

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

H.812.4

(11/2017)

SERIES H: AUDIOVISUAL AND MULTIMEDIA SYSTEMS

E-health multimedia services and applications – Personal
health systems

Interoperability design guidelines for personal connected health systems: Services interface: Authenticated Persistent Session capability

Recommendation ITU-T H.812.4



International
Telecommunication
Union

Document Sharing Hub

ITU-T H-SERIES RECOMMENDATIONS
AUDIOVISUAL AND MULTIMEDIA SYSTEMS

CHARACTERISTICS OF VISUAL TELEPHONE SYSTEMS	H.100–H.199
INFRASTRUCTURE OF AUDIOVISUAL SERVICES	
General	H.200–H.219
Transmission multiplexing and synchronization	H.220–H.229
Systems aspects	H.230–H.239
Communication procedures	H.240–H.259
Coding of moving video	H.260–H.279
Related systems aspects	H.280–H.299
Systems and terminal equipment for audiovisual services	H.300–H.349
Directory services architecture for audiovisual and multimedia services	H.350–H.359
Quality of service architecture for audiovisual and multimedia services	H.360–H.369
Telepresence	H.420–H.429
Supplementary services for multimedia	H.450–H.499
MOBILITY AND COLLABORATION PROCEDURES	
Overview of Mobility and Collaboration, definitions, protocols and procedures	H.500–H.509
Mobility for H-Series multimedia systems and services	H.510–H.519
Mobile multimedia collaboration applications and services	H.520–H.529
Security for mobile multimedia systems and services	H.530–H.539
Security for mobile multimedia collaboration applications and services	H.540–H.549
VEHICULAR GATEWAYS AND INTELLIGENT TRANSPORTATION SYSTEMS (ITS)	
Architecture for vehicular gateways	H.550–H.559
Vehicular gateway interfaces	H.560–H.569
BROADBAND, TRIPLE-PLAY AND ADVANCED MULTIMEDIA SERVICES	
Broadband multimedia services over VDSL	H.610–H.619
Advanced multimedia services and applications	H.620–H.629
Ubiquitous sensor network applications and Internet of Things	H.640–H.649
IPTV MULTIMEDIA SERVICES AND APPLICATIONS FOR IPTV	
General aspects	H.700–H.719
IPTV terminal devices	H.720–H.729
IPTV middleware	H.730–H.739
IPTV application event handling	H.740–H.749
IPTV metadata	H.750–H.759
IPTV multimedia application frameworks	H.760–H.769
IPTV service discovery up to consumption	H.770–H.779
Digital Signage	H.780–H.789
E-HEALTH MULTIMEDIA SERVICES AND APPLICATIONS	
Personal health systems	H.810–H.819
Interoperability compliance testing of personal health systems (HRN, PAN, LAN, TAN and WAN)	H.820–H.859
Multimedia e-health data exchange services	H.860–H.869

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

Recommendation ITU-T H.812.4

Interoperability design guidelines for personal connected health systems: Services interface: Authenticated Persistent Session capability

Summary

The Continua Design Guidelines (CDG) defines a framework of underlying standards and criteria that ensure the interoperability of devices and data used for personal connected health services. The Continua Design Guidelines also contains design guidelines (DGs) that further clarify the underlying standards or specifications by reducing options or by adding missing features to improve interoperability.

ITU-T H.812.4 defines the additional design guidelines for the Authenticated Persistent Session (APS), whose function is to provide a secure, long-lived, persistent bidirectional data channel between the Health & Fitness services application and a Personal Health Gateway (PHG) application, suitable for sending unsolicited commands to the PHG or to devices connected via the PHG.

ITU-T H.812.4 is part of the "ITU-T H.810 interoperability design guidelines for personal connected health systems" subseries that covers the following areas:

- ITU-T H.810 – Interoperability design guidelines for personal connected health systems: Introduction
- ITU-T H.811 – Interoperability design guidelines for personal connected health systems: Personal Health Devices interface
- ITU-T H.812 – Interoperability design guidelines for personal connected health systems: Services interface
- ITU-T H.812.1 – Interoperability design guidelines for personal connected health systems: Services interface: Observation Upload capability
- ITU-T H.812.2 – Interoperability design guidelines for personal connected health systems: Services interface: Questionnaire capability
- ITU-T H.812.3 – Interoperability design guidelines for personal connected health systems: Services interface: Capability Exchange capability
- ITU-T H.812.4 – Interoperability design guidelines for personal connected health systems: Services interface: Authenticated Persistent Session capability (this design guidelines document)
- ITU-T H.813 – Interoperability design guidelines for personal connected health systems: Healthcare Information System interface.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T H.812.4	2015-11-29	16	11.1002/1000/12657
2.0	ITU-T H.812.4	2016-07-14	16	11.1002/1000/12917
3.0	ITU-T H.812.4	2017-11-29	16	11.1002/1000/13419

Keywords

CDG, Continua Design Guidelines, healthcare information systems, persistent session, personal connected health systems, personal health devices, services.

