

I n t e r n a t i o n a l T e l e c o m m u n i c a t i o n U n i o n

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1080.2

(10/2021)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Information and network security – Telebiometrics

Biology-to-machine (B2M) protocol

Recommendation ITU-T X.1080.2

ITU-T

ITU-T X-SERIES RECOMMENDATIONS
DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES (1)	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security (1)	X.1140–X.1149
Application Security (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.1350–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1399
Distributed ledger technology (DLT) security	X.1400–X.1429
Application Security (2)	X.1450–X.1459
Web security (2)	X.1470–X.1489
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
Cyber Defence	X.1590–X.1599
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
QUANTUM COMMUNICATION	
Terminologies	X.1700–X.1701
Quantum random number generator	X.1702–X.1709
Framework of QKDN security	X.1710–X.1711
Security design for QKDN	X.1712–X.1719
Security techniques for QKDN	X.1720–X.1729
DATA SECURITY	
Big Data Security	X.1750–X.1759
Data protection	X.1770–X.1789
IMT-2020 SECURITY	X.1800–X.1819

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

Recommendation ITU-T X.1080.2

Biology-to-machine (B2M) protocol

Summary

Recommendation ITU-T X.1080.2 defines a general protocol for the exchange of biometric information from a patient facility to a medical expert facility so that a medical centre could remotely monitor a patient and retrieve information from that patient. It also allows the medical expert facility to control the sensors and other devices at the patient facility and to establish the environment for a monitor session at the patient facility. It defines a versatile and open-ended information model that allows any type of medical and non-medical information to be transferred.

This Recommendation is a biosignal communication protocol between computing devices and biological systems. This protocol is based upon an aggregation of the interactions between a computing device and the biological system. Biometric interactions are described using the telebiometric multimodal model as defined by Recommendation ITU-T X.1081, which is a three-layer model combining the science, sensor and metric layers. It is a horizontal market protocol designed to be used for all IoT biometric metric applications, for example, in the aerospace, medical, automotive, industrial and consumer markets. In the case of clinical medical trials, this protocol enriches the application with a versatile and open-ended information model filled with interaction descriptions thereby ensuring an accurate comparison of measurement processes.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1080.2	2021-10-29	17	11.1002/1000/14795

Keywords

Biometrics, biosignals, e-health, Internet of Things (IoT), telebiometrics.

* 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/software copyrights, 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 appropriate ITU-T databases available via the ITU-T website at <http://www.itu.int/ITU-T/ipr/>.

© ITU 2021

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
SECTION 1 – GENERAL	1
1 Scope.....	1
2 References.....	1
2.1 Identical Recommendations International Standards	1
2.2 Additional references.....	2
3 Definitions	2
3.1 Terms defined elsewhere	2
3.2 Terms defined in this Recommendation.....	2
4 Abbreviations and acronyms	3
5 Conventions	3
6 Basic biometric concepts	3
6.1 Biology-to-machine (B2M) Protocol	3
6.2 The telebiometric multimodal model	4
6.3 B2M packet construction.....	5
7 Overview of the B2M protocol.....	7
7.1 Scope of B2M protocol	7
7.2 Monitoring configuration	7
7.3 Use of security services	8
7.4 Initialization of the B2M protocol.....	8
7.5 The data transfer phase	8
7.6 Data types	9
SECTION 2 – INFORMATION MODEL.....	10
8 The information model	10
8.1 Introduction to the information model	10
8.2 Useful data types	10
8.3 The MONITOR-TYPE information object class	10
8.4 The OPTIONS information object class.....	10
8.6 The UNIT information object class.....	11
8.7 The GEN-INFO information object class.....	11
SECTION 3 – THE BIOLOGY-TO-MACHINE (B2M) PROTOCOL	13
9 Formal specification of the biometric to machine protocol.....	13
9.1 Top-level B2M protocol	13
9.2 Initialization of a monitoring session	13
9.3 Data transfer	15
9.4 Allocation of object identifier arcs	16
SECTION 4 – SELECTED INFORMATION OBJECTS	17
10 Unit information objects	17

