International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1094

(03/2019)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Information and network security – Telebiometrics

Telebiometric authentication using biosignals

Recommendation ITU-T X.1094

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 (1)	
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 (1)	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 (2)	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1319
Smart grid security	X.1330–X.1339
Certified mail	X.1340–X.1349
Internet of things (IoT) security	X.1360–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1389
Distributed ledger technology security	X.1400–X.1429
Distributed ledger technology security	X.1430–X.1449
Security protocols (2)	X.1450–X.1459
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.1094

Telebiometric authentication using biosignals

Summary

Biometric technology in mobile devices is frequently used in various areas that require a high level of reliability, such as a smart car, e-banking, e-payment, telemedicine and e-healthcare services. In particular, it is necessary to implement countermeasures, which can pre-emptively cope with fake physiological biometrics to ensure mobile telebiometric data security, to presentation attacks. Recommendation ITU-T X.1094 specifies new secure and strong telebiometric authentication methods using biosignals.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1094	2019-03-16	17	11.1002/1000/13873

Keywords

Biosignals, biosignal sensors, telebiometric authentication model for biosignals, wearable devices.

* 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/.

Table of Contents

Recommendation ITU-T X.1094

Telebiometric authentication using biosignals

1 Scope

This Recommendation specifies biosignal sensor requirements and an architecture for a biosignal authentication model that allows mobile users to ensure personal identification using biosignals, such as those obtained from a ballistocardiogram (BCG), electroencephalogram (EEG), electrocardiogram (ECG) and photoplethysmogram (PPG), for telebiometric applications of wearable and mobile devices.

Biosignal sensor requirements and functional architecture identified in this Recommendation are intended for telebiometric applications that can provide personal identification using biosignals to meet the needs of customers, manufacturers and mobile service providers for wearable and mobile devices.

Concretely, this Recommendation covers:

– Biosignal sensor requirements and an authentication architecture for wearable and mobile devices using biosignals.

– General related secure and accurate authentication methods to ensure personal identification for telebiometric applications on wearable and mobile devices using biosignals.

This Recommendation also focuses on the functional requirements, functional architecture and mechanisms for authentication using biosignals as well as defining general requirements for telebiometric authentication using only ECG and PPG.

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 – Part 1: A guideline of technical and managerial countermeasures for biometric data security.*

3 Definitions

3.1 Terms defined elsewhere

None.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 analogue-to-digital conversion resolution: Resolution of data in regards to the number of bits used to represent each sample signal during an analogue-to-digital signal conversion.

3.2.2 biosignal: Any measureable signal in living beings (physical, chemical or electrical) that can be measured or monitored, such as a ballistocardiogram (BCG), electroencephalogram (EEG), electrocardiogram (ECG) and photoplethysmogram (PPG).

3.2.3 biosignal information: Any raw data or derived information obtained from biological signals, such as an electrocardiogram waveform.

3.2.4 biosignal sensor: An analytical device for detection of biosignals that can measure a physical quantity and convert it into a signal.

3.2.5 common mode rejection ratio (CMRR): A measure for the deviation from an ideal electrical symmetry of a device symmetrically built to its environment.

3.2.6 differential amplifier: An amplifier that has two input circuits and that amplifies the difference between the two input signals.

3.2.7 electrocardiogram: An electrophysiological monitoring is a method used to record the electrical activity of the heart over a period of time using electrodes placed on the skin. These electrodes detect the tiny electrical changes on the skin that arise from the electrophysiological depolarization pattern of the heart muscle during each heartbeat.

3.2.8 frequency bandwidth: The difference between the upper and lower frequencies measured in hertz.

3.2.9 lead: Insulated conductor having a means of connecting to a stimulator at one end and a means of connecting to an electrode at the other end, and is intended for conducting output signals from a stimulator to an electrode.

3.2.10 personal authentication: A technology that determines an individual's identity when a user wants to access secure information.

3.2.11 photoplethysmogram: An optical measurement signal of the heart rate or skin blood pulse wave by means that illuminate the skin and measure changes in light absorption.

3.2.12 signal sampling frequency: The number of samples per second, measured in hertz, taken from a continuous signal to make a discrete or digital signal.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ADC	Analog-to-Digital Converter
AES	Advanced Encryption Standard
API	Application Program Interface
BCG	Ballistocardiogram
CMRR	Common Mode Rejection Ratio
CSRK	Connection Signature Resolving Key
DB	Database
ECDH	Elliptic Curve Diffie-Hellman
ECG	Electrocardiogram
EEG	Electroencephalogram
EER	Equal Error Rate
ID	Identification

IRK	Identity Resolving Key
LTK	Long-Term Key
MITM	Man-In-The-Middle
PAD	Presentation Attack Detection
PPG	Photoplethysmogram
PII	Personally Identifiable Information
SKP	Secure Key Pair
STK	Short Term Key

5 Conventions

None.

6 Overview of biosignals

6.1 Type of biosignal

6.1.1 Electric biosignal

These are biosignals that are measured by variations in voltage, current, resistance and conductivity.

6.1.2 Mechanical – Physical biosignals

Biosignals that are determined by variables of power, acceleration, temperature, sound and pressure.

6.1.3 Optica l – Chemical biosignals

Biosignals that are measured by optical methods, including changes in chemical concentration.

6.2 Characteristics of biosignals for personal identification

Figure 1 gives an example of an electrocardiogram biosignal obtained from a wearable device sensor.

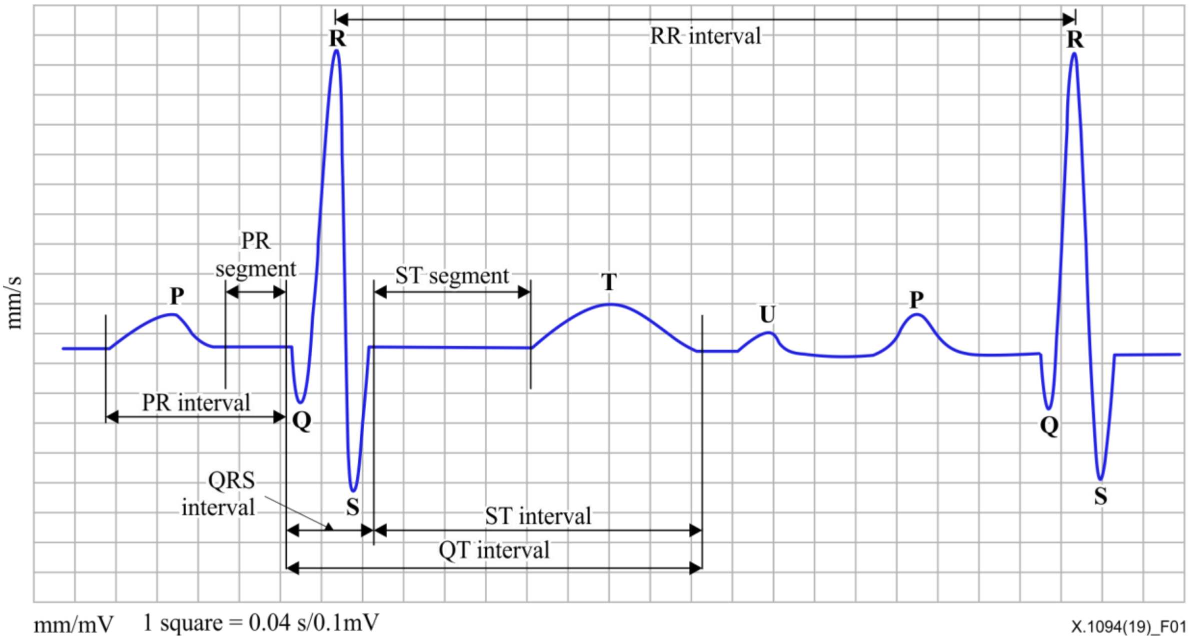


Figure 1 – Characteristics of an electrocardiogram

P wave: The first small vertical waveform represents the contraction of the atrium.

