H.812.4 Authenticated Persistent Session Capability

Version 2016

August 4, 2016

Table of Contents

Figures

Tables

0 Introduction

The Continua Design Guidelines (CDG) define a framework of underlying standards and criteria required to ensure the interoperability of devices used for applications monitoring personal health and wellness. It also contains additional design guidelines for interoperability that further clarify or reduce the options in underlying standards or specifications, or by adding a feature missing in an underlying standard or specification.

This guidelines document defines the additional design guidelines for the Authenticated Persistent Session (APS), whose function is to provide a secure, long-lived, persistent bi-directional data channel between the Health & Fitness application and a PHG application, suitable for sending Unsolicited Commands to the PHG or to devices connected via the PHG.

This guidelines document is one of the "H.810 Interoperability design guidelines for personal health systems" documents [H.810]

0.1 Organization

This CCC guideline is organized in the following manner.

Clause 0-5: Introduction and Terminology - Provides an overview of how H.812.4 is structured
Clause 0: Use Cases – A descriptive scenario that motivates the class of problems that the APS is addressing.
Clause 7: Authenticated Persistent Session Overview – A Technical overview of the operation of the Authenticated Persistent Session.
Clause 8: Authenticate Persistent Session Management - This clause describes the interactions between the information exchange parties.
Clause 9: Behavioral Model: MQTT- This clause is an overview of sequences of interactions under this CCC and summarizes typical iterations, constraints, and exceptions.
Clause 10: Behavioral Model: SMS Shoulder Tap Capability
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 CCC Guideline Releases and Versioning

Information on releases and versioning of these guidelines can be found in Clause 0.2 of [H.810]

0.3 What's New

To see what is new in this release of the design guidelines refer to Clause 0.3 of [H.810]

1 Scope

This guidelines document defines two certified capabilities classes. Both certified capabilities 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 Premise Equipment known as a Personal Health Gateway (PHG). The two certified capabilities classes are for the Services Application (APS-CCC-Services) and for the PHG (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 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

All referenced documents can be found in Clause 2 of [H.810]

3 Definitions

This guidelines document uses terms defined in [H.810]

4 Abbreviations and Acronyms

This guidelines document uses abbreviations and acronyms defined in [H.810]

5 Conventions

This guidelines document follows the conventions defined in [H.810]

6 Authenticated Persistent Session Use Case

The Authenticated Persistent Session provides a mechanism by which future Continua Certified Capability Classes 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 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: These Guidelines define an Authenticate Persistent Session Certified Capability Class for a PHG application (APS-CCC-PHG) and for a Health & Fitness 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 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 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 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.

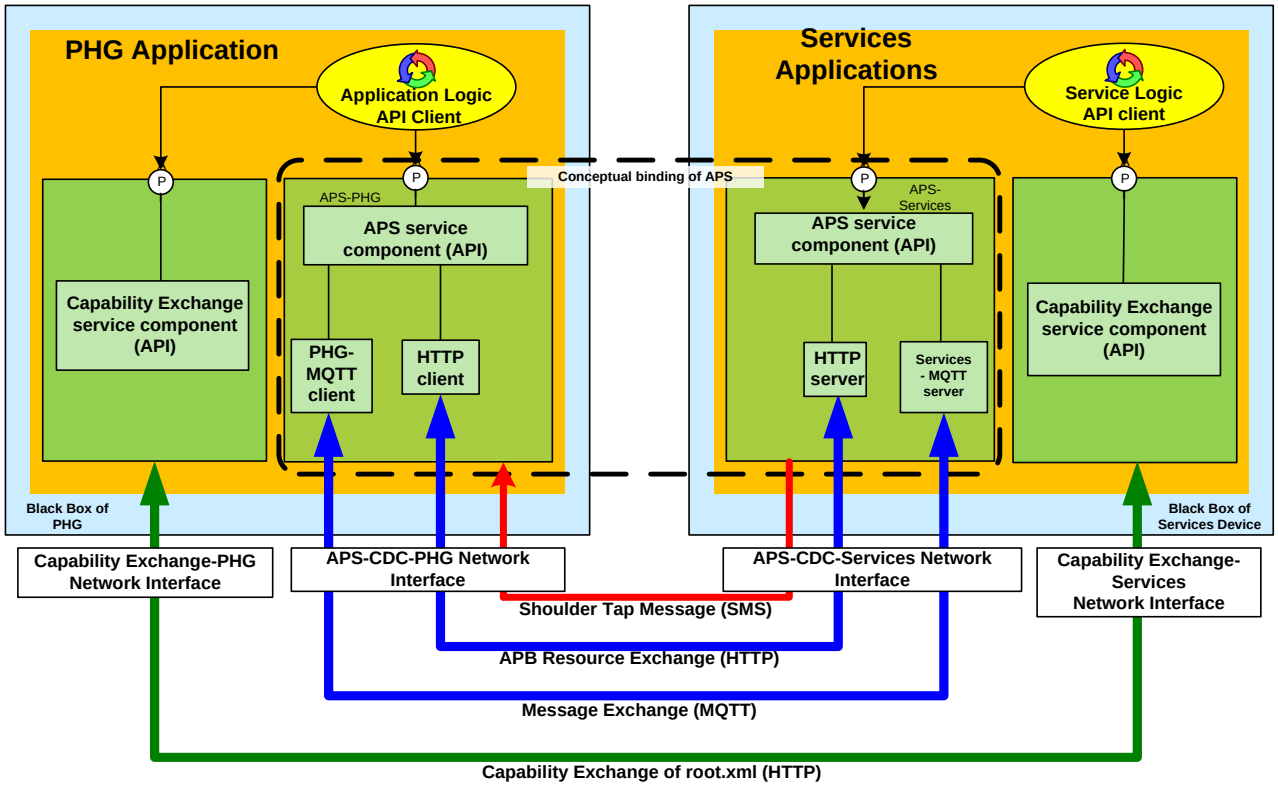

Figure 7-1 – APS Framework

An Authenticated Persistent Session (APS) is a binding between two *APS service components*, one in the *Health & Fitness 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 application* using the APS *API client* component (see [H.810] *Devices Components and Interfaces*) can securely issue commands to the PHG application, across service disruptions, without needing to manage the connectivity or authenticity of the peer.

> *Note: Figure 7-1 represents an architectural model and does not mandate a particular implementation.*
> *Note: 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: 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 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 [H.812.3]) - In this phase the PHG application obtains information from the Health & Fitness application using HTTP. The information identifies if the Health & Fitness application has support for APS-CCC-Services. The information is contained in the root.xml file of the Health & Fitness application and includes the URL to use for APS establishment. See Clause 8.1.
- APS Establishment (see Clauses 8.2.3 and 8.2.4 – The PHG application, using a secure HTTPS connection, creates the APB resource on the Health & Fitness application indicating its desire to establish a persistent session. During this phase the PHG application authenticates itself to the Health & Fitness 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 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 TLS connection is established by the PHG application connecting it to the MQTT server exposed by the Health & Fitness 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 Applicationis 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: The dispatcher does not use any information in the MQTT payload. The payload is opaque to the dispatcher*.

Figure 7-2 gives 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 CCCs 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: This description is illustrative and does not proscribe a particular method of implementation.*

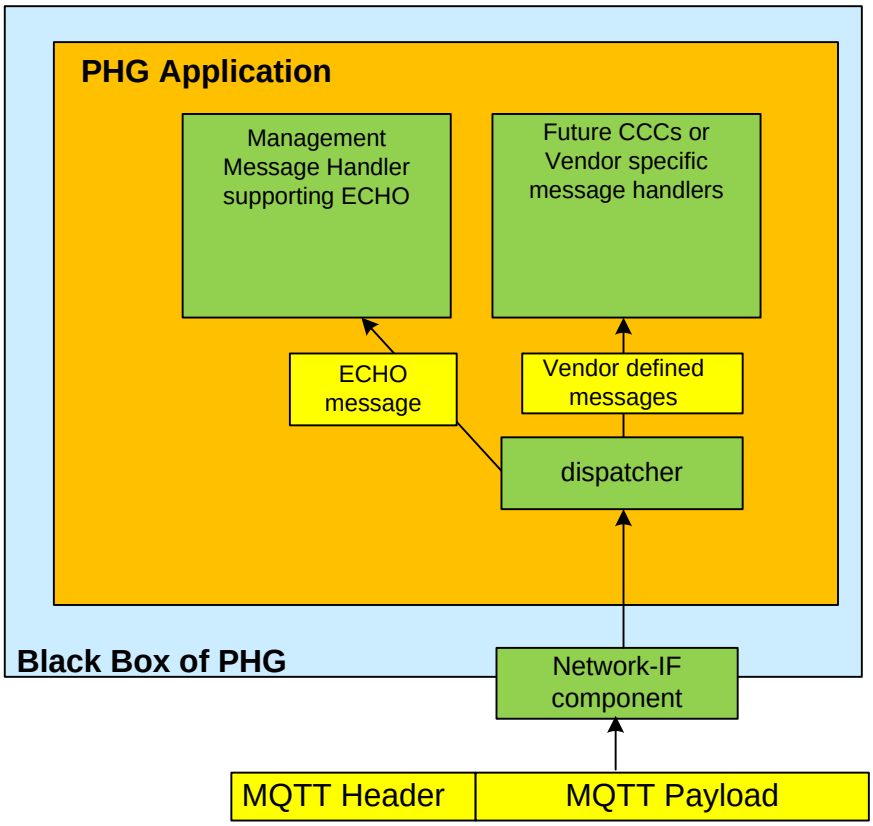

Figure 7-2 – Example of payload delivery to different message handlers.

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 Figure 7-3.

Figure 7-3 – 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 application **shall** have write access to any message topics containing its Services APBI
- A Health & Fitness 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 application and MQTT server, but how the Health & Fitness application and MQTT server actually interact is implementation dependent. In many implementations the Health & Fitness application is also the authenticated management application.

7.3 Shoulder Tap

If the Health & Fitness 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 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 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 application and the other with the PHG application. Authentication is performed using TLS in conjunction with OAUTH as outlined in Annex B of the *H.812 Health & Fitness Services IF Common Certified Capability Class Guidelines*.

The Health & Fitness 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 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 application implementing the APS-CCC uses hData to present to the PHG application three items relating to APSes in the root.xml file. The first item is a *profile*. The profile is an entry that indicates that the Health & Fitness 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 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 application when it receives the APB resource from the PHG application fills in the remaining elements as defined in Table 8-2.

During the establishment of an APS, a pair of identifiers is allocated by the Health & Fitness 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 application (Services APBI). The Services APBI together with the PHG APBI identify the APB instance **and shall** be unique across all the APS being managed by the Health & Fitness 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 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:

Figure 8-1 – Profile Element Indicating Capability

```
<profile>
  <!-- Specified value -->
  <id>APS-CCC-Services</id>
  <reference>
    http:// handle.itu.int/11.1002/3000/hData/APS/2015/01/H.812.4.pdf
  </reference>
</profile>
```

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

Figure 8-2 – ResourceType Element describing APB content

```
<resourceType>
  <resourceTypeID>APB</resourceTypeID>
  <!-- location of reference that describes the APS standard -->
  <reference>
    http:// handle.itu.int/11.1002/3000/hData/APS/2015/01/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/2015/01/APBConfigResource.xsd    </validator>
  </representation>
<resourceType>
```

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.

Figure 8-3 – Section Element describing where to POST

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

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 characterize the APS.