* 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 2018

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
0	Introduction..... vi
0.1	Organization vi
0.2	Guideline releases and versioning vi
0.3	What's new..... vi
1	Scope..... 1
2	References..... 1
3	Definitions 1
4	Abbreviations and acronyms 1
5	Conventions 1
6	Authenticated Persistent Session use case 1
7	Authenticated Persistent Session (APS) overview 1
7.1	Support for multiple CCCs..... 3
7.2	Topics used in MQTT 4
7.3	Shoulder tap 5
8	APS management..... 5
8.1	APB resources 6
8.2	APS behaviour 11
8.2.1	APS session state..... 11
8.2.2	Authenticated persistent binding identifiers (APBI)..... 11
8.2.3	Authenticated persistent binding establishment..... 12
8.2.4	Accepting an authenticated persistent binding..... 12
8.2.5	Authenticated persistent binding and session termination 12
8.2.6	APS-CCC diagnostic message 13
9	Behavioural model: MQTT 15
9.1	Overview of operation..... 15
9.1.1	Graceful APS termination 16
9.2	Interaction of the Health & Fitness services application with the PHG application 17
9.3	State of the PHG's connection to the HFS MQTT server..... 17
9.3.1	Interaction of a PHG application with the MQTT server..... 18
10	Behavioural model: SMS shoulder tap capability 21
10.1	Shoulder tap overview 21
10.2	Scope 22

Rec. ITU-T H.812.4 (11/2017)



Documents

Document Sharing Hub

iii

	Page
10.3 Shoulder tap invocation determination.....	22
10.4 PHG SMS information	23
10.5 SMS message structure.....	23
10.6 PHG application requirements	24
10.7 Semantic behaviour of the PHG application relative to ST reception.....	24
Annex A – Normative guidelines for the APS-CCC	25
A.1 Guidelines for the APS components in capabilities exchange	25
A.2 Guidelines for PHG APS management (APS-CCC-PHG)	26
A.3 Guidelines for the PHG application interactions with the MQTT server	28
A.4 Guidelines for HFS application APS management.....	31
A.5 Guidelines for the PHG application SMS shoulder tap	36
A.6 Guidelines for the Health & Fitness services application SMS shoulder tap	36
Annex B – XML schema for the APB resource.....	37
Appendix I – APS details.....	39
I.1 APS information in the root.xml	39
I.2 APS authentication: Resource owner password credentials approach	39
I.3 APS establishment: PHG application POST with partial APB	40
I.3.1 APS establishment: PHG GET for completed APB	40
I.3.2 APS establishment: PHG setup with MQTT server.....	42
I.3.3 MQTT: PHG application subscribes to commands	42
I.3.4 MQTT: PHG Application Publishes "CONNECTED"	42
I.4 APS establishment: PHG application enables APS	42
I.5 Operation	42
Appendix II – Example Health & Fitness service root.xml file.....	44
Bibliography.....	45

List of Tables

	Page
Table 7-1 – Topics used in MQTT.....	4
Table 8-1 – APB xml elements provided by PHG application	7
Table 8-2 – APB xml elements provided by Health & Fitness application	9
Table 8-3 – Fields of the APS-CDC diagnostic message	13
Table 9-1 – State table for the status topic.....	17
Table 9-2 – Information contained in the PHG application's MQTT connect message	19
Table 9-3 – Information contained in MQTT SUBSCRIBE message.....	20
Table 9-4 – Information contained in the PHG's Publish Status message	20
Table 9-5 – Information contained in the PHG application's MQTT Publish Response message	21
Table 10-1 – Structure of payload.....	24
Table 10-2 – Continua information elements	24
Table A-1 – APS elements of capabilities exchange	25
Table A-2 – APS management PHG.....	26
Table A-3 – PHG-MQTT exchanges	28
Table A-4 – APS management requirements for the Health & Fitness services application	31
Table A-5 – SMS shoulder tap PHG.....	36
Table A-6 – HFS application SMS shoulder tap.....	36