PR interval: The distance between the P wave and the QRS complex.

QRS complex: The first downward movement of the trace after the P wave is called the Q wave, then the first upward movement is the R wave. The downward movement after the R wave is the S wave – this set pattern of three waves is called the QRS complex**.**

ST segment: The distance from the end of the S wave to the start of the T wave.

PR segment: The distance from the end of the P wave to the start of the QRS complex wave.

PR interval: The distance between the P wave and the PR segment.

ST interval: The distance between the ST segment and the T wave.

RR interval: The distance between the highest point of a P wave to the highest point of the next P wave.

U wave: A small waveform after the T wave.

7 Requirements of biosignal sensors for authentication

7.1 Types of biosignal sensor on wearable devices

Types of sensor for measuring biological signals include, body implantable, body attachment, accessory, textile/clothing or embedded object**.** The body attachment type consists of a thin, flexible circuit sensor, such as a lens or patch. The accessory type is a body wearable sensor, such as a watch, spectacles or necklace. The textile/clothing type consists of a sensor placed in daily wearable items, such as a shirt, socks, underwear or shoes. A biosignal sensor must be designed for comfortable use over extended periods and to be worn on or attached to areas of the body from where it can obtain the most accurate biosignals. An ECG sensors to receive biosignal can be designed as a chest patch, socks (textile type), a watch (wrist monitor) or ankle band (foot monitor).

7.1.1 Body implantable type

The spatial resolution and signal to noise ratio of implanted sensors are excellent; nonetheless, placing a sensor within the body runs a higher risk of infection and may be inconvenient for measurement.

7.1.2 Body attachment type

Sensors attached to the body, e.g., an ECG chest sensor, require the use of a gel or an extra glue agent to ensure continuous good direct skin contact. Stable signal measurements are critical for accuracy and longevity. However, the repeated use of such agents can be uncomfortable and add the sense of a foreign body attached to the individual.

7.1.3 Accessory type

Accessory type sensors include watches, bracelets or necklaces with a built-in biosensor. The bracelet type worn around the wrist, such as a smart-watch or smart-band, to measure PPG signals is the most common.

7.1.4 Textile/clothing type

Sensors that are integrated into clothing, such as sports bras or smart shirts, can measure ECG biosignals from the chest area.

7.1.5 Embedded object type

Embedded object type sensors can be incorporated into furniture, such as a chair or a bed. A key-differentiating feature of this type is that they do not require body contact. Although such sensors enable unconscious measurement, they are susceptible to motion and environmental noise.

7.2 Functional requirements for authentication on biosignal sensors

Biosignal sensors require functional requirements depending on their characteristics. In the case of an ECG, a biosignal has a frequency bandwidth of 0.05 Hz to about 150 Hz and its signal amplitude is weak, of the order of millivolts. Therefore, the signal must be amplified and unexpected signals, such as noise signals, filtered. Pre-processed signals must be transmitted from at least one lead, which is a dry rather than a wet electrode, and require appropriate signal measurement channel sensing and protection circuits to prevent electrical surges. In addition it is also required to have an appropriate signal sampling frequency and analogue-to-digital conversion resolution that is higher than the conventionally required level.

Furthermore, since the output waveform of the signal depends on the frequency component bandwidth, a biosignal sensor system must include the minimum required bandwidth for each signal. However, the system frequency component characteristics must cover more than the 0.5 Hz to approximately 35 Hz frequency bandwidth.

The analogue signal from the lead is converted to a digital signal with an analogue-to-digital converter (ADC). Conversion speed depends on the sampling frequency, which is based on the Nyquist sampling theory. The sampled signal is quantized to a digitized value, which is a finite length bit sequence. (The length of the quantized bit sequence is the ADC conversion resolution. It affects the system characteristics.) Considering the minimum requirements of a biosignal system, the signal sampling frequency must be higher than 256 Hz and analogue-to-digital conversion resolution must be higher than 10 bit.

7.3 Data interchange format for biosignal sensors

For personal authentication using biosignals the procedures shown in Figure 2 must be followed. The procedure has a client-server structure based on sensors for biosignals and can be either separable or integral, depending on whether or not there is a communication unit.

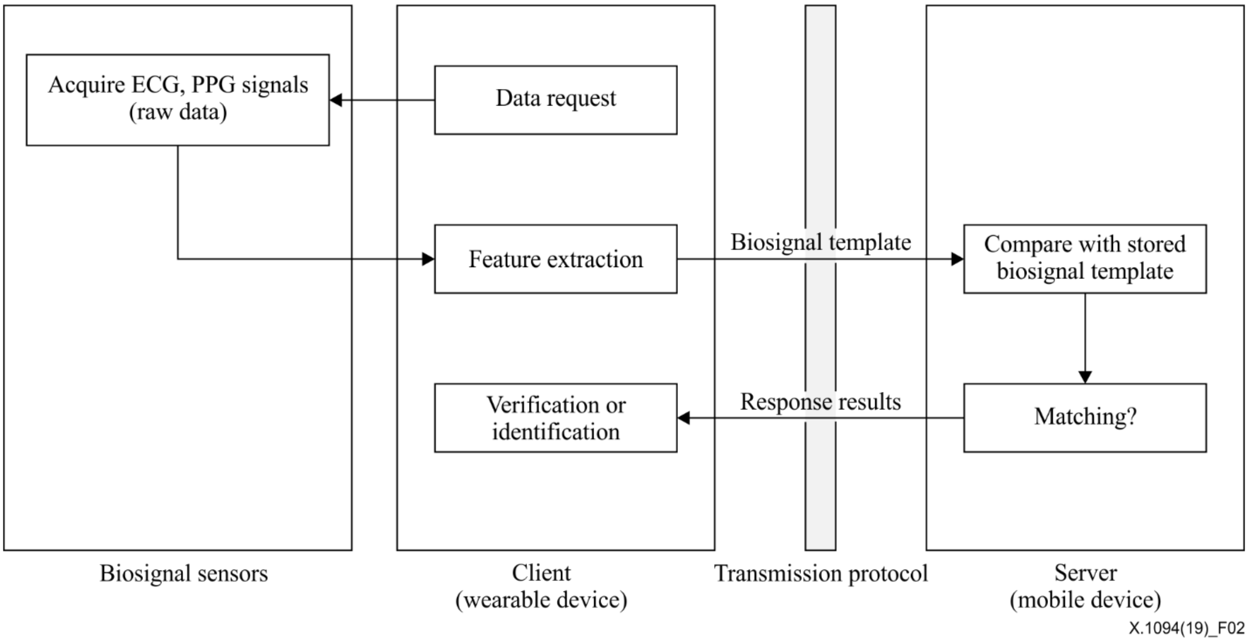


Figure 2 – Biosignal data flow for biosignal sensors based on a client-server structure

Figure 3 depicts the data interchange format for biosignal sensors. This data interchange format consists of a file header representing basic information, biosignal raw and feature data. The security block can be configured as necessary.