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 application. Note: If a vendor specific 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 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 application to reestablish 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 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 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 application will use in order to perform the shoulder tap operation. The SMS element is the parent element for SMSHeaderDstPort, SMSApplicatonId, and MSISDN. This value **shall** be ignored by the PHG application whenever the APB resource is obtained from the Health & Fitness 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 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 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 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 APSes 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 application.
APSState	See description of the element in Table 8-2

Table 8-2 – APB xml Elements Provided by Health & Fitness application

Element	Usage
WANAPBI	Mandatory – The identifier for the WAN component of the Authenticated Persistent Binding resource that was created. The WANAPBI **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 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 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 mqtts. 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 application whenever the APB resource is obtained from the PHG application.
APSState	Mandatory – The state of the APS. The Health & Fitness 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 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 application. The Health & Fitness application **shall** support a valid XPath representation of the APSState element of the APS when setting the value of APSState.
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 application **Should** terminate the APS. However, if the APB resource is in the ENABLED state the Health & Fitness application **shall** attempt to issue the ECHO management message before terminating the APS. The Health & Fitness application **Should** not terminate the APS if a response is received to the ECHO message. (Note that the Health & Fitness application may terminate an APS at any time though that action may not represent graceful behavior.). This element **shall** be expressed as an ISO8601 duration – for example a 12 hour expirationTime is represented as PT12H.
requiredResponseTime	Mandatory – The maximum delay in seconds that the Health &

	Fitness application can tolerate for a response to the ECHO message. This value provides the PHG application with information that it can use to determine how to best allocate APS resources. A PHG application **Should Not** establish an APS with a Health & Fitness application if it is unable or unwilling to meet, in normal operation, the requiredResponseTime for an ECHO message. This element **shall** be expressed as an ISO8601 duration – for example a 10 second requiredResponseTime is represented as PT10S. This value **shall** be ignored by the Health & Fitness application whenever the APB resource is obtained from the PHG application.
clientId	Conditionally required – This element **shall** be present if an exchangeMechanism of MQTT is selected. The clientId **shall** be used by the PHG application when it issues an MQTT CONNECT. The value of the clientId is generated by the Health & Fitness application. This value **shall** be ignored by the Health & Fitness application whenever the APB resource is obtained from the PHG application.
PHGCredential	Conditionally required – This element **shall** be present if an exchangeMechanism of MQTT is selected. The PHGCredential **shall** be used by the PHG application as the password when it issues a MQTT CONNECT. This value **shall** be ignored by the Health & Fitness application whenever the APB resource is obtained from the PHG application.

The APB resource is expressed as an xml document - an example of which follows. This example shows a PHG application supporting MQTT and an SMS shoulder tap.

```
<?xml version="1.0" encoding="UTF-8"?>
  <aps:APB xmlns:aps="http:// handle.itu.int/11.1002/3000/hData/APS"
      xmlns:xsi = "http://www.w3.org/2001/XMLSchema-instance"
      xsi:schemaLocation = " handle.itu.int/11.1002/3000/hData/APS/2015/01/APBConfigResource.xsd">

 <!-- These fields are filled in by the PHG -->
  <supportedMH>APS lampreynetworks.com/private</supportedMH>
  <exchangeMechanism>MQTT privateMessageProtocol</exchangeMechanism>
  <shoulderTapMechanism>SMS</shoulderTapMechanism>
  <SMS>
     <MSISDN>441111223344</MSISDN>
     <SMSHeaderDstPort>1234</SMSHeaderDstPort>
     <SMSApplicationId>4827351</SMSApplicationId>
  </SMS>

  <!-- These fields are filled in by the Health & Fitness application -->
  <WANAPBI>WANAPBI_1</WANAPBI>
  <PHGAPBI>5468233453aae3fd224</PHGAPBI>
  <APSExchangeURL>mqtts://example.org:1883</APSExchangeURL>

  <!-- State set by Health & Fitness application when first created -->

  <APSState>NEW</APSState>
  <expirationTime>PT50H</expirationTime>  <!--  Time in hours  -->
  <requiredResponseTime>PT30S</requiredResponseTime>   <!--  Time in seconds  -->
  <clientId>RestPHG</clientId>
  <PHGCredential>PHGCredential55555</PHGCredential>
</aps:APB>
```

See Appendix II for the APB resource schema.

8.2 APS Behavior

8.2.1 APS Session State

An APS is in one of three states: NEW, ENABLED, or TERMINATED. A Health & Fitness application **shall** only issue messages to a PHG application when the state of the APS is ENABLED. An APS is in the NEW state when it is first created during the APS Establishment procedure. Once the PHG application agrees to establish the APS the PHG application moves the APS into the ENABLED state where it remains until either the PHG application or Health & Fitness capability terminates it. See Table 8-2 for additional information on the APSState element in the APB resource.

8.2.2 Authenticate Persistent Binding Identifiers (APBI)

During the establishment of an APS between a PHG application and a Health & Fitness application, the Health & Fitness application allocates and maintains a pair of identifiers for the life of the APS. One identifier in the pair is associated with an APS instance on the PHG application (PHG APBI) and the other identifier is associated with the APS instance in the Health & Fitness application (Services APBI). The pair of identifiers is used, to bind the sending and receiving APS endpoints together. It is the responsibility of the Health & Fitness application to manage the allocation of both the Services APBI and the PHG API such that every distinct APS that is created by the Health & Fitness application can be uniquely identified by the pair of APBIs alone. Further, the Health & Fitness application must assure that this unique APB resource is only exchanged with a PHG application possessing the security credential (e.g. X.509 certificate) that was used when the APS was first created. The PHG APBI must be unique across the full set of existing APSes maintained by the Health & Fitness application.

8.2.3 Authenticated Persistent Binding Establishment

APS Establishment refers to the process by which the PHG application and Health & Fitness application exchange information in order to enable and configure the APS. An APS must be established before messages can be exchanged. The PHG initiates APS establishment after it completes capability exchange with a Health & Fitness application and determines that the Health & Fitness application supports the APS CCC.
APS establishment requires that the PHG application authenticate itself to the Health & Fitness application (acting as an OAUTH Authorization server) using some method that results in the PHG obtaining an authorized OAUTH bearer token. A successfully authenticated TLS connection in which the PHG application possesses a valid OAUTH access token represents mutual authentication for the purposes of an APS.

When there has been mutual authentication the Health & Fitness application has the required security credentials it needs in order to identify and associate an APS with a given PHG application, in this and all subsequent transactions. How the Health & Fitness application uses the certificate to link the APS to a PHG application is up to the implementation.

Within this mutually authenticated context, the PHG application establishes the APS by performing an HTTP POST to the Health & Fitness application. The resource posted is an xml document containing the APB resource but the PHG application fills in only those elements as specified in Table 8-1.
The element values provide the Health & Fitness application the information it needs to configure and allocate the internal resources needed to support the APS. The reply to this POST contains a URL to a modified version of the APB resource containing the Services provided elements of Table

8-2. The PHG application then retrieves the APB resource via an HTTP GET to the provided URL. The Health & Fitness application may refuse to establish an APS due to resource limitations.

8.2.4 Accepting an Authenticated Persistent Binding

The PHG application examines the response of the GET. If the parameters are acceptable to the PHG application, it establishes a secured connection to the MQTT server and sets up the MQTT link performing the necessary subscription and publishing actions. Upon successful completion of these steps, the PHG application **shall** indicate that it accepts the APS by performing an HTTP PUT to the Health & Fitness application, using the URL provided in the POST response with APSState appended to it (URL/APSState). The value of the APSState element identified by the URL in the PUT operations **shall** be set to ENABLED. See Appendix I.4 for details. At this point the APS is enabled and the PHG application can receive messages. The Health & Fitness application **shall** only update the APSState of its APB resource in this transaction. Should the PHG application provide an XPath that references something other than <APSState> the Health & Fitness application **shall** return an appropriate HTTP error. A PHG application may perform additional PUT operations to update the APSState of the APS as needed.

8.2.5 Authenticated Persistent Binding Termination

A PHG application may terminate the APS at any time by setting the APSState value to TERMINATED (see Appendix I.5). The PHG application should then perform appropriate operations to release resources used in association with the APS, including clearing the MQTT server (see Clause 9.1.1). The APBI is no longer valid after the PHG application terminates the APS. The Health & Fitness application may terminate the APS session if the PHG application has failed to renew the APS within the specified expirationTime interval, or due to a decision by the application logic. The Health & Fitness application does not remove the APS session due to a termination of a transport connection.
The Health & Fitness application removes information that associated the APS with the authentication key such that if the PHG application initiated another APS capability exchange with the same authentication credential, the Health & Fitness application would return NEW for the APSState element value in the APB resource. The Health & Fitness application can release resources associated with a terminated APS. Terminating an APS is an abortive process that may cause a currently in operation command to fail.
An APS can be terminated by administrative procedures.

8.2.6 APS-CCC Diagnostic Message

The APS-CCC provides the basic framework by which application oriented CCCs can initiate message exchange from the Health & Fitness application. These application oriented CCCs are expected to have well defined operations that are specific to the application's needs. These operations are out of scope for the APS-CCC
The APS-CCC does define a message structure in order to support managing the APS-CCC itself. Only one command is defined for supporting the APS-CCC, the ECHO command. In future releases, other commands may be added. All entities implementing the APS-CCC **shall** support the management message ECHO command.

8.2.6.1 Diagnostic Message Structure for the APS-CCC Message Exchange

8.2.6.1.1 Payload

The APS-CCC message exchange facility (MQTT) supports a diagnostic message format that defines a small set of commands that can be exchanged between APS-CCC peer entities. These commands are carried in the payload section of the diagnostic message. A diagnostic message **shall** contain only one command. The content of the payload depends upon the command. The diagnostic message **shall** be sent in Network Byte Order and has the following layout:

Table 8-3 – Fields of the APS-CCC diagnostic message

Field Name	Description	Size in Bits	Values
Operation **Octet 0**	Identifies the operation to be performed. The two MSB bits in the operation field are reserved and **shall** be sent as 0 and ignored on reception. Responses to commands **shall** be formed by performing a logical OR of the command with 0x40. Thus a command of 0x03 causes a value of 0x43 to be returned in the operation field.	8	0x00 – 0x3F: command 0x40 – 0x7F: response 0x80 – 0xFF: reserved
Handle **Octet 1-4**	A handle **shall** be provided by the sender of the command and returned by the receiver. The handle is opaque to the receiver of the command. The sender **shall** not reuse a handle that is associated with an outstanding command.	32	
Status **Octet 5**	The status field **shall** be present in both command and response messages. In commands it **shall** be set to 0x00 by the sender, and ignored by the receiver. If the status field is not 0x00 in a response message the sender **Should not** process the rest of the message.	8	The validity of fields after the status field may not be reliable when the status field is not 0x00.
Length **Octet 6-7**	The payload length **shall** be present in all diagnostic messages. The length field **shall** be given in octets and represents the number of octets in the message payload from the first octet after the length field through the last octet of the message payload.	16	Since the payload field includes the 21 octets used to represent time the minimum value of length is 21.
Payload	The payload **shall** start with a fixed length subfield of 21 octets. This subfield holds the current value of time as being reported by the sender or responder to the command. The payload **May** contain additional octets of echo data. The sender of the ECHO command **shall** ensure that the length field properly identifies the number of	Depends upon the command. Specified in the length field	If a receiver is able to detect a mismatch between the number of octets of data in the message and the length of the payload is should return an appropriate error code

	octets of ECHO data. The time subfield **shall** be encoded as a string of UTF-8 characters and formatted in accordance with [ITU H.812.1] Clause *Timestamping and Time Synchronization*. Since the timestamp is reported in a fixed length field the fractions of a second component is NULL padded for each level of accuracy not reported in the timestamp.		

Note: the term payload can be confusing since it is used in several contexts in this document. The diagnostic message itself is the payload of an MQTT message. The payload here refers to the set of bytes that are associated with a given command instruction. For example, the payload of an ECHO command diagnostic message is a timestamp followed by an arbitrary string of bytes that is returned by the recipient.

