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

ITU-T

International Telecommunication Union

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/.

Table of Contents

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.

Recommendation ITU-T X.1092

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

1 Scope

To provide secure biometric telemedicine and e-health services, user authentication and service aspects should be considered. This Recommendation provides an integrated framework for the protection of biometric data and private information in e-health and telemedicine. It defines a model of e-health services using telebiometrics for user identification and authentication. It identifies the threats in transmitting various sensory data related to human health and provides the countermeasures for secure transmission when applying this integrated framework.

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*.

[ITU-T X.1089] Recommendation ITU-T X.1089 (2008), *Telebiometrics authentication infrastructure (TAI).*

[ISO/IEC 24761] ISO/IEC 24761:2009, *Information technology – Security techniques – Authentication context for biometrics.*

3 Terms and definitions

3.1 Terms defined elsewhere

This Recommendation uses the following term defined elsewhere:

3.1.1 e-health [b-WHO]: e-health is the transfer of health resources and health care by electronic means.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 e-health centre: Servers that hold patient information; this includes medical information and identification information (to recognize) the patients. The e-health centre is also responsible for server management.

3.2.2 e-health terminal: Gateways that transmit the collected patient's medical information to the remote medical system. This is a device for checking the diagnosis information transmitted by medical staff who have examined the patient.

3.2.3 medical staff: All users related to remote clinical services such as doctors, nurses, etc.

3.2.4 **sensor**: A device for collecting medical information of patients, and a device for collecting biometric information for user certification. It must be able to store device certifications, in order to certify the device.

3.2.5 **user**: All users related to remote medical services such as patients, medical staff, remote medical service administrations, insurance administrators, etc.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ACBio Authentication Context for Biometrics

DNA Deoxyribonucleic Acid

DoB Date of Birth

ID Identity

ID&PW Identity and Password

MAC Medium Access Layer

PIN Personal Identification Number

PKI Public-Key Infrastructure

TSM Telebiometrics System Mechanism

5 Relationship between the biometric e-health service model and privacy

The sensors measuring the well-being of a person may be either wearable or integrated into the environment.

While wearable devices are often used for user identification and hence their results may be associated with a specific user, this is not true in all cases. For example, a single heart-rate monitor might be used by many people. A method of user identification is required in order to associate the measurement data with the right person.

5.1 e-health sensor types

Wearable sensors may be attached to clothes, jewellery, wristwatches, etc., or they may be worn separately. Environmental sensors for e-health may be embedded in the house, furniture, car, etc.

5.2 Biometric information

Biometric information means information related to the authentication or identification of an individual via biometrics. It contains:

– Biometric template: set of stored biometric features comparable directly to biometric features of a recognition biometric sample.

– Biometric sample: analogue or digital representation of biometric characteristics prior to a biometric feature extraction process and obtained from a biometric capture device or biometric capture subsystem.

– Biometric feature: output of a completed biometric feature extraction process.

– Biometric reference: one or more stored biometric samples, biometric templates or biometric models attributed to a biometric data subject and used for comparison.

Biometric characteristics can be divided in two main classes:

– Physiological, related to the shape of the body. Examples include, but are not limited to, fingerprint, face recognition, deoxyribonucleic acid (DNA), palm print, hand geometry and iris recognition.

– Behavioural, related to the behaviour of a person. Examples include, but are not limited to, typing rhythm, gait and voice.

5.3 Privacy information

Privacy information (body status information for healthcare) may include the following sub-information.

– Fixed information: gender, age, height, weight and other items.

– Measurement information: body temperature, pulse, cardiac sound, electrocardiogram, blood pressure, exercise levels and other items.

– Inference information: number of steps, calories consumed, sleep hours, exercise hours and other items.

– Input information: food intake, neighbouring environment information and other items.

– Output information: sleep hours control, weight control, exercise control, risk detection/notification and other items.

6 General overview of the integration model

The following functional requirements could be defined in the integration model.

6.1 Functional requirements

– The e-health terminal is connected to the home network, and allows user authentication through an identity and password (ID&PW) or biometric authentication method. In addition, it should acquire the health and medical information from e-health sensors and send such information to the e-health centre.

– If the e-health terminal supports biometric functions, user convenience and the identification of individuals can be strengthened through approaches such as face or fingerprint recognition. Biometrics provide an appropriate authentication method for e-health, as it can authenticate users faster than ID&PW type authentication, and biometrics support more robust security.