File header	Biosignal raw data	Biosignal feature data	Security block (Optional)

X.1094(19)_F03

Figure 3 – Data interchange format for biosignal sensors

7.3.1 File header

Figure 4 depicts the file header in the data interchange format, which consists of basic information that summarizes the characteristics of the biosignal raw and feature data, and includes sensor, time and measurement information.

		Sensor information				Time information			Measurement information					
Preamble	Length of header	Version	Biosignal type	Device ID	Manufacturer ID	Date of acquisition	Date of destruction	Measurement time	Signal indicator	Total number of channels	Signal sampling frequency	ADC resolution	Channel number	Number of consecutive acquired signal
4 bytes	4 bytes	1 byte	1 byte	1 byte	1 byte	1 byte	1 byte	1 byte	1 byte	1 byte	1 byte	1 byte	1 byte	4 bytes

X.1094(19)_F04

Figure 4 – File header

File header consists of the following information:

- preamble: the string bit signalling the beginning of a signal transmission – it indicates in binary sequence;
- length of header: given within 4 bytes;
- version: given within 1 byte;
- biosignal type: biosignal measurement sensor type;
- device ID: identification of the biosignal measurement device;
- manufacturer ID: the manufacturer identification of biosignal measurement device;
- date of acquisition: the date of biosignal acquisition;
- date of destruction: the date of biosignal data destruction;
- measurement time: the time of acquiring the biosignal;
- signal indicator: the type of measured biosignal – it distinguishes between ECG and PPG;
- total number of channels: the total number of channels in measured biosignal within 1 byte;
- signal sampling frequency: sampling frequency of the biosignal converted digitally;
- ADC resolution: the ADC resolution of the digital biosignal in the bit stream;
- channel number: the number of the corresponding channel;
- number of consecutive acquired signal: the sequence number of a consecutive acquired signal using continuous authentication.

7.3.2 Biosignal raw data

The raw data format of a biosignal consists of a length header indicating the length of the raw data, signal quality and raw data array measured from biosignal sensors.

7.3.3 Biosignal feature data

7.3.3.1 Electrocardiogram feature data

The electrocardiogram feature data is given Table 1.

Table 1 – Electrocardiogram feature data format

	Features	Notation	Data type	Data size byte
Amplitude	RQ amplitude RS amplitude RP amplitude RT amplitude	RQ_A RS_A RP_A RT_A	unsigned integer	4
Interval	PR interval PR segment QT interval ST segment ST interval RpeaktoPonsetsegment RpeaktoPpeaksegment RpeaktoPoffsetsegment RpeaktoQpeaksegment RpeaktoSpeaksegment RpeaktoTonsetsegment RpeaktoToffsetsegment RR interval	PRI PRS QTI STS STI RPL RP RPR RQ RS RTL RTS RR	unsigned integer	13
Angle	Angle Q Angle R Angle S	∠Q ∠R ∠S	unsigned integer	3

7.3.3.2 Photoplethysmogram feature data

Table 2 lists the PPG feature data format, which can be divided into the time and frequency domains. The time domain feature is also composed of time interval, amplitude and angle.

Table 2 – Photoplethysmogram feature data format

	Features	Notation	Data type	Data size byte
Amplitude	Amplitude of maximum of PPG Amplitude of minimum PPG I_{onset}/I_{DC} Amplitude from minimum to maximum of PPG Amplitude from minimum of dicrotic notch to maximum of PPG	I_{onset} I_{DC} I_{onset}/I_{DC} I_{AC} PP_A	unsigned integer	8
	Amplitude from maximum of dicrotic notch to maximum of PPG	PP_B		

Table 2 – Photoplethysmogram feature data format

	Features	Notation	Data type	Data size byte
	PP_A/I_{AC} PP_B/I_{AC}	PP_A/I_{AC} PP_B/I_{AC}		
Interval	Time from minimum to minimum of dicrotic notch in PPG	T_A	unsigned integer	6
	Time from minimum to maximum of dicrotic notch in PPG	T_B		
	Time from maximum of first derivative to minimum of dicrotic notch in PPG	TD_A		
	Time from maximum of first derivative to maximum of dicrotic notch in PPG	TD_B		
	Time from maximum to minimum of dicrotic notch in PPG	TS_A		
	Time from maximum to maximum of dicrotic notch in PPG	TS_B		
Angle	Slope from maximum to minimum of dicrotic notch in PPG	Slope A	unsigned integer	4
	Slope from maximum to maximum of dicrotic notch in PPG	Slope B		
	Slope A normalized with I_{AC}	Slope A_{norm}		
	Slope B normalized with I_{AC}	Slope B_{norm}		

7.3.4 Security block

The security block is optional and contains additional security parameters. It indicates whether or not all biosignal data are signed and if the raw or feature data of biosignal are encrypted.

8 Architecture of telebiometric authentication model for biosignals

8.1 Overview

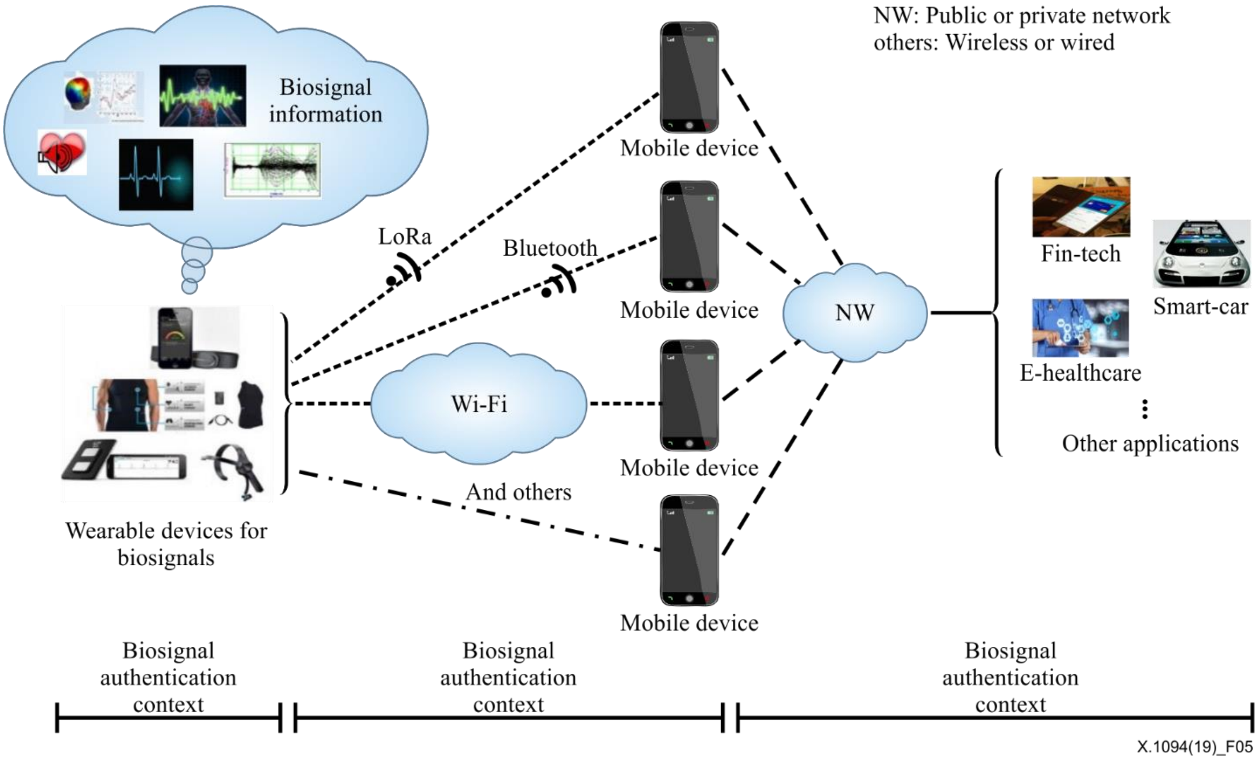

NW: Public or private network
others: Wireless or wired
Biosignal information
Mobile device
LoRa
Bluetooth
Mobile device
NW
Wi-Fi
Mobile device
And others
Mobile device
Wearable devices for biosignals
Fin-tech
Smart-car
E-healthcare
Other applications
Biosignal authentication context
Biosignal authentication context
Biosignal authentication context
X.1094(19)_F05