8.2.6.1.2 Supported Diagnostic Message Commands

All diagnostic messages defined by this design guidelines have associated responses. The responding entity **shall** form a reply to a command by structuring the fields as documented in Table 8-3. The commands supported are identified below:

ECHO (Operation Field value of 0x01 for command, and 0x41 for response)

The ECHO command enables the Health & Fitness application to determine if the PHG application is able to receive and respond to diagnostic messages and allows the Health & Fitness application to obtain the PHG application's sense of time.

The entity sending the ECHO command **shall** provide a payload in which the first 21bytes contain the time of the sender as defined above in Table 8-3. The remaining bytes, if any, may be set to any value of interest to the sender. The length field is set to the length of the ECHO payload.
The responder to the ECHO command **shall** set the operation field to 0x81.

The ECHO response **shall** contain the handle provided by the Health & Fitness application from the corresponding ECHO command, the status field, the length field and the payload received from the ECHO command with the time field replaced by the time of the ECHO responder using the same format as defined for the sender. The ECHO response **Should** be sent in an expeditious manner. The responder to the ECHO message **shall** examine the length field to determine if the sent value exceeds the implementation defined limit. If it does, it **shall** set the status code appropriately, and return the local time and the maximum number of additional bytes supported by the implementation. The payload length field **shall** reflect the number of bytes in the returned payload. If the implementation can support the number of bytes sent in the ECHO command it **shall** return the sent payload. All implementations **shall** support ECHO payloads that are less than or equal to 256 bytes.

8.2.6.1.3 Status Field

The status field is composed of a bit indicating valid time and a status code. The most significant bit in the status field is the time synchronized bit. It **shall** be set to indicate that valid NTP synchronized time, or equivalent, is being reported in the time field of the payload, and **shall** be cleared otherwise.
The following status codes values are defined for the ECHO response

- 0x0000 – Success – No error was detected in processing the command
- 0x0001 – Unknown Failure – The requested command was not successfully performed. The length field may be set to a positive value. When the length field is a positive value the payload contains a message of length bytes that may provide additional insight as to the error encountered.
- 0x0002 – Command not supported. The responding entity **shall** return this value whenever the value in the operation field (byte 0) of a received diagnostic message is not supported.
- 0x0003 – Length of command exceeds maximum supported value
- 0x0004 – Error in field values

9 Behavioral Model : MQTT

MQTT [OASIS MQTT] is a required capability for applications that support the APS-CCC. This clause describes the usage of MQTT in supporting the transmission of messages in the context of an APS.

9.1 Overview of Operation

The Health & Fitness application for APS implements an MQTT server. The hostname or IP address and TCP port number of the server is provided in the APB resource. The exchange of messages between the PHG application and the Health & Fitness application uses an MQTT server that is associated with the Health & Fitness application, using the topics defined in Clause 7.2. The following figure provides an overview of the exchanges between the PHG application and the Health & Fitness application. The topic strings, as shown in the figure, are dependent on the PHG APBI, the Services APBI, and the message handlers used by different CCCs as described in the following clause.

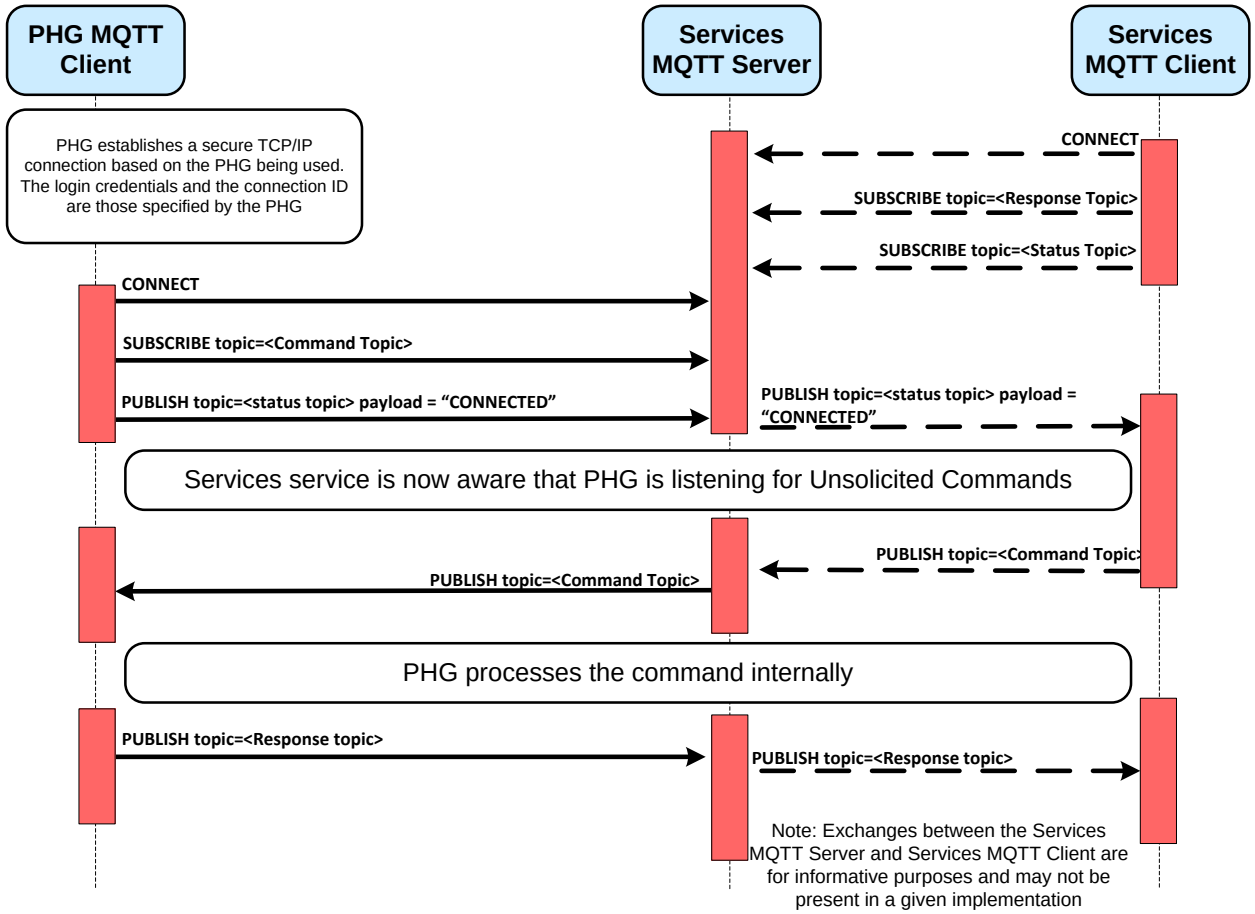

Figure 9-1 – PHG Application and Health & Fitness application MQTT Client Interactions

In the Clause 8.2, APS Behavior, interactions are described from the point of view, respectively, of the PHG application and the Health & Fitness application. It is important to note that how the Health & Fitness application communicates with its MQTT server is up to the application. The only normative components of the APS interface are the exchanges between the PHG application and the Health & Fitness and MQTT services.

9.1.1 Graceful APS termination

When possible, a PHG application should terminate an APS gracefully.
To terminate an APS gracefully the following steps **shall** be taken by the PHG application:

- Establish a connection with the Health & Fitness application that owns the APB resource defining the APS that is to be terminated
- Perform a PUT operation of an APB resource with the <APSState> element set to TERMINATED to disable further use of the APS by the Health & Fitness application.
- CLOSE any active connection used by the APS to exchange messages over MQTT.
- Perform an MQTT CONNECT with the clean session flag set to true (clears the PHG's subscriptions on the MQTT server), the state of the retained Will flag to cleared, and the Will topic and Will message absent (prevents the allocation of any resources to send a status message when the connection to the PHG application is lost).
- Publish a zero length message to the status topic with the retain flag set to true to release the status resource.
- Disconnect from the MQTT server.

9.2 Interaction of the Health & Fitness application with the PHG Application

The Health & Fitness application interacts with the PHG application via its associated MQTT server component. The precise way in which the Health & Fitness application interfaces with its MQTT server is not specified in these Guidelines.

The Health & Fitness application, if it has determined that a message is to be sent using the APS, sends this message by issuing a PUBLISH packet to the appropriate message topic. The MQTT server uses a QoS level of 2 when issuing the PUBLISH packet.

If the Health & Fitness application has a message to send and the status topic indicates that the PHG application is not connected, it may attempt to bring the connection back up (if the PHG application supports shoulder tapping) by sending the out of band shoulder tap.

(Informative Note) The Health & Fitness application may subscribe to any APS response topics of interest. It may also subscribe to status topics, should it wish to track the online/offline status of its APSes. To listen for status updates from all APSes it can subscribe to the following wildcarded topic expression:

```
pcha/status/<Services APBI>/#
```

9.3 State of the PHG's Connection to the WAN MQTT Server

Figure 9-1 documents the states that the status topic can be in, and the events that cause transitions between states.

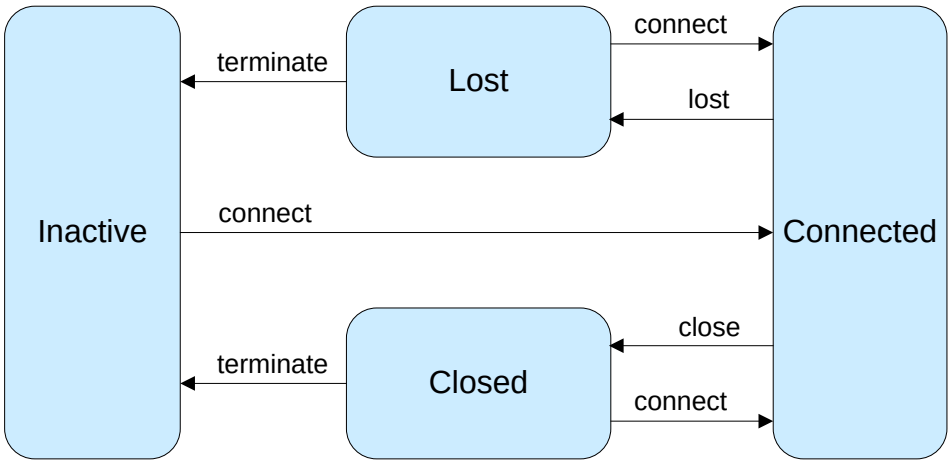

Figure 9-2 – State Diagram for the Status Topic

The following normative table documents the states and state transitions of the status topic. The status topic is used by the Health & Fitness application to track the status of the PHG application's connectivity to the APS.

Table 9-1 – State Table for the Status Topic

State	Event	Next State	Description
INACTIVE	connect	CONNECTED	The PHG application has established an MQTT session by logging in with a new client ID and a clean session flag set to false. The PHG application publishes a message to the status topic with a payload content of CONNECTED.
CONNECTED	lost	LOST	The Services (MQTT) service has detected a TCP disconnection or a timeout event due to the absence of MQTT ping messages. The Services (MQTT) service will publish a Will message to the status topic containing a payload of LOST.
CONNECTED	close	CLOSED	The PHG application closes the MQTT connection (sends an MQTT DISCONNECT control packet) but does not terminate the MQTT session. The PHG application publishes a message to

			status topic with a payload of CLOSED prior to disconnecting.
LOST	connect	CONNECTED	The PHG application has reconnected to an MQTT session by logging in with its existing client ID and a clean session flag set to false. The PHG application publishes a message to status topic with a payload content of CONNECTED.
LOST	terminate	INACTIVE	The PHG application has decided to terminate the APS by logging in with its existing client id and setting the clean session flag to true. It signals this condition by publishing a zero length message to the status topic. It then logs out by sending an MQTT DISCONNECT control packet.
CLOSED	connect	CONNECTED	The PHG application has reconnected to an MQTT session by logging in with its existing client ID and a clean session flag set to false. The PHG application publishes a message to status topic with a payload content of CONNECTED.
CLOSED	terminate	INACTIVE	The PHG application has decided to terminate the APS by logging in with its existing client id and setting the clean session flag to true. It signals this condition by publishing a zero length message to the status topic. It then logs out by sending an MQTT DISCONNECT control packet.