List of Figures

	Page
Figure 7-1 – APS framework	2
Figure 7-2 – Example of payload delivery to different message handlers.....	4
Figure 8-1 – Profile element indicating capability.....	6
Figure 8-2 – ResourceType element describing APB content	7
Figure 8-3 – Section element describing where to POST	7
Figure 8-4 – Example of PHG application supporting MQTT and an SMS shoulder tap	11
Figure 9-1 – PHG application and Health & Fitness services application MQTT client interactions	16
Figure 9-2 – State diagram for the status topic	17
Figure 10-1 – Shoulder tap overview.....	22
Figure 10-2 – Payload of binary SMS message	23
Figure I-1 – Example APB posted by PHG application	40
Figure I-2 – APB created by Health & Fitness service application	41

0 Introduction

The Continua Design Guidelines (CDG) defines a framework of underlying standards and criteria that ensure the interoperability of devices and data used for personal connected health services. The Continua Design Guidelines also contain additional design guidelines that further clarify the underlying standards or specifications by reducing options or by adding missing features to improve interoperability.

This design guidelines defines the additional design guidelines for the Authenticated Persistent Session (APS), whose function is to provide a secure, long-lived, persistent bidirectional data channel between the Health & Fitness services application and a Personal Health Gateway (PHG) application, suitable for sending unsolicited commands to the PHG or to devices connected via the PHG.

This design guidelines is part of the "ITU-T H.810 interoperability design guidelines for personal health systems" subseries. See [ITU-T H.810] for more details.

0.1 Organization

This design guidelines document is organized in the following manner:

Clauses 0 to 5: Introduction and terminology – These clauses provide useful background information to help understand the structure of the design specifications.

Clause 6: Use cases – This clause provides a descriptive scenario that motivates the class of problems that the APS is addressing.

Clause 7: Authenticated Persistent Session overview – This clause provides a technical overview of the operation of the Authenticated Persistent Session (APS).

Clause 8: Authenticated Persistent Session management – This clause describes the interactions between the information exchange parties.

Clause 9: Behavioural model: MQTT – This clause is an overview of sequences of interactions under this Certified Capability Class (CCC) and summarizes typical iterations, constraints and exceptions.

Clause 10: Behavioural model: SMS shoulder tap capability – This clause defines an SMS-based capability that facilitates operation of the APS with networks that remove IP infrastructure for inactive connections.

Annex A: The guidelines that document the normative elements for the Authenticated Persistent Session are presented in a tabular format in this annex. The annex references other locations with normative content.

Annex B: root file for an Authenticated Persistent Session.

Appendix I: APS details.

Appendix II: APB resource schema.

0.2 Guideline releases and versioning

See clause 0.2 of [ITU-T H.810] for release and versioning information.

0.3 What's new

To see what is new in this release of the design guidelines, refer to clause 0.3 of [ITU-T H.810].

Recommendation ITU-T H.812.4

Interoperability design guidelines for personal connected health systems: Services interface: Authenticated Persistent Session capability

1 Scope

This design guidelines document defines two Certified Capability Classes. Both Certified Capability Classes contain guidelines that document a secure mechanism by which a services application can initiate communications with an application residing within a transient piece of customer premises equipment known as a Personal Health Gateway (PHG). The two Certified Capability Classes are respectively for the services application (APS-CCC-Services) and for the PHG application (APS-CCC-PHG).

The mechanism addresses: (1) the establishment and management of a persistent long term session between the services application and the PHG application, (2) the use of the message queuing telemetry transport (MQTT) protocol for message exchange and (3) the use of short message service (SMS) to re-establish IP level connectivity with transient PHGs that have a cellular interface.

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 H.810] Recommendation ITU-T H.810 (2017), *Interoperability design guidelines for personal connected health systems: Introduction*.

All other referenced documents can be found in clause 2 of [ITU-T H.810].

3 Definitions

This design guidelines document uses terms defined in [ITU-T H.810].

4 Abbreviations and acronyms

This design guidelines document uses abbreviations and acronyms defined in [ITU-T H.810].

5 Conventions

This design guidelines document follows the conventions defined in [ITU-T H.810].

6 Authenticated Persistent Session use case

The Authenticated Persistent Session provides a mechanism by which future Continua Certified Capability Classes (CCCs) can initiate communications from cloud based services to the PHG.

7 Authenticated Persistent Session (APS) overview

The Authenticated Persistent Session Certified Capability Class defines a long lived, persistent context for exchanging messages between a Health & Fitness services application and a PHG application. The context is persistent in that it maintains operational state across TCP connections, pausing when the underlying TCP connection is lost and resuming when it is re-established. The session is long lived in that applications maintain the session for whatever time duration is required.

Long lived persistent sessions support applications that send occasional messages requiring a timely response.

NOTE 1 – These guidelines define an Authenticated Persistent Session Certified Capability Class for a PHG application (APS-CCC-PHG) and for a Health & Fitness services application (APS-CCC-Services Interface). The notation APS-CCC is used as a shorthand when it is not necessary to disambiguate between the actual service and PHG CCCs.