Figure 5 – Telebiometric authentication model for biosignals

8.2 Functional requirements for biosignal authentication mechanism

8.2.1 Data acquisition and pre-processing

A biosignal is measured from the biosignal sensors and is pre-processed for signal optimization before the feature is extracted. Biosignal raw data are pre-processed through analogue or digital filters. Each filter should be optimized to minimize power line noise or noise due to motion artifacts. The original signal, filtered by optimized frequency bandwidth, is converted to a digital circuit through an ADC, and the converted data are ready for the extraction of feature points.

8.2.2 Feature extraction and registration on a biosignal database

Individual characteristic feature points are extracted from the biosignal. An algorithm extracts biosignal features that minimize intravariability and maximize intervariability for each biosignal characteristic. Biosignal features can be extracted as time domain-based features, such as peak amplitude, duration and shape, or frequency domain-based features, such as frequency, power and coherence. Extracted biosignal features are registered on a database (DB). If the same user tries to authenticate later, the biosignal feature dataset is loaded on to the DB through the ID and the user is authenticated through feature point comparison.

8.2.3 Matching algorithm

In the 1:1 matching method, registered biosignal feature data are compared one-to-one with the feature data of the user attempting authentication. When the user tries to authenticate, the features extracted from the measured biosignal are compared with the registered features on the DB. The user's ID is presented and the registered biosignal feature from the DB is loaded as shown in Figure 6. A similarity score between features is calculated and the results are passed if the score exceeds a threshold level. The similarity score should be calculated through objective mathematical calculations, such as Euclidean distance or Mahalanobis distance.

In 1:*N* authentication, the data of the user to be authenticated are compared with all the data on the registration DB. Since the biosignal input is compared with all the biosignal data on the DB, the matching process must be repeated as many times as the number of registered people on the DB. In this analysis process, it is preferable that a majority of agreement analysis methods are used in order to increase the reliability of the calculation of the agreement, and a process of comprehensively evaluating the results of the calculation is also required. A person who has the highest degree of agreement may be judged to be a recognition requester and the result should be provided.

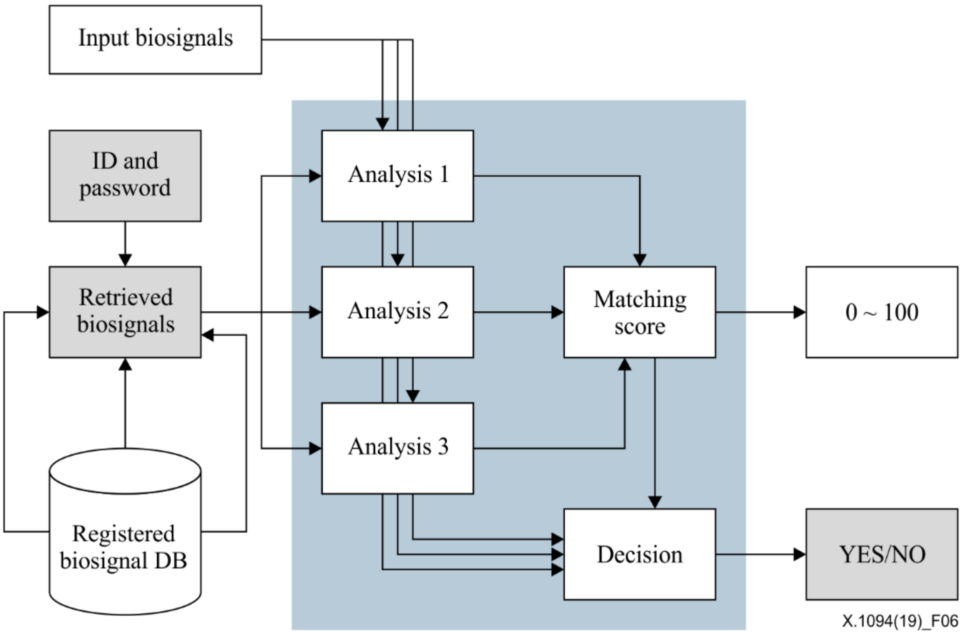


Figure 6 – Biosignal authentication process (1:1 matching)

8.3 Functional requirements for biosignal transmission protocols

This clause defines the functional requirements for a biosignal transmission protocol. Transferred biosignal data must demonstrate a certain measure of compliance, interoperability and security. A biosignal transmission protocol is an application protocol and is implemented in combination with standards-based communication protocols whether wired or wireless. Figure 7 depicts a biosignal transmission protocol between a biosignal sensor and mobile device.

The biosignal transmission protocol defines methods for discovery, secure pair bonding, transmission, reception and connection termination.