9.3.1 Interaction of a PHG Application with the MQTT server

The PHG application establishes the APS session by performing an HTTP POST to the Health & Fitness application in the context of a secure connection providing some security credential. Once the PHG application has received this information, it interacts with the Health & Fitness application by creating a TLS connection with the MQTT server component associated with the Health & Fitness application.

Once it has established a TLS connection, the PHG application sends an MQTT CONNECT control packet to the MQTT server on that connection. The PHG application waits for a response from the MQTT server. If it receives a data packet that is not an MQTT Connection Acknowledgement, then the PHG application closes the TCP/IP connection.

The PHG application sets the following fields in its MQTT Connect message (normal connection).

Table 9-2 – Information Contained in the PHG Application's MQTT Connect Message

Information Element	Value set by the PHG	Comments
Flags	0xEC	• User Name & Password are present • Retained Will Message requested (with QoS 2) • Clean Session not requested
Keep Alive	Chosen by the PHG implementation	If no activity has taken place during a given keep alive time period the PHG application should send an MQTT PING to keep the connection open. It may set a value of 0 to indicate that it doesn't commit to send any PING messages
Client Identifier	A string provided by the Health & Fitness application in the APB resource.	The MQTT server uses the Client Identifier to identify the MQTT session. When operating in the context of a particular APS the PHG application must always use the string specified by the Health & Fitness application in the APB resource
Will Topic	The PHG's *status* topic	Topic used to track the status of the connection
Will Message	The string "LOST"	Payload of MQTT message that is to be generated (internal to the Health & Fitness application) indicating that the PHG has gone offline unexpectedly.
User Name	The PHG APBI provided by the Health & Fitness application in the APB resource	Used to authorize PHG application access to topics.
Password	The PHGCredential provided by the Health & Fitness application in the APB resource	Used to authenticate the PHG application

The Will flag, Will Retain flag and Will Message ensure that the Health & Fitness application is informed when communications with the PHG are unexpectedly disrupted. This notification process is internal to the implementation of the Health & Fitness application, but is controlled by these parameters. The PHG application is required to set them to the values specified above.

The MQTT Keep Alive value determines how quickly the MQTT Server will detect the loss of connectivity to the PHG application. It also commits the PHG application to periodically send an MQTT PING packet if there has been no other activity.

When it has a received a positive Connection Acknowledgement from the MQTT server, the PHG application then proceeds to send MQTT SUBSCRIBE requests to its command Topics. These command topics are qualified by the CCC message handler as shown in clause 7.2. The PHG application **shall** subscribe on behalf of all the message handlers it has advertised in the APB resource. It sets the following information in the MQTT SUBSCRIBE request:

Table 9-3 – Information Contained in MQTT SUBSCRIBE Message

Information Element	Value	Comments
Topic	The *command* topic name	A set of topics from which the PHG application wishes to receive PUBLISH messages
Requested QoS	2	This allows the Health & Fitness application to define the QoS level based on the value of QoS selected in the PUBLISH control packet

When it has a received a positive SUBSCRIBE Acknowledgement from the MQTT server, the PHG application sends a PUBLISH control packet to update the *status* topic to show that it has come online. The publish status is sent with QoS 2. The message parameters are shown in Table 9-3.

Table 9-4 – Information Contained in the PHG's Publish Status Message

Information Element	Value	Comments
Retain Flag	True	Message is to be retained by the MQTT server so that later subscribers can be informed of the PHG application's current connection status
Topic	The *status* topic name	Topic that is tracking the connection state of the APS
QoS	2	
Payload	The string "CONNECTED" Or "CLOSED"	Status information to be sent to the Health & Fitness application indicating that the PHG application associated with the APS is online Or Status information to be sent to the Health & Fitness application indicating that the PHG application is disconnecting from the MQTT server but maintaining the APS enabled

There is a second type of publish status message defined in this standard. This message is used only when the PHG application is in the process of terminating the APS. The publish status message in

this case has the retain flag set to true and an empty payload. The purpose of this message is to clear resources associated with the APS on the MQTT server.

After the PHG application has completed the SUBSCRIBE operation it is ready to receive messages from the Health & Fitness application.

At this point the PHG application enables the APS performing an HTTP PUT operation to the URL provided by the Health & Fitness application during APS establishment. The HTTP PUT contains the APB resource with the <APSState> element value set to ENABLED. No message can be received before the PHG application enables the APS.

When the PHG application has processed a message, it responds by sending an MQTT PUBLISH control packet as follows:

Table 9-5 – Information Contained in the PHG application's MQTT Publish Response Message

Information Element	Value	Comments
Retain Flag	False	Message does not need to be retained once it has been delivered to the Health & Fitness application
Topic	The *response* topic name	See 7.2 Topics used in MQTT
QoS	2	The response shall be delivered exactly once
Payload	Dependent on entity using the APS service	Response to be sent to the Health & Fitness application

If the PHG application detects loss of its MQTT connection, or loss of the underlying TCP/IP connection then it may attempt to reconnect immediately, following the process described at the beginning of this clause. If it is able to tell that the disconnection happened because of a total loss of network connectivity, then it should defer a reconnection attempt until the network is restored.

The PHG application may elect to disconnect the MQTT connection while still maintaining the APS. In this case, the PHG application should publish a status update message, but with a payload of CLOSED rather than CONNECTED, prior to sending the MQTT DISCONNECT message. It may reconnect at a future time of its choosing.

If the PHG application supports a shoulder tap mechanism it must attempt to reconnect when it receives a shoulder tap.

Upon reconnection, the PHG application should be prepared to handle incoming messages immediately, since some messages might have been queued up for it during the time when it was disconnected.

10 Behavioral Model : SMS Shoulder Tap Capability

These Guidelines defines a capability that facilitates operation of the APS with networks that remove IP infrastructure for inactive connections. This capability is based on the Short Message Service (SMS) as defined in [GSM/UMTS][CDMA 2000]. Future versions of these Guidelines may

provide different mechanisms to implement this capability as cellular network providers deploy additional services.

10.1 Shoulder Tap Overview

When there is no data exchanged between a Health & Fitness application and a PHG application, both wireless network resources and PHG energy consumption can be reduced by tearing down the wireless data connection, resulting in a loss of IP connectivity. A wireless data connection can also be lost due to coverage issues, or lack of energy (available battery capacity) on a PHG. The loss of IP connectivity does not terminate the APS and when IP connectivity is re-established, the software entities bound by the APS can once again use the IP network to exchange information.

This clause defines an out-of-band mechanism called a Shoulder Tap (ST), which the Health & Fitness application can use to accelerate the re-establishment of IP connectivity. The mechanism can be used with any PHG application that has a cellular interface supporting SMS.

Figure 10-1 presents a high level overview of the sequence of events in a Shoulder Tap.

The first step of the ST process is an exchange of information between the PHG application and the Health & Fitness application. This takes place during APS establishment. At some subsequent point in time, the network connection between the PHG application and the Health & Fitness application is discontinued causing the underlying exchange mechanism to mark the connection as being lost. When an application activity using the APS-CCC requires the Health & Fitness application to send a message, the Health & Fitness application recognizes the fact that the IP connectivity to the PHG application has been lost. At this point it transmits a Shoulder Tap message to the PHG application using an out-of-band capability such as SMS to wake up the PHG. Receipt of the Shoulder Tap message informs the PHG application that the Health & Fitness application wishes to exchange a message with it. The PHG application then re-establishes IP data connectivity and resumes message exchange with the Health & Fitness application in the context of the APS.

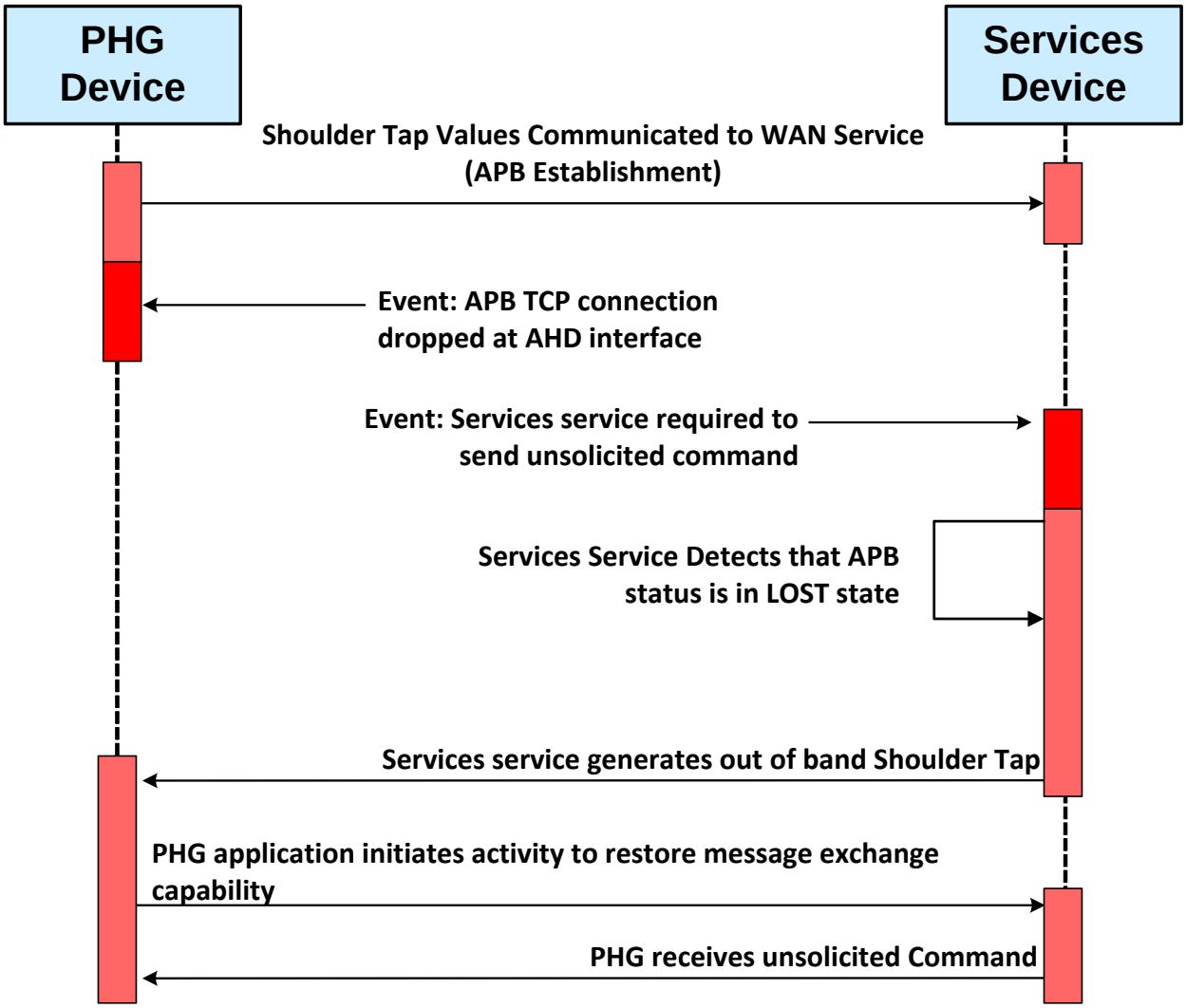

Figure 10-1 – Shoulder Tap Overview

10.2 Scope

The availability of an out-of-band Shoulder Tap mechanism is a function of the capabilities of the networks that the PHG application and the Health & Fitness application are associated with, the capability of the Health & Fitness application to initiate the Shoulder Tap, and the capability of the PHG application to receive and process the Shoulder Tap. This implies that all entities including the Health & Fitness application, the network, and the PHG application, must be able to operate in accordance with these Guidelines to implement Shoulder Tap functionality. However, these Guidelines only document the interface behaviour between the PHG application and the Health & Fitness application as seen at PHG's interface to the network. It is the responsibility of the system integrator to ensure that the required network infrastructure is in place to enable the Health & Fitness application to meet the interface requirements defined here.