10.1	Introduction	17
10.2	The seven defining constants of the SI.....	17
		Page
10.3	The seven base units	18
10.4	SI derived units.....	19
11	Personal and identifying general information items.....	23
11.1	General	23
11.2	Surname general information item	23
11.3	Given name general information item	23
11.4	Initials general information item	23
11.5	Generation qualifier general information item	23
11.6	Serial number general information item.....	23
11.7	Pseudonym general information item.....	24
11.8	Uniform resource identifier (URI) general information item.....	24
11.9	Uniform resource name (URN) general information item	24
11.10	Uniform resource locator (URL)general information item	24
11.11	Domain name general information item.....	24
11.12	E-mail general information item	25
11.13	Country name general information item.....	25
11.14	Country name with three characters general information item	25
11.15	Locality name general information item	25
11.16	Street address general information item	25
11.17	House identifier general information item	25
11.18	Universal Transverse Mercator (UTM)coordinates general information item	26
11.19	Organization name general information item.....	26
11.20	Organizational unit name general information item.....	26
11.21	Title general information item.....	26
11.22	Organization identifier general information item.....	26
11.23	Description general information item.....	27
11.24	Business category general information item	27
11.25	Postal code general information item	27
11.26	Post office box general information item	27
11.27	Telephone number general information item	27
11.28	Mobile number general information item.....	27
	SECTION 5 – SPECIFIC APPLICATIONS	28
12	Motion detection.....	28
12.1	Motion sensing techniques	28
12.2	Monitor type specifications	28
	Annex A – General introduction to sensing.....	34

A.1	Scope of annex	34
A.2	Types of physical interaction.....	34
		Page
A.3	Body position.....	34
A.4	Sensing session.....	34
Annex B – Biology-to-machine (B2M) protocol in ASN.1.....		35
Annex C – Defined information objects in ASN.1		38
Annex D – Monitor types in ASN.1		44
Annex E – Motion detection monitor type in ASN.1		45
Bibliography.....		49

Introduction

This Recommendation is organized as follows:

- SECTION 1 includes general information such as an overview of the biology-to-machine (B2M) protocol and the associated information models.
- SECTION 2 is a specification of the information models as the basis for the B2M protocol.
- SECTION 3 is the formal specification OF the B2M protocol.
- SECTION 4 is A list of information types to be carried in the B2M protocol.
- SECTION 5 includes application specific monitor type specifications. Currently, only moving detection monitor type is included.
- Annex A, which is an integral part of this Recommendation, provides a general introduction to sensing.
- Annex B, which is an integral part of this Recommendation, provides the formal ASN.1 specification for the B2M protocol and associated information model.
- Annex C, which is an integral part of this Recommendation, provides the formal ASN.1 specification for a list of defined information objects.
- Annex D, which is an integral part of this Recommendation, provides the formal ASN.1 specification for information objects representing monitor types.
- Annex E, which is an integral part of this Recommendation, provides the formal ASN.1 specification for the moving detection monitor types.

Recommendation ITU-T X.1080.2

Biology-to-machine protocol

SECTION 1 – GENERAL

1 Scope

The scope of this Recommendation is to include a versatile information model and an associated protocol entitled the biology-to-machine (B2M) protocol, a framework for communicating biosignals through biometric interactions using the telebiometrics multimodal model as defined by [ITU-T X.1081], which is a three-layer model combining the science, sensor and metric layers.

The scope is limited to the communication between a medical centre (medical expert facility) and a patient location.

The scope also includes definitions of some information objects to be carried by the protocol. Future editions of this Recommendation and other ITU-T Recommendations and/or international standards may add additional information objects.

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.

2.1 Identical Recommendations | International Standards

- [ITU-T X.510] Recommendation ITU-T X.510 (2020) | ISO/IEC 9594-11:2020, *Information technology – Open Systems Interconnection – The Directory: Protocol specifications for secure operations*.
- [ITU-T X.660] Recommendation ITU-T X.660 (2011) | ISO/IEC 9834-1:2012, *Information technology – Procedures for the operation of object identifier registration authorities: General procedures and top arcs of the international object identifier tree*.
- [ITU-T X.680] Recommendation ITU-T X.680 (2021) | ISO/IEC 8824-1:2021, *Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation*.
- [ITU-T X.681] Recommendation ITU-T X.681 (2021) | ISO/IEC 8824-2:2021, *Information technology – Abstract Syntax Notation One (ASN.1): Information object specification*.
- [ITU-T X.682] Recommendation ITU-T X.682 (2021) | ISO/IEC 8824-3:2021, *Information technology – Abstract Syntax Notation One (ASN.1): Constraint specification*.
- [ITU-T X.683] Recommendation ITU-T X.683 (2021) | ISO/IEC 8824-4:2021, *Information technology – Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications*.

