

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.1087

(10/2016)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Information and network security – Telebiometrics

Technical and operational countermeasures for telebiometric applications using mobile devices

Recommendation ITU-T X.1087

ITU-T

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
PKI related Recommendations	X.1340–X.1349
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
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699

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

Recommendation ITU-T X.1087

Technical and operational countermeasures for telebiometric applications using mobile devices

Summary

Biometric technology in mobile devices is frequently used in various areas which require a high level of reliability such as e-banking, and procurement services. It is necessary to make efforts to develop a security system that can pre-emptively cope with potential security threats for the purpose of ensuring mobile biometric data security. Since biometric technology handles sensitive personally identifiable information (PII), some of the privacy issues for biometric in mobile devices should be considered.

Recommendation ITU-T X.1087 specifies the implementation model and threats in the operating telebiometric systems in mobile devices. It provides a general guideline for security countermeasures from both the technical and operational perspectives in order to establish a safe mobile environment for the use of telebiometric systems.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1087	2016-10-14	17	11.1002/1000/13061

Keywords

E-payment, fast identity on-line, FIDO, mobile device, telebiometric applications, telebiometric authentication model.

* To access the Recommendation, type the URL <http://handle.itu.int/> in the address field of your web browser, followed by the Recommendation's unique ID. For example, <http://handle.itu.int/11.1002/1000/11830-en>.

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 2017

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.....	2
4	Abbreviations and acronyms	2
5	Conventions	3
6	Prerequisites.....	3
7	Authentication models	3
7.1	Overview	3
7.2	Model 1.....	4
7.3	Model 2.....	5
7.4	Model 3.....	5
7.5	Model 4.....	6
7.6	Model 5.....	6
7.7	Model 6.....	7
7.8	Model 7.....	8
7.9	Model 8.....	8
7.10	Model 9.....	8
7.11	Model 10.....	9
7.12	Model 11.....	10
7.13	Model 12.....	10
8	Vulnerabilities of telebiometrics mobile devices	11
8.1	Insufficient application programming interface management.....	11
8.2	Insecure wireless channels	11
9	Security threats for each model	11
	Appendix I – Use cases.....	16
I.1	Micro secure digital (SD)-based approach match on card using applet.....	16
	Appendix II – Mobile storage study for biometrics.....	18
II.1	Off-card comparison.....	18
II.2	On-card comparison (sensor-off-card)	18
II.3	Work-sharing on-card comparison	19
II.4	System-on-card comparison	20

	Page
Appendix III – Use case study for mobile payment services.....	21
III.1 Type A Pay payment procedure	21
III.2 Type B Pay payment procedure	21
III.3 Type B Pay's built-in security.....	22
Bibliography.....	25

Copyright © 2016, IHS Markit. All rights reserved.

Recommendation ITU-T X.1087

Technical and operational countermeasures for telebiometric applications using mobile devices

1 Scope

This Recommendation provides a framework to ensure security and reliability of the flow of biometric information for telebiometric applications using mobile devices. This Recommendation defines 12 telebiometric authentication models depending on the configuration of the biometric sensor, the mobile device, and the server. It also specifies the threats in the operating telebiometric systems in the mobile devices and proposes a general guideline for security countermeasures from both the technical and operational perspectives in order to establish a safe mobile environment for the use of telebiometric systems.

The following topics are addressed within the scope of this Recommendation:

- Telebiometric security reference models in operating telebiometric systems using a mobile device including cloud computing services.
- General related threats and countermeasures to ensure security and reliability for telebiometric applications using mobile devices.

The related standard environment is depicted in Figure 1.

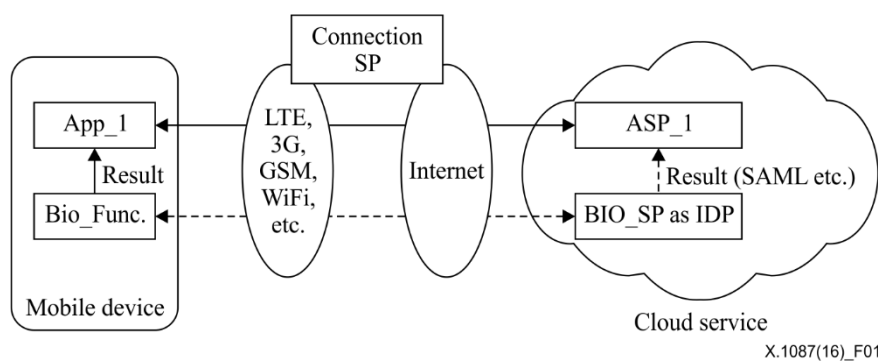


Figure 1 – Standard environment for telebiometric applications using mobile devices

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.1089] Recommendation ITU-T X.1089 (2008), *Telebiometrics authentication infrastructure (TAI)*.
- [IETF RFC 4346] IETF RFC 4346 (2008), *The Transport Layer Security (TLS) Protocol Version 1.2*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 biometric (adjective) [b-ISO/IEC 19784-1]: Pertaining to the field of biometrics.

