Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

H.812.4

(11/2017)

SERIE H: SISTEMAS AUDIOVISUALES Y MULTIMEDIA

Sistemas, servicios y aplicaciones multimedios de cibersalud – Sistemas personales de salud

Directrices de diseño para la interoperabilidad de sistemas de salud personal conectados: Interfaz de servicios: capacidad de sesión persistente autenticada

Recomendación UIT-T H.812.4

RECOMENDACIONES UIT-T DE LA SERIE H

SISTEMAS AUDIOVISUALES Y MULTIMEDIA

CARACTERÍSTICAS DE LOS SISTEMAS VIDEOTELEFÓNICOS	H.100–H.199
INFRAESTRUCTURA DE LOS SERVICIOS AUDIOVISUALES	
Generalidades	H.200–H.219
Multiplexación y sincronización en transmisión	H.220–H.229
Aspectos de los sistemas	H.230–H.239
Procedimientos de comunicación	H.240–H.259
Codificación de imágenes vídeo en movimiento	H.260–H.279
Aspectos relacionados con los sistemas	H.280–H.299
Sistemas y equipos terminales para los servicios audiovisuales	H.300–H.349
Arquitectura de servicios de directorio para servicios audiovisuales y multimedia	H.350–H.359
Arquitectura de la calidad de servicio para servicios audiovisuales y multimedia	H.360–H.369
Telepresencia	H.420–H.429
Servicios suplementarios para multimedia	H.450–H.499
PROCEDIMIENTOS DE MOVILIDAD Y DE COLABORACIÓN	
Visión de conjunto de la movilidad y de la colaboración, definiciones, protocolos y procedimientos	H.500–H.509
Movilidad para los sistemas y servicios multimedia de la serie H	H.510–H.519
Aplicaciones y servicios de colaboración en móviles multimedia	H.520–H.529
Seguridad para los sistemas y servicios móviles multimedia	H.530–H.539
Seguridad para las aplicaciones y los servicios de colaboración en móviles multimedia	H.540–H.549
PASARELAS VEHICULARES Y SISTEMAS DE TRANSPORTE INTELIGENTES (STI)	
Arquitectura de las pasarelas vehiculares	H.550–H.559
Interfaces de pasarelas vehiculares	H.560–H.569
SERVICIOS MULTIMEDIOS DE BANDA ANCHA, DE TRÍADA Y AVANZADOS	
Servicios multimedia de banda ancha sobre VDSL	H.610–H.619
Servicios y aplicaciones multimedios avanzados	H.620–H.629
Aplicaciones de red de sensores ubicuos e Internet de las cosas	H.640–H.649
SERVICIOS MULTIMEDIOS Y APLICACIONES PARA LA TELEVISIÓN POR REDES IP	
Aspectos generales	H.700–H.719
Dispositivos terminales para la televisión por redes IP	H.720–H.729
Soportes intermedios para la televisión por redes IP	H.730–H.739
Tratamiento de eventos en las aplicaciones de televisión por redes IP	H.740–H.749
Metadatos para la televisión por redes IP	H.750–H.759
Marcos de las aplicaciones multimedios para la televisión por redes IP	H.760–H.769
Exploración de los servicios hasta el punto del consumo en la televisión por redes IP	H.770–H.779
Señalización digital	H.780–H.789
SISTEMAS, SERVICIOS Y APLICACIONES MULTIMEDIOS DE CIBERSALUD	
Sistemas de salud personal	**H.810–H.819**
Realización de pruebas de conformidad para el interfuncionamiento de los sistemas de salud personales (HRN, PAN, LAN, TAN y WAN)	H.820–H.859
Servicios multimedios de intercambios de datos de cibersalud	H.860–H.869

Para más información, véase la Lista de Recomendaciones del UIT-T.

Recomendación UIT-T H.812.4

Directrices de diseño para la interoperabilidad de sistemas de salud personal conectados: Interfaz de servicios: capacidad de sesión persistente autenticada

Resumen

Las Directrices de Diseño Continua (CDG) definen un marco de criterios y normas subyacentes necesario para garantizar la interoperabilidad de los dispositivos y datos utilizados en sistemas de salud personal conectados. Además, incluyen una serie de directrices de diseño (DG), que aclaran las normas o especificaciones subyacentes reduciendo las opciones o añadiendo características que faltaban para mejorar la interoperabilidad.

En la Recomendación UIT-T H.812.4 se definen las directrices de diseño adicionales para la sesión persistente autenticada (APS), cuya función es proporcionar un canal de datos bidireccional seguro, de larga duración y persistente entre la aplicación de servicios de salud y fortalecimiento físico (HFS) y una aplicación de pasarela de salud personal (PHG) que sea adecuado para el envío de instrucciones no solicitadas a la PHG o a dispositivos conectados a través de ella.

La Recomendación UIT-T H.812.4 forma parte de la subserie de Recomendaciones "UIT-T H.810 – Directrices de diseño para la interoperabilidad de sistemas de salud personal conectados", que abarca lo siguiente:

– ITU-T H.810 – Directrices de diseño para la interoperabilidad de sistemas de salud personal conectados: introducción

– ITU-T H.811 – Directrices de diseño para la interoperabilidad de sistemas de salud personal conectados: interfaz de los dispositivos de salud personal

– ITU-T H.812 – Directrices de diseño para la interoperabilidad de sistemas de salud personal conectados: interfaz de servicios

– ITU-T H.812.1 – Directrices de diseño para la interoperabilidad de sistemas de salud personal conectados: interfaz de servicios; capacidad certificada de carga de observaciones

– ITU-T H.812.2 – Directrices de diseño para la interoperabilidad de sistemas de salud personal conectados: Interfaz de servicios: cuestionarios

– ITU-T H.812.3 – Directrices de diseño para la interoperabilidad de sistemas de salud personal conectados: Interfaz de servicios: clase de capacidad certificada de intercambio de capacidades

– ITU-T H.812.4 – Directrices de diseño para la interoperabilidad de sistemas de salud personal conectados: Interfaz de servicios: capacidad de sesión persistente autenticada (es decir, las presentes directrices de diseño)

– ITU-T H.813 – Directrices de diseño para la interoperabilidad de sistemas de salud personal conectados: interfaz del sistema de información sanitaria.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	ITU-T H.812.4	2015-11-29	16	11.1002/1000/12657
2.0	ITU-T H.812.4	2016-07-14	16	11.1002/1000/12917
3.0	ITU-T H.812.4	2017-11-29	16	11.1002/1000/13419

Palabras clave

CDG, directrices de diseño Continua, dispositivos de salud personal, servicios, sistemas de información sanitaria, sistemas de salud personal conectados, sesión persistente.

* Para acceder a la Recomendación, sírvase digitar el URL http://handle.itu.int/ en el campo de dirección del navegador, seguido por el identificador único de la Recomendación. Por ejemplo, http://handle.itu.int/11.1002/1000/11830-en.

PREFACIO

La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones y de las tecnologías de la información y la comunicación. El Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT no ha recibido notificación de la existencia de propiedad intelectual, protegida por patente o derecho de autor, que puede ser necesaria para implementar esta Recomendación. Sin embargo, debe señalarse a los implementadores que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar las correspondientes bases de datos del UIT T disponibles en el sitio web del UIT T en http://www.itu.int/ITU-T/ipr/.

ÍNDICE

Lista de cuadros

Página

Lista de figuras

Página

0 Introducción

Las Directrices de Diseño Continua (CDG) definen un marco de criterios y normas subyacentes necesario para garantizar la interoperabilidad de los dispositivos y datos utilizados en sistemas de salud personal conectados. Además, incluyen directrices de diseño adicionales que aclaran las normas o especificaciones subyacentes reduciendo las opciones o añadiendo características que faltaban para mejorar la interoperabilidad.

Estas directrices de diseño definen las directrices de diseño adicionales para la sesión persistente autenticada (APS), cuya función es proporcionar un canal de datos bidireccional seguro, de larga duración y persistente entre la aplicación HFS y una aplicación PHG que sea adecuado para el envío de instrucciones no solicitadas a la PHG o a dispositivos conectados a través de la PHG.

Las presentes directrices de diseño forman parte de la subserie de Recomendaciones "UIT-T H.810 – Directrices de diseño para la interoperabilidad de sistemas de salud personal conectados". Para obtener más información al respecto, véase [UIT-T H.810].

0.1 Organización

Las presentes directrices de diseño se articulan como sigue:

Apartados 0-5: **Introducción y terminología** – En estos apartados se proporciona información de antecedentes útil que ayuda a comprender la estructura de las especificaciones de diseño.

Apartado 6: Casos de uso – En este apartado se describe una situación que provoca la clase de problemas de los que se ocupa la APS.

Apartado 7: Visión de conjunto de la sesión persistente autenticada – En este apartado se incluye una presentación técnica del funcionamiento de la APS.

Apartado 8: Gestión de la sesión persistente autenticada – En este apartado se describen las interacciones entre las partes en el intercambio de información.

Apartado 9: Modelo de comportamiento: MQTT – En este apartado se presentan las secuencias de interacciones de esta clase de capacidad certificada (CCC) y se resumen las iteraciones, limitaciones y excepciones habituales.

Apartado 10: Modelo de comportamiento: Capacidad de interrupción SMS – En este apartado se define una capacidad del SMS que facilita el funcionamiento de la APS con redes que eliminan la infraestructura de IP de las conexiones inactivas.

Anexo A: En este anexo se presentan las directrices que documentan los elementos normativos de la sesión persistente autenticada en formato tabular. Se ofrecen referencias a otras ubicaciones con contenido normativo.

Anexo B: Fichero raíz de la sesión persistente autenticada.

Apéndice I: Información detallada de la APS.

Apéndice II: Esquema del recurso de APB.

0.2 Publicación y versiones de las directrices

Para obtener información sobre publicaciones y versiones, véase el apartado 0.2 de [UIT-T H.810].

0.3 Novedades

Para conocer las novedades de la presente versión de las directrices de diseño, véase el apartado 0.3 de [UIT-T H.810].

Recomendación UIT-T H.812.4

Directrices de diseño para la interoperabilidad de sistemas de salud personal conectados: Interfaz de servicios: capacidad de sesión persistente autenticada

1 Alcance

En el presente documento de directrices de diseño se definen dos clases de capacidad certificada (CCC). Las dos CCC contienen directrices que documentan un mecanismo seguro por medio del cual una aplicación de servicios de salud y fortalecimiento físico (HFS) puede iniciar la comunicación con una aplicación alojada en un equipo transitorio de las instalaciones del cliente denominada pasarela de salud personal (PHG). Las dos CCC se aplican respectivamente a la aplicación de servicios (APS-CCC-Services) y a la aplicación PHG (APS-CCC-PHG).