10.3 Shoulder Tap Invocation Determination

It is possible that an active data connection is currently available to the PHG application so that a Shoulder Tap does not need to be invoked by the Health & Fitness application. This can be

determined by looking at the status of the connection state in the underlying message exchange facility. When using MQTT the connection state is maintained in the status topic. The Shoulder Tap should not be performed if the status topic already indicates that the connection is operational (CONNECTED state).

10.4 PHG SMS Information

When a PHG application uses SMS Shoulder Tapping the PHG application communicates the following information to the Health & Fitness application during APS establishment:

- The supported types of Shoulder Tapping, which must include SMS
- The address (MSISDN) to which the SMS message is to be sent
- The port number used in the SMS User Data Header (UDH) to identify the UDH defined end point (port) that will receive the SMS message.
- A PHG application specified identifier that is returned to the PHG in the SMS payload.

The Health & Fitness application uses the PHG provided information to generate the SMS message as defined in this clause. In the event that a third party SMS provider is used to generate or deliver the SMS message to the PHG, the third party SMS provider is considered to be part of the Health & Fitness application and proper behaviour at the PHG interface is determined by the structure of the SMS message delivered to the PHG by the third party provider.

10.5 SMS Message Structure

The Health & Fitness application creates a SMS message as defined herein and sends the message toward the PHG. The following bullet points describe the SMS message as it is delivered to the PHG.

- The message is a binary SMS message
- The message is delivered to the MSISDN provided by the PHG application.
- The SMS message contains a User Data Header and the TP-UDHI (Transfer Layer Protocol Data Header Indicator) bit is set.
- The layout of the SMS payload is given in Figure 10-2
- The SMSHeaderDstPort is encoded into the UDH

  Note: The corresponding Source Port associated with Information Element 0x04 in the UDH is not used by the PHG application.

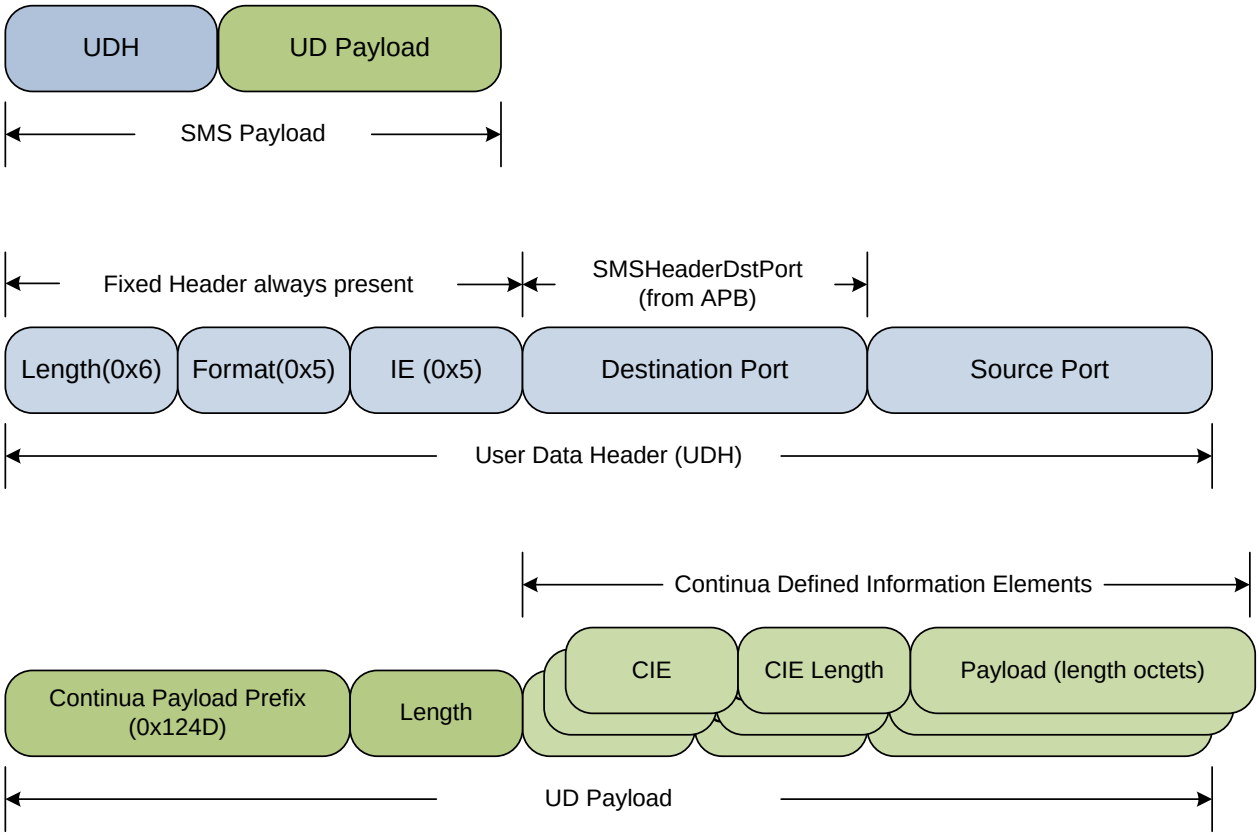

Figure 10-2 – Payload of Binary SMS Message

The UDH is six octets long with the information in the header formatted in hexadecimal (0x05). The header contains one Information Element (value 0x05 – Application port addressing scheme, 16 bit addressing).

The payload contains a Continua defined prefix value of 0x124D and a repeating sequence of Continua Information Elements (CIE) as defined in Table 10-2.

Table 10-1 – Structure of Payload

Field	**Length**
Continua Prefix ‘0001001001001101’b =0x124D	2 octets
Length of Shoulder tap payload excluding first three octets	1 octet
Type of Information-element “A”	1 octet
Length of Information-element “A”	1 octet
Value of Information-element “A”	0 to “n” octets
(repeated for other information elements as needed)	

Table 10-2 – Continua Information Elements

CIE Type	Length	Requirement	MEANING
00	1-148	optional	Shoulder Tap Application Identifier – This value is communicated to the Health & Fitness application in the APB element <SMSApplicationId>. In the SMS message it is encoded using UTF-8.
01	1	optional	Shoulder Tap Semantic – This value indicates the action that the PHG application should take upon reception of the Shoulder Tap. Currently defined values are: 0x01: Re-establish transport level connectivity – The Health & Fitness application wishes to send a message to the PHG application and is waiting for the transport level connectivity to be re-established.

10.6 PHG Application Requirements

When the PHG application is running on an OS platform that processes the arriving SMS message, that platform will need to provide an interface to the PHG application that allows the PHG application to be notified when the binary SMS message arrives. The mechanisms used to notify the PHG application are not specified by these Guidelines.

10.7 Semantic Behavior of the PHG application relative to ST reception

Upon receipt of a Shoulder Tap with Reason ‘Re-establish connection to message exchange server’, the PHG application **shall** re-establish its TCP connection to the WAN MQTT server and submit a CONNECT message. This procedure may need re-establishment of the connection to the packet-switched network.

Annex A Normative Guidelines for the APS-CCC

These tables list the guideline specifications for Continua Certification of a PHG application and Health & Fitness application that support Authenticated Persistent Sessions.

A.1 Guidelines for the APS components in Capabilities Exchange

A Health & Fitness application that supports an Authenticated Persistent Session (APS-CCC-Services) **shall** provide a root.xml file in accordance with Table A-1. A PHG application that supports an Authenticated Persistent Session (APS-CCC-PHG) is also required to support Table A-1.

Table A-1 – APS Elements of Capabilities Exchange

Name	Description	Comments
APS-CCC-Services-Root-Support	A Health & Fitness application **shall** indicate that it supports the APS-CCC-Services by providing a profile with the value of the id element set to APS-CCC-Services in the root.xml file.	See Figure 8-1.
APS-CCC-PHG-Root-Support	A PHG application that POSTs a root.xml file to a Health & Fitness application during Capability Exchange **shall** provide a profile with the id element set to APS-CCC-PHG in the root.xml file.	See Figure 8-1. Note that APS-CCC-Services is replaced byh APS-CCC-PHG.
APS-CCC-Services-Description-Information	A Health & Fitness application **shall** describe the content of the APB resource using a <resourceType> entry in the root.xml in accordance with Figure 8-2.	This entry in the root.xml describes the content of the APB resource as well as referencing a validator for the formatting of the APB resource.
APS-CCC-Services POST-Location	A Health & Fitness application **shall** provide a URL where the PHG application is to perform the initial POST to establish an APS in a <section> entry in the root.xml in accordance with Figure 8-3.	

Name	Description	Comments
APS-CCC-Services-Resource-Prefix	The <resourcePrefix> child element of the <section> entry **shall** be present and the value **shall** be set to true.	The resource prefix is required to be present and true in this specification though it is optional in the hDATA specification.
APS-CCC-Services-Profile-ID	The <profileID> value of the <section> described in Figure 8-3 and the <id> value of the <profile> described in Figure 8-1 **shall** be set to APS-CCC.	The profileID element value of the section identifies the profile to which it is associated.

A.2 Guidelines for PHG APS Management (APS-CCC-PHG)

A PHG application that supports the Authenticated Persistent Session Certified Capability Class **shall** operate in accordance with Table A-2.

Table A-2 – APS Management PHG

Name	Description	Comments
APS-CCC-PHG-Initiate-APS-Establishment	If a PHG application indicates support for an APS during capability exchange then it **shall** initiate APB establishment by POSTing its APB resource.	These Guidelines do not define the exact time by which the APS is to be established. However management services of the APS-CCC should be made available to the Health & Fitness Service in a timely manner
APS-CCC-PHG-POST-Location	A PHG application establishing an APS session **shall** POST the APB resource to the URL specified in the <path> child element of the <section> defined in Figure 8-3.	The PHG application obtains the URL for the POST in a <section> element of the root.xml. Since there may be many sections in the root.xml, the <profileID> element value identifies the correct <section>.
APS-CCC-PHG-APB-POST-XML	A PHG application establishing an APS session **shall** POST the APB resource as an xml document	The APS is described by an APB resource which is expressed as an xml document.