– The repository is managed by the e-health terminal, and it stores terminal identification information, user identification information and the biometric reference. The terminal identification information includes a device certificate for the terminal or medium access layer (MAC) – device authentication information and product serial number, whereas the ID&PW are used as the user identification information. The biometric reference stores the face and fingerprint reference information in order to use them for user authentication.

– Through wired or wireless communication with e-health sensors, the e-health terminal collects health and medical information, such as the user's weight, blood pressure, blood sugar, body fat, body temperature and amount of exercise engaged in.

– The e-health centre authenticates terminals and users, stores the received health and medical information, analyses it according to the information previously received, and then checks the overall health conditions to prescribe treatment and preventive actions. If any abnormal symptoms are found, the user is contacted or an emergency process is undertaken.

– The user's health and medical information history is stored and managed in the e-health centre, in order to enable an analysis of the user's overall health and medical information.

– The repository is located inside the e-health centre, and stores the identification information to authenticate e-health terminals and individuals.

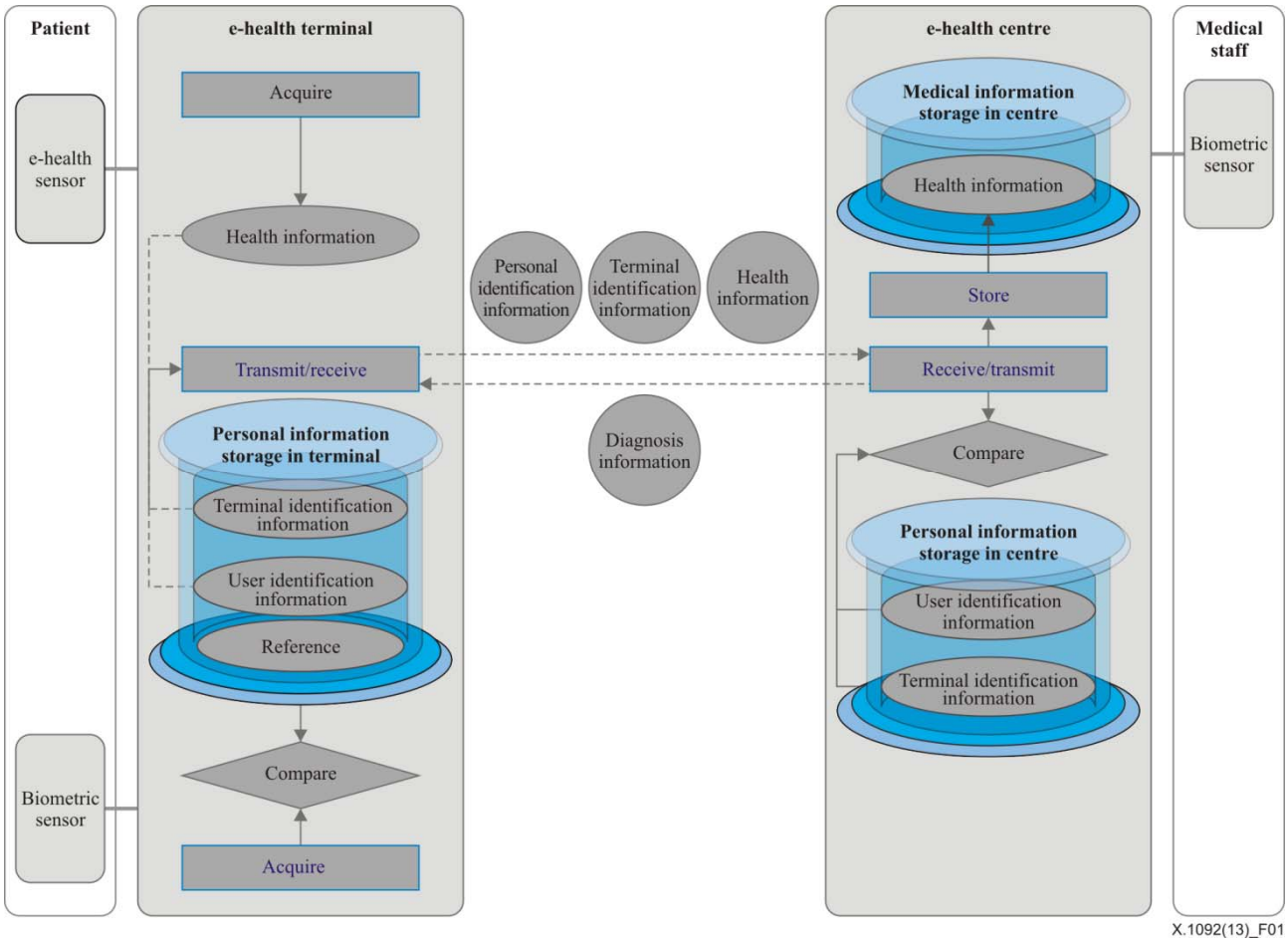

Figure 1 – Biometric-based e-health integration model

6.2 Authentication procedure

To protect personal information, the user's biometric reference is not saved in the e-health centre, but in the e-health terminal only.

The telemedicine (e-health) environment is composed of the end-user, a biometric sensor, an e-health sensor, an e-health terminal (platform), and an e-health centre; it involves a two-step authentication procedure.

– Step 1: The user performs biometric authentication at the e-health terminal using a biometric sensor.

– Step 2: The e-health terminal performs user authentication and e-health terminal authentication procedures at the e-health centre, sending the health information to the e-health centre.

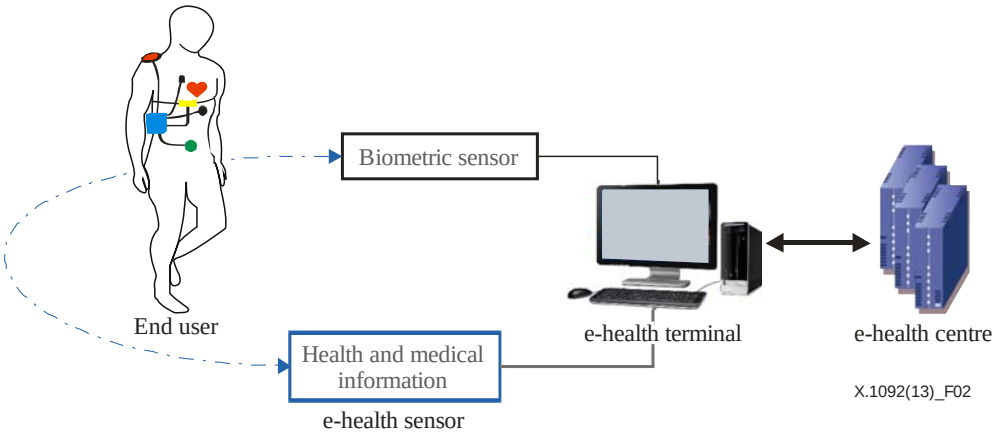

Figure 2 – Telemedicine/e-health authentication procedure