El mecanismo se ocupa de lo siguiente: 1) el establecimiento y la gestión de una sesión a largo plazo persistente entre la aplicación de servicios y la aplicación PHG, 2) el uso del protocolo de transporte de telemetría de puesta en cola de mensajes (MQTT) para el intercambio de mensajes y 3) el uso del servicio de mensajes cortos (SMS) para restablecer la conectividad IP con PHG transitorias que disponen de una interfaz celular.

2 Referencias

Las siguientes Recomendaciones UIT-T y demás referencias contienen disposiciones que, por referencia a las mismas en este texto, constituyen disposiciones de esta Recomendación. En la fecha de publicación, las ediciones citadas estaban en vigor. Todas las Recomendaciones y demás referencias están sujetas a revisión, por lo que se alienta a los usuarios de esta Recomendación a que consideren la posibilidad de aplicar la edición más reciente de las Recomendaciones y demás referencias que se indican a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T vigentes. La referencia a un documento en el marco de esta Recomendación no confiere al mismo, como documento autónomo, el rango de Recomendación.

[UIT-T H.810] Recomendación UIT-T H.810 (2017), *Directrices de diseño para la interoperabilidad de sistemas de salud personal conectados: Introducción*.

Los demás documentos a los que se hace referencia se incluyen en el apartado 2 de [UIT-T H.810].

3 Definiciones

En las presentes directrices de diseño se utilizan los términos definidos en [UIT-T H.810].

4 Abreviaturas y acrónimos

En las presentes directrices de diseño se utilizan las abreviaturas y los acrónimos definidos en [UIT-T H.810].

5 Convenios

Las presentes directrices de diseño se ajustan a los convenios definidos en [UIT-T H.810].

6 Caso de uso de sesión persistente autenticada

La sesión persistente autenticada (APS) es un mecanismo que permite que las CCC Continua futuras inicien comunicaciones entre servicios en la nube y la PHG.

7 Visión de conjunto de la sesión persistente autenticada

La CCC APS define un contexto persistente de larga duración para el intercambio de mensaje entre una aplicación HFS y una aplicación PHG. El contexto es persistente en la medida en que mantiene el estado operacional en las conexiones TCP, pausando la sesión cuando se pierde la conexión TCP subyacente y reanudándola cuando se restablece. La sesión es de larga duración puesto que las aplicaciones la mantienen durante todo el tiempo que resulte necesario. Las sesiones persistentes de larga duración soportan las aplicaciones que envían mensajes ocasionales y requieren una respuesta rápida.

NOTA 1 – En las presentes directrices se define una CCC APS para una aplicación PHG (APS-CCC-PHG) y para una aplicación HFS (APS-CCC-Interfaz de servicios). Se emplea la notación abreviada CCC APS cuando no es necesario eliminar la ambigüedad entre el servicio real y las CCC de PHG.

La CCC APS está optimizada para el envío de mensajes a través de redes con anchura de banda, potencia y recursos IP limitados. Para conseguir la optimización, se elimina la interrogación basada en la aplicación PHG. La CCC APS define una capacidad de activación opcional basada en el SMS que se puede utilizar cuando la PHG tiene conectividad de red celular. Esta capacidad permite que la aplicación HFS active una aplicación PHG que ya no tiene conectividad IP a raíz de la reasignación de los recursos inactivos por la red celular. Las implementaciones compatibles con el SMS podrían aprovechar esta capacidad opcional para minimizar su uso de la red.

El término "sesión persistente autenticada" (APS) describe el concepto de la sesión persistente conforme a la definición de este documento de directrices de diseño. Se utiliza el término conexo "vinculación persistente autenticada" (APB) para describir el recurso de información intercambiado durante el establecimiento de la sesión persistente. Al añadir el calificativo "autenticado" a "sesión persistente" y "vinculación persistente" se pone de relieve la relación que crea la aplicación HFS entre el recurso de APB y la credencial de seguridad de la aplicación PHG a fin de garantizar que, cuando la aplicación PHG reanuda una sesión persistente, la autenticación se realiza de forma adecuada.

En la Figura 7-1 se presenta el marco de la APS.

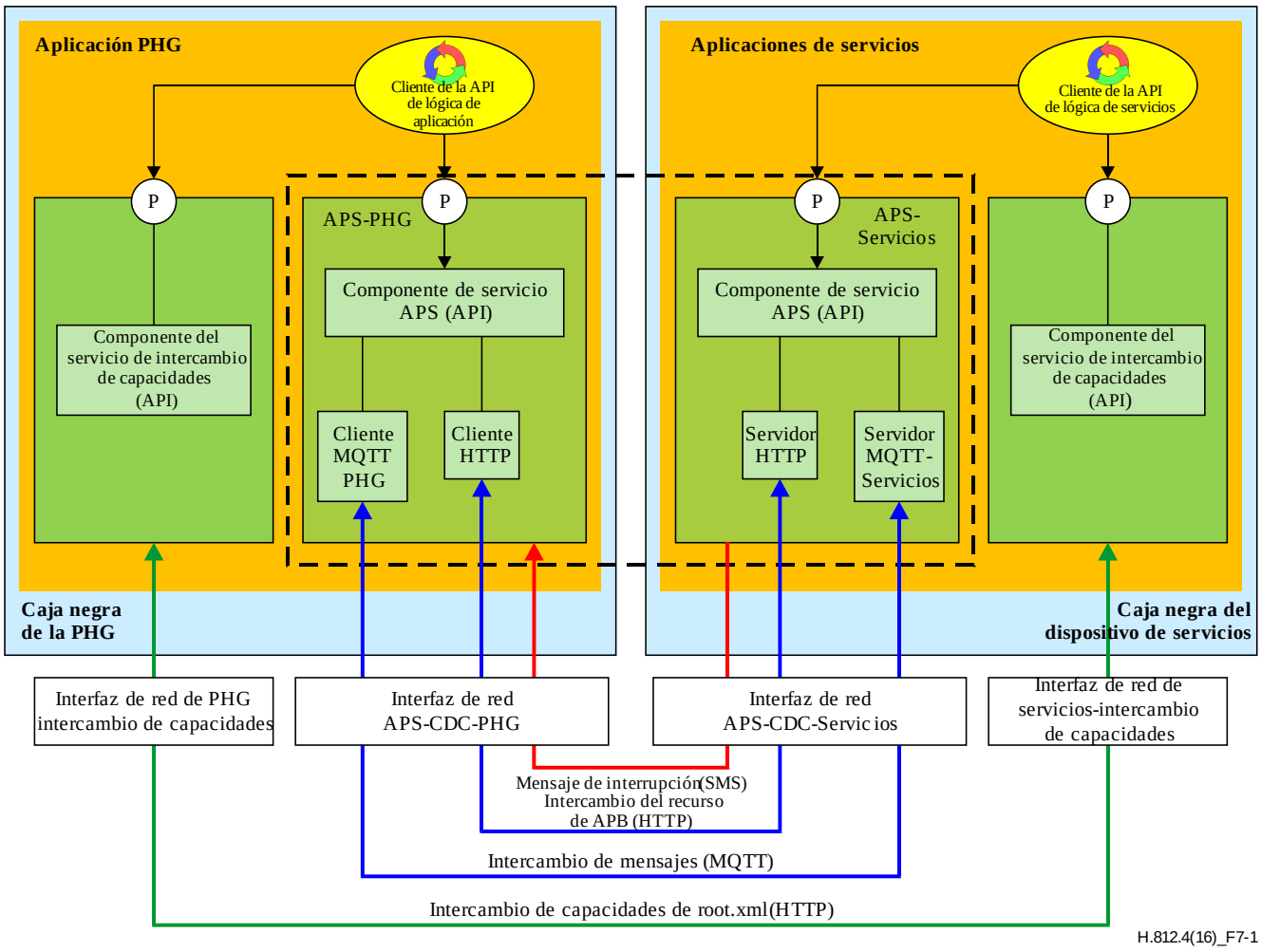

Figura 7-1 – Marco de la APS

Una sesión persistente autenticada (APS) es una vinculación entre dos *componentes de servicio APS (*uno en la *aplicación HFS* y otro en la *aplicación PHG*) que permite que los *clientes de la API* se comporten como si siempre estuvieran conectados por una línea. En la Figura 7-1, los *componentes de servicio de la API de APS* son las entidades homólogas que aplican estas directrices para proporcionar el servicio de sesión persistente a sus *clientes de la API*. La *aplicación HFS* que utiliza el *componente cliente de la API* de APS (véase el apartado 6.1.1 "Dispositivos, componentes, aplicaciones e interfaces" de [UIT-T H.810]) puede emitir instrucciones para la aplicación PHG con seguridad durante las interrupciones del servicio, sin necesidad de gestionar la conectividad o autenticidad del homólogo.

NOTA 2 – En la Figura 7-1 se presenta un modelo arquitectónico y no se exige una implementación concreta.

NOTA 3 – La existencia de una APS entre dos componentes no implica que esos componentes puedan intercambiar mensajes en un momento dado. Los mensajes solo se pueden entregar cuando existe conectividad en la capa de transporte.

El recurso de APB que define la APS se basa en el intercambio de credenciales de seguridad a través de una fuente de información de autenticación específica. Cualquier entidad que proporciona la información de autenticación correcta podrá acceder a la APS y continuar con la sesión persistente.

NOTA 4 – Se puede mover una APS de un dispositivo físico a otro siempre que la implementación PHG presente las mismas credenciales. Por consiguiente, las aplicaciones HFS no deberían presuponer que una APS constituye una conexión a una plataforma de hardware PHG concreta; la APS está vinculada con una credencial de seguridad, como un certificado X.509, un testigo OAuth o un testigo SAML.

La creación y el intercambio de mensajes en una APS se desarrollan en tres pasos. Una vez establecida la APS, solo se necesita el último paso para enviar otros mensajes. La secuencia de tres pasos es la siguiente:

– Intercambio de capacidades, véase [UIT-T H.812.3]: En esta fase, la aplicación PHG obtiene información de la aplicación HFS a través del protocolo HTTP. La información determina si la aplicación HFS es compatible con APS-CCC-Services. La información se recoge en el fichero root.xml de la aplicación HFS e incluye el URL que se utilizará para el establecimiento de la APS. Véase el apartado 8-1.

