

International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.2075

(09/2015)

SERIES Y: GLOBAL INFORMATION
INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS
AND NEXT-GENERATION NETWORKS

Next Generation Networks – Frameworks and functional
architecture models

Capability framework for e-health monitoring services

Recommendation ITU-T Y.2075

ITU-T



ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Enhancements to NGN	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Packet-based Networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
FUTURE NETWORKS	Y.3000–Y.3499
CLOUD COMPUTING	Y.3500–Y.3999

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

Recommendation ITU-T Y.2075

Capability framework for e-health monitoring services

Summary

Recommendation ITU-T Y.2075 specifies the capability framework for support of the requirements of e-health monitoring (EHM) services (Recommendation ITU-T Y.2065).

To facilitate the identification of the capabilities in support of EHM services, an EHM conceptual framework is provided making usage of five components (i.e., EHM terminal, EHM end point, EHM gateway, Internet of things (IoT) platform and EHM application server) and the relationships among these components.

Based on the EHM conceptual framework and the requirements specified in Recommendation ITU-T Y.2065, the EHM capability framework is provided including the per-layer and cross-layer distribution of EHM capabilities in the five EHM components.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.2075	2015-09-29	13	11.1002/1000/12582

Keywords

Capability framework, capability requirements, e-health monitoring, EHM, Internet of Things, IoT.

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

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at <http://www.itu.int/ITU-T/ipr/>.

© ITU 2016

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

	Page
1 Scope.....	1
2 References.....	1
3 Definitions	1
3.1 Terms defined elsewhere	1
3.2 Terms defined in this Recommendation.....	2
4 Abbreviations and acronyms	2
5 Conventions	2
6 Introduction.....	2
7 EHM conceptual framework.....	3
7.1 EHM conceptual framework overview	3
7.2 EHM components	4
8 EHM capability framework	6
8.1 Distribution map of the EHM capabilities.....	7
8.2 Application layer capabilities of EHM components	8
8.3 SSAS layer capabilities of EHM components.....	9
8.4 Network layer capabilities of EHM components	11
8.5 Device layer capabilities of EHM components	11
8.6 Management capabilities of EHM components	12
8.7 Secure capabilities of EHM components	13
Annex A – Overview of EHM component capabilities	15
Appendix I – EHM service deployment technical scenarios	17
I.1 Technical scenario for community EHM services	17
I.2 Technical scenario for mobile EHM services	18

Recommendation ITU-T Y.2075

Capability framework for e-health monitoring services

1 Scope

This Recommendation specifies the capability framework for support of the requirements of e-health monitoring (EHM) services [[ITU-T Y.2065](#)].

The scope of this Recommendation includes:

- EHM conceptual framework
- EHM capability framework

An overview of the EHM capabilities in the various EHM components is provided in Annex A.

Two EHM service deployment technical scenarios are described in Appendix I.

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 Y.2060](#)] Recommendation ITU-T Y.2060 (2012), *Overview of the Internet of things*.

[[ITU-T Y.2065](#)] Recommendation ITU-T Y.2065 (2014), *Service and capability requirements for e-health monitoring services*.

[[ITU-T Y.2067](#)] Recommendation ITU-T Y.2067 (2014), *Common requirements and capabilities of a gateway for Internet of things applications*.

[[ITU-T Y.2068](#)] Recommendation ITU-T Y.2068 (2015), *Functional framework and capabilities of the Internet of things*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 e-health monitoring (EHM) service [[ITU-T Y.2065](#)]: A service which consists of observing and recording information based on [the collection of] a customer's physiological data, environmental data and other data, with the aim of monitoring the customer's state of health through the use of information and communication technologies.

3.1.2 EHM device [[ITU-T Y.2065](#)]: A device, as defined in [[ITU-T Y.2060](#)], which has sufficient qualification for e-health monitoring (EHM) service provisioning.

3.1.3 EHM end point [[ITU-T Y.2065](#)]: An e-health monitoring (EHM) device connected to the communication network through gateway(s).

3.1.4 EHM terminal [[ITU-T Y.2065](#)]: An e-health monitoring (EHM) device directly connected to the communication network.

3.1.5 Internet of things (IoT) [ITU-T Y.2060]: A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.

NOTE 1 – Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled.

NOTE 2 – From a broader perspective, the IoT can be perceived as a vision with technological and societal implications.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

EHM	E-Health Monitoring
EHMH	E-Health Monitoring Healthcare
EHMR	E-Health Monitoring Rehabilitation
EHMT	E-Health Monitoring Treatment
ICT	Information and Communication Technology
IoT	Internet of Things
QoS	Quality of Service
SSAS	Service Support and Application Support

5 Conventions

In this Recommendation:

The keywords "is required to" indicate a requirement that must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keywords "is recommended" indicate a requirement that is recommended, but which is not absolutely required. Thus this requirement need not be present to claim conformance.