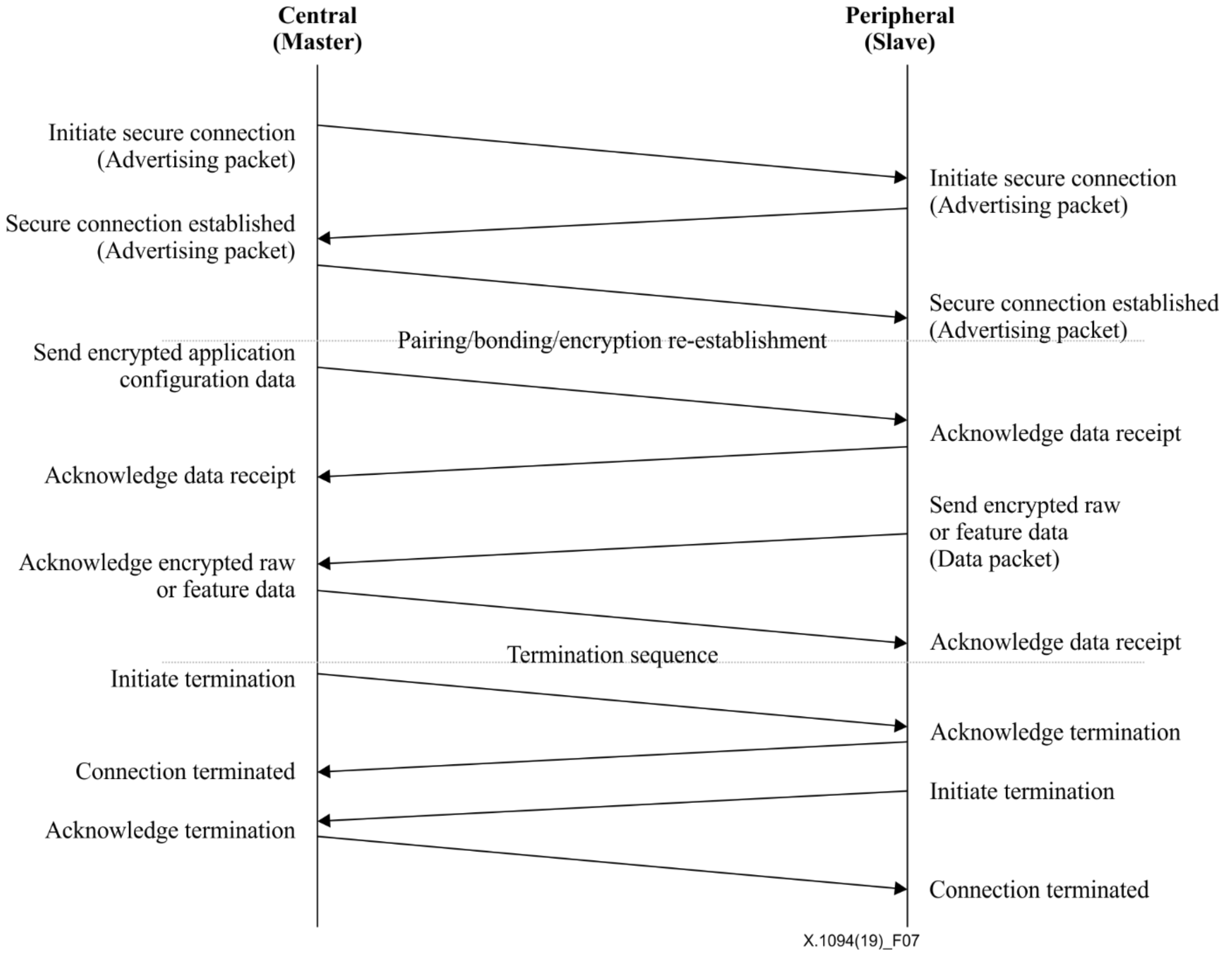


Figure 7 – Biosignal transmission protocol between a biosignal sensor and a mobile device

A biosignal transmission protocol is required for functional modes such as discovery, pairing or connecting, connection, security, transmission of biosignal raw and feature datasets and a termination sequence.

8.3.1 Discovery

The discovery mode uses an enquiry mode to discover nearby devices. If two devices know absolutely nothing about each other, one must run an enquiry to try to discover the other and its location. One device sends out the enquiry request and any device listening for such a request responds with its address, and possibly its name and other information. The procedure may also discover the device address, clock, class of device field and a list of services supported by the device. The protocol may include a device-filtering procedure, such as a white list, that prevents the scanning device from discovering all devices in a given area.

8.3.2 Pairing or connecting

Pairing is the process of forming a connection between two devices, that is, the host and the device. Before this connection can be initiated, each device needs to know the address of the other, which is found during the enquiry process. At this point, a secure session is implemented, ensuring privacy. The security goal pairing is to protect against passive eavesdropping and man-in-the-middle (MITM) attacks, which constitute active eavesdropping. The master initiates the pairing procedure by sending a pairing request to slaves. If security procedures are not initiated by the master, a slave can request a master to initiate them. Once the security requests have been received by the slave, the master reinitiates the pairing process.

8.3.3 Connection

Upon completion of the pairing process, the two devices enter a secure connection state. While connected, a device can be either actively participating or put into a low power sleep mode. Different modes determine how active the connection mode is maintained. For instance, in a high power mode, the two devices may remain active, where the device is actively transmitting or receiving data. To benefit from power saving, devices can enter a sniffing mode in which the on-time duty cycle is smaller, and devices only listen for transmission at set intervals, such as 100 ms. For better power saving, a hold mode can be used to put the device to sleep for a defined period and then to revert to active mode when that interval has passed. The master can command a slave device to hold connection.

8.3.4 Security

Security must be implemented using features such as, pairing, bonding, device authentication, encryption and message integrity. The role of pairing is to create one or more shared keys. The host generates a private and public key pair and secure connection is created by taking factors from both devices participating in creating the communication. A master and slave exchange identity resolving key (IRK) is required for device identity and a connection signature resolving key (CSRK) for authentication of unencrypted data. Short term keys (STKs) are generated based on a selected pairing method, such as just works, passkey entry and out of band. Generated secure key pairs (SKPs) are used to establish a secure channel between the participating devices. Bonding is the function for storing keys generated during the pairing sequence for use in subsequent connections in order to retain the bond between the trusted device pair. After STK generation and encryption of the links, transport specific keys are distributed. Keys to be distributed are determined by the pairing request and response parameters. Keys exchanged in this phase can include the long-term key (LTK), IRK and signature key. Device authentication verifies that the master and slave have the same keys. Encryption encodes the message in such a way that only the authorized parties can access it, ensuring message confidentiality. The keys are generated by the host that encrypts the messages. The minimum form of encryption is in accordance with the 256 bit advanced encryption standard (AES). Elliptic curve Diffie-Hellman (ECDH) initially exchanges the keys over a publicly insecure channel and then enables secure channel communication between the devices participating in the process.

Lastly, the application protocol must utilize a message-integrity function to protect against message forgeries. Even while devices are not paired, devices can still maintain data privacy by signing it. The sender uses a CSRK to sign the data and the receiver verifies the signature. On successful signature verification, the receiver assumes that a message has arrived from a trusted source.

Figure 8 describes secure channel session for security.

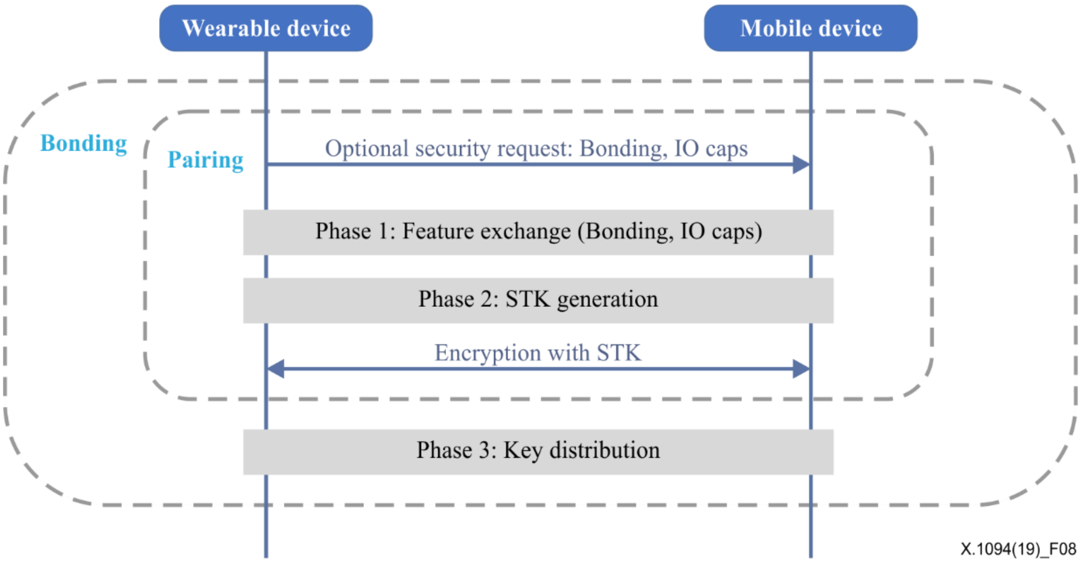

Wearable device
Mobile device
Bonding
Pairing
Optional security request: Bonding, IO caps
Phase 1: Feature exchange (Bonding, IO caps)
Phase 2: STK generation
Encryption with STK
Phase 3: Key distribution
X.1094(19)_F08

Figure 8 – Security enablement during pair and bonding

8.3.5 Transmission for biosignal raw and feature datasets

Upon successful completion of the secure registration and aliveness protocol procedure, the mobile device can configure and request of one or more raw ECG or PPG datasets from the wearable device. The ECG/PPG raw and feature biosignals are defined in clause 7. Figure 9 depicts transmission of biosignal raw and feature datasets.