The APS-CCC is optimized for sending messages over networks where bandwidth, power, and IP resources are limited. The optimization is obtained by eliminating PHG application based polling. The APS-CCC defines an optional wake up capability based on the short message service (SMS) for use when the PHG has cellular network connectivity. This capability allows the Health & Fitness services application to wake up a PHG application that no longer has IP connectivity due to the cellular network reallocating inactive resources. Implementations that support SMS may be able to take advantage of this optional capability in order to minimize their network utilization.

The term *Authenticated Persistent Session* (APS) describes the concept of the persistent session as defined in this design guidelines document. A related term, *authenticated persistent binding* (APB) is used to describe the information resource exchanged during persistent session establishment. We qualify *persistent session* and *persistent binding* with *authenticated* to emphasize a relationship that the Health & Fitness services application creates between the APB resource and a PHG application security credential in order to ensure proper authentication when the PHG application resumes a persistent session.

Figure 7-1 depicts the framework of the APS.

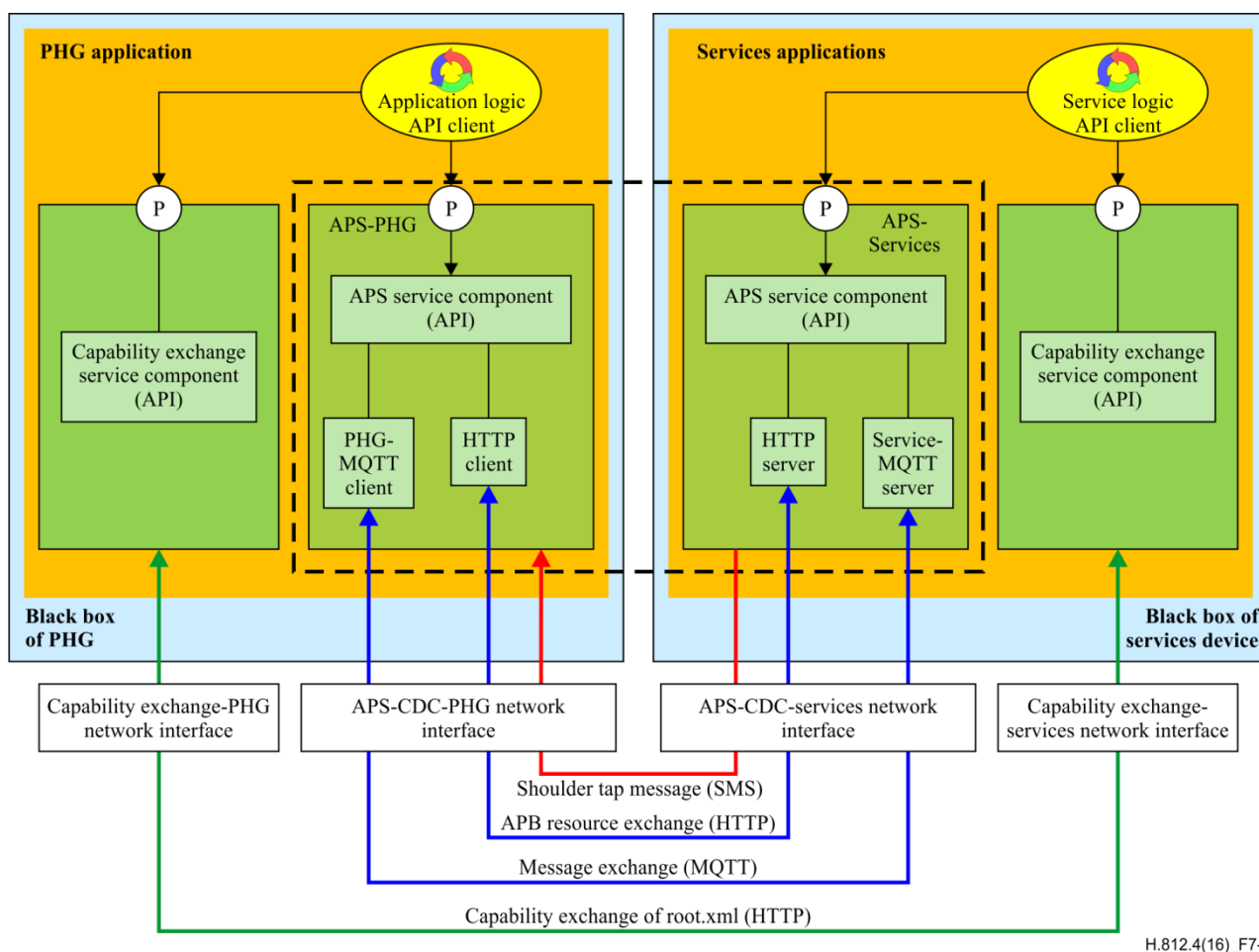


Figure 7-1 – APS framework

An Authenticated Persistent Session (APS) is a binding between two *APS service components*, one in the *Health & Fitness services application* and one in the *PHG application*, which enables the *API clients* to behave as if there is an always connected pipe between them. In Figure 7-1 the *APS API service components* are the peer entities that implement these guidelines in order to deliver the persistent session service to their *API clients*. The *Health & Fitness services application* using the *APS API client* component (see clause 6.1.1 *Devices, components, applications and interfaces* of [ITU-T H.810]) can securely issue commands to the PHG application, across service disruptions, without needing to manage the connectivity or authenticity of the peer.

NOTE 2 – Figure 7-1 represents an architectural model and does not mandate a particular implementation.

NOTE 3 – The existence of an APS between two components does not mean that messages can be exchanged between the components at a given point in time. Message delivery is only possible when there is connectivity at the transport layer.

The APB resource that defines the APS is based on exchanged security credentials using a given source of authentication information. Any entity that provides the appropriate authentication information may gain access to the APS and continue the persistent session.

NOTE 4 – It is possible for an APS to move from one physical device to a different physical device as long as the PHG implementation presents the same credentials. Therefore, a Health & Fitness services application should not assume that an APS represents a connection to a particular PHG hardware platform; the APS is bound to a security credential such as an X.509 certificate, an OAuth token, or SAML token.