[ITU-T X.691] Recommendation ITU-T X.691 (2021) | ISO/IEC 8825-2:2021, *Information technology – ASN.1 encoding rules: Specification of Packed Encoding Rules (PER)*.

2.2 Additional references

[ITU-T X.1080.0] Recommendation ITU-T X.1080.0 (2017), *Access control for telebiometrics data protection*.

[ITU-T X.1080.1] Recommendation ITU-T X.1080.1 (2018), *E-health and worldwide telemedicines – Generic telecommunications protocol*.

[RFC 5890] IETF RFC 5890 (2010), *Internationalized Domain Names for Applications (IDNA): Definitions and Document Framework*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 association [ITU-T X.510]: A cooperative relationship between two application entities, which enables the communication of information and the coordination of their joint operation for an instance of communication.

3.1.2 biometrics [b-ITU-T X.1081]: Automated recognition of living persons based on observation of behavioural and biological (anatomical and physiological) characteristics.

3.1.3 client [ITU-T X.510]: The entity that initiates an association.

3.1.4 information object [ITU-T X.681]: An instance of some information object class, being composed of a set of fields which conform to the field specifications of the class.

3.1.5 information object class [ITU-T X.681]: A set of fields, forming a template for the definition of a potentially unbounded collection of information objects, the instances of the class.

3.1.6 object identifier [ITU-T X.660]: An ordered list of primary integer values from the root of the international object identifier tree to a node, which unambiguously identifies that node.

3.1.7 protected protocol data unit (PrPDU) [ITU-T X.510]: Application protocol data unit (APDU) defined by an application protocol to be protected by the wrapper protocol.

3.1.8 protocol data unit [ITU-T X.510]: Data that is transmitted as a single unit at the application layer between two application entities.

3.1.9 server [ITU-T X.510]: The entity that accepts or rejects an association.

3.1.10 telebiometrics [b-ITU-T X.1081]: The application of biometrics to telecommunications and of telecommunications to remote biometric sensing.

3.1.11 wrapper protocol data unit (WrPDU) [ITU-T X.510]: An application protocol data unit (APDU) carrying security protocol control information and, when relevant, carrying a protected protocol data unit.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 microwave motion detector: A type of sensor that emits electromagnetic pulses and measures the changes in frequency (Doppler) due to the reflection from a moving object.

3.2.2 passive infrared (PIR) sensor: An electronic sensor that measures infrared light radiating from objects in its field of view. They are most often used in PIR-based motion detectors.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

APDU	Application Protocol Data Unit
ASN.1	Abstract Syntax Notation One
B2M	Biology-to-Machine
ECG	Electrocardiogram
IDN	Internationalized Domain Name
LDH	Letters, Digits, Hyphen
M2M	Machine-to-Machine
OTA	Over-The-Air
PER	Packed Encoding Rules
PIR	Passive Infrared
PrPDU	Protected protocol Data Unit
SDO	Standards Development Organization
URL	Uniform Resource Locator
URN	Uniform Resource Name
UTM	Universal Transverse Mercator
WrPDU	Wrapper protocol Data Unit

5 Conventions

When ASN.1 types and values are referenced in normal text, they are differentiated from normal text by presenting them in the **10 pt bold Courier New** typeface.

This Directory Specification makes extensive use of the Abstract Syntax Notation One (ASN.1) for the formal specification of data types and values, as specified in Recommendations, ITU-T X.680 | ISO/IEC 8824-1, ITU-T X.681 (2015) | ISO/IEC 8824-2, ITU-T X.682 (2015) | ISO/IEC 8824-3, ITU-T X.683 (2015) | ISO/IEC 8824-4 and ITU-T X.691 | ISO/IEC 8825-2.

6 Basic biometric concepts

Traditionally, biometrics has been primarily limited to identity applications. However, biometrics literally means "life-measurements". Life-measurement applications far exceed identity applications and serve a greater need, which is not only to detect and quantify life, but also to protect life. Hence, biometrics is an essential component of biosafety and biosecurity applications. Attaching the prefix 'tele-' to biometrics further describes the telecommunication component required for networked and over-the-air (OTA) biometric applications.