3.1.2 biometrics (noun) [b-ISO/IEC 19784-1]: Automated recognition of individuals based on their behavioural and biological characteristics.

3.1.3 biometric reference [b-ISO/IEC 19784-1]: One or more stored biometric samples, biometric templates or biometric models attributed to a biometric data subject and used for comparison.

3.1.4 biometric sample [b-ISO/IEC 2382-37]: Analogue or digital representation of biometric characteristics prior to biometric feature extraction process.

3.1.5 biometric template [b-ISO/IEC 19784-1]: Set of stored biometric features comparable directly to probe biometric features.

3.1.6 comparison (match/matching) [b-ISO/IEC 19794-1]: Estimation, calculation or measurement of similarity or dissimilarity between biometric probe(s) and biometric reference(s).

3.1.7 comparison decision [b-ISO/IEC 2382-37]: Determination of whether the recognition biometric probe(s) and biometric reference(s) have the same biometric source, based on a comparison score(s), a decision policy(ies) including a threshold, and possibly other inputs.

3.1.8 comparison score [b-ISO/IEC 19784-1]: Numerical value (or set of values) resulting from a comparison.

3.1.9 false match [b-ISO/IEC 2382-37]: Comparison decision of "match" for a biometric probe and a biometric reference that are not from different biometric capture subjects.

3.1.10 false non-match [b-ISO/IEC 2382-37]: Comparison decision of "non-match" for a biometric probe and a biometric reference that are from the same biometric capture subject and of the same biometric characteristics.

3.1.11 match [b-ISO/IEC 2382-37]: Comparison decision stating that the biometric probe(s) and the biometric reference are from the same source.

3.1.12 mobile device [b-ITU-T X.1158]: A small, hand-held computing device with a subscriber identity module (SIM) card, typically having a display screen with touch input and/or a miniature keyboard and is not heavy.

3.1.13 non-match [b-ISO/IEC 2382-37]: Comparison decision stating that the biometric probe(s) and the biometric reference are not from the same source.

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 biometric hardware security module: A physically combined hardware consisting of a hardware security module and a biometric module equipped with one or multiple biometric sensors.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

APDU	Application Protocol Data Unit
API	Application Programming Interface
App	Application

BC	Biometric Certificate
BioAPI	Biometric Application Programming Interface
CPU	Central Processing Unit
FIDO	Fast Identity On-line
ICC	Integrated Circuit Card
ID	Identification
MNO	Mobile Network Operator
MoC	Match on Card
NFC	Near Field Communication
OS	Operating System
OTA	Over The Air
PAN	Private Access Network
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
POS	Point-Of-Sale
SD	Secure Digital
SE	Secure Element
SP	Service Provider
TSP	Token Service Provider
USB	Universal Serial Bus
USIM	Universal Subscriber Identity Module
TLS	Transport Layer Security
TSM	Telebiometrics System Mechanism
WiFi	Wireless Fidelity

5 Conventions

None.

6 Prerequisites

None.

7 Authentication models

7.1 Overview

This Recommendation takes into account the three perspectives below, dividing the models into 12 categories depending on the configuration of the biometric sensor, the mobile device, and the server. It also specifies the threats in the operating telebiometric systems in the mobile devices and proposes a general guideline for security countermeasures from both the technical and operational perspectives in order to establish a safe mobile environment for the use of telebiometric systems.

Table 1 – Authentication models

	Biometric sensor	Mobile device	Server
Model 1	Capturing	Comparison Store*	
Model 2	Capturing	Comparison	Store
Model 3	Capturing		Comparison Store
Model 4	Capturing Comparison		Store
Model 5	Capturing Comparison	Store	
Model 6	Capturing Comparison Store		
Model 7	Capturing Store	Comparison	
Model 8	Capturing Store		Comparison
Model 9	Capturing	Store	Comparison
Model 10		Capturing Comparison Store	
Model 11		Capturing	Comparison Store
Model 12		Capturing Comparison	Store
* Biometric reference template location.			

7.2 Model 1

Figure 2 illustrates model 1.