The keywords "can optionally" and "may" indicate an optional requirement that is permissible, without implying any sense of being recommended. These terms are not intended to imply that the vendor's implementation must provide the option and the feature can be optionally enabled by the network operator or service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

6 Introduction

E-health monitoring (EHM) services include three types of services, i.e., EHM treatment (EHMT), EHM rehabilitation (EHMR) and EHM healthcare (EHMH), covering the person in healthy state, sub-healthy state and illness state respectively [ITU-T Y.2065]. It is expected that moving from one of these three types of EHM service to another is transparent from the customer's point of view, i.e., the customer can benefit from the EHM service required according to their change in state of health while minimizing the impact on the customer from the information and communication technology (ICT) point of view.

In practice, the ICT solutions adopted by EHM services vary among different scenarios and use cases. For example, as shown in Appendix I, an EHM service in community scenarios generally uses fixed devices and wired network technologies for network access, while in mobile scenarios, an EHM service uses mobile devices and wireless network technologies for network access. Actually, for real deployment scenarios, the situation is possibly even more complex than that described in Appendix I. Standardization is one way to reduce the negative impact of ICT heterogeneity on customers.

High-level standardization approaches with respect to EHM services, technical details related to specific devices, gateways, platforms and application servers used in the large variety of EHM service deployments lie outside the scope of this Recommendation. In this perspective, this Recommendation uses the concept of "component" on behalf of this large variety of specific EHM devices, gateways, platforms and application servers, and focuses on general characteristics of EHM devices, gateways, platforms and application servers.

Five types of component are identified in this Recommendation: EHM terminal, EHM end point, EHM gateway, Internet of things (IoT) platform and EHM application server.

For each component, "layers" as specified by the IoT reference model [[ITU-T Y.2060](#)] are introduced as an abstraction to illuminate the functionalities of the component.

The capabilities of a layer represent at high level the layer's functions.

NOTE – These functions are represented as functional entities at a detailed functional level.

A given component includes at least the capabilities of one of the layers as shown in Figure 1.

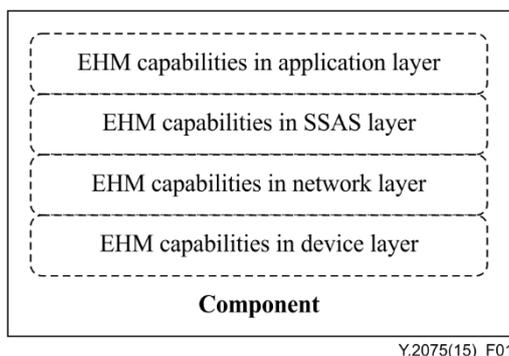


Figure 1 – Capabilities and layers in a component

Clauses 7 and 8 introduce the EHM conceptual framework and the EHM capability framework, respectively.

7 EHM conceptual framework

The EHM conceptual framework is used to identify functions and relationships of the different EHM components in order to support the EHM capability framework.

7.1 EHM conceptual framework overview

The EHM conceptual framework, shown in Figure 2, exhibits the components for the deployment of EHM services: EHM end point [[ITU-T Y.2065](#)], EHM terminal [[ITU-T Y.2065](#)], EHM gateway, IoT platform and EHM application server.

The EHM end point is an EHM device connected with the communication network through gateway(s).

The EHM terminal is an EHM device directly connected with the communication network.

The EHM gateway is a kind of gateway [ITU-T Y.2067] that provides support to the EHM end points to access the communication network.

The IoT platform is a technical infrastructure that provides generic support capabilities and specific support capabilities for EHM devices and EHM application server(s).

The EHM application server is a kind of server that runs EHM applications in order to provide EHM services.

NOTE – In Figure 2, the EHM components are represented as rectangles.

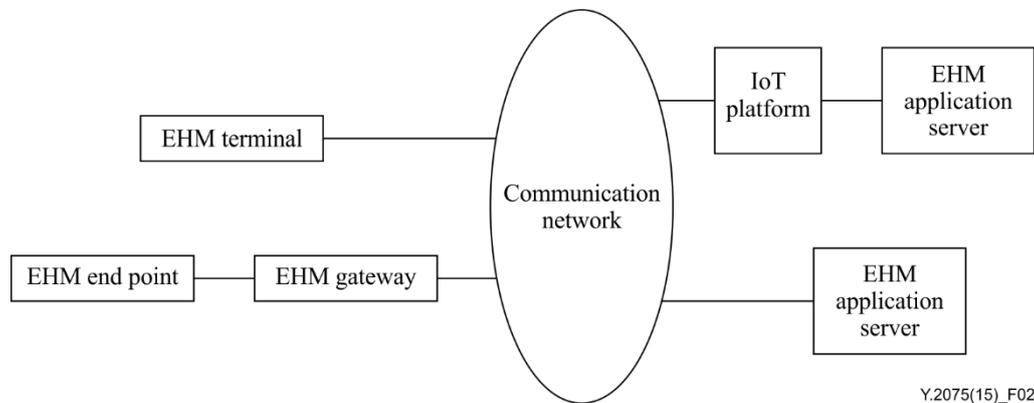


Figure 2 – EHM conceptual framework

7.2 EHM components

7.2.1 EHM terminal

The EHM terminal is defined as an EHM device directly connected to the communication network [ITU-T Y.2065]. The characteristics of an EHM terminal are given according to the following aspects:

7.2.1.1 Functions

The functions of the EHM terminal include:

(F-ET-1) EHM data sensing and collection:

The EHM terminal can sense and collect the EHM data from the bodies of EHM customers or their EHM environment.