As the market for autonomous systems grows so does their interaction with people, for example, autonomous vehicles and human interaction robots. Autonomous systems may leverage standardized guidelines to identify and protect life. The biology-to-machine (B2M) protocol is an interaction based language that supports telecommunication networks' ability to communicate between biological systems and Internet of Things (IoT) networks.

6.1 Biology-to-machine (B2M) Protocol

B2M expands the IoT to include not only electrically but also biologically based computation systems. B2M enables autonomous systems to recognize life and enable life-protecting measures, e.g., autonomous systems and medical devices. B2M also provides a common data format for mobile health devices independent of their manufacturer, e.g., wearables including but not limited to electrocardiogram (ECG or EKG) and continuous glucose monitors. B2M is designed to connect biological systems, which include but are not limited to people, livestock and plants, to computers and the network. B2M's purpose is to extend the IoT to include biological endpoints with a universal language and make B2M a native protocol to IoT devices globally.

Biological entities comprise complex computational actuator systems constructed of proteins, fats and carbohydrates. Since electronic systems attempt to emulate biological systems, we can conclude that both systems are computational entities, one organic and the other synthetic and much more primitive.

6.2 The telebiometric multimodal model

At the heart of the B2M protocol is a "telebiometric multimodal model" [b-ITU-T X.1081] which organizes all data collected or derived by the primary sciences: physics, chemistry, biology, culturology and psychology. A simple analogy equates the body as a territory and the primary scientific fields are the borders of the body. The aggregation of the following layers is what comprises the B2M protocol.

Primary science	Example
Physics	Temperature, ECG,
Chemistry	Blood test, urine Test, alcohol breath test, drug tests and blood oxygen saturation
Biology	DNA/protein, heart rate, sex and age
Culturology	Ethnic origin, nationality and religion
Psychology	Beliefs, psychiatric or personality disorders and syndromes

6.2.1 Interaction modality layer

Interaction modality per [b-ITU-T X.1081] is a layer that describes how an individual perceives an interaction, such as through touch, taste, sound and visually. Examples of interaction modalities across the biosphere are chemo-in (smell), audio-in, audio-out, etc. Music and speech are subcategories of audio. Gesture and facial expression are subcategories of video-out.

Biometric types	Interaction modality
Face image, iris, retina, hand geometry, vein pattern, finger image	Depends upon the technology used, video-in (input of artificial light is usually needed), video-ut, or tango-ut
Lip movement, thermal face image, thermal hand image, ear shape, finger geometry	Video-out
Voice	Audio-out
Signature dynamics, keystroke dynamics, footprint	Tango-out
Body Odour, DNA, blood and/or urine analysis	Chemo-out

6.2.2 Measurement system layer

By adding a measurement system layer such as the International System of Units (SI) including values and units, how the biological system was influenced by its environment can be quantified.

6.3 B2M packet construction

From this model (Figure 1), a data packet is structured containing essential information about the biological entity, hardware and the type of interaction. The data is extracted, managed and protected enhancing the value of the application by creating sets of raw data, derived data, and graphical data supported by deep learning algorithms. The datasets collected are considered biosignals. Biosignals flow to and from the biological entity. The B2M protocol enables an IoT network to bidirectionally communicate with a biological entity.