The e-health terminal maintains the registration and manages the user profile. The user profile is composed of a biometric reference, identity (ID), password, authentication key, max count, and other information. By default, the user is authenticated by 1:N authentication using the biometric reference data, and additional authentication using an ID and a password is provided. The authentication key is used for e-health sensor and e-health terminal equipment authentication, whereas the max counter information is used for e-health terminal and e-health centre equipment authentication.

The following prerequisites should be satisfied in the telemedicine/e-health environment:

– The e-health environment should have enhanced user identification processes and a lightweight protocol at the real-time level in the provision of e-health services.

– To enhance user identification, biometric authentication is performed using a biometric sensor and an e-health terminal. Authentication is carried out at the e-health terminal to improve communication speed and to protect the biometric information.

– The e-health terminal and the e-health centre should be provided with a lightweight protocol, compared with the current public-key infrastructure (PKI)-based authentication protocol.

7 Application of the biometric-based integrated e-health model – Terminal application

The terminal application is in charge of authenticating the e-health terminal user, and acquiring and sending the user's health and medical information. User authentication is required to use the e-health service; face or fingerprint recognition is used for user authentication. The terminal application acquires the health and medical information of the user, such as weight, blood pressure, body fat and body temperature, from the e-health sensors. Subsequently, it sends such information to the e-health centre, together with the information identifying the terminal and the user.

– **Server application**: The server application permits authentication using the terminal and user identification information received from the e-health terminal, and provides the appropriate medical information to the user by storing and analysing the user's health and medical information. The server application can interface with the external information system with regard to the user information, and is capable of carrying out separate contingency actions in the event of an emergency.