(F-ET-2) EHM application running and management support

EHM applications can run on the EHM terminal, and the EHM terminal can provide support for the management of applications by both EHM customers and EHM application server.

(F-ET-3) Connection to the communication network

The EHM terminal can connect to and communicate with other components via the communication network.

(E-ET-4) Interworking with IoT platform and EHM application servers

The EHM terminal can interwork with the IoT platform and EHM application server, and handle operations and data exchanges with the IoT platform and EHM application server.

7.2.1.2 Relationships with other components

The EHM terminal can access the EHM application server and IoT platform via the communication network. It can access the EHM application server directly or via the help of the IoT platform.

7.2.2 EHM end point

The EHM end point is defined as an EHM device connected with the communication network via gateway(s) [ITU-T Y.2065]. The characteristics of an EHM end point are given according to the following aspects:

7.2.2.1 Functions

The functions of the EHM end point include:

(F-EEP-1) EHM data sensing and collection:

The EHM end point can sense and collect EHM data from EHM customers or related environment.

(F-EEP-2) EHM application running

The EHM end point can support running of EHM applications according to the EHM end point's usage purpose.

(F-EEP-3) Connection to EHM gateway

The EHM end point can connect to the EHM gateway via local wireless or wired communication technologies.

7.2.2.2 Relationships with other components

The EHM end point can directly connect to and access the communication network via the EHM gateway. The EHM end point can also access the IoT platform and EHM application server via the EHM gateway and the communication network.

7.2.3 EHM gateway

The characteristics of an EHM gateway are given according to the following aspects:

7.2.3.1 Functions

The functions of the EHM gateway include:

(F-EG-1) Gateway application running

Gateway applications can run on the EHM gateway.

(F-EG-2) Connection to the communication network

The EHM gateway can connect to and can communicate with other components via the communication network.

(F-EG-3) Connection to EHM end points

The EHM gateway can connect to EHM end points via local wireless or wired communication technologies.

(F-EG-4) EHM end point connection support

The EHM gateway can provide support for the connection of EHM end points to the communication network.

(F-EG-5) EHM service support

The EHM gateway can support the interworking of EHM end points with the IoT platform and EHM application server. Also, it can handle operations and data exchanges with the IoT platform and EHM application server.

7.2.3.2 Relationships with other components

The EHM gateway can locally connect to the EHM end points, and also can access the IoT platform and EHM application server via the communication network.

7.2.4 IoT platform

The IoT platform is a platform that can provide service support and application support capabilities for EHM devices and the EHM application server. The characteristics of the IoT platform are given according to the following aspects:

7.2.4.1 Functions

The functions of the IoT platform include:

(F-MP-1) Application running

Applications can run on the IoT platform.

(F-MP-2) Connection to the communication network

The IoT platform can connect to and communicate with other components via the communication network.

(F-MP-3) Service support and application support

The IoT platform can provide service support and application support for EHM devices and EHM applications using the service support and application support capabilities.

7.2.4.2 Relationships with other components

The IoT platform can access the EHM application server, EHM gateway and EHM terminals via the communication network.

7.2.5 EHM application server

The EHM application server is a kind of server that runs EHM applications. The characteristics of the EHM application server are given according to the following aspects:

7.2.5.1 Functions

The functions of the EHM application server include:

(F-EAS-1) EHM application running and management support

EHM applications can run on the EHM application server, and the EHM application server can provide support for their management.

(F-EAS-2) Connection to the communication network

The EHM application server can connect to and communicate with other components via the communication network.

(F-EAS-3) EHM service support

The EHM application server can interwork with the IoT platform, EHM gateway and EHM terminals. It can also handle operations and data exchanges with the IoT platform, EHM gateway and EHM terminals.

7.2.5.2 Relationships with other components

The EHM application server can connect to and access the IoT platform, EHM gateway and EHM terminals via the communication network.

8 EHM capability framework

The EHM capability framework maps the layered EHM capabilities identified in [[ITU-T Y.2065](#)] to each EHM component as specified in the EHM conceptual framework.

8.1 Distribution map of the EHM capabilities

The EHM essential IoT capabilities, based on the requirements identified in [ITU-T Y.2065], are specified in this Recommendation.

NOTE – IoT basic capabilities and IoT capabilities for integration of key emerging technologies, as specified in [ITU-T Y.2068], are also applicable to the support of EHM services.

According to the EHM capability requirements [ITU-T Y.2065] and based on the components of the EHM conceptual framework, the distribution of the EHM capabilities in the four layers of the IoT reference model [ITU-T Y.2060] is shown in Figure 3. As all EHM components have cross-layer EHM management and security capabilities, these cross-layer capabilities are not shown in Figure 3, the purpose of Figure 3 being to show the differences from a capability viewpoint among the EHM components.