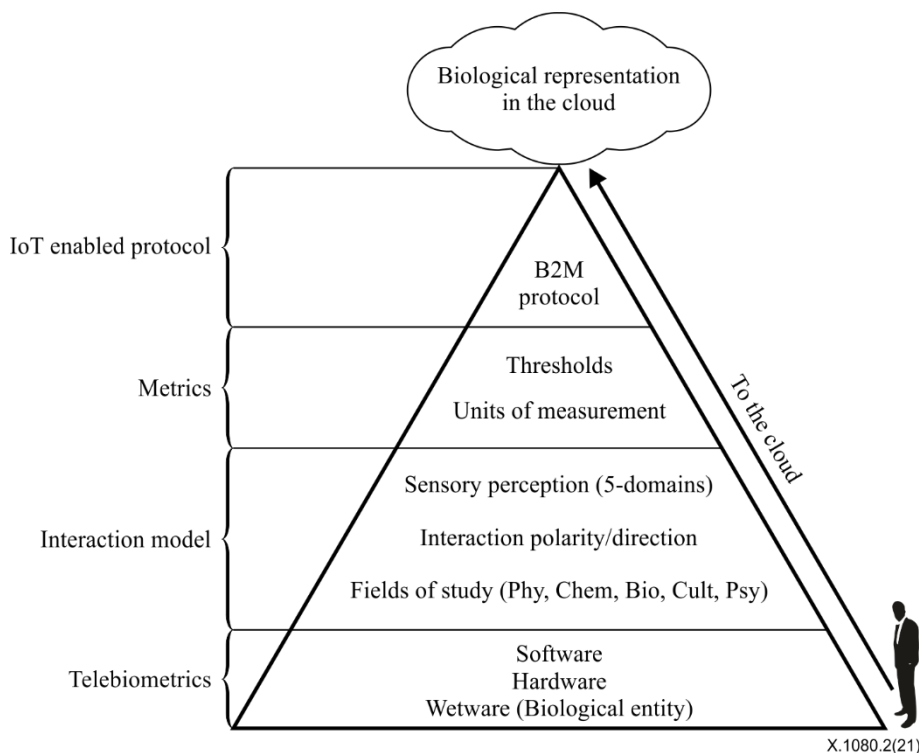


Figure 1 – The hierarchical components of the B2M model

B2M descriptors are included directly in machine-to-machine (M2M) protocols, thereby extending the IoT to include biological entities. The value of the B2M protocol is that it is application and market independent and supports unlimited devices, thereby increasing the biological representation in the cloud in a universally accessible and useful manner.

The B2M information model and exchange can be viewed from two complementary angles. Both are important:

- a) A biosignal point of view, where the interaction between a patient and his or her environment is considered.
- b) A pure protocol point of view, where the information generated according to item a) is transferred securely and unmodified from one point to another.

This clause is mostly concerned with the signal point of view, while protocol aspects are treated in clause 7.

The basic biosignal concept is to accurately describe the interaction(s) between a sensor or actuator and a biological entity, i.e., a person, animal or plant. A biosignal is either an IN or OUT interaction determined by the direction of the interaction (Figure 2).