– Establecimiento de la APS: La aplicación PHG crea el recurso de APB en la aplicación HFS a través de una conexión HTTPS segura e indica si quiere establecer una sesión persistente. Durante esta etapa, la aplicación PHG se autentica a sí misma para la aplicación HFS y recibe información del recurso de APB. Al finalizar esta fase, la PHG ha establecido la APS y puede comenzar a intercambiar mensajes con la aplicación HFS o ha concluido el proceso de establecimiento de la APS y, con ello, ha provocado la retirada del recurso de APB. Véase el apartado 8.2.3.

– Intercambio de mensajes con MQTT (véase el apartado 9): En esta etapa, la aplicación PHG establece una conexión de seguridad a nivel de transporte (TLS) y la conecta con el servidor MQTT expuesto por la aplicación HFS. Esta conexión se utiliza para el intercambio ordinario de mensajes. En una APS, la información de gestión está recogida en el recurso de APB, que se manipula mediante operaciones RESTful por HTTPS. El flujo de datos asociado al funcionamiento de la APS se transporta en mensajes que se transmiten por la conexión MQTT. Una vez creada una APS, normalmente no hay actividad de gestión adicional y, por tanto, toda la actividad se realiza a través de MQTT.

7.1 Soporte para múltiples CCC

En el futuro, una aplicación PHG podrá contener varias CCC (o componentes específicos del proveedor) que utilizan la APS. Un ejemplo es una CCC para configuración PHG remota. Estas CCC contarán con manejadores de mensajes que procesarán los mensajes recibidos. Cada mensaje que se envía desde la aplicación de servicios se transmite a uno de estos manejadores de mensajes a través del nombre de tema utilizado en la instrucción MQTT PUBLISH. Es responsabilidad del implementador de la APS garantizar que los mensajes recibidos por la aplicación PHG se transmiten al manejador de mensajes correcto.

NOTA 1 – El despachador no utiliza información contenida en la carga útil MQTT. La carga útil es opaca para el despachador.

En la Figura 7-2 se presenta un ejemplo de la entrega de la carga útil en un mensaje MQTT a dos manejadores de mensajes diferentes: 1) el manejador de mensajes de gestión de la APS, que es compatible con el mensaje ECHO; 2) un futuro manejador de mensajes indeterminado de proveedores o CCC específicas. El componente N-IF recibe el mensaje MQTT y lo remite al despachador. El despachador extrae el encabezamiento MQTT, que contiene el nombre de tema asociado al manejador de mensajes al que se debe entregar la carga útil. El nombre de tema es una cadena que identifica unívocamente la CCC que previsiblemente procesará el mensaje.

NOTA 2 – Esta descripción se ofrece a título ilustrativo y no prohíbe ningún método de implementación concreto.

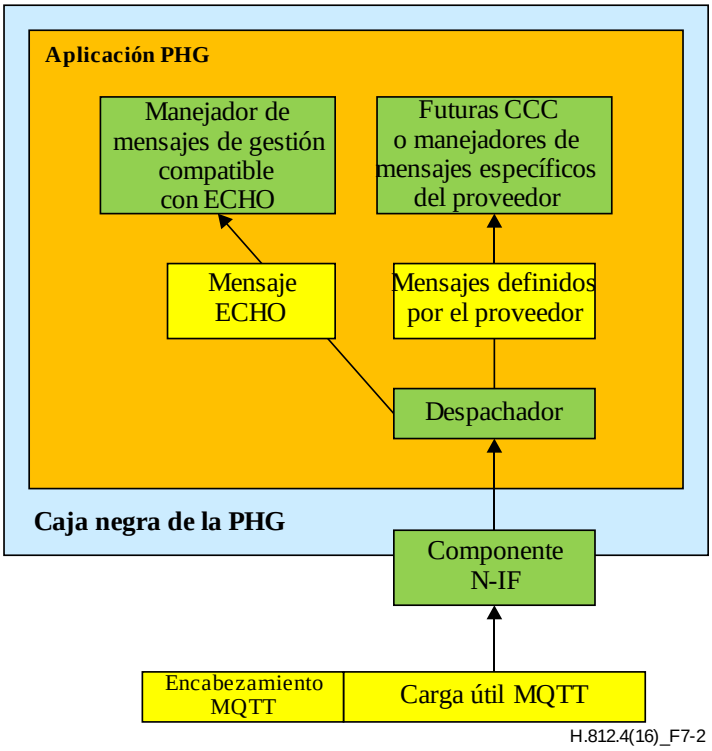

Figura 7-2 – Ejemplo de entrega de la carga útil a diferentes manejadores de mensajes

7.2 Temas utilizados en MQTT

Las entidades conformes con las especificaciones Continua que implementan la CCC APS **deben** admitir el uso del protocolo MQTT para publicar mensajes y suscribirse a ellos. El protocolo MQTT emplea un mecanismo de direccionamiento basado en temas, y esta norma especifica los tres tipos de temas que utilizará una APS y que se muestran en el Cuadro 7-1.

Cuadro 7-1 – Temas utilizados en MQTT

Nombre utilizado en este documento	Formato de la cadena de tema utilizado en MQTT	Descripción
Temas de mensaje	`pcha/message/<HFS APBI>/<PHG APBI>/<mh>`	Temas utilizados para transmitir mensajes a los componentes de cliente de la API de APS en la aplicación PHG.
Tema de estado	`pcha/status/<HFS APBI>/<PHG APBI>`	Tema utilizado para rastrear el estado de la APS
Temas de respuesta	`pcha/response/<HFS APBI>/<PHG APBI>/<mh>`	Tema utilizado para recibir respuestas de la aplicación PHG.

Cada APS se identifica con un par de identificadores APB (APBI) en el recurso de APB correspondiente, y estos APBI **deben** introducirse en las cadenas de tema en lugar de los caracteres <PHG APBI> y <Services APBI>. Se puede obtener información adicional sobre los APBI en el apartado 8.2.2. <mh> **debe** ser sustituido por un identificador especificado por la CCC que está utilizando el mecanismo de intercambio APS. El identificador permite que diferentes homólogos CCC intercambien mensajes en el contexto de una única APS. Un ejemplo de tema de mensaje para una APS tendría el aspecto siguiente:

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

El servidor MQTT **debe** controlar el acceso a estos temas con las reglas siguientes:

– La aplicación HFS **debe** tener acceso de escritura a todos los temas de mensaje que contengan su APBI de servicios.

– La aplicación HFS **debe** tener acceso de lectura a todos los temas de estado y respuesta que contengan su APBI de servicios.

– La aplicación PHG **debe** tener acceso de lectura a todos los temas de mensaje que contengan su APBI de PHG.

– La aplicación PHG **debe** tener acceso de escritura a todos los temas de estado que contengan su APBI de PHG.

– La aplicación PHG **debe** tener acceso de escritura a todos los temas de respuesta que contengan su APBI de PHG.

– Las aplicaciones de gestión debidamente autenticadas PUEDEN tener acceso de lectura a cualquier tema.

– NO se **permitirá** ningún otro acceso.

En general, los requisitos anteriores establecen que la CCC APS solo tendrá acceso a los temas definidos para esa CCC APS. En teoría, existe una relación similar entre la aplicación HFS y el servidor MQTT, pero la interacción real entre ellos depende de la implementación. En muchas implementaciones, la aplicación HFS también es la aplicación de gestión autenticada.

7.3 Interrupción

Si la aplicación HFS debe enviar un mensaje a una aplicación PHG y esta ya no está conectada al servidor MQTT, la aplicación HFS puede utilizar uno de los métodos de interrupción admitidos por la aplicación PHG para anunciarle que hay un mensaje en espera. Al recibir la interrupción, la aplicación PHG se vuelve a conectar con el servidor MQTT y vuelve a poder recibir mensajes de la aplicación HFS. Actualmente, el único método de interrupción definido es la mensajería SMS binaria.

8 Gestión de la APS

Una APS es una asociación a largo plazo entre dos entidades homólogas que se autentican entre sí, una de ellas asociada a la aplicación HFS y la otra a la aplicación PHG. La autenticación se realiza con TLS y OUATH combinados, según se indica en el Anexo B de [UIT-T H.812].

Tras autenticar que la aplicación PHG asigna un recurso, la aplicación HFS invoca la APB, que contiene un conjunto de atributos que definen la APS y constituyen la base de su gestión. Es responsabilidad de la aplicación HFS garantizar que un testigo portador OAUTH dado cumple los requisitos siguientes: 1) se **devolverá** la misma APB para peticiones repetidas del recurso de APS, y 2) si se proporciona un testigo portador OAUTH diferente, se **devolverá** un recurso APS diferente (o un error).

El recurso de APB es un documento XML con un conjunto de elementos, como se indica en el Cuadro 8-1 y el cuadro 8-2. La gestión de los recursos de APB se aborda en este apartado.

La aplicación HFS que implementa la CCC APS utiliza hData para presentar tres elementos del fichero root.xml relacionados con las APS a la aplicación PHG. El primer elemento, *profile*, es una entrada que indica que la aplicación HFS es compatible con la CCC APS. El segundo elemento, *resourceType*, describe el contenido del recurso de APB y contiene una referencia a un esquema XML que se puede utilizar para su validación. El tercer elemento, *section*, es una entrada que indica a la aplicación PHG dónde puede publicar (POST) su contribución al recurso de APB al establecer por primera vez la APS.

El contenido inicial del recurso de APB se define de manera conjunta por las aplicaciones HFS y PHG. La aplicación PHG proporciona un recurso de APB estructurado de conformidad con el esquema XML indicado en el elemento *resourceType* del fichero root.xml. La aplicación PHG facilita los valores de un subconjunto de elementos APB, según se indica en el Cuadro 8-1. Al recibir el recurso de APB de la aplicación PHG, la aplicación HFS cumplimenta los elementos restantes de acuerdo con el Cuadro 8-1.

Durante el establecimiento de una APS, la aplicación HFS asigna un par de identificadores. Estos identificadores forman parte del recurso de APB: uno de ellos está asociado a la aplicación PHG (APBI de PHG) y el otro, a la aplicación HFS (APBI de servicios). El APBI de servicios y el APBI de PHG identifican la instancia de APB y **tienen que** ser unívocos en todas las APS que está gestionando la aplicación HFS.

8.1 Recursos de APB

APS-CCC-Services define una interfaz de gestión que utiliza HTTPS y hData. Estos mecanismos requieren un mecanismo de acceso RESTful seguro a la información por la que se define la APS, contenida en el recurso de APB. El punto de partida de la disposición hData de esta interfaz es el fichero root.xml. En las aplicaciones HFS que implementan APS-CCC-Services, el fichero root.xml **debe** contener las entradas según se especifica en la Figura 8-1, la Figura 8-2 y la Figura 8-3.