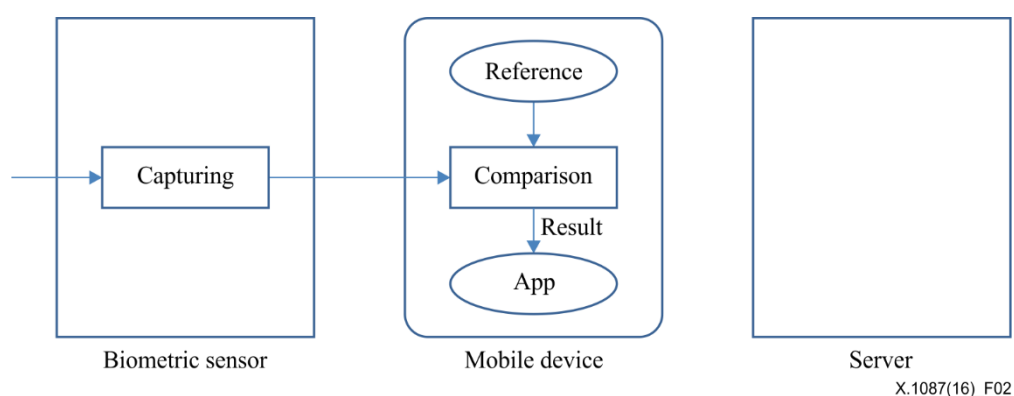


Figure 2 – Model 1

The mobile device takes the request from the application (App); it acquires sample data, compares it with the registered user's template, and transfers the result to the App.

Template identification (ID) information is required, which is the comparison result. For model 1, it is assumed that the mobile device is in a difficult situation to telecommunicate with the server including the wireless environment, and the mobile device side such as smartphones is given sufficient processing resources. The processing resources must be sufficient to acquire sample data and compare it. External biometric sensors communicate with the mobile device using near field communication (NFC) when the mobile device cannot support the sensor because of a modality or applicability characteristic. This model can be used when the server side trusts the mobile device-side processing procedures.

7.3 Model 2

Figure 3 illustrates model 2.

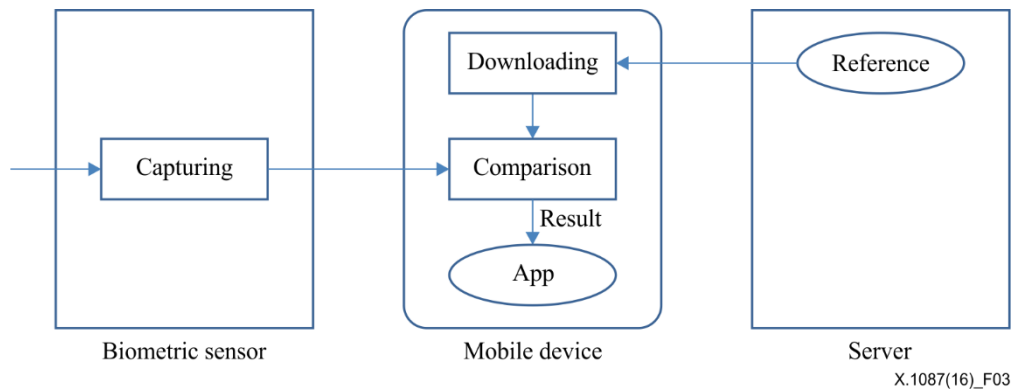


Figure 3 – Model 2

The App requests verification from the server. The server sends the registered user's template. The mobile device compares the acquired sample data with the received template, and sends the result to the App Model 2 that has the same sequence as model 1, with the exception of the transfer of the template from the server. Template ID information is required. This then forms the comparison result. Under this structure, it is recommended to use as many terminals as possible. This is suitable for the web-verification model, as users can connect to the server from any mobile device. Model 2 requires the registration of the biometric reference template with the server. This model also requires the server to trust the mobile device processing procedure.

7.4 Model 3

Figure 4 illustrates model 3.

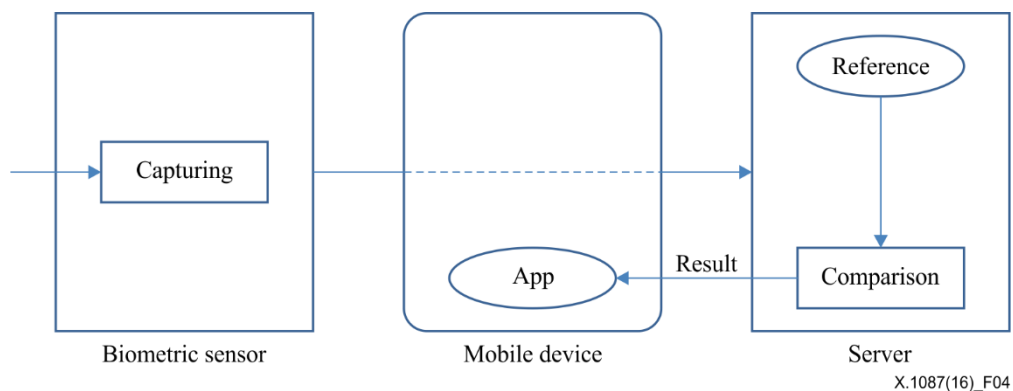


Figure 4 – Model 3