– **Administration application**: The administration application manages the number of connections between an e-health terminal and an e-health centre, and monitors the overall service status of the e-health centre. The e-health centre can be managed continuously, because the administrator is immediately notified of any symptoms of abnormal e-health terminal and e-health centre communication and service operation.

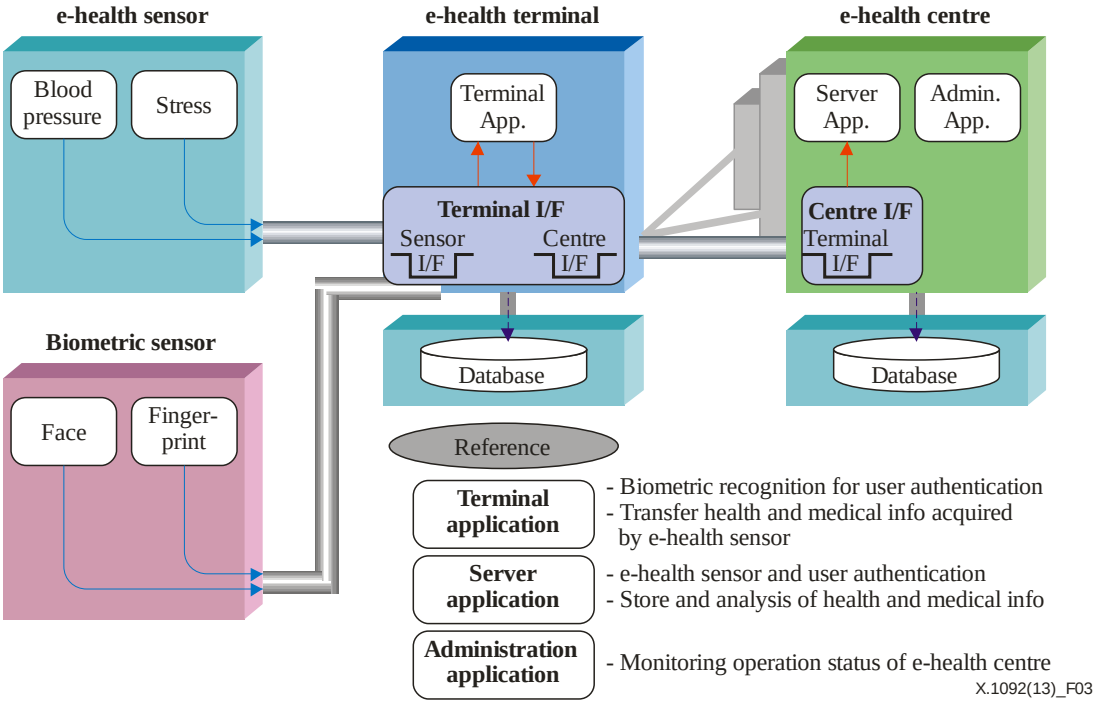

Figure 3 – Application of the biometric-based integrated e-health model

8 Threat for telemedicine (e-health)

The e-health service requires two-phase authentication, and its environment consists of the user, the biometric sensor, the e-health sensor, the e-health terminal, and the e-health centre. Figure 4 and clauses 8.1 to 8.7 describe possible threats that have been identified and could be associated with the biometric-based e-health integration model.