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

Figura 8-1 – Elemento profile que indica capacidad

La entrada de la Figura 8-1 indica a la aplicación PHG que la aplicación HFS admite la infraestructura de transferencia de mensajes de APS (APS-CCC-Services). Esta entrada se **debe** mostrar tal y como aparece en la Figura 8-1.

```
<resourceType>
 <resourceTypeID>APB</resourceTypeID>
 <!-- ubicación de referencia que describe la norma APS -->
 <reference>
  http://handle.itu.int/11.1002/3000/hData/APS/2017/01/H.812.4.pdf
 </reference>
 <representation>
 <mediaType>application/xml</mediaType>
 <!-- Esquema para el xml recurso de APB -->
 <validator>
  http://handle.itu.int/11.1002/3000/hData/APS/2017/01/APBConfigResource.xsd
  </validator>
 </representation>
<resourceType>
```

Figura 8-2 – Elemento resourceType que describe el contenido de APB

La entrada de la Figura 8-2 proporciona una descripción y la estructura (por ejemplo, un esquema) de la APB. La entrada se **debe** mostrar tal y como aparece en la Figura 8-2.

```
<section>
 <!-- escogido por la aplicación HFS -->
 <path>path/to/post/folder</path>
 <profileID>APS-CAC-Services</profileID>
 <!-- obligatorio en esta especificación; opcional pero recomendado en hData; --
>
 <resourcePrefix>true</resourcePrefix>
 <resourceTypeID>APB</resourceTypeID>
</section>
```

Figura 8-3 – Elemento section que describe dónde realizar la acción POST

La entrada de la Figura 8-3 identifica un URL en el que la aplicación PHG ejecuta la acción POST inicial durante el establecimiento de la APS. El valor del elemento <profileID> **debe** ser el valor del elemento <id> del elemento <profile> y el valor de <resourceTypeID> **debe** ser APB. El elemento <resourcePrefix> **debe** estar presente en esta especificación y definido en true (es opcional en la especificación hData). El elemento <path> **debe** estar presente pero el valor del URL viene determinado por la aplicación.

En el Cuadro 8-1 y el Cuadro 8-2 se describe el contenido del recurso de APB que caracteriza la APS.

El recurso de APB se expresa como documento xml, como se observa en el ejemplo de la Figura 8-4. El ejemplo de la Figura 8-4 muestra una aplicación PHG que admite MQTT y una interrupción SMS. Se puede consultar el plan del recurso de APB en el Apéndice II.

Cuadro 8-1 – Elementos xml de APB proporcionados por la aplicación PHG

Elemento	Uso
supportedMH	Obligatorio: Una lista separada por espacios que identifica los manejadores de mensajes admitidos por la aplicación PHG. Todas las aplicaciones PHG compatibles con la transferencia de mensajes APS admitirán el manejador de diagnóstico APS en la forma que se indica a continuación. – Los tres caracteres "APS" en mayúsculas La aplicación PHG omitirá este valor siempre que el recurso de APB se obtenga de la aplicación HFS. Nota: Si se utiliza un manejador de mensajes específico de un proveedor, la cadena de identificación debería tener propiedades que minimicen la probabilidad de una colisión con otro manejador de mensajes de proveedor no coordinado.
exchangeMechanism	Obligatorio: Una lista separada por espacios que identifica las tecnologías subyacentes que está utilizando la aplicación PHG para permitir los intercambios de mensajes. La aplicación PHG creará una lista ordenada con todas las tecnologías que admite, y la primera entrada de la lista será su opción preferida. El único mecanismo de intercambio admitido en la actualidad es MQTT. La aplicación PHG omitirá este valor siempre que el recurso de APB se obtenga de la aplicación HFS.
shoulderTapMechanism	Obligatorio: Lista separada por espacios que identifica las tecnologías subyacentes utilizadas por la aplicación PHG para aceptar una interrupción. La interrupción permite que la aplicación HFS restablezca una conexión TCP con la aplicación PHG si se han

Cuadro 8-1 – Elementos xml de APB proporcionados por la aplicación PHG

Elemento	Uso
	eliminado los recursos empleados para mantener esa conexión. La aplicación PHG crea una lista ordenada con todas las tecnologías que admite, y la primera entrada de la lista será su opción preferida. La aplicación HFS seleccionará la primera tecnología de la lista con la que sea compatible. Si la aplicación PHG no admite una interrupción, la lista que proporcionará estará vacía. Actualmente, el SMS es el único mecanismo definido para realizar una interrupción. La aplicación PHG omitirá este valor siempre que el recurso de APB se obtenga de la aplicación HFS.
SMS	Requerido con condiciones: Este elemento estará presente si se selecciona un mecanismo de interrupción del SMS. El elemento SMS contiene la información que utilizará la aplicación HFS para realizar la operación de interrupción. El elemento SMS es el elemento de nivel superior de SMSHeaderDstPort, SMSApplicationId y MSISDN. La aplicación PHG omitirá este valor siempre que el recurso de APB se obtenga de la aplicación HFS.
MSISDN	Nivel inferior de SMS obligatorio: MSISDN es el número SMS utilizado para contactar con la aplicación PHG, es decir, es el "número de teléfono" de la aplicación PHG. Estará formado por dígitos numéricos [0-9], con "+" como prefijo opcional. En total, la cadena contendrá 15 caracteres como máximo. La aplicación PHG omitirá este valor siempre que el recurso de APB se obtenga de la aplicación HFS.
SMSHeaderDstPort	Nivel inferior de SMS obligatorio: SMSHeaderDstPort proporciona el valor que se utilizará como puerto de destino de 16 bits en el encabezamiento de datos de usuario del SMS (valor 0x05 para el identificador del elemento de información UDH). Se puede obtener información adicional en el apartado 9.3.1. La información representada en este elemento tendrá el formato de número decimal. La aplicación PHG omitirá este valor siempre que el recurso de APB se obtenga de la aplicación HFS.
SMSApplicationId	Nivel inferior de SMS opcional: SMSApplicationID debe ser una secuencia de caracteres Unicode. Cuando esté codificada con UTF8, la longitud de esta cadena no debe exceder de 148 octetos. Esta cadena se enviará en la carga útil de una interrupción. El objetivo del elemento es proporcionar un identificador de aplicación en la interrupción, que podrá utilizarse para encaminar el mensaje de interrupción hasta la aplicación PHG adecuada. En las presentes directrices no se define la semántica exacta asociada a la ejecución de este encaminamiento en una plataforma PHG dada. Si la plataforma en la que la aplicación está formando la APS puede contener APS creadas por otras aplicaciones, es posible que sea necesario gestionar el valor de SMSApplicationId. La aplicación PHG omitirá este valor siempre que el recurso de APB se obtenga de la aplicación HFS.
APSState	Se puede consultar la descripción del elemento en el Cuadro 8-2.

Cuadro 8-2 – Elementos xml de APB proporcionados por la aplicación HFS

Elemento	Uso
HFSAPBI	Obligatorio: Identificador del componente HFS del recurso de vinculación persistente autenticada que se ha creado. HFSAPBI se representará como una cadena con una longitud inferior a 2 048 caracteres UTF-8. La cadena no puede contener ninguno de los caracteres siguientes: "/", "#", "+", "*". No se puede utilizar el carácter Unicode NULL. La aplicación HFS omitirá este valor siempre que el recurso de APB se obtenga de la aplicación PHG.
PHGAPBI	Obligatorio: Identificador del componente de la aplicación PHG del recurso de vinculación persistente autenticada que se ha creado. PHGAPBI se representará como una cadena con una longitud inferior a 2 048 caracteres UTF-8. La cadena no puede contener ninguno de los caracteres siguientes: "/", "#", "+", "*". No se puede utilizar el carácter Unicode NULL. La aplicación HFS omitirá este valor siempre que el recurso de APB se obtenga de la aplicación PHG.
APSExchangeURL	Obligatorio: URL que se utilizará al establecer la sesión TLS en la que se intercambiarán los mensajes MQTT. El esquema de URI será mqtts. Es posible que la aplicación PHG necesite cambiar el esquema de URI para que funcione con un cliente MQTT dado. La aplicación HFS omitirá este valor siempre que el recurso de APB se obtenga de la aplicación PHG.
APSState	Obligatorio: Estado de la APS. Si la APS no existe, la aplicación HFS definirá este elemento como NEW en respuesta a una operación POST de la aplicación PHG. Si la aplicación HFS ya cuenta con una APS establecida con la aplicación PHG, determinada mediante autenticación de la credencial de seguridad, este valor se establecerá en ENABLED. La PHG definirá este valor como TERMINATED para cerrar y eliminar la sesión persistente establecida con la aplicación HFS, la cual admitirá una representación XPath válida del elemento APSState de la APS al definir el valor de APSState.
expirationTime	Obligatorio: Tiempo máximo que puede transcurrir después de que la aplicación PHG emita la última operación POST en el recurso de ABP, o desde la última actividad en el canal de mensajes en el que se detectó que la aplicación PHG homóloga estaba activa. Si se supera este límite, la aplicación HFS debería terminar la APS. No obstante, si el recurso de ABP tiene el estado ENABLED, la aplicación HFS intentará emitir el mensaje de gestión ECHO antes de terminar la APS. La aplicación HFS no debería terminar la APS si se recibe una respuesta al mensaje ECHO. (Cabe destacar que la aplicación HFS puede terminar una APS en cualquier momento, aunque no sea un comportamiento adecuado.) Este elemento se expresará como una duración ISO8601; por ejemplo, un plazo de expiración de 12 horas se representa como PT12H.
requiredResponseTime	Obligatorio: Retardo máximo, en segundos, que permite la aplicación HFS para una respuesta al mensaje ECHO. Con la información que le facilita este valor, la aplicación PHG puede determinar la mejor asignación de los recursos de la APS. Una aplicación PHG no debería establecer una APS con una aplicación HFS si, en funcionamiento normal, no puede o no quiere cumplir el requiredResponseTime de un mensaje ECHO. Este elemento se expresará como una duración