Name	Description	Comments
APS-CCC-PHG-APB-Schema	A PHG application establishing an APS session **shall** always transmit APB resources in accordance with the APB Resource Schema of Appendix II.	
APS-CCC-PHG-APB-FILL	A PHG application establishing an APS session **shall** fill in elements of the APB resource in accordance with Table 8-1	
APS-CCC-PHG-Supported-MH-List	The entries in the <supportedMH> element **shall** be a space separated list.	The list may contain proprietary entries.
APS-CCC-PHG-APS-MH	A PHG application APSes **shall** include the string "APS" as one of the list entries in the supportedMH element of the APB resource.	This implies that all PHG applications will respond to APS-CCC defined management messages from the Health & Fitness application.
APS-CCC-PHG-Supported-MX-List	The entries in <exchangeMechanism> **shall** be a space separated list ordered from the most desired to the least desired with the first element being the most desired by the PHG.	This guideline specifies the format of the listing in the element value
APS-CCC-PHG-MQTT-MX	The PHG application **shall** specify "MQTT" in its list of supported exchange mechanisms.	Continua compliant PHG applications implementing the APS-CCC must support MQTT.
APS-CCC-PHG-Supported-ST-list	The entries in <shoulderTapMechanism> **shall** be a space separated list ordered from the most desired to the least desired with the first element being the most desired by the PHG.	This guideline specifies the format of the listing in the element value

Name	Description	Comments
APS-CCC-PHG-ST-BASE	The PHG application **shall** provide an empty list for shoulderTapMechanism if it does not support a should tap mechanism	
APS-CCC-PHG-ST-SMS	If the PHG application supports SMS as a shoulder tap mechanism then the PHG application **shall** include the <SMS> element in the APB resource	
APS-CCC-PHG-SMS-MSISDN	If the PHG application supports SMS as a shoulder tap mechanism then the PHG application **shall** include the number to reach the PHG application in the <MSISDN> child element of the <SMS> element in the APB resource	
APS-CCC-PHG-SMS-Destination-Port	If the PHG application supports SMS as a shoulder tap mechanism the PHG application **shall** include the port associated with the PHG application in the <SMSHeaderDstPort> child element of the <SMS> element in the APB resource	The source port and the source number do not need to be specified in the APB since the PHG application never sends an SMS message to the Health & Fitness application.
APS-CCC-PHG-SMS-APP-ID	If the PHG application supports SMS as a shoulder tap mechanism the PHG application **may** include the <SMSApplicationId> child element of the <SMS> element in the APB resource	This message contains an identifier that the PHG application can use to identify the received SMS message as being for itself.
APS-CCC-PHG-SMS-APP-ID-Limit	The PHG application **shall** not provide a string that when encoded inUTF-8 will exceed 148 octets for <SMSApplicationId>	

Name	Description	Comments
APS-CCC-PHG-SMS-APB-GET	A PHG application **shall** obtain the completed APB resource by invoking an HTTP GET using the URL provided by the Health & Fitness application in response to the PHG application's successful POST request.	The PHG application gets a URL in the POST return. This URL identifies the location of the APB resource which the PHG application can obtain using an HTTP GET.
APS-CCC-PHG-Ignore-XML	A PHG application **shall** ignore any XML elements it does not understand in the APB.	Supports migration to future versions of the APB
APS-CCC-PHG-Process-WAN-Elements	On receipt of an APB resource from the Health & Fitness application the PHG application **shall** only process theelements defined in Table 8-2.	The PHG application is defined to provide values for particular elements in the APB. If a Health & Fitness application incorrectly updates the values for these elements the PHG should ignore them.
APS-CCC-PHG-APS-ENABLE	The PHG application **shall** invoke an HTTP PUT of the APB/APSState resource with the value set to ENABLED to indicate it is ready to accept messages	
APS-CCC-PHG-APS-Termination	A PHG application **shall** indicate that the APS is terminated by invoking an HTTP PUT on the current APB resource with the <APSState> element value set to TERMINATED.	This action is the first step taken in APS termination.
APS-CCC-PHG-immutable	An APB resource obtained from a Health & Fitness application **shall not** be modified except for the <APSState> element	The PHG cannot modify fields of the APB resource and communicate those back to the Health & Fitness application

A.3 Guidelines for the PHG application interactions with the MQTT server

Table A-3 covers the interaction of the PHG application with respect to MQTT exchanges. A PHG application implementing the APS-CCC-PHG **shall** operate in accordance with Table A-3.

Table A-3 – PHG-MQTT exchanges

Name	Description	Comments
APS-CCC-PHG-Message-Exchange	A PHG application **shall** support the use of MQTT as a method of message exchange	Future versions of these Guidelines may support other methods of message exchange.
APS-CCC-PHG-MQTT-conformance	A PHG application **shall** be compliant with the requirement for a client as specified in [MQTT]	
APS-CCC-PHG-MQTT-Connect-URL	A PHG application's MQTT client **shall** use the information identified in the <APS_ExchangeURL> element of the APB resource in order to establish the transport connection to the MQTT server.	The Health & Fitness application indicates to the PHG application the URL that allows it to connect to the MQTT server in the <APS_ExchangeURL> element value. See Table 8-2
APS-CCC-PHG-MQTT APS-Connect-Setup	The MQTT client component of the PHG application **shall** issue the MQTT CONNECT control packet in accordance with Table 9-2.	The APS requires specific MQTT settings to be used in a CONNECT control packet.
APS-CCC-PHG-MQTT Connect-User -Name	A PHG application **shall** use the value of the <PHGAPBI> element provided by the Health & Fitness application in the APB resource as the user name in the MQTT connect message.	See Table 8-2
APS-CCC-PHG-MQTT-Connect -Password	A PHG application **shall** use the value of the <PHGCredential> element provided by the Health & Fitness application in the APB resource as the password in the MQTT connect message.	See Table 8-2

Name	Description	Comments
APS-CCC-PHG-MQTT-Client-Identifier	A PHG application **shall** use the value of the <clientId> element provided by the Health & Fitness application in the APB resource as the client identifier in the MQTT connect message.	See Table 8-2
APS-CCC-PHG-MQTT-Connect-Will-Topic	A PHG application **shall** set the Will Topic of the connect message to the status topic for this APS as defined in Figure 7-3.	The setting tells the MQTT server to publish the Will Message on the status topic when the connection to the PHG application is lost.
APS-CCC-PHG-MQTT APS-Connect-Will-Message	A PHG application **shall** set the Will Message of the connect message to “LOST”	A LOST message will be sent to the Health & Fitness application if connection to the PHG application is lost.
APS-CCC-PHG-MQTT-Normal Connect-Flags	A PHG application **shall** set the flags field of the connect control packet to indicate that the user name and password are present, that a clean session is NOT requested, and that a retained WILL message is retained.	The MQTT connection is to require a user name and password login, a retained WILL message, with no clean session. The latter indicates that any messages for the PHG application will be received once the connection is complete and the PHG application has completed its subscription to the command topic
APS-CCC-PHG-PHG-Command-Subscribe	A PHG application **shall** subscribe to the message topics as defined in Figure 7-3.	
APS-CCC-PHG-Subscribe-QoS	A PHG application **shall** set the QoS of the message topic subscription requests to 2 in accordance with Table 9-3	

Name	Description	Comments
APS-CCC-PHG-PHG Subscribe-All-Supported-mh	A PHG application **shall** subscribe to all message topics for Message Handlers that it has indicated support for in its <supportedMH> element value.	Since the PHG application does not know which CCCs are supported by the Health & Fitness application, it needs to subscribe to all of them.
APS-CCC-PHG-Publish-Status-Topic	A PHG application **shall** publish on the status topic for this APS as defined in Figure 7-3	
APS-CCC-PHG-Status Publish-Retain	A PHG application **shall** issue a PUBLISH control packet in accordance with Table 9-4 when writing values to the status topic.	In the case where the PHG is retaining the APS in the enabled state, publishing is done with the retain flag true.
APS-CCC-PHG-Clear-Queue	A PHG application **shall** set the retain flag of the PUBLISH control packet to **true** when setting the payload to a zero-length message.	In the case where the PHG is terminating the APS, publishing is done with the retain flag true since the publishing is to clear any outstanding status messages. See Clause 9.1.1
APS-CCC-PHG-Status-Publish-QoS	A PHG application **shall** set the QoS level of the PUBLISH control packet on the status topic message to 2	A QoS of 2 applies to all PUBLISH control packets
APS-CCC-PHG-Status-Publish-Payload -Values	A PHG application **shall** set the Payload of the PUBLISH control packet on the status topic to one of either “CONNECTED” or “CLOSED” or be of zero-length.	In these Guidelines the status message payload published by the PHG application may take on one of the following values “CONNECTED” “CLOSED” or of zero length, the last of which is used only in the case of clearing MQTT when the APS is terminated by the PHG application.

Name	Description	Comments
APS-CCC-PHG-Response-Publish-Topic	A PHG application **shall** PUBLISH on the response topic in accordance with Table 9-4	The response topic is specified in Figure 7-3. The proper substitutions must be made.
APS-CCC-PHG-Response-Publish -Retain	A PHG application **shall** set the retain flag to **false** when publishing on a response topic	The message does not need to be retained since it has been delivered to the Health & Fitness application. The MQTT server is internal to the Health & Fitness application.
APS-CCC-PHG-Response-Publish-QoS	A PHG application **shall** set the QoS level of the PUBLISH control packet on a response topic message to 2	A QoS of 2 applies to all PUBLISH control packets
APS-CCC-PHG-ECHO -Support	A PHG application **shall** support the APS-CCC-WAN diagnostic message ECHO command as described in Clause 8.2.6	
APS-CCC-PHG-Status-Behavior	A PHG application **shall** manage the status topic in accordance with Table 9-1	
APS-CCC-PHG-Status-Publish -Clear-MQTT	A PHG application **shall** set the status topic to INACTIVE when it successfully connects to the MQTT server under the conditions of setting the clean session flag to true with a payload of zero-length and a retain flag set to true.	This guideline defines the publish action of the PHG after connecting to MQTT server to clear it of resources. This status update is part of a sequence of events that take place when the PHG has terminated the APS.

Name	Description	Comments
APS-CCC-PHG-Graceful-APS-Termination-Procedure	A PHG application **shall** terminate an APS following the procedure in Clause 9.1.1	This guideline intends to validate that the graceful APS termination procedure follows all the steps in Clause 9.1.1 in order; terminate the APS on the APS management connection, put the MQTT server into the LOST or CLOSED state if not already in the LOST or CLOSED state, connect using the clear-connect configuration, publish using the clear-status configuration, and close the MQTT connection.

A.4 Guidelines for Health & Fitness application APS Management

The Health & Fitness application configures several elements of the APB resource for the APS. It is also responsible for assuring that a given APS is associated with a given security credential where the security credential identifies the PHG that is authenticated to use the APS. A Health & Fitness application implementing the APS-CCC-WAN **shall** operate in accordance with Table A-4.

Table A-4 – APS Management Requirements for the Health & Fitness application

Name	Description	Comments
APS-CCC-Services-Enforce-Authorized-APB-Access	A Health & Fitness application **shall** assure that the APB resource created to represent a given APS can only be accessed by an entity possessing the security credential that was used to establish the APS.	This guideline requires that the Health & Fitness application assure that any reconnection made by the PHG application for APS management is only able to operate within the APS authorized for the PHG application.
APS-CCC-Services-Enforce-Topic-Space-Access	A Health & Fitness application **shall** enforce access control to the topic space as defined in Clause 7.2	
APS-CCC-Services-XPath	A Health & Fitness application shall support references to the <APSState> element defined in the APB when this reference is expressed in accordance with [XPath].	
APS-CCC-Services-MQTT-Support	A Health & Fitness application **shall** support the use of MQTT as a mechanism for APS message exchange.	How the Health & Fitness application interacts with the MQTT server is implementation dependent but the interface exposed to the PHG application is that specified by the MQTT standard.
APS-CCC-Services-APS-Management-Support	A Health & Fitness application supporting the APS-CCC **shall** support the APS management messages defined in 8.2.6.1.1	

Name	Description	Comments
APS-CCC-Services-APB-POST-RESPONSE-APB-CREATED	If a Health & Fitness application creates an APS with the PHG application it **shall** set the return code to 201	
APS-CCC-Services-APB-POST-RESPONSE-APB-NOT-CREATED	If a Health & Fitness application does not create or update an APB on a client request to do so, it **shall** return an appropriate status code in either the 400 group or 500 group.	
APS-CCC-Services-Process-Services-Elements	On receipt of an APB resource from the PHG application the Health & Fitness application **shall** only process the elements defined in Table 8-1 .	
APS-CCC-Services-Ignore-XML	A Health & Fitness application **shall** ignore any XML elements it does not understand in the APB.	Supports migration to future versions of the APB
APS-CCC-Services-No-Modify	A Health & Fitness application **shall** not modify any elements in table Table 8-1 when presenting or processing the elements of the APB.	
APS-CCC-Services-APB-Schema	A Health & Fitness application establishing an APS session **shall** always transmit APB resources in accordance with the APB Resource Schema of Appendix II.	