In Figure 3, the boxes represent the components specified in the EHM conceptual framework, the dashed rounded rectangles represent the four layers of [ITU-T Y.2060] and the circles represent the presence of EHM capabilities at a given layer in a given component.

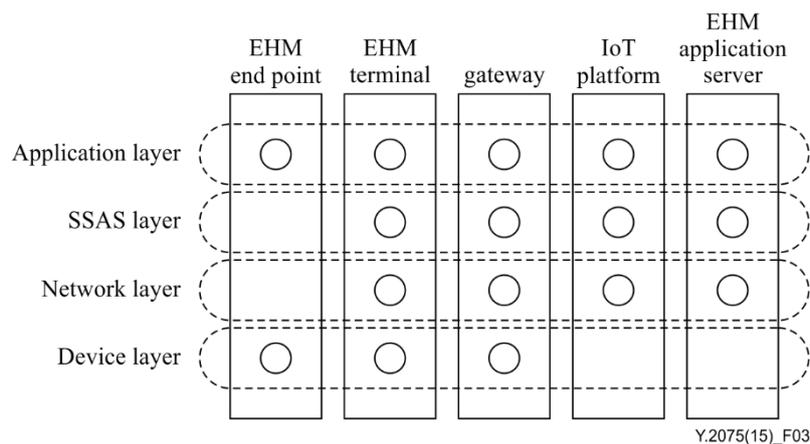


Figure 3 – Distribution map of EHM capabilities

In the EHM end point, the EHM capabilities are distributed in the device layer and application layer, as well as cross-layer EHM management and security capabilities.

In the EHM terminal, the EHM capabilities are distributed in the device layer, network layer, service support and application support layer and application layer, as well as cross-layer EHM management and security capabilities.

In the gateway, the EHM capabilities are distributed in the device layer, network layer, service support and application support layer, application layer, as well as cross-layer EHM management and security capabilities.

On the IoT platform, the EHM capabilities are distributed in the network layer, service support and application support layer, application layer, as well as cross-layer EHM management and security capabilities.

In the EHM application server, the EHM capabilities are distributed in a network layer, service support and application support layer, application layer, as well as cross-layer EHM management and security capabilities.

Clauses 8.2 to 8.7 provide details of this distribution map.

Annex A provides an overview of EHM capabilities, summarizing their distribution in the different EHM components.

8.2 Application layer capabilities of EHM components

8.2.1 Information sharing

According to the capability requirements described in clause 9.2.1 of [ITU-T Y.2065], the application layer of the components is recommended for support of standard interfaces and policy-based mechanisms [ITU-T Y.2065] to enable the sharing of EHM information among EHM components.

Table 1 shows the EHM components involved in the information sharing capability of application layer: the first column indicates the EHM components providing the EHM information, the first row indicates the EHM components receiving the EHM information.

Table 1 – EHM components involved in the information sharing capability of application layer

Provider	Receiver				
	EHM end point	EHM terminal	EHM gateway	IoT platform	EHM application server
EHM end point	✓		✓		
EHM terminal		✓	✓	✓	✓
EHM gateway		✓	✓	✓	✓
IoT platform		✓	✓	✓	✓
EHM application server		✓	✓	✓	✓

8.2.2 Accounting-related information provision

According to the capability requirements described in clause 9.2.2 of [ITU-T Y.2065], some EHM components are recommended for provision of the capability for accounting-related information provision.

The specific requirements of the accounting-related information provision capability of application layer for each EHM component are described in Table 2.

Table 2 – EHM components and accounting-related information provision capability of the application layer

EHM components	Accounting-related information provision
EHM end point	The application layer of the EHM end point is recommended to report accounting-related information, including, but not limited to, service class (i.e., EHMH or EHMR or EHMT), number of times and duration time of EHM service usage.
EHM terminal	The application layer of the EHM terminal is recommended for the reporting of accounting-related information to the service support and application support (SSAS) layer of the EHM terminal. This information includes, but is not limited to, service class (i.e., EHMH or EHMR or EHMT), number of times and duration time of EHM service usage.
EHM gateway	The application layer of the EHM gateway is recommended to report accounting-related information about the connected EHM end points to the SSAS layer of the EHM gateway. This information includes, but is not limited to, service type (EHMH, EHMR and EHMT), number of duration times and duration time of application usage.
IoT platform	None.
EHM application server	The application layer of the EHM application server is recommended to report accounting-related information to the SSAS layer of the EHM application server. This information includes, but is not limited to, number of times and duration time of EHM service usage.

8.2.3 QoS related information provision

According to the capability requirements described in clause 9.2.3 of [ITU-T Y.2065], the application layer of the EHM end point, EHM terminal, EHM gateway and EHM application server is recommended to provide Quality of Service (QoS) information to the SSAS layer or network layer for QoS configuration purposes.