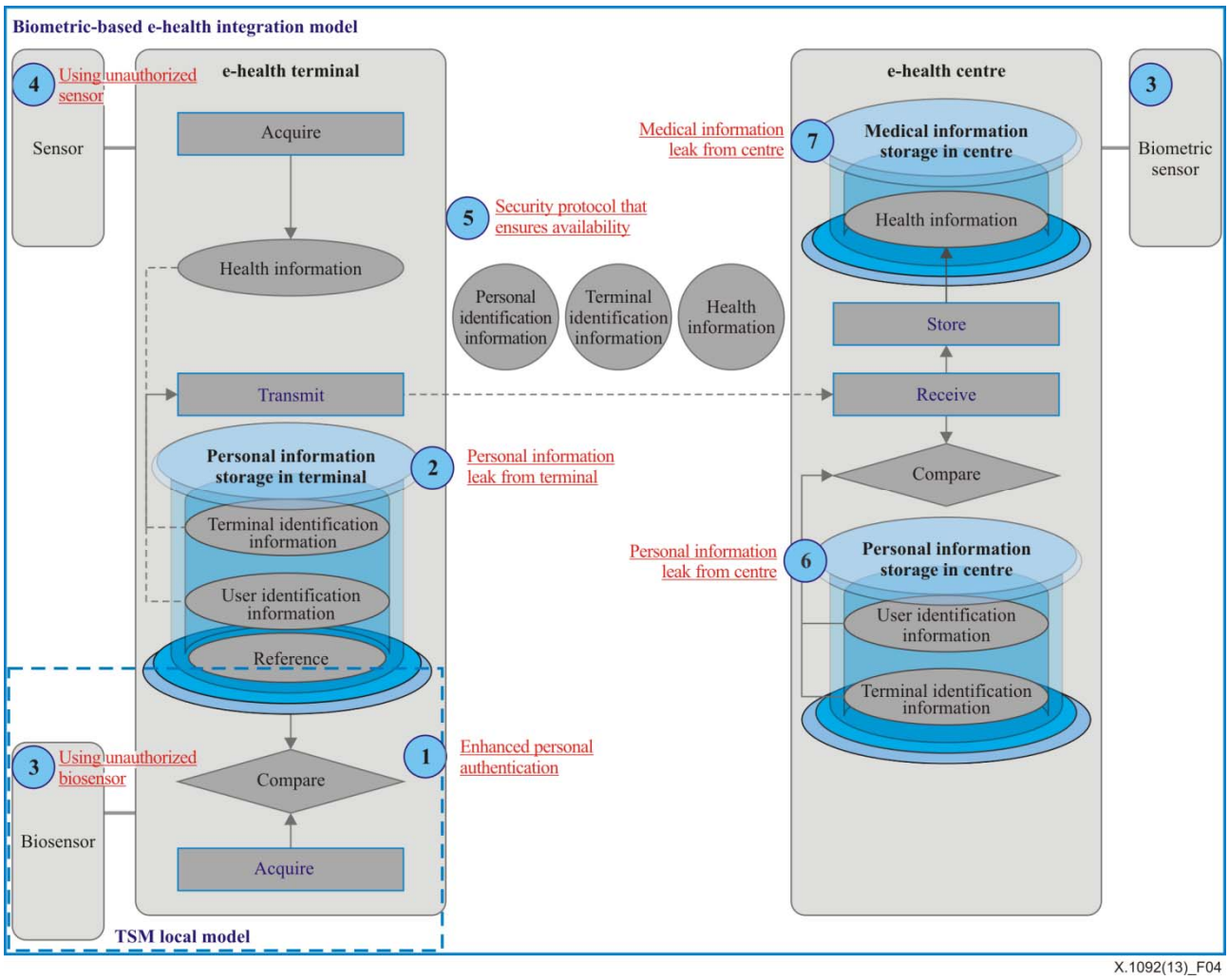

Figure 4 – Threat analysis for the biometric-based e-health integration model

There are seven threats associated with the e-health integration model. These threats are related to enhanced personal authentication, personal information leaks from the e-health terminal, unauthorized use of biosensors and sensors, security protocols that ensure availability, personal information leaks from e-health centres and medical information leaks from e-health centres.

8.1 Enhanced personal authentication

Enhanced personal authentication is used to identify the user by biosensor, and more enhanced means are required because a remote healthcare service is provided to the user.

8.2 Personal information leak from e-health terminal

It presents a possible security risk for stored information relating to user information and so on.

8.3 Use of unauthorized biosensor

There is a risk of exposing biometric information in the event of the unauthorized use of a biosensor by the e-health service.

8.4 Use of unauthorized sensor

There is a risk of exposing biometric information in the event of the unauthorized use of a sensor by the e-health service.

8.5 Security protocol that ensures availability

The e-health service requires a security protocol that ensures availability to cope with emergencies, as it provides a remote service.

8.6 Personal information leak from centre

There is a risk of exposing information stored at the e-health centre, such as user and terminal identification information.

8.7 Medical information leak from centre

There is a risk of exposing medical information stored at the e-health centre.

9 Security requirements for each threat

The following describes security requirements for each threat in the e-health integration model. Requirements include privacy protection such as un-observability, un-linkability and un-traceability, as well as conventional security requirements such as authentication, authorization, confidentiality, integrity, access control and availability.