Name	Description	Comments
APS-CCC-Services-Unique-PHGAPBI	A Health & Fitness application **shall** create an <PHGAPBI> element value that is unique across all APSes that are known to be valid for the Health & Fitness application.	At any given time, if the Health & Fitness application has N APSes, the <PHGAPBI> value of each one of the N associated APB resources must be unique. This requirement does not exclude the reuse of a value from an APS that was terminated.
APS-CCC-Services-PHGAPBI-Constraints	The Health & Fitness application **shall** restrict the <PHGAPBI> element's value according to the PHGAPBI entry in Table 8-2	
APS-CCC-Services-WANAPBI -Constraints	The Health & Fitness application **shall** restrict the <WANAPBI> element's value according to the WANAPBI entry in Table 8-2	
APS-CCC-Services-Unique-ClientId	A Health & Fitness application **shall** create a <clientId> value that is unique across all APSes currently in service.	Recall that this value serves as the MQTT PHG client identifier.
APS-CCC-Services-ClientId-Contraints	A Health & Fitness application **shall** restrict the <clientId> value according to the clientId entry in Table 8-2	The current MQTT specification restricts the length of the string to be 23 UTF-8 characters.

Name	Description	Comments
APS-CCC-Services-NEW-APSState	The Health & Fitness application **shall** set the <APSState> value to NEW if the PHG application does an HTTP POST and there exists no APS for the given security credential.	When the Health & Fitness application handles a POST from the PHG application and no APS currently exists for that security credential, the Health & Fitness application will need to complete the APB resource POSTed by the PHG and in that case the state is set to NEW.
APS-CCC-Services-ExpirationTime	A Health & Fitness application **shall** provide an expiration time in the <expirationTime> element value which represents the time duration for which the Health & Fitness application will tolerate inactivity.	This value represents the length of time the Health & Fitness application will accept no activity from the PHG application within the APS before testing the PHG application to see if it is still engaged. After this time if the Health & Fitness application receives no timely response to a APS “ECHO” management message after a shoulder tap wake up OR the PHG application does not respond to the shoulder tap wake up, the Health & Fitness application may terminate the APS

Name	Description	Comments
APS-CCC-Services-ResponseTime	A Health & Fitness application **shall** provide a required response time to a APS “ECHO” management message in the <requiredResponseTime> element value which represents the duration in time for which it is prepared to wait for a response to the ECHO.	This value represents how long a PHG application has to respond to a UC “ECHO” message before the Health & Fitness application considers the PHG application out of service at which time the Health & Fitness application may terminate the APS.
APS-SUPPORT-TERMINATE	A Health & Fitness application **shall** support the termination of a APS as defined in 8.2.5.	
APS-CCC-Services-MQTT-URL	A Health & Fitness application **shall** provide the URL to the Services MQTT end point in the <APSExchangeURL> element value.	

Name	Description	Comments
APS-CCC-Services-APB-EXISTS	If the PHG application invokes an HTTP POST and an APS already exists for the security credential the Health & Fitness application **shall** ignore the contents of the POST and return the URL to the existing APB.	A PHG application that performs a POST to recover an APB using a security credential associated with an existing APB will get the already existing APB resource. The value of the APSState element in this case is set to ENABLED. It is advisable to check the state of APSState to ensure the expected value is returned. *Notice that when and APB already exists on the Health & Fitness device, it will ignore all information the PHG includes in the APB POST. Therefore, when the PHG receives and APB with APSState set to ENABLED, it should check that all PHG related details in the APB are still correct. If the PHG related details are not correct anymore the PHG will first need to terminate this existing APB and subsequently create a new APB with updated information.*
APS-CCC-Services-APB-URL	A Health & Fitness application **shall** respond to a HTTP POST that successfully created an APB resource with a URL that points to the APB resource	

Name	Description	Comments
APS-CCC-Services-Provide-APB	A Health & Fitness application **shall** provide the completed APB resource when the PHG application performs a GET using the POST URL. The POST URL is the URL returned by the Health & Fitness application in response to the PHG applications POST operation.	When the PHG application does an HTTP GET for the APB resource, the Health & Fitness application delivers the APB resource that the PHG application has been authenticated to operate with.
APS-CCC-Services-NO-APB-GET	If a PHG does an HTTP GET for the APB resource but the Health & Fitness application finds no APB resource that is authorized for use by this PHG application, the Health & Fitness application **shall** respond with code 404 resource not found.	This case could happen, for example, when a trusted PHG has neglected to do a POST but still has the correct URL to point to the resource.
APS-CCC-Services-APSState-Update	A Health & Fitness application **shall** update the <APSState> element value of the APB resource to the <APSState> element value sent by the PHG application in an HTTP PUT transaction if the value is either ENABLED or TERMINATED, otherwise it **shall** return the status code 403	
APS-CCC-Services-APSState-Only	A Health & Fitness application **shall** ignore all values in the APB resource except the <APSState> element value sent by the PHG application in an HTTP PUT transaction.	

Name	Description	Comments
APS-CCC-Servoces-NO-APB-PUT	If a PHG application does an HTTP PUT of an APB resource but the Health & Fitness application finds no existing APB resource authenticated for use by the PHG application, the Health & Fitness application **shall** respond with code 404 resource not found	
APS-CCC-Services-WAIT-FOR-ENABLE	A Health & Fitness application **shall** refrain from sending messages to a PHG application until the <APSState> is set to ENABLED	Though the PHG application is technically able to receive messages as soon as it has connected and subscribed to the message topic, no message are sent until the APS state has been set to enabled. Only the PHG application can set the state. The PHG application does not set the state to enabled until it is ready to handle messages.
APS-CCC-Services-APB-Remove-On-Terminate	A Health & Fitness application **shall** terminate the APS associated with the APB when the PHG sets the <APSState> to TERMINATED. The Health & Fitness application **shall** ensure that a MQTT connection based on the terminated APB resource will fail	
APS-CCC-Services-ExpirationTime	A Health & Fitness application **shall** operate in accordance to Table 8-2 relative to inactivity exceeding <expirationTime>	See Table 8-2, <expirationTime>

A.5 Guidelines for the PHG Application SMS Shoulder Tap

A PHG application implementing the APS-CCC-PHG **shall** operate in accordance with Table A-5.

Table A-5 – SMS Shoulder Tap PHG

Name	Description	Comments
APS-CCC-PHG-ST-Missing-ID	If the PHG application supports a Shoulder Tap using SMS, and it provides a SMSApplicationId then it **shall** ignore all messages that do not contain the application identifier it set in the APB resource.	The identifier is a number the PHG application created in order to identify the SMS message as being for itself.
APS-CCC-PHG-ST-Reestablish	If the PHG application supports shoulder tap using SMS, then it **shall** attempt to re-establish TCP connectivity with the Health & Fitness application when a SMS message containing the CEI of 01 (Re-establish transport level connectivity) is received.	This guideline assumes the message is addressed to the address and port specified in the APB resource.

A.6 Guidelines for the Health & Fitness application SMS Shoulder Tap

A Health & Fitness application implementing the APS-CCC-Services shall operate in accordance with Table A-6.

Table A-6 – SMS Shoulder Tap WAN

Name	Description	Comments
APS-CCC-Services-ST-Send-Contents	If the Health & Fitness application supports shoulder tap using SMS, then when generating the shoulder tap message it **shall**: a) use the MSISDN and SMSHeaderDstPort elements within the APB resource, and b) include the shoulder tap payload.	
APS-CCC-Services-ST-Format	A Health & Fitness application **shall** format the Shoulder Tap payload as specified in 10.5.	This guideline specifies details such as the presence of the Continua header and TLV messages
APS-CCC-Services-ST-Include-APP-ID	A Health & Fitness application **shall** include the <SMSApplicationId> element value of the APB resource in the payload of the SMS in accordance with Clause 10.5.	This value is a means for the PHG application to identify the SMS message as being for itself.

Annex B XML Schema for the APB Resource

The XML structure as seen by the PHG application performing the GET of the APB.

```
<?xml version="1.0" encoding="UTF-8"?>
<schema xmlns="http://www.w3.org/2001/XMLSchema"
        targetNamespace="handle.itu.int/11.1002/3000/hData/APS"
        xmlns:tns="http:// handle.itu.int/11.1002/3000/hData/APS" elementFormDefault="unqualified">
  <complexType name="APBType">
    <sequence>
      <element name="supportedMH">
        <simpleType>
          <list itemType="string" />
        </simpleType>
      </element>
      <element name="exchangeMechanism">
        <simpleType>
          <list itemType="string" />
        </simpleType>
      </element>
      <element name="shoulderTapMechanism">
        <simpleType>
          <list itemType="string" />
        </simpleType>
      </element>
      <element name="SMS" type="tns:SMSType" minOccurs="0"/>
      <group ref = "tns:WANServerFields" minOccurs="0"/>
      <any namespace="##other" minOccurs="0" maxOccurs="unbounded" processContents="lax" />
    </sequence>
  </complexType>
  <element name="APB" type="tns:APBType"></element>
  <complexType name="SMSType">
    <sequence>
      <element name="MSISDN">
        <simpleType>
          <restriction base="string">
            <maxLength value="15"></maxLength>
            <pattern value="\d+"></pattern>
          </restriction>
        </simpleType>
      </element>
      <element name="SMSHeaderDstPort" type = "unsignedShort"/>
      <element name="SMSApplicationId" minOccurs="0">
        <simpleType>
          <restriction base="string">
            <maxLength value="128"/>
          </restriction>
        </simpleType>
      </element>
    </sequence>
  </complexType>
  <simpleType name="APBI">
    <restriction base="string">
      <maxLength value="2047"></maxLength>
      <pattern value="[^/#+*]+"></pattern>
    </restriction>
  </simpleType>
  <group name="WANServerFields">
    <sequence>
      <element name="WANAPBI" type="tns:APBI" />
      <element name="PHGAPBI" type="tns:APBI" />
      <element name="APSExchangeURL" type="anyURI" />
      <element name="APSState">
        <simpleType>
          <restriction base="string">
            <enumeration value="NEW"></enumeration>
            <enumeration value="ENABLED"></enumeration>
            <enumeration value="TERMINATED"></enumeration>
          </restriction>
        </simpleType>
      </element>
      <element name="expirationTime" type="duration"/>
      <element name="requiredResponseTime" type="duration" />
```

```
      <element name="clientId" type="string" minOccurs="0"/>
      <element name="PHGCredential" type="string" minOccurs="0"/>
    </sequence>
  </group>
</schema>
```

Appendix I APS Details

I.1 APS information in the root.xml

A PHG obtains information regarding the capabilities supported by a Health & Fitness application through examining the Health & Fitness application's hData defined resource layout. This information is obtained through the root.xml file that is made available by the Health & Fitness application using the Capability Exchange facility documented in *H.812.3 Capability Exchange Certified Capability Class Guidelines.*

A Health & Fitness application that supports the APS includes three entries related to the APS in its *root.xml*. The first entry indicates to the PHG application that the APS capability is supported. This entry is provided in a profile element and appears as shown in Figure 8-1.

A second entry provides both a reference to and a validator (such as an xml schema) for the APB descriptor (such as an xml schema). This entry is provided in a resourceType element and appears as shown in Figure 8-2.

The third entry provides the URL the PHG application is to use when it wishes to establish an APS with the Health & Fitness application. This URL is where the PHG application POSTs a description of its APS related capabilities. This entry is provided in a section element and appears as shown in Table 8-3.

> *NOTE: The Continua Device Classes (CCCs) documented in the root.xml are not the message handlers supported by the PHG application. These are found in the APB resource. The Health & Fitness application does not expose which protocols will use the APS service.*

I.2 APS Authentication: Resource Owner Password Credentials Approach

There are several techniques for associating an APS with a security credential. The following description illustrates the use of the resource owner password credentials as a method of obtaining access to the APB resource associated with the APS. For additional details see Annex B of the Continua *H.812 WAN IF Common Certified Capability Class Guidelines*.