There are three steps involved in creating and exchanging a message using an APS. Once the APS is in place only the final step is needed to send additional messages. The three steps, in order are:

- Capability Exchange, see [ITU-T H.812.3] – In this phase the PHG application obtains information from the Health & Fitness services application using HTTP. The information identifies if the Health & Fitness services application has support for APS-CCC-Services. The information is contained in the root.xml file of the Health & Fitness services application and includes the URL to use for APS establishment. See clause 8.1.
- APS establishment – The PHG application, using a secure HTTPS connection, creates the APB resource on the Health & Fitness services application indicating its desire to establish a persistent session. During this phase the PHG application authenticates itself to the Health & Fitness services application and is provided with APB resource information. When this phase completes the PHG has either established the APS and is ready to exchange messages with the Health & Fitness services application, or has terminated the APS establishment process causing the APB resource to be removed. See clause 8.2.3.
- Message exchange using MQTT (see clause 9) – In this phase a transport level security (TLS) connection is established by the PHG application connecting it to the MQTT server exposed by the Health & Fitness services application. This connection is used for the normal exchange of messages. In an APS the management information is contained in the APB resource, which is manipulated using RESTful operations over HTTPS. The data flow associated with the operation of the APS is carried in messages flowing over the MQTT connection. Once an APS has been created there is typically no additional management activity, so all activity is over MQTT.

7.1 Support for multiple CCCs

A PHG application in the future may contain multiple CCCs (or vendor specific components) that make use of the APS. An example of this might be a CCC for remote PHG configuration. These CCCs will have message handlers to process the received messages. Each message that is transmitted from the services application is addressed to one of these message handlers via the topic name used in the MQTT PUBLISH command. It is the responsibility of the APS implementer to ensure that messages received by the PHG application are dispatched to the correct message handler.

NOTE 1 – The dispatcher does not use any information in the MQTT payload. The payload is opaque to the dispatcher.

Figure 7-2 shows an example of delivering the payload in an MQTT message to different message handlers. There are two message handlers in this example: 1) the APS management message handler which supports the ECHO message; 2) an undefined future CCC or vendor specific message handler. The MQTT message is received by the Network-IF component which forwards it to the dispatcher. The dispatcher extracts the MQTT header. The MQTT header contains the topic name which identifies the message handler to which the payload needs to be delivered. The topic name is a string that uniquely identifies the CCC that is expected to process the message.

NOTE 2 – This description is illustrative and does not proscribe a particular method of implementation.