NOTE – Refer to clause 9.2.3 of [ITU-T Y.2065] for the recommended QoS parameters.

8.3 SSAS layer capabilities of EHM components

8.3.1 Message conversion

According to the capability requirements described in clause 9.3.2 of [ITU-T Y.2065], the SSAS layer of the EHM terminal, EHM gateway, IoT platform and EHM application server is required to provide message conversion capability at the syntactic or semantic level.

NOTE – "Message" is intended here as the carrier of information transmitted between EHM technical components.

8.3.2 Data storage

According to the capability requirements described in clause 9.3.3 of [ITU-T Y.2065], the SSAS layer of the EHM terminal, EHM gateway, IoT platform and EHM application server is required to provide data storage.

The data stored in the SSAS layer are recommended to be stored in standard format so that the information can be easily exchanged among different EHM application servers, gateways and EHM terminals.

The specific requirements for data storage capability of the SSAS layer for each EHM component are described in Table 3.

Table 3 – EHM components and data storage capability of SSAS layer

EHM components	Data storage
EHM end point	None
EHM terminal	The EHM application data stored in the SSAS layer of the EHM terminal and EHM gateway are required to be marked with collection time.
EHM gateway	
IoT platform	The EHM application data stored in the SSAS layer of the IoT platform and EHM application server are required to be associated with time information, e.g., collection time and expiration time.
EHM application server	

8.3.3 Time synchronization

According to the capability requirements described in clause 9.3.4 of [ITU-T Y.2065], the SSAS layer of the EHM terminal, EHM gateway, IoT platform and EHM application server is required to be able to retrieve time parameters from authoritative time servers or via other ways.

The SSAS layer of the IoT platform is required to be able to publish the time parameters to the EHM gateway, EHM terminals and EHM application servers. It is recommended that the time parameters be published periodically.

8.3.4 Location provisioning

According to the capability requirements described in clause 9.3.5 of [ITU-T Y.2065], the SSAS layer of the EHM terminal and EHM gateway is required to collect the location information from the network layer or device layer according to the collection strategy, such as event-triggered collection or periodic collection.

According to the capability requirements described in clause 9.3.5 of [ITU-T Y.2065], the SSAS layer of the EHM terminal and EHM gateway is required to report the location information required by the application layer in standard format.

According to the capability requirements described in clause 9.3.5 of [ITU-T Y.2065], the SSAS layer of the IoT platform and EHM application server is required to be able to collect the position of EHM terminals and gateways according to the collection strategy, such as event-triggered collection.

8.3.5 Service accounting and charging

According to the capability requirements described in clause 9.3.1 of [ITU-T Y.2065], the SSAS layer of the IoT platform is required to gather data about the usage of EHM services for charging purposes. Different policies may be considered for service accounting and charging, e.g., the number of times the service is used, the amount of time the service is used or the volume of used service data.

The service accounting and charging capability in the SSAS layer of the IoT platform has the following requirements:

- 1) It is required that service accounting and charging be provided to EHM service users.
- 2) It is recommended that service accounting and charging be provided according to the QoS of EHM services.
- 3) It is recommended that service accounting and charging also be provided in support of roaming scenarios for EHM services among networks owned by different network providers.
- 4) It is recommended that service accounting and charging be provided according to the frequency of access to EHM services.
- 5) As a user may use several EHM devices at the same time, it is recommended that unified service charging per user be supported.

8.4 Network layer capabilities of EHM components

8.4.1 Policy-based communication

According to the capabilities requirements described in clause 9.4.1 of [ITU-T Y.2065], the network layer of the EHM terminal, EHM gateway, IoT platform and EHM application server is required to support policy-based communication capability and is required to be able to set the network policy in order to support the QoS of EHM services.

8.4.2 Network-based locating

According to the capability requirements described in clause 9.4.2 of [ITU-T Y.2065], the EHM capabilities on the network layer are recommended to provide the location-related information from the network layer (e.g., IP address, access point location, and so on) to locate the position of EHM terminals and EHM gateways.

Specifically, the network layer of the EHM terminal and EHM gateway is recommended to provide the location-related information. In addition, the network layer of the EHM terminal and EHM gateway is recommended to support event-triggered location information notification. In this way, when the EHM terminal or EHM gateway moves out of a preconfigured network area, a network location information notification may be triggered by the event.

8.4.3 Network resource provision

According to the capability requirements described in clause 9.4.3 of [ITU-T Y.2065], the EHM capabilities on the network layer are required to provide the network resources (e.g., network address, network bandwidth) to establish network connectivity.

Specifically, the network layer of the EHM terminal, EHM gateway, IoT platform and EHM application server is required to be able to provide the network resources (e.g., network address, network bandwidth) to establish network connectivity. The network layer of each of these components is recommended to inform the other EHM components about the provided network resources (e.g., network address, network bandwidth).