Cuadro 8-1 – Elementos xml de APB proporcionados por la aplicación PHG

Elemento	Uso
	ISO8601; por ejemplo, un valor de 10 segundos para requiredResponseTime se representa como PT10S. La aplicación HFS omitirá este valor siempre que el recurso de APB se obtenga de la aplicación PHG.
clientId	Requerido con condiciones: Este elemento estará presente si se selecciona un exchangeMechanism de MQTT. La aplicación PHG utilizará clientId al emitir una MQTT CONNECT. El valor de clientId es generado por la aplicación HFS. La aplicación HFS omitirá este valor siempre que el recurso de APB se obtenga de la aplicación PHG.
PHGCredential	Requerido con condiciones: Este elemento estará presente si se selecciona un exchangeMechanism de MQTT. La aplicación PHG utilizará PHGCredential como contraseña al emitir una operación MQTT CONNECT. La aplicación HFS omitirá este valor siempre que el recurso de APB se obtenga de la aplicación PHG.

```
<?xml version="1.0" encoding="UTF-8"?>
 <aps:APB
xmlns:aps="http://handle.itu.int/11.1002/3000/hData/APS/2017/01/H.812.4.pdf "
     xmlns:xsi = "http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation =
"http://handle.itu.int/11.1002/3000/hData/APS/2017/01/APBConfigResource.xsd ">

 <!-- La PHG cumplimenta estos campos -->
 <supportedMH>APS lampreynetworks.com/private</supportedMH>
 <exchangeMechanism>MQTT privateMessageProtocol</exchangeMechanism>
 <shoulderTapMechanism>SMS</shoulderTapMechanism>
 <SMS>
  <MSISDN>441111223344</MSISDN>
  <SMSHeaderDstPort>1234</SMSHeaderDstPort>
  <SMSApplicationId>4827351</SMSApplicationId>
 </SMS>

 <!-- La aplicación HFS cumplimenta estos campos -->
 <HFSAPBI>HFSAPBI_1</HFSAPBI>
 <PHGAPBI>5468233453aae3fd224</PHGAPBI>
 <APSExchangeURL>mqtts://example.org:1883</APSExchangeURL>

 <!-- Estado definido por la aplicación HFS durante la primera creación -->

 <APSState>NEW</APSState>
 <expirationTime>PT50H</expirationTime> <!-- Tiempo en horas -->
 <requiredResponseTime>PT30S</requiredResponseTime>  <!-- Tiempo en segundos -->
 <clientId>RestPHG</clientId>
 <PHGCredential>PHGCredential55555</PHGCredential>
</aps:APB>
```

Figura 8-4 – Ejemplo de aplicación PHG que admite MQTT y una interrupción SMS

8.2 Comportamiento de la APS

8.2.1 Estado de la sesión APS

Los tres estados posibles para una APS son: NEW, ENABLED o TERMINATED. La aplicación HFS solo **emitirá** mensajes para una aplicación PHG cuando el estado de la APS sea ENABLED. Una APS tiene el estado NEW cuando se crea por primera vez durante el procedimiento de establecimiento de la APS. Una vez que ha aceptado establecer la APS, la aplicación PHG cambia el estado de la APS a ENABLED, que se mantiene hasta que la aplicación PHG o la aplicación HFS terminan la sesión. Se puede consultar información adicional sobre el elemento APSState del recurso de ABP del Cuadro 8-2.

8.2.2 Identificadores de vinculación persistente autentificados (APBI)

Durante el establecimiento de una APS entre una aplicación PHG y una aplicación HFS, esta asigna un par de identificadores a la APS y los mantiene mientras perdura la sesión. Un identificador del par está asociado a la aplicación PHG (APBI de PHG) y el otro, a la aplicación HFS (APBI de servicios). El par de identificadores se utiliza para vincular entre sí los extremos emisor y receptor de la APS. Es responsabilidad de la aplicación HFS gestionar la asignación del APBI de servicios y del APBI de PHG de tal manera que cada APS individual creada por la aplicación HFS pueda identificarse de forma unívoca solo con el par de APBI. Además, la aplicación HFS debe garantizar que este recurso de APB exclusivo se intercambia únicamente con una aplicación PHG que posee la credencial de seguridad utilizada cuando se creó la APS por primera vez. El APBI de PHG debe ser único en todo el conjunto de APS existentes que son mantenidas por la aplicación HFS.

8.2.3 Establecimiento de la vinculación persistente autenticada

El establecimiento de la APB hace referencia al proceso por el que la aplicación PHG y la aplicación HFS intercambian información para habilitar y configurar la APS. Para poder intercambiar mensajes, primero se debe establecer la APB. La PHG inicia el establecimiento de la APS cuando ha completado el intercambio de capacidades con una aplicación HFS y determina que esta aplicación admite la CCC APS.

Para establecer la APB, es necesario que la aplicación PHG se autentique a sí misma ante la aplicación HFS (actuando como servidor de autorización OAUTH) con un método adecuado para que la PHG obtenga un testigo portador OAUTH autorizado. Una conexión TLS autenticada de forma correcta en la que la aplicación PHG posee un testigo portador OAUTH válido sirve como autenticación mutua a efectos de una APS.

Cuando se ha realizado la autenticación mutua, la aplicación HFS cuenta con las credenciales de seguridad obligatorias necesarias para identificar una APS y asociarla con una aplicación PHG dada, en esta transacción y en todas las posteriores. La manera en que la aplicación HFS utiliza el certificado para vincular la APS con una aplicación PHG depende de la implementación.

En este contexto de autenticación mutua, la aplicación PHG establece la APS mediante una operación POST HTTP en la aplicación HFS. El recurso publicado es un documento xml que contiene el recurso de APB, pero la aplicación PHG solamente cumplimenta los elementos especificados en el Cuadro 8-1.

Al disponer de los valores de los elementos, la aplicación HFS tiene la información necesaria para configurar y asignar los recursos internos necesarios para la compatibilidad con la APS. La respuesta a esta operación POST contiene un URL a una versión modificada del recurso de APB que contiene los elementos proporcionados por la aplicación de servicios del Cuadro 8-2. A continuación, la aplicación PHG recupera el recurso de APB mediante una operación HTTP GET al URL facilitado. Si los recursos son limitados, la aplicación HFS puede negarse a establecer una APS.

8.2.4 Aceptación de una vinculación persistente autenticada

La aplicación PHG examina la respuesta de GET. Si los parámetros le parecen aceptables, establece una conexión segura al servidor MQTT y configura el vínculo MQTT ejecutando las acciones de suscripción y publicación necesarias. Tras completar correctamente estos pasos, la aplicación PHG debe indicar que acepta la APS mediante una operación HTTP PUT a la aplicación HFS, utilizando el URL facilitado en la respuesta POST y agregándole APSState (URL/APSState). El valor del elemento APSState identificado por el URL en las operaciones PUT se establecerá en ENABLED. Se puede obtener más información en el apartado I.4. A partir de ahora, la APS está habilitada y la aplicación PHG puede recibir mensajes. La aplicación HFS tan solo actualizará el valor de APSState de su recurso de APB en esta transacción. Si la aplicación PHG proporciona un XPath que hace referencia a un elemento distinto de <APSState>, la aplicación HFS devolverá el error HTTP correspondiente. La aplicación PHG puede realizar operaciones PUT adicionales para, en caso necesario, actualizar el valor de APSState de la APS.

8.2.5 Vinculación persistente autenticada y terminación de sesión

La aplicación PHG puede terminar la APS en cualquier momento estableciendo APSState en TERMINATED (véase el apartado I.5). A continuación, la aplicación PHG debería realizar las operaciones pertinentes para liberar los recursos utilizados en asociación con la APSI, lo que incluye borrar el servidor MQTT (véase el apartado 9.1.1). Cuando la aplicación PHG termina la APS, el APBI deja de ser válido. La aplicación HFS puede terminar la sesión APS si la aplicación PHG no ha renovado la APSI dentro del intervalo expirationTime especificado o a raíz de una decisión de la lógica de la aplicación. La aplicación HFS no elimina la sesión APS debido a la terminación de una conexión de transporte.

La aplicación HFS elimina la información que asocia la APS con la clave de autenticación, de tal manera que, si la aplicación PHG inició otro intercambio de capacidades de APS con la misma credencial de autenticación, la aplicación HFS puede liberar los recursos asociados con una APS terminada. La terminación de una APS es un proceso interruptor que puede provocar el fallo de una instrucción que se está ejecutando en ese momento.

Las APS se pueden terminar conforme a ciertos procedimientos administrativos.

8.2.6 Mensaje de diagnóstico de la CCC APS

La CCC APS proporciona el marco básico que pueden aplicar las CCC orientadas a las aplicaciones para iniciar el intercambio de mensajes desde la aplicación HFS. Es de esperar que las CCC orientadas a las aplicaciones cuenten con operaciones bien definidas y específicas para las necesidades de la aplicación. Estas operaciones quedan fuera del alcance de la CCC APS.

La CCC APS define una estructura de mensaje para apoyar la gestión de la propia CCC APS. Solo se define una instrucción (a saber, la instrucción ECHO) para soportar la CCP APS. Puede que se añadan otras instrucciones en versiones futuras. Todas las entidades que implementan la CCC APS **deben** admitir la instrucción ECHO del mensaje de gestión.

8.2.6.1 Estructura del mensaje de diagnóstico para el intercambio de mensajes de CCC APS

8.2.6.1.1 Carga útil

La facilidad de intercambio de mensajes de la CCC APS (MQTT) admite un formato de mensaje de diagnóstico que define un pequeño conjunto de instrucciones intercambiables entre entidades homólogas de la CCC APS. Estas instrucciones se transportan en la sección de carga útil del mensaje de diagnóstico. Un mensaje de diagnóstico contendrá una única instrucción. El contenido de la carga útil depende de la instrucción. El mensaje de diagnóstico se envía en el orden de los bytes de la red con la disposición que se muestra en el Cuadro 8-3.