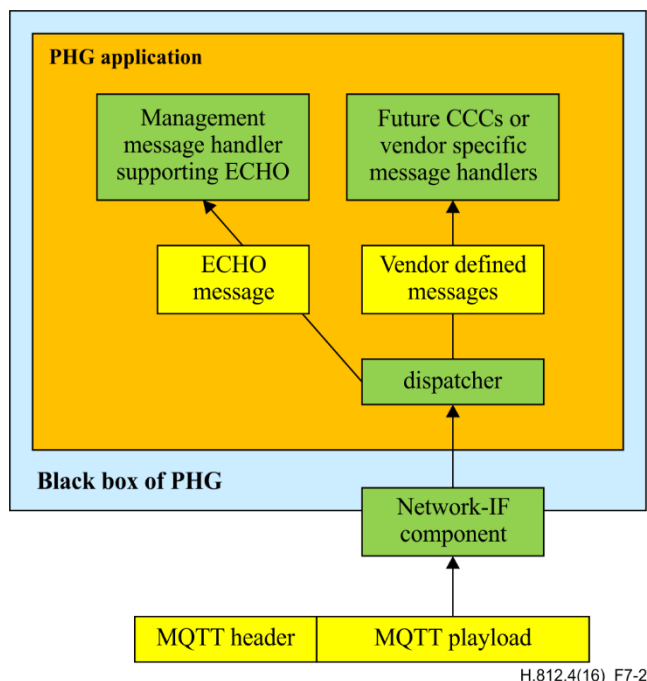


Figure 7-2 – Example of payload delivery to different message handlers

7.2 Topics used in MQTT

Continua compliant entities implementing the APS-CCC **shall** support the use of the MQTT protocol to publish and subscribe to messages. The MQTT protocol uses a topic-based addressing mechanism, and this standard specifies three kinds of topics to be used by an APS. They are shown in Table 7-1.

Table 7-1 – Topics used in MQTT

Name used in this document	Format of the topic string used in MQTT	Description
Message topics	pcha/message/<HFS APBI>/<PHG APBI>/<mh>	Topics used to transmit messages to the APS API client components in the PHG application.
Status topic	pcha/status/<HFS APBI>/<PHG APBI>	Topic used to track status of the APS
Response topics	pcha/response/<HFS APBI>/<PHG APBI>/<mh>	Topic used to receive responses from the PHG application

Each APS is identified by a pair of APB identifiers (APBIs) in the corresponding APB resource, and these APBIs **shall** be inserted in the topic strings in place of the characters <PHG APBI> and <Services APBI>. See clause 8.2.2 for more details on the APBIs. The <mh> **shall** be replaced by an identifier specified by the CCC that is using the APS exchange mechanism. The identifier allows different CCC peers to exchange messages in the context of a single APS. An example of a message topic for an APS might appear as follows:

```
pcha/message/1/34521ee41da2eff/APS.
```

The MQTT server **shall** control access to these topics using the following rules:

- A Health & Fitness services application **shall** have write access to any message topics containing its Services APBI.
- A Health & Fitness services application **shall** have read access to the status and response topics containing its Services APBI.
- A PHG application **shall** have read access to any message topics containing its PHG APBI.
- A PHG application **shall** have write access to any status topics containing its PHG APBI.
- A PHG application **shall** have write access to any response topics containing its PHG APBI.
- Suitably authenticated management applications **MAY** have read access to any topic.
- All other access **shall** NOT be permitted.

In general the above requirements are stating that an APS-CCC shall only have access to topics defined for that APS-CCC. A similar relationship holds, in theory, between the Health & Fitness services application and MQTT server, but how the Health & Fitness services application and MQTT server actually interact is implementation dependent. In many implementations the Health & Fitness services application is also the authenticated management application.

7.3 Shoulder tap

If the Health & Fitness services application needs to send a message to the PHG application and the PHG application is no longer connected to the MQTT server, the Health & Fitness services application can use one of the shoulder tap methods supported by the PHG application to alert it that a message is waiting. The PHG application, upon reception of the shoulder tap, reconnects to the MQTT server. The PHG is then able to receive messages from the Health & Fitness services application. Currently the only defined shoulder tap method is binary SMS messaging.

8 APS management

An authenticated persistent session (APS) is a long term association between two mutually authenticated peer entities, one associated with the Health & Fitness services application and the other with the PHG application. Authentication is performed using TLS in conjunction with OAUTH as outlined in Annex B of [ITU-T H.812].

The Health & Fitness services application, after it has successfully authenticated the PHG application allocates a resource, called the authenticated persistent binding (APB). The APB contains a set of attributes that both define the APS and provide the basis for its management. It is the responsibility of the Health & Fitness services application to ensure that for a given OAUTH bearer token: (1) the same APB **shall** be returned on repeated requests for the APS resource, and that (2) if a different OAUTH bearer token is provided a different APS resource (or an error) **shall** be returned.

The APB resource is an XML document with a set of elements as defined in Table 8-1 and Table 8-2. The management of APB resources is covered in this clause.