8.5 Device layer capabilities of EHM components

8.5.1 Device identification

According to the capability requirements described in clause 9.5.1 of [ITU-T Y.2065], the EHM capabilities on the device layer of the EHM terminal and EHM end point are required to provide device profiles in order to identify the intended use of EHM devices, such as for support of EHMH, EHMR or EHMT services.

8.5.2 Data sensing and processing

According to the capability requirements described in clause 9.5.3 of [ITU-T Y.2065], the EHM capabilities on the device layer of the EHM terminal and EHM end point are required to support data sensing and processing capability to obtain the EHM data.

This capability includes:

1) Data sensing

Data sensing is used to obtain the raw EHM data according to regulation and laws.

2) Data processing

Data processing is used to process the raw EHM data, such as filtering, aggregating and compressing, in order to improve the quality and usage efficiency of EHM data.

The device layer of the EHM terminal is recommended to support data sensing for multiple EHM parameters in a single EHM terminal.

8.5.3 Data collection time provision

According to the capability requirements described in clause 9.5.4 of [\[ITU-T Y.2065\]](#), the EHM capabilities on the device layer of the EHM terminal and EHM gateway are recommended to support data collection time provision, so that the collected EHM data can be marked with the collection time.

This capability includes:

- 1) Time calibration
The time calibration capability is used to obtain time parameters from the SSAS layer and calibrate the built-in time clock of EHM devices.
- 2) Time provision
The time provision capability is used to provide calibrated collection time along with the collected EHM data.

8.5.4 Device-based locating

According to the capability requirements described in clause 9.5.5 of [\[ITU-T Y.2065\]](#), the EHM capabilities on the device layer of the EHM terminal and EHM gateway are recommended to support device-based locating capability.

NOTE – Different techniques (e.g., GPS, gyroscope and motion state sensor) can be used to get the position of EHM terminals or EHM gateways.

It is recommended that location accuracy be indicated along with the location information.

8.5.5 Gateway

According to the capability requirements described in clause 9.5.2 of [\[ITU-T Y.2065\]](#), the device layer of the EHM gateway is required to provide gateway capabilities [\[ITU-T Y.2067\]](#) for connected EHM end points or EHM terminals, e.g., network adaptation capability and raw data processing capability.

8.6 Management capabilities of EHM components

According to the capability requirements described in clause 9.6 of [\[ITU-T Y.2065\]](#), the EHM components are required to support the following management capabilities:

- 1) fault management
The EHM gateway and IoT platform are required to recognize, isolate, correct and log faults. The EHM end point, EHM terminal and EHM application server are required to recognize, correct and log faults.
- 2) configuration management
The EHM terminal and EHM end point are required to be able to be configured remotely. The IoT platform and EHM application server are required to support remote device configuration. The EHM gateway is required to be able to configure the connected EHM end points according to configuration requests from the IoT platform or EHM application server.
- 3) initialization and registration management
The EHM terminal is required to support initialization set-up and registration capability. The EHM end point is required to complete the initialization set-up and registration procedure by itself or with the help of the EHM gateway. The EHM gateway is required to support the initialization set-up and registration capability to help EHM end points, where necessary, in order to complete the initialization set-up and registration.

8.7 Secure capabilities of EHM components

According to the capability requirements described in clause 9.7 of [\[ITU-T Y.2065\]](#), the EHM components are required to support the following security capabilities:

1) Authentication and authorization

The EHM gateway, EHM terminal, IoT platform and EHM application server are required to support authentication and authorization mechanisms.

The EHM gateway and IoT platform are required to support authentication and authorization for EHM devices and EHM application servers.

The EHM devices and EHM application servers are recommended to support a mutual authentication and authorization when accessing the EHM gateway or IoT platform.

The authentication and authorization mechanisms among the EHM gateway, IoT platform, EHM devices and EHM application servers can be based on network level authentication mechanisms (e.g., IP based or SIM card based) or application level authentication mechanisms (e.g., certificate based or account and password based).

The authentication and authorization mechanisms between EHM devices and the EHM gateway can be additionally based on authentication mechanisms (e.g., Bluetooth based, wired connection based) of the local network among EHM devices and gateways.

The EHM terminal and EHM application server are required to support authentication and authorization for EHM customer access.

NOTE – EHM gateways that support EHM customer access are also required to provide authentication and authorization for accessing users.

2) Secure communications

All EHM components are required to support secure communications. The EHM application, EHM terminal and IoT platform are required to support secure communications through the communication network. The EHM end point is required to support secure communications through the local network among EHM devices and gateways. The EHM gateway is required to support secure communications through both the communication network and the local network among EHM devices and EHM gateways.

3) Confidentiality

All EHM components are required to enforce the confidentiality of the data whenever the data are exchanged, stored or processed.

4) Integrity

All EHM components are required to guarantee the integrity of data when the data are transmitted. Any loss of integrity of the transmitted data must be recognizable by the receiving components.

5) Access control

The EHM gateway, EHM terminal, IoT platform and EHM application server are required to ensure that only authorized EHM components are able to access protected data and only authorized users can access the EHM components.

6) Audit trail

The EHM gateway, EHM terminal, IoT platform and EHM application server are required to trace and record any access or attempt to access EHM data.