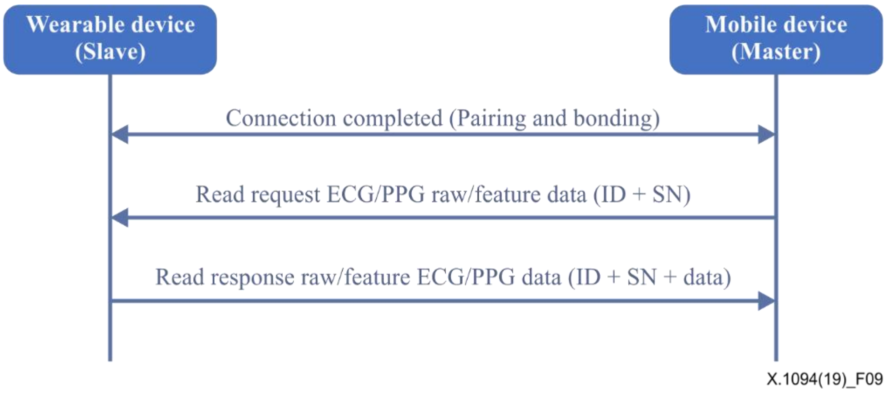

Wearable device (Slave)
Mobile device (Master)
Connection completed (Pairing and bonding)
Read request ECG/PPG raw/feature data (ID + SN)
Read response raw/feature ECG/PPG data (ID + SN + data)
X.1094(19)_F09

Figure 9 – Raw and feature dataset transmission sequence for electrocardiogram and photoplethysmogram

8.3.6 Termination sequence

For the termination sequence, the procedure is completely symmetrical in that both the wearable and the mobile device can terminate the connection at any time. A reason code and disconnect event should be provided to the application verifying that the termination event has completed. Figure 10 depicts a termination sequence for a biosignal transmission protocol.

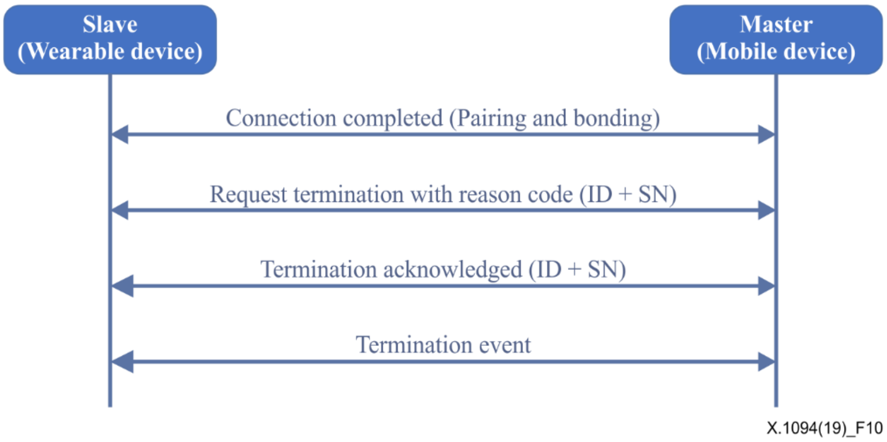

Slave
(Wearable device)
Master
(Mobile device)
Connection completed (Pairing and bonding)
Request termination with reason code (ID + SN)
Termination acknowledged (ID + SN)
Termination event
X.1094(19)_F10

Figure 10 – Termination sequence for biosignal transmission protocol

A master is a device that determines the method of connecting, configuring and establishing security mechanisms for the channel communicating with the slave.

A slave is a device that is open to the master's configuration and captures biosignal data, enables security mechanisms configured by the master and transmits biosignal data packets.

8.4 Functional requirements for biosignal testing database construction

8.4.1 Biosignal information acquisition conditions

Since biosignal information is generated by a physiological mechanism, a signal may appear differently depending on various factors, such as external environment, physical condition and emotional states. In this process, in order to objectively analyse the accuracy of individual authentication from biosignal information, it is necessary to precisely specify and control the conditions and environment for measuring biosignals.

Biosignal change factors are classified into external and internal types. An external factor refers to an element that can be affected by the external environment, such as temperature, humidity, sound and noise. An internal factor refers to an element that can occur spontaneously in the body, such as physical state (exercise, rest, posture, presence of eye opening, etc.) and emotional state (joy, sorrow, angry, horror, etc.).

In order to construct a practical personal authentication DB, an experiment to collect biosignal information under various conditions (environment) should be conducted and a test DB for securing objectivity constructed.

8.4.2 Biosignal database metadata features

8.4.2.1 Common metadata

Common metadata of a biosignal DB include DB information, biosignal information and environmental information.

8.4.2.2 Characteristic metadata

Characteristic metadata of a biosignal DB include file information, subject information, annotation information and miscellaneous information.

8.4.3 Security operation guidelines for a biosignal testing database

The individual identification information and the biometric information should be separated logically or physically. In this case, a common identifier that can commonly refer to two pieces of identification information is required. However, even in this situation, the following security requirements must be met.

- The common identifier should not be able to extract biometric or personally identifiable information (PII) on its own.
- If one of the two DBs is infringed and the contents are illegally modified to cause integrity problems, DB operators should be able to detect this.
- Even if DB contents are modified by the operator who has a proper secret key during DB operation, the operator of the other DB should be able to detect this fact.

9 Performance testing methodology for the biosignal authentication mechanism

This clause provides guidelines for evaluation metrics and procedures for technology evaluation for performance testing of a biosignal authentication algorithm. The biosignals to be targeted are limited to ECG and PPG signals. The technology evaluation of the biosignal authentication algorithm is an offline evaluation that repeatedly evaluates the processing speed, together with the recognition performance of the algorithm, targeting an evaluation DB composed of biosignal samples already collected and a standardized DB. The performance of various algorithms can be compared during regular use. Such physical environmental conditions for acquiring biological signals, behavioural conditions of biosignal providers and IDs for distinguishing between the individual and other persons require accurate recording.

This Recommendation assumes that the biosignal testing DB for technology evaluation is constructed according to the specifications of clause 8.4, and evaluates only the performance of 1:1 authentication using registered biosignals from one sample.

This Recommendation also specifies guidelines for the following aspects in conducting technology evaluation and some scenario for evaluating the performance of biosignal authentication recognition algorithms and commercial products:

- definition of performance metrics for biosignal authentication;
- procedures of reporting the results of performance evaluation.

10 Personally identifiable information protection for the biosignal authentication model

10.1 Vulnerabilities of the biosignal authentication model applying [ITU-T X.1086]

Figure 11 illustrates the threats associated with the biometric component through a network in the telebiometric authentication model for biosignals. Compared to a general biometric functional model, in a telebiometric authentication model for biosignals, processed biosignal data can be transmitted between components through telecommunication media as denoted *NW* in Figure 6. Figure 6 shows that not only each component in the model is vulnerable to outside attacks but also the transmission between the components. Examples of outside attacks are invasion from outside when biometric data are delivered to the next step or modification of processed biosignal data. For a detailed description of vulnerabilities and the corresponding countermeasures for telebiometric systems, see [ITU-T X.1086].

