

International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1092

(06/2013)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Information and network security – Telebiometrics

Integrated framework for telebiometric data protection in e-health and telemedicine

Recommendation ITU-T X.1092



International
Telecommunication
Union

Documents
Document Sharing Hub

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.

Recommendation ITU-T X.1092

Integrated framework for telebiometric data protection in e-health and telemedicine

Summary

Recommendation ITU-T X.1092 provides an integrated framework to protect biometric data and private information in e-health and telemedicine. It defines a model of health services using telebiometrics for user identification and authentication. It identifies threats in transmitting various sensory data related to human health and provides countermeasures for secure transmission when applying the integrated framework.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T X.1092	2013-06-13	17

Keywords

Biometric-based e-health integration model, security requirements for each threat, telebiometric data protection, threats for telemedicine (e-health), use cases.

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	Terms and definitions	1
	3.1 Terms defined elsewhere	1
	3.2 Terms defined in this Recommendation.....	1
4	Abbreviations and acronyms	2
5	Relationship between the biometric e-health service model and privacy.....	2
	5.1 e-health sensor types.....	2
	5.2 Biometric information	2
	5.3 Privacy information	3
6	General overview of the integration model	3
	6.1 Functional requirements	3
	6.2 Authentication procedure	4
7	Application of the biometric-based integrated e-health model – Terminal application	5
8	Threat for telemedicine (e-health)	6
	8.1 Enhanced personal authentication	7
	8.2 Personal information leak from e-health terminal.....	7
	8.3 Use of unauthorized biosensor	7
	8.4 Use of unauthorized sensor	7
	8.5 Security protocol that ensures availability	8
	8.6 Personal information leak from centre	8
	8.7 Medical information leak from centre	8
9	Security requirements for each threat	8
	9.1 Enhanced personal authentication	8
	9.2 Personal information leak from terminal.....	8
	9.3 Unauthorized use of biometric sensor	9
	9.4 Unauthorized use of e-health sensor.....	9
	9.5 Security protocol that ensures availability	9
	9.6 Personal information leak from centre	9
	9.7 Medical information leak from the e-health centre	10
10	Countermeasures for each threat	10
	10.1 Enhanced personal authentication	10
	10.2 Personal information leaks from e-health terminal	10
	10.3 Unauthorized use of biometric sensor	10
	10.4 Unauthorized use of e-health sensor.....	10

	Page
10.5 Personal information leaks from e-health centre	10
10.6 Medical information leaks from e-health centre	10
Appendix I – Use cases.....	11
I.1 Introduction	11
I.2 Use cases	11
Bibliography.....	14

Introduction

Remote medical systems are technologies in which medical services are transmitted using computers and data communication technologies, and they are also defined as medical systems that diagnose and treat patients in remote locations. Devices are used to transmit the patient's physical information (electrocardiogram, X-rays, voice, etc.) to the hospital or doctor, which is then examined by the doctor. The doctor's instructions for treatment based on a diagnosis are then sent from the hospital to the patient to commence treatment. The patient's physical information is shared not only between the patient and doctor, but also between hospitals. However, this kind of remote medical system may be at risk of potential infringements of personal privacy, due to the disclosure of personal and medical information. For this reason, security technologies are required to protect such a system from vulnerabilities, while effectively safeguarding it against external attacks.

To provide stable biometric telemedicine and e-health services, user authentication and service aspects should be considered. Because medical services requiring user health information are provided remotely in the application of biometric telemedicine and e-health services, user identification is a highly important factor. The existing password-based user authentication system has the vulnerability of potential exposure on the open network, whereas public-key infrastructure (PKI)-based user authentication creates inconveniences regarding key management and entering electronic signature passwords. It could potentially be quite difficult for a patient suffering from a chronic disease to input their electronic signature password whenever they access the terminal for e-health services. Therefore, the introduction of biometric technology is indispensable in providing identification and also convenient in the e-health environment.

The following reasons outline why biometrics should be integrated into the telemedicine and e-health environment.

- E-health provides medical services related to a user's health and life. Therefore, if there is a single error in user authentication, fatal medical problems may arise. As a result, biometrics should be used for enhanced user identification processes.
- If sufferers of chronic diseases access e-health services, the current password or PKI-based user authentication systems are quite inconvenient, as they require the input of a password. If biometrics are adopted, user convenience will be enhanced through an authentication system that is based on physical feature information, such as the face or fingerprint.