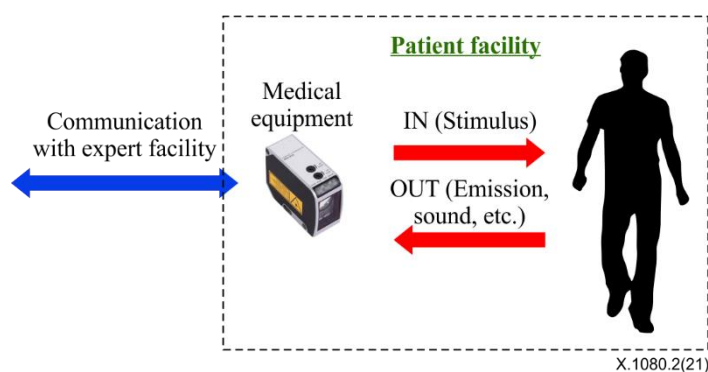
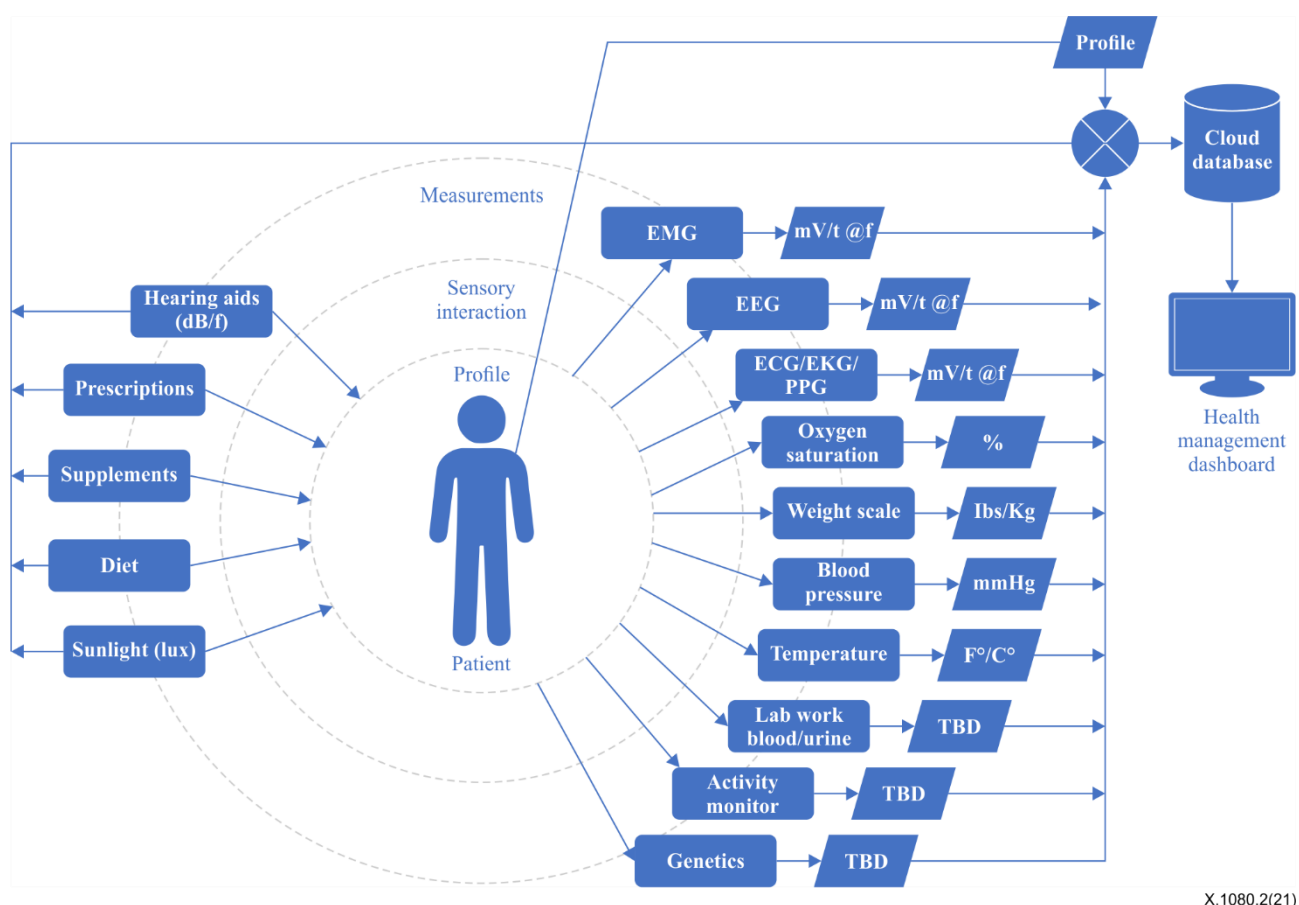


Figure 2 – IN and OUT interaction

The biological entity and sensor or actuator require an object identifier thereby enabling the postprocessing of biosignals searchable by their biological hierarchy and sensor or actuator type. The B2M protocol is structured at the biological endpoint/device and can postprocess to create new B2M protocol strands with the ability to transfer the B2M strand back to the network. For an ECG interaction example, a B2M packet may transfer mV/t (measurement system) as measured in the physics domain (scientific layer), whereas a postprocessed calculation of the ECG signal to determine heart rate is classified in the biology domain (scientific layer).



Key: EMG – electromyography; electroencephalography; PPG – photoplethysmogram;
TBD – to be defined

Figure 3 – Monitoring types and resulting diagnosis

In Figure 3, an array of B2M interaction devices demonstrates the types of measurements, interactions and direction of information to and from the patient. Each B2M string is searchable, postprocessable,

and linked to the patient's identity. Parts of the information are searchable while maintaining the privacy of the patient. For example, information related to a global outbreak can be shared by government health agencies in real time without revealing the patient's identity.

7 Overview of the B2M protocol

7.1 Scope of B2M protocol

The B2M protocol is used to establish communication between a medical expert facility and a remote patient facility.