7) Data storage security

All EHM components that support data storage are required to support data integrity validation and data privacy protection. In addition, the IoT platform and EHM application server are required to support data backup, anti-hacker data protection, uninterruptible power of data storage and data recovery.

Annex A

Overview of EHM component capabilities

(This annex forms an integral part of this Recommendation.)

Table A.1 summarizes the capabilities of the different EHM components and assigns the following indicators:

- "MA" means this capability is required in the EHM component.
- "REC" means this capability is recommended in the EHM component.
- "NA" means this capability is not supported by the EHM component.

Table A.1 – Overview of EHM component capabilities

Capabilities		EHM component				
		EHM end point	EHM terminal	EHM gateway	IoT platform	EHM application server
Application layer capabilities	Information sharing	MA	MA	MA	MA	MA
	Accounting-related information provision	REC	REC	REC	NA	REC
	QoS information provision	REC	REC	REC	NA	REC
SSAS layer capabilities	Message conversion	NA	MA	MA	MA	MA
	Data storage	NA	MA	MA	MA	MA
	Time synchronization	NA	MA	MA	MA	MA
	Location provisioning	NA	MA	MA	MA	MA
	Service accounting and charging	NA	NA	NA	MA	NA
Network layer capabilities	Policy-based communication	NA	MA	MA	MA	MA
	Network-based locating	NA	REC	REC	NA	NA
	Network resource provision	NA	REC	REC	REC	REC
Device layer capabilities	Device identification	MA	MA	NA	NA	NA
	Data sensing and processing	MA	MA	NA	NA	NA
	Data collection time provision	NA	REC	REC	NA	NA
	Device-based locating	NA	REC	REC	NA	NA
	Gateway	NA	NA	MA	NA	NA

Table A.1 – Overview of EHM component capabilities

Capabilities		EHM component				
		EHM end point	EHM terminal	EHM gateway	IoT platform	EHM application server
Management capabilities	Fault management	NA	MA	MA	MA	MA
	Configuration management	MA	MA	MA	MA	MA
	Initialization and registration management	MA	MA	MA	NA	NA
Secure capabilities	Authentication and authorization	NA	MA	MA	MA	MA
	Security communications	MA	MA	MA	MA	MA
	Confidentiality	MA	MA	MA	MA	MA
	Integrity	MA	MA	MA	MA	MA
	Access control	NA	MA	MA	MA	MA
	Audit trail	NA	MA	MA	MA	MA
	Data storage security	NA	MA	MA	MA	MA

Appendix I

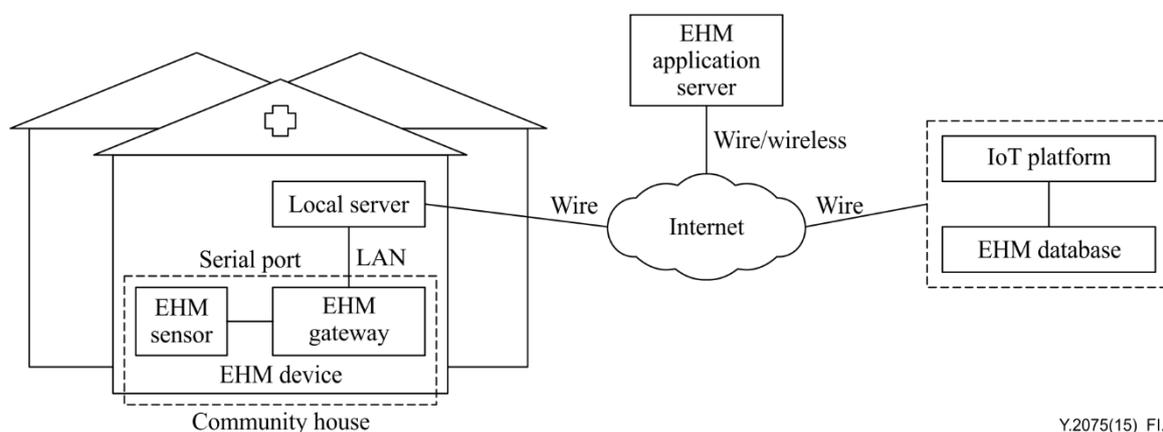
EHM service deployment technical scenarios

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

This appendix gives examples of EHM service deployment technical scenarios involving EHM components.

I.1 Technical scenario for community EHM services

In community environment, EHM services are provided by qualified facilities and serve all inhabitants of a community. Figure I.1 shows a deployment case for community EHM service.



Y.2075(15)_FI.1

Figure I.1 – EHM services deployed in community environment

As shown in Figure I.1, the EHM devices, including EHM sensors and EHM gateways, are deployed in the community house. Usually, there are several EHM sensors, such as ECG, blood pressure meter, weighing scales, thermometer and densitometer, with which general practitioners can check the health states of inhabitants. In the current market, most EHM sensors just have limited communication capabilities, e.g., a lot of EHM sensors just have serial port interfaces in order to reduce sensor cost.