Cuadro 8-3 – Campos del mensaje de diagnóstico de la CCC APS

Nombre de campo	Descripción	Tamaño en bits	Valores
Operación Octeto 0	Identifica la operación que se ejecutará. Los dos bits MSB del campo de operación están reservados y deben enviarse como 0 y omitirse en la recepción. Las respuestas a las instrucciones se formarán mediante la ejecución de un OR lógico de la instrucción con 0x40. Por tanto, una instrucción de 0x03 conlleva la devolución de un valor de 0x43 en el campo de operación.	8	0x00 – 0x3F: instrucción 0x40 – 0x7F: respuesta 0x80 – 0xFF: reservado
Manejador Octeto 1-4	El emisor de la instrucción proporcionará un manejador, que será devuelto por el receptor. El manejador es opaco para el receptor de la instrucción. El emisor no reutilizará ningún manejador que esté asociado a una instrucción pendiente.	32	
Estado Octeto 5	El campo de estado formará parte tanto de los mensajes de instrucción como de los mensajes de respuesta. En las instrucciones, el emisor le asignará el valor de 0x00 y el receptor lo omitirá. Si el campo de estado de un mensaje de respuesta no es 0x00, el emisor no debe procesar el resto del mensaje.	8	No se puede garantizar la validez de los campos que siguen al campo de estado cuando el valor de este es distinto de 0x00.
Longitud Octeto 6-7	La longitud de la carga útil se incluirá en todos los mensajes de diagnóstico. El campo de longitud se indica en octetos y representa el número de octetos de la carga útil del mensaje, empezando por el campo de longitud y hasta el último octeto de la carga útil del mensaje.	16	Dado que el campo de carga útil incluye los 21 octetos utilizados para representar el tiempo, el valor mínimo de la longitud es 21.
Carga útil	La carga útil debe comenzar por un subcampo de longitud fija de 21 octetos. El subcampo muestra el valor de tiempo actual que ha comunicado el emisor o el respondedor de la instrucción. La carga útil puede contener octetos adicionales de datos ECHO. El emisor de la instrucción ECHO debe garantizar que el campo de longitud identifica correctamente el número de octetos de datos ECHO. El subcampo de tiempo debe	Depende de la instrucción. Especificado en el campo de longitud.	Cuando un receptor detecta la falta de concordancia entre el número de octetos de los datos del mensaje y la longitud de la carga útil, debe devolver un código de error adecuado.

Cuadro 8-3 – Campos del mensaje de diagnóstico de la CCC APS

Nombre de campo	Descripción	Tamaño en bits	Valores
	codificarse como una cadena de caracteres UTF-8 y formatearse de conformidad con el apartado D.1.5 sobre marcación y sincronización temporales de [UIT-T H.812.1]. Dado que el sello de tiempo se transmite en un campo de longitud fija, la fracción de un componente de segundo es NULL con relleno para cada nivel de precisión no transmitido en la marcación.		

NOTA – En este documento de directrices de diseño, el término "carga útil" puede resultar confuso ya que se utiliza en varios contextos. El mensaje de diagnóstico es en sí mismo la carga útil de un mensaje MQTT. En este caso, la carga útil hace referencia al conjunto de bytes asociados a una instrucción dada. Por ejemplo, la carga útil de un mensaje de diagnóstico de la instrucción ECHO es un sello de tiempo seguido por una cadena arbitraria de bytes que devuelve el destinatario.

8.2.6.1.2 Instrucciones de mensaje de diagnóstico admitidas

Todos los mensajes de diagnóstico definidos en las presentes directrices de diseño cuentan con respuestas asociadas. Para formar una respuesta a una instrucción, la entidad respondedora estructurará los campos de acuerdo con el Cuadro 8-3. A continuación se detallan las instrucciones admitidas:

ECHO

(Valor del campo de operación como 0x01 para la instrucción y como 0x41 para la respuesta)

Con la instrucción ECHO, la aplicación HFS puede determinar si la aplicación PHG es capaz de recibir mensajes de diagnóstico y responder a ellos, así como obtener el concepto de tiempo de la aplicación PHG.

La entidad que envía la instrucción ECHO debe proporcionar una carga útil de manera que sus primeros 21 bytes indiquen el tiempo del emisor como se ha establecido en el Cuadro 8-3. En los bytes restantes, si los hubiere, se podrá definir cualquier valor de interés para el emisor. El campo de longitud está configurado como la longitud de la carga útil ECHO.

El respondedor de la instrucción ECHO fijará el valor 0x81 para el campo de operación.

La respuesta ECHO contendrá el manejador facilitado por la aplicación HFS de la instrucción ECHO correspondiente, el campo de estado, el campo de longitud y la carga útil recibida de la instrucción ECHO tras sustituir el campo de tiempo por el tiempo del respondedor ECHO, con el formato definido para el emisor. La respuesta ECHO se debería enviar con prontitud. El respondedor al mensaje ECHO debe examinar el campo de longitud a fin de determinar si el valor enviado supera el límite definido para la implementación. En caso afirmativo, debe ajustar el código de estado en consecuencia y devolver la hora local y el número máximo de bytes adicionales admitido por la implementación. El campo de longitud de la carga útil debe reflejar el número de bytes de la carga útil devuelta. Si la implementación puede admitir el número de bytes enviados en la instrucción ECHO, devolverá la carga útil enviada. Todas las implementaciones deben ser compatibles con las cargas útiles ECHO que son iguales o menores de 256 bytes.

8.2.6.1.3 Campo de estado

El campo de estado está formado por un bit que indica el tiempo válido y un código de estado. El bit más importante del campo de estado es el bit de tiempo sincronizado, que se definirá de forma que indique que se está transmitiendo el tiempo sincronizado NTP válido, o su equivalente, en el campo de tiempo de la carga útil; en caso contrario, se borrará.

Se han definido los valores de código de estado siguientes para la respuesta ECHO:

– 0x0000 – Completado correctamente; no se ha detectado ningún error al procesar la instrucción.

– 0x0001 – Error desconocido; la instrucción solicitada no se ha completado correctamente. Se puede definir un valor positivo para el campo de longitud. Cuando el campo de longitud es un valor positivo, la carga útil contiene un mensaje de bytes de longitud que puede ofrecer información adicional sobre el error detectado.

– 0x0002 – Instrucción no admitida. La entidad respondedora devolverá este valor siempre que no se admita el valor del campo de operación (byte 0) de un mensaje de diagnóstico recibido.

– 0x0003 – La longitud de la instrucción supera el valor máximo admitido.

– 0x0004 – Error en los valores de campo.

9 Modelo de comportamiento: MQTT

MQTT [OASIS MQTT] es una capacidad requerida para las aplicaciones que admiten la CCC APS. En este apartado se describe la utilización de MQTT como apoyo a la transmisión de mensajes en el contexto de una APS.

9.1 Visión de conjunto del funcionamiento

La aplicación HFS de la APS implementa un servidor MQTT. El nombre de anfitrión o la dirección IP y el número de puerto TCP del servidor se proporcionan en el recurso de APB. El intercambio de mensajes entre la aplicación PHG y la aplicación HFS emplea un servidor MQTT que está asociado a la aplicación HFS, con los temas definidos en el apartado 7.2. En la figura siguiente se presenta una visión general de los intercambios entre la aplicación PHG y la aplicación HFS. Como se muestra en la Figura 9-1, las cadenas de tema dependen del APBI de PHG, el APBI de servicios y los manejadores de mensajes que utilizan las diferentes CCC, como se detalla en el apartado siguiente.

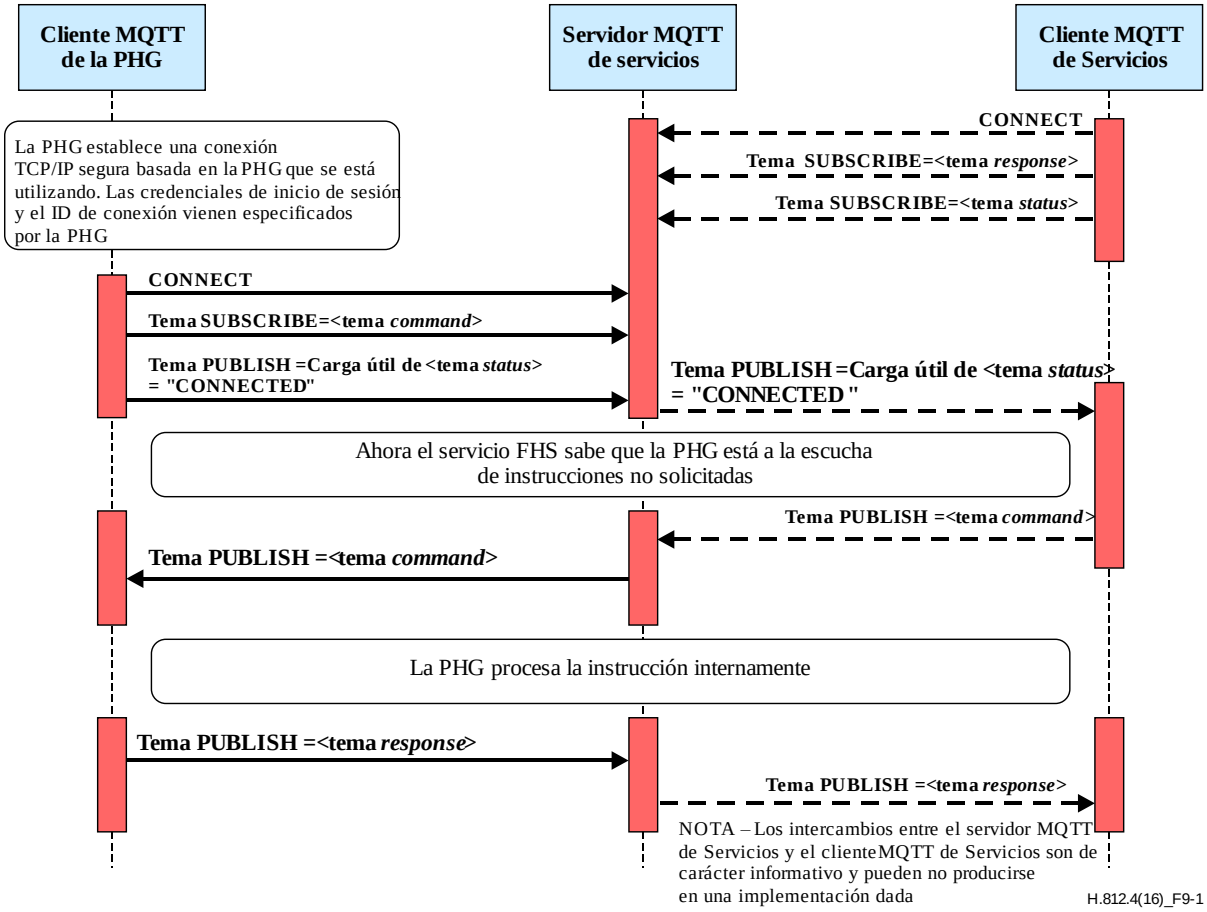

Figura 9-1 – Interacciones del cliente MQTT con la aplicación PHG y la aplicación HFS

En el apartado 8.2, las interacciones se describen desde el punto de vista de la aplicación PHG y la aplicación HFS respectivamente. Es importante señalar que el método de comunicación entre la aplicación HFS y su servidor MQTT depende de la aplicación. Los únicos componentes normativos de la interfaz APS son los intercambios entre la aplicación PHG y la aplicación HFS y los servicios MQTT.