9.1 Enhanced personal authentication

It shall have security requirements in respects of authentication, authorization and availability as below.

– Authentication: It is required to have a means of biometric authentication of the identity of the user.

– Authorization: It is required to identify which rights the authorized user has, and the users are required to be identified as a patient, doctor, medical staff, or insurance-related party.

– Availability: The authentication method requires, but is not restricted to, several conditions such as a user's age, education level, and mobility convenience when authenticating users.

9.2 Personal information leak from terminal

It shall have security requirements in respect of access control, confidentiality, integrity, un-linkability, un-observability and un-traceability as follows:

– Access control: Only authenticated/authorized users should be able to access the personal information (user information, biometric information, etc.) in the terminal.

– Confidentiality: The information in the terminal should be encrypted and stored safely.

– Integrity: The information stored in the terminal should be identical to that entered by or collected from the user.

– Un-linkability: It should not be possible for personal information to be inferred from other information.

– Un-observability: The information should not be observable from the outside when personal information stored in the terminal is being used.

– Un-traceability: When personal information stored in the terminal is used, the record should not be logged.

9.3 Unauthorized use of biometric sensor

It shall have security requirements in respect of authentication and authorization as below.

– Authentication: It is required to have a means of checking whether the biometric sensor is legal, as it is an important device for authentication.

– Authorization: It is required to check the level of confidence that a biometric sensor has, and assign different rights for each level.

9.4 Unauthorized use of e-health sensor

It shall have security requirements in respect of authentication and authorization as below.

– Authentication: It is required to have a means of checking whether the e-health sensor is legal, as it is an important device to collect a user's health information.

– Authorization: It is required to check the level of confidence that an e-health sensor has, and assign different rights for each level.

9.5 Security protocol that ensures availability

It shall have security requirements in respect of confidentiality, integrity and availability as follows:

– Confidentiality: The protocol designed to exchange the information between an e-health terminal and e-health centre and perform mutual authentication should encrypt the information contained in the protocol and transmit it securely.

– Integrity: The received information should be identical to the sent information, when exchanging the information between an e-health terminal and e-health centre using the secure communication protocol.

– Availability: It is required to use a lightweight protocol in order to reduce the burden on the e-health centre, because the information exchanged using the secure communication protocol is in large volume and could be used by many users simultaneously.

9.6 Personal information leak from centre

It shall have security requirements in respect of access control, confidentiality, integrity, un-linkability, un-observability and un-traceability as follows:

– Access control: Only authenticated/authorized users should be able to access the personal information (user information, biometric information, etc.) in the e-health centre.

– Confidentiality: The information in the e-health centre should be encrypted and stored safely.

– Integrity: The information stored in the e-health centre should be identical to that entered by or collected from the user.

– Un-linkability: It should not be allowed that personal information in the e-health centre be inferred from other information.

– Un-observability: The information should not be identifiable from the outside when personal information stored in the e-health centre is used.

– Un-traceability: When personal information stored in the e-health centre is used, the record should not be logged.

9.7 Medical information leak from the e-health centre

It shall have security requirements in respect of access control, confidentiality and integrity as follows:

– Access control: Only authenticated/authorized users should be able to access the personal information in the e-health centre.

– Confidentiality: The information in the e-health centre should be encrypted and stored safely.

– Integrity: The information stored in the e-health centre should be identical to that entered by or collected from the user.

10 Countermeasures for each threat

Proposed countermeasures are summarized in the following subclauses. Countermeasures include the TSM local model, ACBio, device certification standard, and existing standards and database security technology. Countermeasures are defined for personal information leaks from the e-health terminal, personal information leaks from the e-health centre, and a security protocol that ensures availability.

10.1 Enhanced personal authentication

In order to enhance personal authentication, biometric-based personal authentication shall be provided and shall adopt the TSM local model standard which improves privacy control over bio information (privacy protection) and reduces the biometric information load at the e-health centre (ensuring availability).

10.2 Personal information leaks from e-health terminal

In order to protect personal information leaks from the e-health terminal, technology for protecting the personal information in an e-health terminal shall be used.

The TSM local model does not define the security protocol, nor specify the technology to protect bio information reference storage.

10.3 Unauthorized use of biometric sensor

To avoid the unauthorized use of biometric sensors, [ISO/IEC 24761] shall be used.