To obtain extended communication capabilities, EHM sensors connect to EHM gateways to communicate and interwork with the local server(s), as shown in Figure I.1. The EHM gateways provide communication protocol translation between the EHM sensors and local server. The southbound ports of the EHM gateways usually use point-to-point short-distance communication protocols (e.g., serial port and USB); the northbound ports of the EHM gateways usually use the Ethernet protocol. Multiple EHM gateways can be connected to the local server via star topology.

The local server, as shown in Figure I.1, has four main functions: firstly, it manages the EHM gateways and EHM sensors in the community house; secondly, it analyses and stores the EHM data sent by the EHM sensors; thirdly, it reports the local EHM data to the EHM application server and IoT platform; fourth, it receives notification from the IoT platform to update the local software.

The EHM application server, as shown in Figure I.1, has two main functions: firstly, it analyses and stores the EHM data sent by the local server in the community house; secondly, it can share EHM data, analysis results and computing capability with other EHM application servers.

The IoT platform, as shown in Figure I.1, provides capabilities to facilitate reliability, security, efficient interworking between the EHM application server and the local server in the community house. Usually the IoT platform connects with an EHM database which stores and manages EHM data.

I.2 Technical scenario for mobile EHM services

In the mobile EHM services scenario, users usually use a handset (e.g., mobile phone or pad) to access the EHM services via a wireless network (e.g., cellular network or carrier-WiFi network).

The technical deployment for this scenario shown in Figure I.2 involves such entities as sensor, handset, network, EHM application server, IoT platform and EHM database. Solid boxes represent mandatory entities in this scenario. The dashed boxes represent an optional entity, and the dot dashed boxes mean that the included entities can be integrated as an entity.

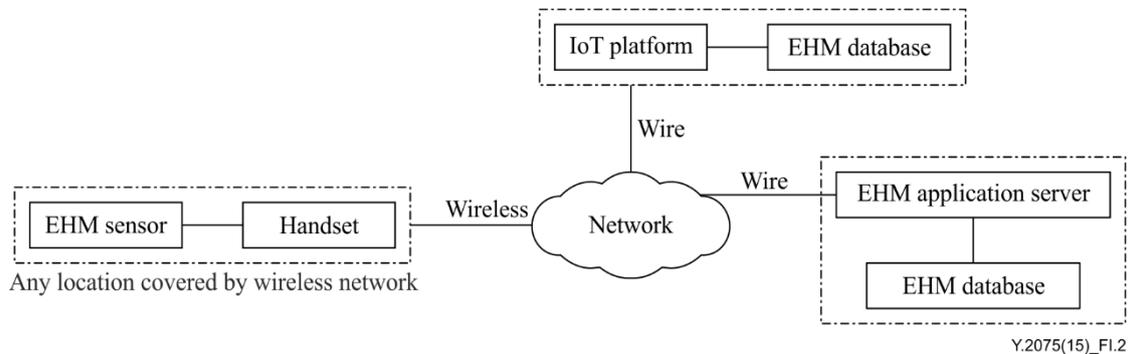


Figure I.2 – Mobile EHM services

1) EHM sensor

The EHM sensor can be seen as a type of EHM end point, which can sense EHM-related data from the body of a user, but cannot access the communication network directly. There are two methods for the deployment of a sensor. One is to deploy the EHM sensor inside the handset, which can use the communication capability of the handset via an internal interface. The other is to deploy the EHM sensor as a single device outside the handset. The sensor can access the handset via a local communication protocol (e.g., Bluetooth or USB).

2) Handset

The handset is a type of communication terminal, which can access the communication network via wireless communication. In the mobile EHM service deployment scenario, it can play the role of communication gateway and provide the EHM data collected by the EHM sensors to a remote EHM application server and IoT platform. Besides the communication capability, the handset can also process and manage the EHM data collected by EHM sensors or feedback from the EHM application server and IoT platform based on the EHM application running on them and show the results to users.

3) Network

The network in the mobile EHM service deployment scenario is a type of communication network, which can provide wireless access to the handset and also provide wired access to the EHM application server and IoT platform. It supports interconnection among the handset, EHM application server and IoT platform.

4) EHM application server

The EHM application server provides capabilities for analysing and managing the EHM data provided by the handset or IoT platform and feeds the corresponding diagnosis results back to the handset or IoT platform.

The IoT platform connects the handset with the EHM application server. It provides the service support and application support capabilities for the handset and the EHM application server. In practical deployment scenarios, multiple IoT platforms with different capability sets may be deployed to form a virtual IoT platform.

5) EHM database

The EHM database is used for EHM data storage. Both the handset and EHM application server can access the EHM database by authorization. There are three possible methods for the deployment of the EHM database. The first consists of deploying the EHM database in the IoT platform and opening secure access to the EHM database for the EHM application server and the handset. The second consists of deploying the EHM database on the EHM application server. The last is a hybrid method, consisting of deploying the EHM database both in the IoT platform and the EHM application server.

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	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	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