Once the PHG application determines that the Health & Fitness application supports creating an APS through capability exchange, the PHG application can initiate the process of APS establishment. The first step in this process is for the PHG application to validate the Health & Fitness application through establishing a TLS connection with the Health & Fitness application. The PHG application may be aware of several different URLs associated with the Health & Fitness application. In this case we assume that the PHG application and Health & Fitness application have exchanged information relative to an authentication service. The login service accepts a username/password (resource owner credentials) from the PHG application and if these match returns an OAUTH access token of type bearer. With this access token in hand the PHG application is able to perform HTTPS operations to obtain the APB resource associated with the Authenticated Persistent Session service advertised in the root.xml file.

I.3 APS Establishment: PHG Application POST with Partial APB

Once the connection has been established the PHG application does a POST to the URL provided in the *root.xml* of the Health & Fitness application. The POST contains an xml document describing the PHG application's APS capabilities (Table 8-1) as follows:

Figure I-1 Example APB Posted by PHG Application

```
<?xml version="1.0" encoding="UTF-8"?>
  <aps:APB xmlns:aps="http:// handle.itu.int/11.1002/3000/hData/APS"
      xmlns:xsi = "http://www.w3.org/2001/XMLSchema-instance"
      xsi:schemaLocation = "
      http://handle.itu.int/11.1002/3000/hData/APS/2015/01/APBConfigResource.xsd">
        <!-- These fields are filled in by the PHG -->
        <supportedMH>APS lampreynetworks.com/private</supportedMH>
        <exchangeMechanism>MQTT privateMessageProtocol</exchangeMechanism>
        <shoulderTapMechanism>SMS</shoulderTapMechanism>
        <SMS>
          <MSISDN>441111223344</MSISDN>
          <SMSHeaderDstPort>1234</SMSHeaderDstPort>
          <SMSApplicationId>4827351</SMSApplicationId>
        </SMS>
      </aps:APB>
```

The Health & Fitness application can examine the space separated list of supported message handlers in the <supportedMH> element to see if the PHG application supports services that the Health & Fitness application can issue messages to. The Health & Fitness application can also inspect the space separated list of exchange mechanisms and the space separated list of shoulder tap mechanisms. If the Health & Fitness application supports a transfer mechanism advertised by the PHG application, the Health & Fitness application will be able to establish an APS. In this case the Health & Fitness application responds with an appropriate HTTP code such as 201 CREATED and provides a URL to the Authenticated Persistent Binding (APB) resource. If the PHG application does not support any CCCs or transfer mechanisms that the Health & Fitness application supports, the Health & Fitness application responds with HTTP error code such as 501 (Not Implemented).

I.3.1 APS Establishment: PHG GET for Completed APB

The PHG application can then issue a GET request for the APB resource. The PHG application must properly format the resource path according to the <resourcePrefix> entry in the *root.xml*. The Health & Fitness application creates the APB resource for the APS. The APB resource created is associated with the authentication credentials of the PHG application. The Health & Fitness application fills in the remaining elements of the xml document describing the APB resource in accordance with Table 8-2

The resulting APB, as would be obtained by the PHG using the GET operation, is outlined below.

Figure I-2 APB Created by Health & Fitness Application

Note:This example includes a private message handler (lampreynetworks.com/private) as well as the required APS message handler.

```
<?xml version="1.0" encoding="UTF-8"?>
<aps:APB xmlns:aps="http://handle.itu.int/11.1002/3000/hData/APS"
      xmlns:xsi = "http://www.w3.org/2001/XMLSchema-instance"
      xsi:schemaLocation =
      "http://handle.itu.int/11.1002/3000/hData/APS/2015/01/APBConfigResource.xsd">


        <!-- These fields are filled in by the PHG -->
        <supportedMH>APS lampreynetworks.com/private</supportedMH>
        <exchangeMechanism>MQTT privateMessageProtocol</exchangeMechanism>
        <shoulderTapMechanism>SMS</shoulderTapMechanism>
        <SMS>
          <MSISDN>441111223344</MSISDN>
          <SMSHeaderDstPort>1234</SMSHeaderDstPort>
          <SMSApplicationId>4827351</SMSApplicationId>
```

```
        </SMS>

        <!-- chosen by the Health & Fitness application; may be the same for every APS -->
  <HFSAPBI>HFSAPBI</HFSAPBI>
  <!-- chosen by the Health & Fitness application; must be unique in all APSes on the Health &
Fitness application
       It is used as the 'user name' for MQTT -->
  <PHGAPBI>PHGAPBI</PHGAPBI>
  <!-- The address to the MQTT server -->
  <APSExchangeURL>address to the MQTT server</APSExchangeURL>
  <!-- The APS state which is NEW when first created -->
  <APSState>NEW</APSState>
  <!-- Chosen by the Health & Fitness application; The length of time the PHG may be silent
       before the Health & Fitness application may try and shut it down (after probing) -->
  <expirationTime>expirationTime</expirationTime>
  <!-- Chosen by the Health & Fitness application; The length of time that the PHG has to
       respond to an ECHO -->
  <requiredResponseTime>requiredResponseTime</requiredResponseTime>
  <!-- chosen by the Health & Fitness application and serves as the client identifier for the MQTT
server -->
  <clientId>clientId</clientId>
  <!-- chosen by the Health & Fitness application and serves as the 'password' for the MQTT server
       For example the thumbprint of the PHG certificate -->
  <PHGCredential>PHGCredential</PHGCredential>
</aps:APB>
```

The Health & Fitness application may want to configure the MQTT software component at this time. This standard does not specify how the Health & Fitness application interacts with the MQTT server. The PHG application will publish on the response and status topics. How the Health & Fitness application obtains this information is out of scope.

I.3.2 APS Establishment: PHG Setup with MQTT Server

Once the PHG application receives the APB resource, it needs to establish a secured connection with the MQTT server. The address of the MQTT server is provided in the APB resource.

The MQTT CONNECT command flags are used in a manner to indicate that a username and password are present, that the Will Message will be retained, and that the session is not to be cleaned (this means that undelivered messages will be persisted across teardowns of the TCP connection) as defined in Table 9-2. These settings allow a previously published message on a topic to be received once the PHG application subscribes to that topic. The user name and password are the PHGAPBI and PHGCredential, respectively, provided in the APB resource. The MQTT protocol requires that the PHG application provide a client identifier. The client identifier is provided in the clientID element of the APB resource. The PHG application also specifies a keep alive time which states how long it may remain inactive before issuing an MQTT PING. Specifying a 0 indicates that the PHG application will not send PING packets. The PHG application also sets the WILL message flag. This parameter indicates what the MQTT server will do when the connection to the PHG application is lost. The PHG application sets the WILL parameters to use the status topic with a payload "LOST". Thus when the connection to the PHG application is lost, the MQTT server will publish a message to the status topic with the payload "LOST".

I.3.3 MQTT: PHG Application Subscribes to Commands

Once connected, the PHG application subscribes to the message topic for each CCC it is interested in receiving messages from. A single message topic is specified as follows:
`pcha/message/HFSAPBI/PHGAPBI/mh`
where the WANAPBI and PHGAPBI are provided in the APB resource and the 'mh' parameter is the CCC that is to receive the message. An example message topic may appear as follows:
`pcha/message/WANAPBI/`6d296e99-e5dc-43d0-b455-7c1f3eb35d83`/APS`

I.3.4 MQTT: PHG Application Publishes “CONNECTED”

When all the subscriptions are completed the PHG application publishes a message on the status topic `pcha/status/WANAPBI/`6d296e99-e5dc-43d0-b455-7c1f3eb35d83 with the payload “CONNECTED”. At this time, the PHG application is technically able to receive commands from the Health & Fitness application. However, there is an additional requirement that the Health & Fitness application refrain from sending any messages until the PHG application enables the APS.

I.4 APS Establishment: PHG Application Enables APS

Enabling the APS requires that the PHG application perform a PUT operation to the URL provided in the POST response (response_URL) appended with the XPath representation of the APSState element. (e.g. created_APS_resource_URL/APSState). The mime type is set to application/text and the http body contains the text ENABLED.

The Health & Fitness application responds with success (200 OK) if it is able to change the APSSate.

I.5 Operation

At this point, the PHG application can receive messages for all message strings it has subscribed handlers to receive messages for. The PHG application is able to identify which CCC the message payload is for by examining the ‘mh’ component of the message topic. After handling the message, the PHG application responds by publishing a response-topic message with the payload returned from the CCC (if any).

The PHG application is allowed to disconnect from the MQTT server maintaining the APS session; the APS session is still enabled but the PHG application will not be able to receive messages. The Health & Fitness application will discover that the connection is in the “CLOSED” state by the reception of a CLOSED message on the status topic. The PHG application can re-establish the connection at any time by re-invoking the MQTT connect sequence. The PHG application will publish “CONNECTED” on the status topic when it successfully establishes the MQTT client connection.

However the more likely situation for the PHG application reconnecting is that the Health & Fitness application wakes up the PHG application using one of the mutually supported shoulder-tap mechanisms because the Health & Fitness application needs to send a message.

If there has been no activity for the APB resource for <expirationTime>, the PHG application may receive an ECHO (‘APS’) management message from the Health & Fitness application. The PHG application informs the Health & Fitness application that it is still alive and connected by publishing on the response topic the response to the “ECHO” command. The Health & Fitness application expects to be notified of this response within the <requiredResponseTime> specified in the APB resource. If the PHG application is not connected at the time the Health & Fitness application may choose to use the shoulder-tap process in order to reestablish transport level connectivity.

At any time the PHG application can terminate an APS by performing a PUT operation in the same manner as when it enabled the APS but in this case setting the <APSState> element value of the APB resource to TERMINATED. The PHG application terminates the APS by clearing the MQTT

server of any outstanding commands and UNSUBSCRIBES to associated response and status topics. Both sides may terminate the APS for administrative (out of band) reasons.
Once terminated, the Health & Fitness application removes information that associated the APB resource with the PHG application's authentication credential such that if the PHG application initiated another APS establishment procedure with the same authentication credential, the Health & Fitness application would return NEW for the APS State element value.

Appendix II Example Health & Fitness Service root.xml file

```
<profile>
  <!-- Specified value -->
  <id>APS-CCC-HFS</id>
  <reference>
    http:// handle.itu.int/11.1002/3000/hData/APS/2015/01/H.812.4.pdf
  </reference>
</profile>


<resourceType>
  <resourceTypeID>APB</resourceTypeID>
  <!-- location of reference that describes the APS standard -->
  <reference>
    http:// handle.itu.int/11.1002/3000/hData/APS/2015/01/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/2015/01/APBConfigResource.xsd
    </validator>
  </representation>
<resourceType>


<section>
  <path>APB/</path>
  <profileID>APS-CCC-HFS</profileID>
  <!-- required in this specification; optional but recommended in hData; -->
  <resourcePrefix>true</resourcePrefix>
  <resourceTypeID>APB</resourceTypeID>
</section>
```

Bibliography

[GSM/UMTS] 3GPP TS 23.040 version 11.3.0, *Technical Realization of the Short Message Service* Available at: http://www.3gpp.org/ftp/Specs/archive/23_series/23.040/23040-b30.zip

[CDMA 2000] 3GPP2 C.S0015-C v1.0, *Short Message Service (SMS) for Wideband Spread Spectrum Systems* Available at http://www.3gpp2.org/public_html/specs/C.S0015-C_v1.0_20121126.pdf.

[XPath 2.0] W3C XML Path Language (XPath) 2.0 (Second Edition) Available at: http://www.w3.org/TR/2010/REC-xpath20-20101214/