10.4 Unauthorized use of e-health sensor

To avoid the unauthorized use of e-health sensors, device certificates shall be used according to [ITU-T X.1084] and [ITU-T X.1089].

10.5 Personal information leaks from e-health centre

To protect against personal information leaks from the e-health centre, technology to protect the personal information stored in the e-health centre shall be used.

10.6 Medical information leaks from e-health centre

To protect against medical information leaks from the e-health centre, commercial database security technology shall be used.

Appendix I

Use cases

(This appendix does not form an integral part of this Recommendation.)

I.1 Introduction

Three e-health framework use cases are presented: treatment with medical staff, preventive treatment and emergency treatment.

For each use case, there are different procedures for patient authentication and threats. For each use case, it is assumed that the patient's information is already known to the e-health framework. In other words, only registered patients shall be treated by the e-health framework.

I.2 Use cases

I.2.1 Use case 1: Treatment with medical staff

In this case, the e-health terminal is operated by medical staff. For example, a patient nursed by a visiting nurse or examined by medical staff using an e-health framework. In this situation, the patient may hesitate to input ID&PW in front of observers (medical staff). Thus, biometrics are suitable in this situation, and in contrast with the case of ID&PW, measurements by the medical staff help to build confidence in the result of authentication.

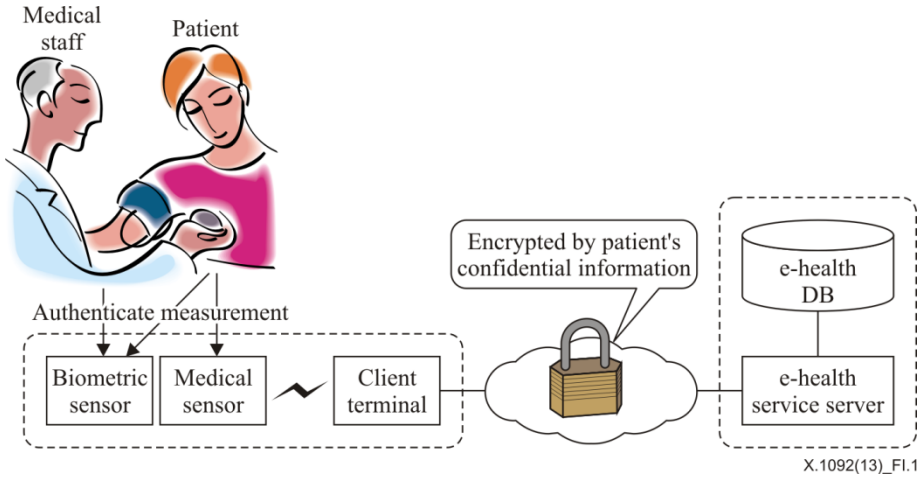

Figure I.1 – Use case 1 of the e-health framework

Usually this use case applies to the elderly at home or in a sanatorium. They are cared for and treated by medical staff.

Basic steps:

1) A medical staff member logs in to the e-health system via a terminal using biometrics, ID&PW or other authentication means.
2) A patient logs in to the e-health system via the same terminal using biometrics.
3) The medical staff member helps to measure the patient's medical information.
4) The medical staff member checks the medical history or other information of the patient.
5) All information transferred is encrypted with confidential information between the patient and the e-health system.

Security threats other than the common threats given in clause 9:

1) A medical staff member might gather the patient's biometric information (e.g., fingerprint, voice, etc.)

2) A medical staff member might gather the patient's personal information (e.g., name, DoB, PIN, address, etc.)

3) A medical staff member might gather the patient's medical history.

I.2.2 Use case 2: Regular preventive treatment without medical staff

In this case, the e-health terminal is operated by the patient. For example, a chronic disease patient buys the e-health terminal and uses it regularly. In this situation, inputting ID&PW every time it is used can be annoying for the patient. Thus, biometrics are more suitable.