The Health & Fitness services application implementing the APS-CCC uses hData to present to the PHG application three items relating to APSs in the root.xml file. The first item is a *profile*. The profile is an entry that indicates that the Health & Fitness services application supports the APS-CCC. The second item, *resourceType*, describes the content of the APB resource and contains a reference to a XML schema that can be used to validate it. The third item, *section*, is an entry that indicates to the PHG application where to POST its contribution to the APB resource when first establishing the APS.

The initial content of the APB resource is jointly established by the PHG and Health & Fitness services applications. The PHG application provides an APB resource structured in accordance with the XML schema identified in the *resourceType* element of the root.xml file. The PHG application provides values for a subset of the APB elements as identified in Table 8-1. The Health & Fitness services application when it receives the APB resource from the PHG application fills in the remaining elements as defined in Table 8-1.

During the establishment of an APS, a pair of identifiers is allocated by the Health & Fitness services application. These identifiers are part of the APB resource. One identifier in the pair is associated with the PHG application (PHG APBI) and the other identifier is associated with the Health & Fitness services application (services APBI). The services APBI together with the PHG APBI identify the APB instance and **shall** be unique across all the APSs being managed by the Health & Fitness services application.

8.1 APB resources

The APS-CCC-Services defines a management interface that uses HTTPS and hData. These mechanisms prescribe a RESTful and secure access mechanism to information defining the APS, which is contained in the APB resource. The starting point for the hData layout of this interface is the root.xml file. For a Health & Fitness services application implementing the APS-CCC-Services the root.xml file **shall** contain the entries as specified in Figure 8-1, Figure 8-2 and Figure 8-3.

```
<profile>
  <!-- Specified value -->
  <id>APS-CCC-Services</id>
  <reference>
    http:// handle.itu.int/11.1002/3000/hData/APS/2017/01/H.812.4.pdf
  </reference>
</profile>
```

Figure 8-1 – Profile element indicating capability

The entry in Figure 8-1 indicates to the PHG application that the Health & Fitness services application supports the APS message transfer infrastructure (APS-CCC-Services). This entry **shall** appear exactly as shown in Figure 8-1.

```

<resourceType>
  <resourceTypeID>APB</resourceTypeID>
  <!-- location of reference that describes the APS standard -->
  <reference>
    http://handle.itu.int/11.1002/3000/hData/APS/2017/01/H.812.4.pdf
  </reference>
  <representation>
    <mediaType>application/xml</mediaType>
    <!-- Schema for the APB resource xml -->
    <validator>
      http://handle.itu.int/11.1002/3000/hData/APS/2017/01/APBConfigResource.xsd
    </validator>
  </representation>
</resourceType>

```

Figure 8-2 – ResourceType element describing APB content

The entry in Figure 8-2 provides a description and the structure (such as a schema) of the APB. The entry **shall** appear exactly as shown in Figure 8-2.

```

<section>
  <!-- chosen by the Health & Fitness application -->
  <path>path/to/post/folder</path>
  <profileID>APS-CAC-Services</profileID>
  <!-- required in this specification; optional but recommended in hData; -->
  <resourcePrefix>true</resourcePrefix>
  <resourceTypeID>APB</resourceTypeID>
</section>

```

Figure 8-3 – Section element describing where to POST

The entry in Figure 8-3 identifies a URL to which the PHG application performs the initial POST in the APS establishment. The <profileID> element value **shall** be that of the <id> element value in the <profile> element and the <resourceTypeID> value **shall** be APB. The <resourcePrefix> element **shall** be present in this specification and it **shall** be set to true (it is optional in the hData specification). The <path> element **shall** be present but the URL value is determined by the application.

Table 8-1 and Table 8-2 describe the contents of the APB resource that characterizes the APS.

The APB resource is expressed as an xml document, an example of which is shown in Figure 8-4. The example in Figure 8-4 shows a PHG application supporting MQTT and an SMS shoulder tap. See Appendix II for the APB resource schema.

Table 8-1 – APB xml elements provided by PHG application

Element	Usage
supportedMH	Mandatory – A space-separated list identifying the message handlers that are supported by the PHG application. All PHG applications that support APS message transfer shall support the APS diagnostic handler as denoted below. – The three uppercase characters "APS" This value shall be ignored by the PHG application whenever the APB resource is obtained from the Health & Fitness services application.

