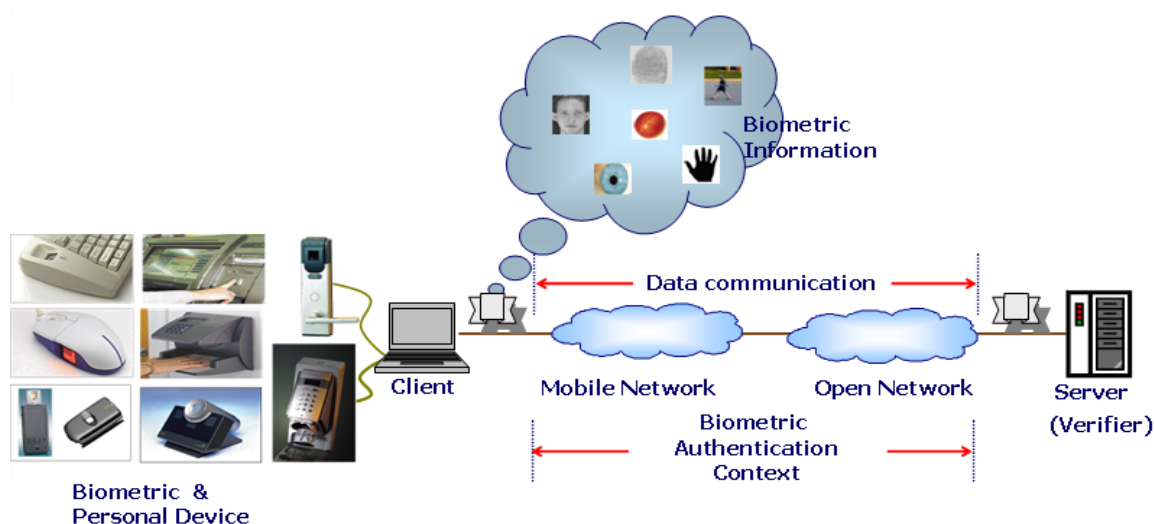


Figure 1 – Telebiometric model

Figure 2 illustrates the threats associated with the biometric component through a network in the biometric verification process model (see Appendix II). In this model, each component sends processed biometric data to the next component (see clause 5.1 of [ISO/IEC 24761]). Compared to a general biometric functional model, in a telebiometric functional model, processed biometric data can be transmitted between components through telecommunication media as denoted by *NW* in Figure 2. Figure 2 describes not only each component in the model but also the points where the transmission between the components is vulnerable to outside attacks. Examples of outside attacks are invasion when biometric data are delivered to the next step, or modification of processed biometric data.