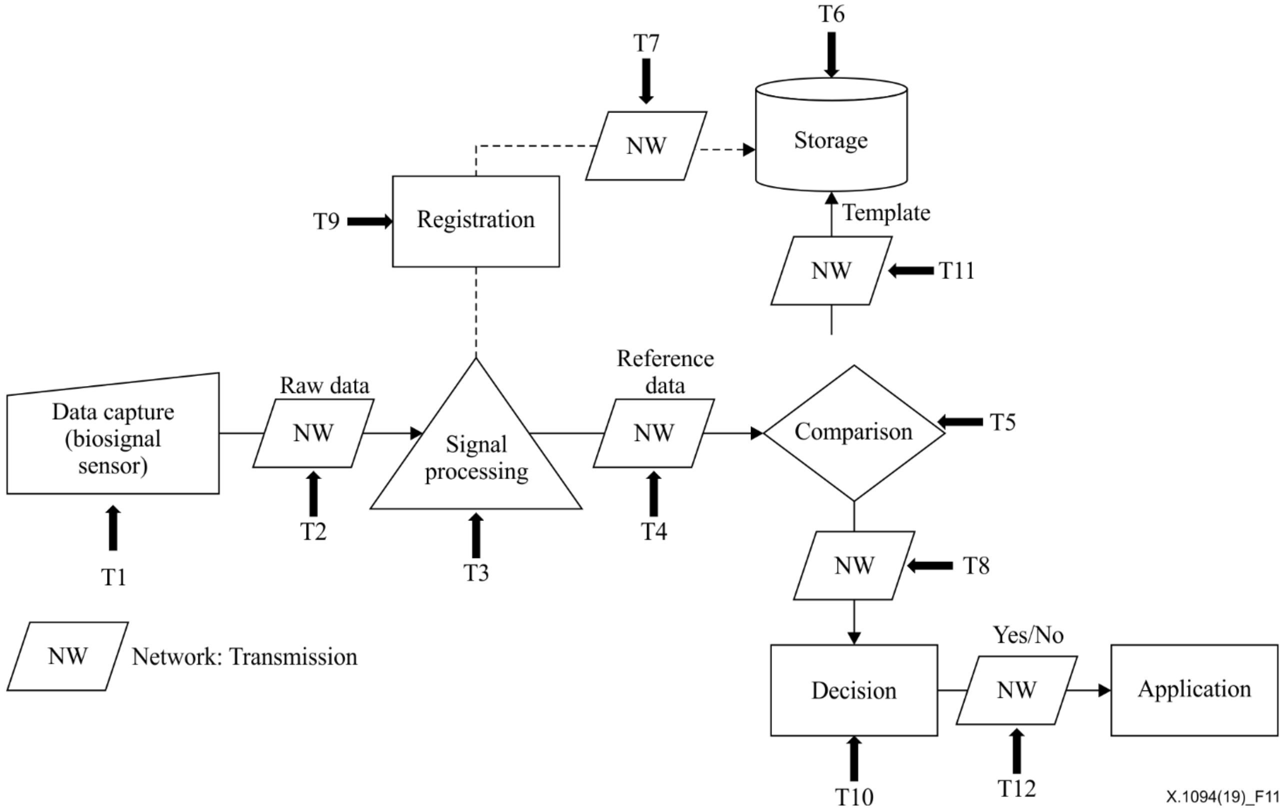


Figure 11 – Vulnerabilities of the telebiometric authentication model for biosignals

The threats associated with each component and transmission in the telebiometric authentication model for biosignals are listed and named as follows.

- T1: Threat to biosignal input devices
- T2: Threat to the process of transmitting biosignal raw data to the signal processing component
- T3: Threat to the signal processing component
- T4: Threat to the process of transmitting the extracted biosignal templates to the comparison component
- T5: Threat to the comparison component
- T6: Threat to the biosignal storage component
- T7: Threat to the process of transferring biosignal templates from the registration component to the storage component
- T8: Threat to the process of transmitting the matching score from the comparison component
- T9: Threat to the registration component
- T10: Threat to the decision component
- T11: Threat to the process of transmitting the stored biosignal template to the comparison component
- T12: Threat to the process of transmitting the decision result to an application system.

Appendix I

Use cases of telebiometric authentication for biosignals

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

The use case examples in clauses I.1 and I.2 illustrate how the concepts discussed throughout this Recommendation can be applied.

I.1 Telebiometric authentication applications using multi-modal biosignals

As defined in clause 8.2, the mobile device receives biosignals from the wearable device. It acquires sample data, compares it with the template of the registered user, and transfers the result to the wearable device. The example telebiometric applications applied in the multi-modal biosignal authentication model are shown in Figure I.1.

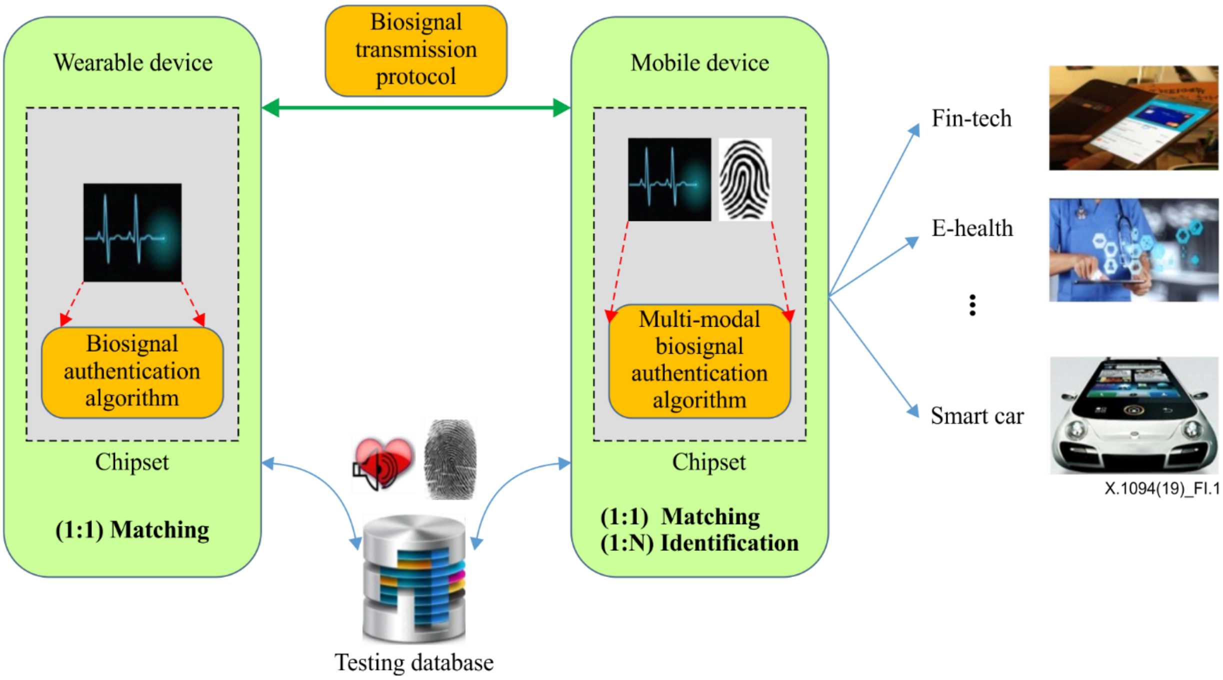


Figure I.1 – Telebiometric applications for the multi-modal biosignal authentication model

I.2 Case study for the multi-modal biosignal authentication model

There are several ways to approach multi-modal biosignal fusion. The following three are the most representative ones:

- Fusing features: This approach is valid when features from both modalities present a similar nature. If that is not the case, then this kind of fusing can only derive results by later splitting the feature vector into those that correspond to one kind, and the other ones. Therefore, in such a case, no vast achievement is expected. This is the case of humans, as fingerprint features are completely different from ECG features.
- Fusing decisions: In this approach, both algorithms are executed in parallel, and both obtain a decision. Then, through a voting system, both decisions are combined to obtain the final decision. This kind of fusion is extremely simple, but does not allow to grade the result depending on the application, i.e., it lacks flexibility and universality.