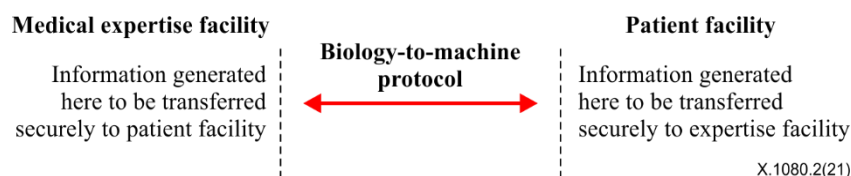


Figure 4 – The scope of the B2M protocol

Figure 4 illustrates the scope of the biology-to-machine protocol. Information is generated at one location and is transmitted to the other location. The details about how information is generated on the sender side and details about its processing by the recipient at the recipient side is outside the scope of this Recommendation. The main scope of the B2M protocol is:

- a) To provide a versatile data structure that allows any relevant type of information to be mapped to that data structure.
- b) To transfer the data so structured to the destination ensuring:
 - authentication, i.e., that the sender is properly authenticated;
 - integrity, i.e., that if data is modified during transmission, it is detected; and
 - optionally, confidentiality by use of encryption.

Details on how information is treated by the recipient is likewise outside the scope of this Recommendation. As an example, information received at the expert facility may be processed in many different ways, such as compared with locally available information, processed by non-standardized analysis systems, combined to establish diagnostics, etc.

7.2 Monitoring configuration

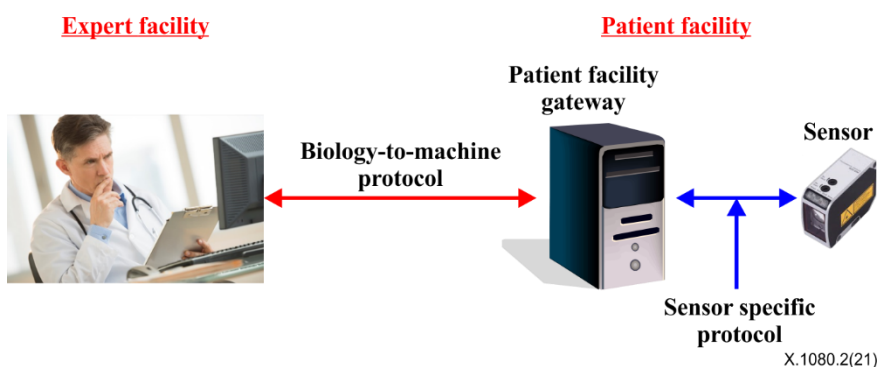


Figure 5 – Physical monitoring configuration

The patient facility is a system at a patient location that collects information about the patient, e.g., by using sensors of different types. The patient facility may be either in the patient's home or in a local medical centre.

The B2M protocol interacts with a gateway at the patient facility, which then provides the local mapping between the B2M protocol and the local interaction.

The medical expert facility may be either a centre with a medical staff or surveillance equipment. The medical expert facility uses the B2M protocol to instruct the patient facility gateway to operate a sensor in a particular way and to request specific information.

The protocol between the patient facility gateway and a sensor is determined by the type of sensor and may be a proprietary protocol. There may not be a one-to-one relationship between the B2M protocol elements and the protocol elements of a sensor specific protocol. The mapping between the sensor specific protocol and the B2M protocol is outside the scope of this Recommendation.

7.3 Use of security services

This Recommendation makes use of the security services of the wrapper protocol, as defined by [ITU-T X.510]. The wrapper protocol provides for authentication, integrity and optionally confidentiality by use of encryption. It also provides a migration path for cryptographic algorithms, e.g., when stronger cryptographic algorithms are required. This allows migration to quantum-safe algorithms in the future without affecting the B2M protocol.

[ITU-T X.510] performs a handshake exchange to establish an association between two entities before the actual data transfer phase may commence. The B2M protocol requires initialization information to be carried in this handshake.

[ITU-T X.510] also defines some terms used by this Recommendation. An application protocol data unit (APDU) specified by this Recommendation is called a protected protocol data unit (PrPDU), as it is protected by the wrapper protocol. When wrapped within the wrapper protocol, the resulting application protocol data unit is called a wrapper protocol data unit (WrPDU). A WrPDU may not in all cases include a PrPDU.