9.1.1 Terminación correcta de la APS

Cuando resulte posible, la aplicación PHG debe terminar la APS de manera correcta.

Para ello, la aplicación deberá seguir los pasos siguientes:

– Establecer una conexión con la aplicación HFS propietaria del recurso de APB que define la APS que se debe terminar.

– Ejecutar una operación PUT de un recurso de APB con el elemento <APSState> en TERMINATED a fin de deshabilitar el uso posterior de la APS por la aplicación HFS.

– Cerrar con la operación CLOSE todas las conexiones activas que utiliza la APS para intercambiar mensajes en MQTT.

– Ejecutar una operación MQTT CONNECT con la bandera de sesión limpia en true (borra las suscripciones de la PHG en el servidor MQTT), el estado de la bandera Will retenida en cleared y sin mensaje ni tema Will (evita que se asignen recursos para enviar un mensaje de estado cuando se pierde la conexión con la aplicación PHG).

– Publicar un mensaje de longitud cero para el tema de estado con la bandera de retención en true para liberar el recurso de estado.

– Desconectar del servidor MQTT.

9.2 Interacción de la aplicación HFS con la aplicación PHG

La aplicación HFS interactúa con la aplicación PHG a través de su componente de servidor MQTT asociado. En estas directrices no se indica la manera exacta en que la aplicación HFS interactúa con su servidor MQTT.

Si determina que se debe enviar un mensaje con la APS, la aplicación HFS envía ese mensaje emitiendo un paquete PUBLISH para el tema de mensaje adecuado. El servidor MQTT utiliza un nivel 2 de calidad de servicio al emitir el paquete PUBLISH.

Si la aplicación HFS debe enviar un mensaje y el tema de estado indica que la aplicación PHG no está conectada, puede intentar recuperar la conexión (si la aplicación PHG admite la interrupción) enviando la interrupción fuera de banda.

Nota informativa: La aplicación HFS puede suscribirse a cualquier tema de interés de respuesta APS. Además, si quiere rastrear el estado en línea/fuera de línea de sus APS, puede suscribirse a temas de estado. Para permanecer a la escucha de las actualizaciones de estado de todas las APS, puede suscribirse a la expresión de tema con comodines siguiente:

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

9.3 Estado de la conexión de la PHG con el servidor HFS MQTT

En la Figura 9-1 se documentan los estados que puede adoptar el tema de estado y los eventos que provocan transiciones entre estados.

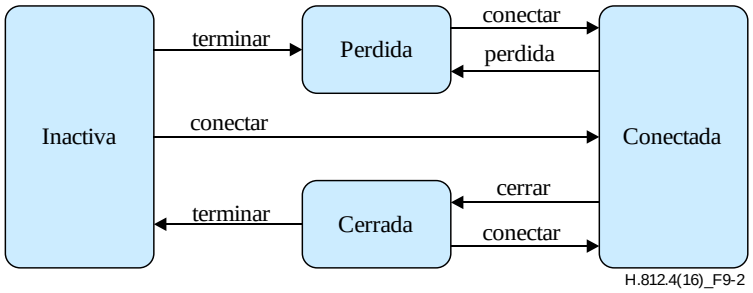

Figura 9-2 – Diagrama de estados para el tema de estado

El Cuadro 9-1 es un cuadro normativo que documenta los estados y las transiciones de estado del tema de estado. La aplicación HFS utiliza el tema de estado para rastrear el estado de la conexión de la aplicación PHG con la APS.

Cuadro 9-1 – Cuadro de estados para el tema estado

Estado	Evento	Siguiente estado	Descripción
INACTIVE	connect	CONNECTED	La aplicación PHG ha establecido una sesión MQTT, para lo cual ha iniciado sesión con un ID de cliente nuevo y una bandera de sesión limpia en false. La aplicación PHG publica un mensaje al tema de estado con el contenido de carga útil CONNECTED.
CONNECTED	lost	LOST	El HFS (MQTT) ha detectado un evento de fin de temporización o desconexión TCP debido a la ausencia de mensajes ping MQTT. El HFS (MQTT) publicará un mensaje Will para el tema de estado con carga útil LOST.

Cuadro 9-1 – Cuadro de estados para el tema estado

Estado	Evento	Siguiente estado	Descripción
CONNECTED	close	CLOSED	La aplicación PHG cierra la conexión MQTT (envía un paquete de control MQTT DISCONNECT) pero no termina la sesión MQTT. La aplicación PHG publica un mensaje al tema de estado con carga útil CLOSED antes de la desconexión.
LOST	connect	CONNECTED	La aplicación PHG ha reconectado con una sesión MQTT, para lo cual ha iniciado sesión con su ID de cliente existente y una bandera de sesión limpia en false. La aplicación PHG publica un mensaje al tema de estado con el contenido de carga útil CONNECTED.
LOST	terminate	INACTIVE	La aplicación PHG ha decidido terminar la APS, para lo cual ha iniciado sesión con su ID de cliente existente y la bandera de sesión limpia en true. Para señalar esta condición, publica un mensaje de longitud cero para el tema de estado. A continuación, cierra la sesión enviando un paquete de control MQTT DISCONNECT.
CLOSED	connect	CONNECTED	La aplicación PHG ha reconectado con una sesión MQTT, para lo cual ha iniciado sesión con su ID de cliente existente y una bandera de sesión limpia en false. La aplicación PHG publica un mensaje al tema de estado con el contenido de carga útil CONNECTED.
CLOSED	terminate	INACTIVE	La aplicación PHG ha decidido terminar la APS, para lo cual ha iniciado sesión con su ID de cliente existente y la bandera de sesión limpia en true. Para señalar esta condición, publica un mensaje de longitud cero para el tema de estado. A continuación, cierra la sesión enviando un paquete de control MQTT DISCONNECT.

9.3.1 Interacción de una aplicación PHG con el servidor MQTT

La aplicación PHG establece la sesión APS mediante la ejecución de HTTP POST en la aplicación HFS en el contexto de una conexión segura que proporciona alguna credencial de seguridad. Tras recibir esta información, la aplicación PHG interactúa con la aplicación HFS creando una conexión TLS con el componente de servidor MQTT asociado a la aplicación HFS.

Una vez establecida una conexión TLS, la aplicación PHG envía un paquete de control MQTT CONNECT al servidor MQTT de esa conexión. La aplicación PHG espera una respuesta del servidor MQTT. Si recibe un paquete de datos que no constituye un acuse de recibo de la conexión MQTT, la aplicación PHG cierra la conexión TCP/IP.

La aplicación PHG define los campos siguientes en su mensaje de conexión MQTT (conexión normal).

Cuadro 9-2 – Información contenida en el mensaje de conexión MQTT de la aplicación PHG

Elemento de información	Valor definido por la PHG	Observaciones
Banderas	0xEC	– Se especifican el nombre de usuario y la contraseña – Mensaje Will retenido requerido (con calidad de servicio 2) – Sesión limpia no requerida
Mantener vigente	Seleccionado por la implementación PHG	Si no se ha producido actividad durante un periodo de tiempo de mantener vigente concreto, la aplicación PHG debe enviar un MQTT PING para mantener abierta la conexión. Puede definir el valor 0 para indicar que no se compromete a enviar mensajes PING.
Identificador de cliente	Cadena facilitada por la aplicación HFS del recurso de APB.	El servidor MQTT utiliza el identificador de cliente para identificar la sesión MQTT. Al operar en el contexto de una APS concreta, la aplicación PHG siempre debe utilizar la cadena especificada por la aplicación HFS en el recurso de APB.
Tema Will	Tema *status* de la PHG	Tema utilizado para rastrear el estado de la conexión
Mensaje Will	La cadena "LOST"	Carga útil del mensaje MQTT que se debe generar (interno de la aplicación HFS) con el que se indica que la PHG ha quedado fuera de línea de manera inesperada.
Nombre de usuario	APBI de la PHG facilitado por la aplicación HFS del recurso de APB.	Utilizado para autorizar el acceso de la aplicación PHG a los temas.
Contraseña	Credencial de PHG facilitada por la aplicación HFS en el recurso de APB.	Utilizada para autenticar la aplicación PHG.

La bandera Will, la bandera Will Retain y el mensaje Will garantizan que se informa a la aplicación HFS cuando se interrumpen de forma imprevista las comunicaciones con la PHG. Se trata de un proceso de notificación interno de la implementación de la aplicación HFS, pero está controlado por estos parámetros. La aplicación PHG debe asignarles los valores especificados más arriba.

El valor MQTT Keep Alive determina la rapidez con la que el servidor MQTT detectará la pérdida de conectividad con la aplicación PHG. También obliga a la aplicación PHG a enviar periódicamente un paquete MQTT PING cuando no se ha registrado otra actividad.

Si ha recibido un acuse de recibo de conexión positivo del servidor MQTT, la aplicación PHG envía peticiones MQTT SUBSCRIBE a sus temas de instrucción. El manejador de mensajes de CCC gestiona estos temas de instrucción como se muestra en el apartado 7-2. La aplicación PHG **debe** realizar una suscripción en representación de todos los manejadores de mensajes que ha anunciado en el recurso de APB. A continuación, define la información de la petición MQTT SUBSCRIBE como se indica en el Cuadro 9-3.

Cuadro 9-3 – Información contenida en el mensaje MQTT SUBSCRIBE

Elemento de información	Valor	Observaciones
Tema	Nombre del tema *command*	Conjunto de temas respecto de los cuales la aplicación PHG quiere recibir mensajes PUBLISH.
Calidad de servicio requerida	2	Esto permite que la aplicación HFS defina el nivel de calidad de servicio sobre la base del valor de la calidad de servicio seleccionada en el paquete de control PUBLISH.

Si ha recibido un acuse de recibo de SUBSCRIBE positivo del servidor MQTT, la aplicación PHG envía un paquete de control PUBLISH para actualizar el tema *status* y mostrar que ha entrado en línea. El estado de publicación se envía con calidad de servicio 2. Los parámetros del mensaje se presentan en el Cuadro 9-4.

Cuadro 9-4 – Información contenida en el mensaje de estado de Publish de la PHG

Elemento de información	Valor	Observaciones
Bandera de retención	True	El servidor MQTT debe retener el mensaje para que los suscriptores tardíos puedan conocer el estado de conexión actual de la aplicación PHG.
Tema	Nombre del tema *status*	Tema que rastrea el estado de conexión de la APS.
Calidad de servicio	2	
Carga útil	La cadena "CONNECTED" o "CLOSED"	Información de estado que se envía a la aplicación HFS para indicar que la aplicación PHG asociada a la APS está en línea. o Información de estado que se envía a la aplicación HFS para indicar que la aplicación PHG se está desconectando del servidor MQTT pero mantiene habilitada la APS.