Table 8-1 – APB xml elements provided by PHG application

Element	Usage
	Note – If a vendorspecific message handler is used, the identifying string should have properties that minimize the potential for a collision with another uncoordinated vendor message handler.
exchangeMechanism	Mandatory – A space-separated list identifying the underlying technologies that are being used by the PHG application to support message exchanges. The PHG application shall identify each technology that it supports in an ordered list with the first entry in the list being its preferred choice. The only currently supported exchange mechanism is MQTT. This value shall be ignored by the PHG application whenever the APB resource is obtained from the Health & Fitness services application.
shoulderTapMechanism	Mandatory – A space-separated list identifying the underlying technologies that the PHG application uses to accept a shoulder tap. The shoulder tap enables the Health & Fitness services application to re-establish a TCP connection with the PHG application in the event that the resources used to maintain that connection have been removed. The PHG application identifies each technology that it supports in an ordered list with the first entry in the list being its preferred choice. The Health & Fitness services application shall select the first technology that it supports from the list. If the PHG application does not support a shoulder tap it shall provide an empty list. SMS is currently the only defined mechanism for performing a shoulder tap. This value shall be ignored by the PHG application whenever the APB resource is obtained from the Health & Fitness services application.
SMS	Conditionally required – This element shall be present if a shoulder tap mechanism of SMS is selected. The SMS element contains the information that the Health & Fitness services application will use in order to perform the shoulder tap operation. The SMS element is the parent element for SMSHeaderDstPort, SMSApplicationId, and MSISDN. This value shall be ignored by the PHG application whenever the APB resource is obtained from the Health & Fitness services application.
MSISDN	Mandatory SMS Child – The MSISDN is the SMS number used to reach the PHG application (the PHG application's 'phone number'). It shall be composed of the numeric digits [0-9] with an optional leading "+". The total string shall be 15 characters of less. This value shall be ignored by the PHG application whenever the APB resource is obtained from the Health & Fitness services application.
SMSHeaderDstPort	Mandatory SMS Child – The SMSHeaderDstPort gives the value to be used as the 16-bit destination port in the SMS User Data Header (UDH information element identifier value of 0x05). See clause 9.3.1 for additional information. The information shall be represented in this element as a decimal number. This value shall be ignored by the PHG application whenever the APB resource is obtained from the Health & Fitness services application.
SMSApplicationId	Optional SMS Child – The SMSApplicationID shall be a sequence of Unicode characters. The length of this string, when encoded using UTF8, shall not exceed 148 octets. This string shall be sent in the payload of a Shoulder Tap. The purpose of the element is to provide an application identifier in the shoulder tap which can be used to route the shoulder tap message to the appropriate PHG application The exact semantics associated

Table 8-1 – APB xml elements provided by PHG application

Element	Usage
	with how this routing takes place on a given PHG platform is not defined by these guidelines. If the APS is being formed by an application on a platform in which other applications may create APSs the value of SMSApplicationId may need to be managed. This value shall be ignored by the PHG application whenever the APB resource is obtained from the Health & Fitness services application.
APSSState	See description of the element in Table 8-2

Table 8-2 – APB xml elements provided by Health & Fitness application

Element	Usage
HFSAPBI	Mandatory – The identifier for the HFS component of the authenticated persistent binding resource that was created. The HFSAPBI shall be represented as a string of size less than 2048 UTF-8 characters. The following characters shall not be present in the string: "/", "#", "+", "*". The Unicode NULL character may not be used. This value shall be ignored by the Health & Fitness services application whenever the APB resource is obtained from the PHG application.
PHGAPBI	Mandatory – The identifier for the PHG application component of the authenticated persistent binding resource that was created. The PHGAPBI shall be represented as a string of size less than 2048 UTF-8 characters. The following characters shall not be present in the string: "/", "#", "+", "*". The Unicode NULL character may not be used. This value shall be ignored by the Health & Fitness services application whenever the APB resource is obtained from the PHG application.
APSExchangeURL	Mandatory – The URL to use when establishing the TLS session on which MQTT messages will be exchanged. The URI scheme shall be mqtt. The PHG application may need to change the URI scheme to work with a given MQTT client. This value shall be ignored by the Health & Fitness services application whenever the APB resource is obtained from the PHG application.
APSSState	Mandatory – The state of the APS. The Health & Fitness services application shall set this element to NEW in response to a PHG application POST operation if the APS does not exist. If the Health & Fitness services application already has an existing APS in place with the PHG application, as determined by the authentication of the security credential, this value shall be set to ENABLED. The PHG shall set this value to TERMINATED to close and remove the persistent session with the Health & Fitness services application. The Health & Fitness services application shall support a valid XPath representation of the APSSState element of the APS when setting the value of APSSState.
expirationTime	Mandatory – The maximum time period that may elapse after the last POST to the APB resource by the PHG application, or the last activity on the message channel in which the peer PHG application was known to be active. If this time period is exceeded the Health & Fitness services application Should terminate the APS. However, if the APB resource is in the ENABLED state the Health & Fitness services application shall attempt