7.4 Initialization of the B2M protocol

[ITU-T X.510] requires the establishment of an association between two communicating entities by a handshake exchange. An association is a cooperative relationship between two entities, which enables the communication of information and the coordination of their joint operation for an instance of communication. To start a monitoring session, an association shall be established between the medical expert facility and the patient facility.

The initiator of an association is called the client, while the target entity is called the server.

This Recommendation does not specify whether the expert facility or the patient facility initiates the association. Any side may initiate an association. However, restriction may be imposed by means outside this Recommendation.

During the association establishment, [ITU-T X.510] allows the client to add B2M protocol initialization parameters for the server to accept or reject (see clause 9.2).

When an association is established, the two communicating entities enter the data transfer phase.

7.5 The data transfer phase

The type of information to be transferred between a medical expert facility and a patient facility depends on several factors, such as:

- a) the type of patient to be monitored;
- b) local policies; and
- c) the facilities available.

The number of information types to be transferred is almost unbounded and new information types will constantly be defined. It is therefore important that the B2M protocol is flexible enough to carry

any information type that fits into one of the information models specified in SECTION 2. Extended and new information models may be developed in future editions of this Recommendation.

7.6 Data types

7.6.1 General

This Recommendation uses a flexible concept of data types that assigns object identifiers to data types allowing the B2M protocol to transfer different kinds of information without having the information types hard coded in the basic protocol.

7.6.2 The concept of monitor types

A monitoring session may involve several monitor types. Monitor types need to be defined to allow the expert facility and the patient facility to negotiate what monitor types to activate during a monitoring session. Movement detection (see clause 12) is an example of a monitor type.

A monitor type is identified by an object identifier. Any organization that is authorized to allocate object identifiers may define new monitor types following the principles set out by this Recommendation. It is recommended that monitor types be defined by standard development organizations (SDOs) and made publicly available.

7.6.3 General information items

A general information item specifies non-medical information associated with a patient, such as name or personal identification number.

This Recommendation does not define types for all general information items that may be required for a specific environment. Future editions of this Recommendation may add new general information item specifications. Other international standards and recommendations may define their own general information items to be transferred by the B2M protocol. An object identifier is allocated to each type of general information item.

7.6.4 Device information

Beyond data items, there is a need for another simple type of information. Devices and sensors at the patient location need to be identified for the purpose of selecting devices for monitoring and for associating additional information to monitoring information.

8 The information model

8.1 Introduction to the information model

The information model is specified using the ASN.1 information object classes concept defined in [ITU-T X.681]. [ITU-T X.510] gives a short introduction to the ASN.1 information object class concept. The use of information object classes is a flexible way to specify information types without hard coding the specific instances of information types.

An information object class is the basis for defining an information object of a specific type. Such an information object is identified by an object identifier. An example of an information object could be a **surname** information object, instances of which may be carried in the protocol.

The use of the information object class concept has the advantage that other organizations, e.g., standards organization may define new information objects based on the information object class specifications within this Recommendation.

8.2 Useful data types

```
Direction ::= ENUMERATED {in(0), out(1)}
```

The **Direction** data type may be inserted at specific places to indicate whether the interaction with a living body is towards the body (in) or away from the body (out). See Figure 2.

```
DeviceInfo ::= SEQUENCE {
    vendor [0] UTF8String OPTIONAL,
    type   [1] UTF8String OPTIONAL,
    id     [2] UTF8String OPTIONAL,
    ... }

```

8.3 The MONITOR-TYPE information object class

A monitor type is specified using the **MONITOR-TYPE** information object class defined in [ITU-T X.681]. It binds an abstract syntax and an identifying object identifier.

```
MONITOR-TYPE ::= TYPE-IDENTIFIER
```

8.4 The OPTIONS information object class

The **OPTION** information object class is used for specifying options for voice and/or video, where such options are dependent on the type of equipment. It is assumed that such a specific option can be specified by a specific data type.

```
OPTIONS ::= CLASS {
    &Voice-options    OPTIONAL,
    &Video-options    OPTIONAL }
WITH SYNTAX {
    [VOICE OPTIONS    &Voice-options]
    [VIDEO OPTIONS    &Video-options] }

```

The **OPTIONS** information object class has the following fields:

- a) The **&Voice-options** optional field is used for specifying a data type for the options for the voice equipment.
- b) The **&Video-options** optional field is used for specifying a data type for the options for the video equipment.