- Fusing scores: A mid-point approach is to execute both algorithms in parallel, but obtaining from each of them the comparison score (i.e., before taking any decision). Then, both scores are combined linearly to generate the final score, where a new threshold is applied to take the decision.

The score fusion approach is taken, where the final result is the linear combination of the results coming out of both recognition algorithms in terms of score. In other words:

$$score_{final} = A * score_{ECG} + B * score_{fingerprint}$$

This equation is valid as soon as scores are normalized (i.e., providing values from 0 to 1). The values of A and B are determined heuristically Table I.1 shows some significant results.

Table I.1 – Score fusion results, using as an ECG reference the sample taken while sitting

ECG sample	A	B	EER
Sitting	1	1	0.119%
Standing	1	1	0.092%
Exercise	1	1	0.137%
Sitting	2	1	0.128%
Standing	2	1	0.101%
Exercise	2	1	0.147%
Sitting	1	2	0.101%
Standing	1	2	0.064%
Exercise	1	2	0.128%

As it can be seen, the values of A and B are not really relevant, as in all cases the equal error rate (EER) is about 0.1%, which improves the performance of fingerprint by itself, reducing it to the half of its value. From a graphical point of view, Figure I.2 represents the distribution curve for the case of A = 1 and B = 2. It can be seen that the non-mated distribution (i.e., the inter-class distribution) is limited to a value of 0, and nearly no mated comparisons falls into the inter-class area.

By itself, ECG has an EER of 5.358%, which is in line with most mid-range biometric modes, such as face recognition or handwritten signature. In combination with a commercial fingerprint system, it can improve the performance of fingerprint by reducing it to half the error rates (from EER = 0.24% to EER = 0.1%).

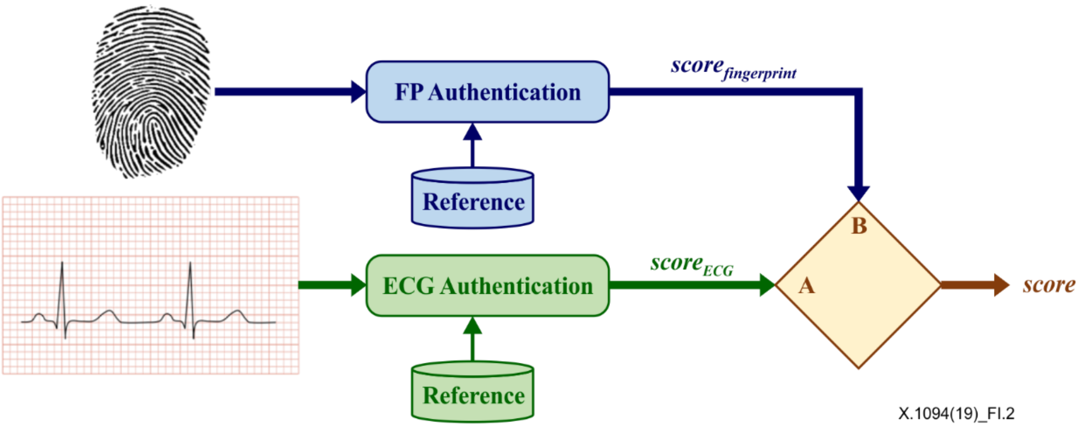
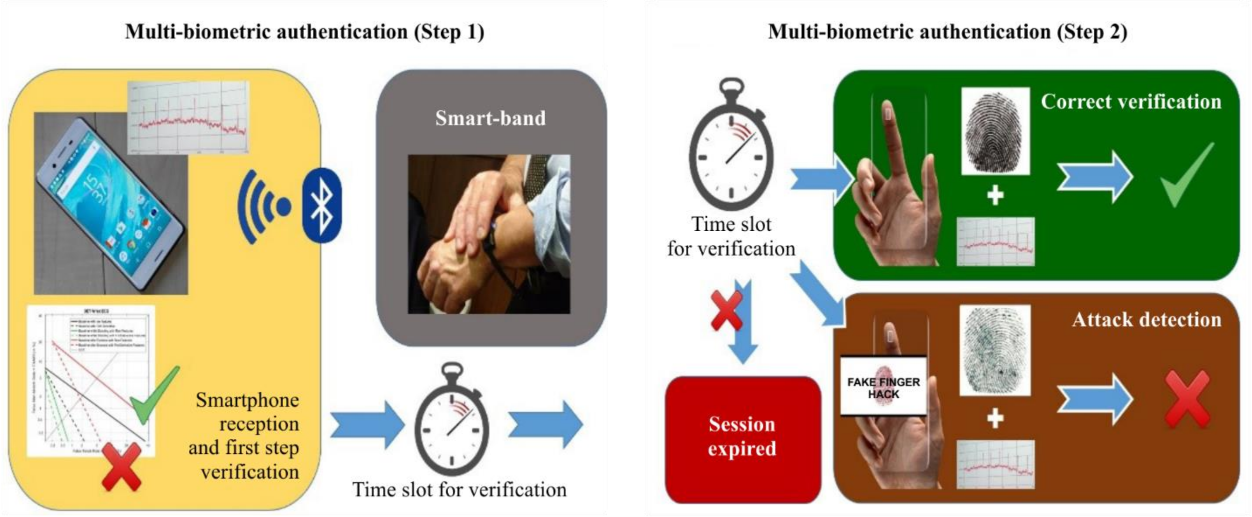


Figure I.2 – ECG-Fingerprint fusion

A proof of concept demo has been developed to show the results. Such proof of concept consisted of the following elements:

- Mock-up banking application, for statement checking as well as transfer issuance.
- Connection to a web service for the execution of the ECG comparison algorithm.
- Verification of the user fingerprint using the Android application program interface (API).
- Integration of both, fusion and the presentation attack detection (PAD) detection combination in the mobile phone.


Multi-biometric authentication (Step 1)
Smart-band
Smartphone reception and first step verification
Time slot for verification
Multi-biometric authentication (Step 2)
Time slot for verification
Correct verification
Attack detection
FAKE FINGER HACK
Session expired

X.1094(19)_FI.3

Figure I.3 – Architecture for using electrocardiogram as a PAD mechanism for fingerprint

Bibliography

[b-IEC 60601-2-10] IEC 60601-2-10:2012, Medical electrical equipment – *Part 2-10: Particular requirements for the basic safety and essential performance of nerve and muscle stimulators.*

[b-IEC 61784-5-3] IEC 61784-5-3:2018, *Industrial communication networks – Profiles – Part 5-3: Installation of fieldbuses – Installation profiles for CPF 3.*

[b-ISO/IEC 2382] ISO/IEC 2382:2015, *Information technology – Vocabulary.*

[b-ISO/IEC 19785-1] ISO/IEC 19785-1:2015, *Information technology – Common Biometric Exchange Formats Framework – Part 1: Data element specification.*

[b-ISO/IEC 30107-3] ISO/IEC 30107-3:2017, *Information technology – Biometric presentation attack detection – Part 3: Testing and reporting*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
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	Environment and ICTs, climate change, e-waste, energy efficiency; 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	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
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, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2019