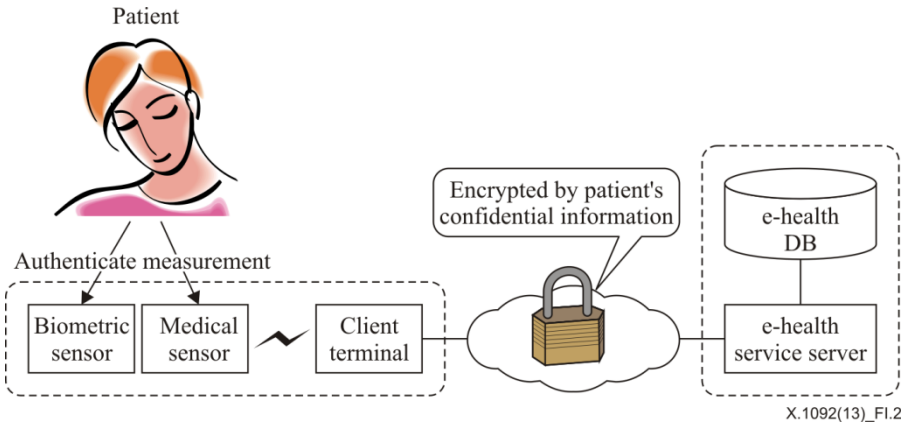

Figure I.2 – Use case 2 of the e-health framework

Usually this use case is used for chronic disease patients or ordinary people to prevent disease at home or at an e-health facility. They know the procedures for using the e-health terminal and are already registered on the e-health terminal.

Basic steps:

1) A patient logs in to the e-health system via the same terminal using biometrics.

2) The patient takes and inputs the necessary medical information by themself.

3) The patient checks their personal medical history or other information.

4) All information transferred is encrypted with confidential information between the patient and the e-health system.

Security threats other than the common threats given in clause 9: None.

I.2.3 Use case 3: Emergency treatment

In this case, the e-health terminal is operated by medical staff, for example, when a patient is taken in an ambulance, there is not enough time to input ID&PW. So, biometrics are suitable in this situation. However, if the patient becomes unconscious, parents or guardians can vouch for the patient's identity. Thus ID&PW or other authentication means might be useful. As in use case 1, the medical staff help to build confidence in the result of authentication.

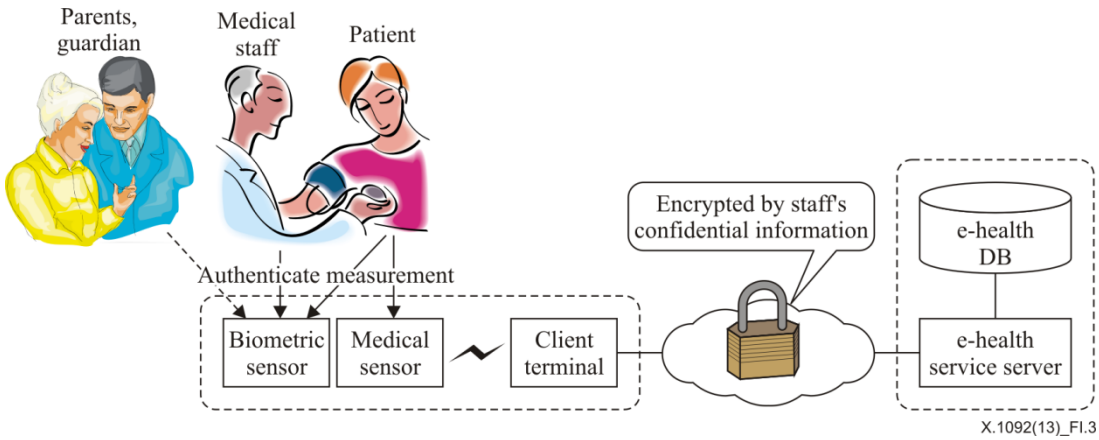

Figure I.3 – Use case 3 of the e-health framework

Usually this use case is used for unconscious patients already registered in the e-health terminal.

Basic steps:

1) A medical staff member logs in to the e-health system via a terminal using biometrics, ID&PW or other authentication means.
2) A patient (if possible, if not, parents or guardians) logs in to the e-health system via the same terminal using biometrics, ID&PW or other authentication means.
3) The medical staff member helps to measure the patient's medical information.
4) The medical staff shall check the medical history or other information of the patient.
5) All information transferred is encrypted with confidential information between the medical staff and the e-health system.

Security threats other than the common threats given in clause 9:

1) A medical staff member might gather the patient's biometric information (e.g., fingerprint, voice, etc.).
2) A medical staff member might gather the patient's personal information (e.g., name, DoB, PIN, address, etc.).
3) A medical staff member might gather the patient's medical history.

Bibliography

[b-WHO] www.who.int/trade/glossary/story021/en/index.html.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2013