En esta norma se define un segundo tipo de mensaje de estado de Publish. Este mensaje se utiliza únicamente cuando la aplicación PHG está ejecutando el proceso de terminación de la APS. En este caso, la bandera de retención del mensaje de estado de Publish está en true y la carga útil está vacía. El objetivo de este mensaje es borrar los elementos asociados con la APS en el servidor MQTT.

Cuando la aplicación PHG ha completado la operación SUBSCRIBE, está lista para recibir mensajes de la aplicación HFS.

En este momento, la aplicación PHG habilita la APS mediante una operación HTTP PUT para el URL facilitado por la aplicación HFS durante el establecimiento de la APS. HTTP PUT contiene el recurso de APB con el elemento <APSState> en ENABLED. No se puede recibir ningún mensaje hasta que la aplicación PHG habilita la APS.

Cuando la aplicación PHG ha procesado un mensaje, responde enviando un paquete de control MQTT PUBLISH de acuerdo con el Cuadro 9-5.

Cuadro 9-5 – Información contenida en el mensaje de respuesta MQTT Publish de la aplicación PHG

Elemento de información	Valor	Observaciones
Bandera de retención	False	No es necesario que el mensaje continúe retenido tras su entrega a la aplicación HFS.
Tema	Nombre del tema *response*	Véase el Cuadro 7-1.
Calidad de servicio	2	La respuesta se entregará una sola vez.
Carga útil	Depende de la entidad que utiliza el servicio APS.	La respuesta se enviará a la aplicación HFS.

Si la aplicación PHG detecta que ha perdido su conexión MQTT o la conexión TCP/IP subyacente, puede intentar reconectar de inmediato, según el proceso descrito al inicio de este apartado. Si es capaz de establecer que la desconexión es el resultado de una pérdida total de conectividad de red, debería posponer el intento de reconexión hasta que se haya restaurado la red.

La aplicación PHG puede optar por desconectar la conexión MQTT y mantener la APS. En este caso, la aplicación PHG debería publicar un mensaje de actualización de estado, pero con la carga útil como CLOSED en lugar de CONNECTED, antes de enviar el mensaje MQTT DISCONNECT. En el futuro, podrá reconectar cuando lo desee.

Si la aplicación PHG admite un mecanismo de interrupción, debe intentar reconectar al recibir una interrupción.

Al reconectarse, la aplicación PHG debe estar preparada para manejar los mensajes entrantes de inmediato, ya que algunos de ellos podrían haber permanecido en cola durante la desconexión.

10 Modelo de comportamiento: Capacidad de interrupción SMS

En estas directrices se define una capacidad que facilita el funcionamiento de la APS con redes que eliminan la infraestructura de IP de las conexiones inactivas. Esta capacidad se basa en el servicio SMS que se define en [b-GSM/UMTS] y [TIA-637-C]. En el futuro, a medida que los proveedores de redes celulares desplieguen servicios adicionales, se podrían elaborar versiones nuevas de estas directrices que proporcionen mecanismos diferentes para implementar esta capacidad.

10.1 Visión de conjunto de la interrupción

Cuando no se produce intercambio de datos entre una aplicación HFS y una aplicación PHG, es posible reducir tanto los recursos de red inalámbrica como el consumo de energía de la PHG eliminando la conexión de datos inalámbrica, lo que se traduce en una pérdida de la conectividad IP. También se puede perder una conexión de datos inalámbrica por problemas de cobertura o falta de energía (capacidad de batería disponible) en una PHG. La pérdida de conectividad IP no termina la APS; cuando se restablece la conectividad IP, las entidades de software vinculadas por la APS pueden volver a utilizar la red IP para intercambiar información.

En este apartado se describe la interrupción, un mecanismo fuera de banda que la aplicación HFS puede utilizar para acelerar el restablecimiento de la conectividad IP. Se puede ejecutar el mecanismo siempre con las aplicaciones PHG cuya interfaz celular admite el servicio SMS.

En la Figura 10-1 se presenta una visión de conjunto de alto nivel de la secuencia de eventos que se producen durante una interrupción.

El primer paso del proceso de interrupción es el intercambio de información entre la aplicación PHG y la aplicación HFS. Este intercambio se realiza durante el establecimiento de la APS. En algún momento posterior, se suspende la conexión de red entre las dos aplicaciones, por lo que el mecanismo de intercambio subyacente marca la conexión como perdida. Cuando una actividad de aplicación que utiliza la CCC de la APS necesita que la aplicación HFS envíe un mensaje, la aplicación HFS reconoce que se ha perdido la conectividad IP con la aplicación PHG. En ese momento, transmite un mensaje de interrupción a la aplicación PHG a través de una capacidad fuera de banda, como el SMS, para despertar la PHG. La recepción del mensaje de interrupción indica a la aplicación PHG que la aplicación HFS quiere intercambiar un mensaje con ella. A continuación, la aplicación PHA restablece la conectividad de datos IP y reanuda el intercambio de mensajes con la aplicación HFS en el contexto de la APS.

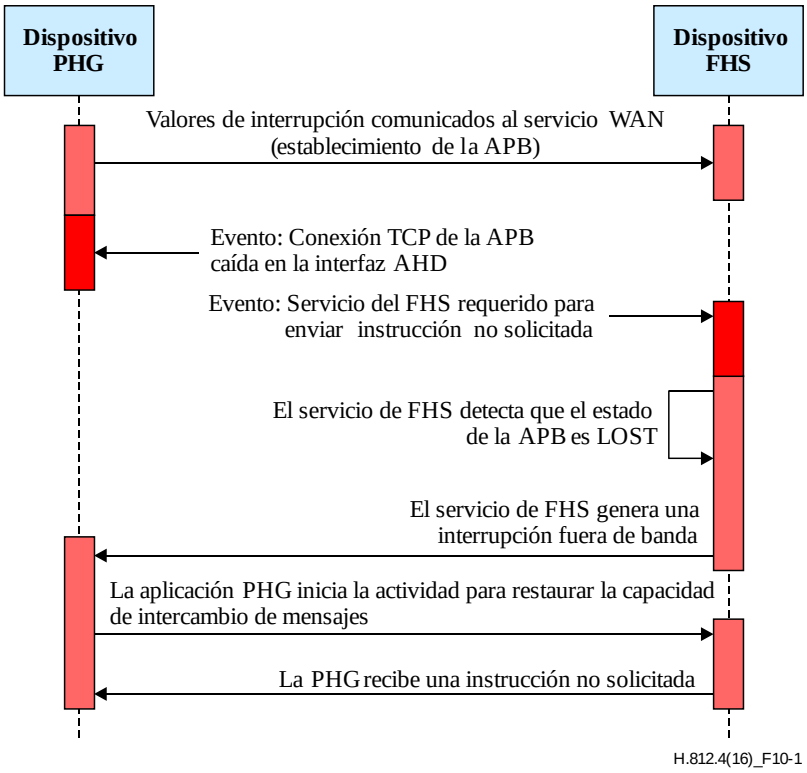

Figura 10-1 – Visión de conjunto de la interrupción

10.2 Alcance

La disponibilidad de un mecanismo de interrupción fuera de banda está condicionada por las capacidades de las redes con las que están asociadas la aplicación PHG y la aplicación HFS, la capacidad de la aplicación HFS para iniciar la interrupción y la capacidad de la aplicación PHG para recibir y procesar la interrupción. Esto implica que todas las entidades, incluidas la aplicación HFS, la red y la aplicación PHG, deben poder operar de conformidad con estas directrices a fin de implementar la funcionalidad de interrupción. Sin embargo, en estas directrices solo se documenta el comportamiento de la interfaz entre la aplicación PHG y la aplicación HFS tal y como se observa en la interfaz de la PHG con la red. Es responsabilidad del integrador de sistemas garantizar que se dispone de la infraestructura de red necesaria para habilitar la aplicación HFS de manera que pueda responder a los requisitos de interfaz definidos en este documento.

10.3 Determinación de la invocación de interrupción

Cabe la posibilidad de que haya una conexión de datos activa disponible actualmente para la aplicación PHG y, por tanto, que no sea necesario que la aplicación HFS invoque una interrupción. Para determinar si es el caso, es preciso examinar el estado de la conexión de la facilidad de

intercambio de mensajes subyacente. Al utilizar MQTT, el estado de la conexión se mantiene en el tema de estado. No se debe ejecutar la interrupción si el tema de estado ya indica que la conexión está operativa (estado CONNECTED).

10.4 Información del SMS de la PHG

Cuando una aplicación PHG utiliza la interrupción SMS, comunica la información siguiente a la aplicación HFS durante el establecimiento de la APS:

– Los tipos de interrupción admitidos, que deben incluir el SMS.

– La dirección (MSISDN) a la que se debe enviar el mensaje SMS.

– El número de puerto utilizado en el encabezamiento de datos de usuario (UDH) del SMS para identificar el punto extremo (puerto) del UDH definido que recibirá el mensaje SMS.

– Un identificador especificado por la aplicación PHG que se devuelve a la PHG en la carga útil del SMS.

La aplicación HFS utiliza la información facilitada por la PHG para generar el mensaje SMS de acuerdo con las indicaciones del presente apartado. Si se utiliza un proveedor de SMS externo para generar o entregar el mensaje SMS a la PHG, se considera que ese proveedor forma parte de la aplicación HFS y el comportamiento correcto en la interfaz PHG viene determinado por la estructura del mensaje SMS entregado a la PHG por el proveedor externo.

10.5 Estructura del mensaje SMS

La aplicación HFS crea un mensaje SMS de acuerdo con el presente apartado y lo envía a la PHG. En los puntos siguientes se describe el mensaje SMS tal y como se entrega a la PHG.

– El mensaje es un mensaje SMS binario.

– El mensaje se entrega al MSISDN facilitado por la aplicación PHG.

– El mensaje SMS contiene un encabezamiento de datos de usuario y el bit indicador del encabezamiento de datos de usuario para el protocolo de la capa de transferencia (TP-UDHI) está definido.

– La disposición de la carga útil del SMS se muestra en la Figura 10-2.

– El valor de SMSHeaderDstPort está codificado en el UDH.

NOTA – La aplicación PHG no utiliza el puerto de origen asociado al elemento de información 0x04 en el UDH.

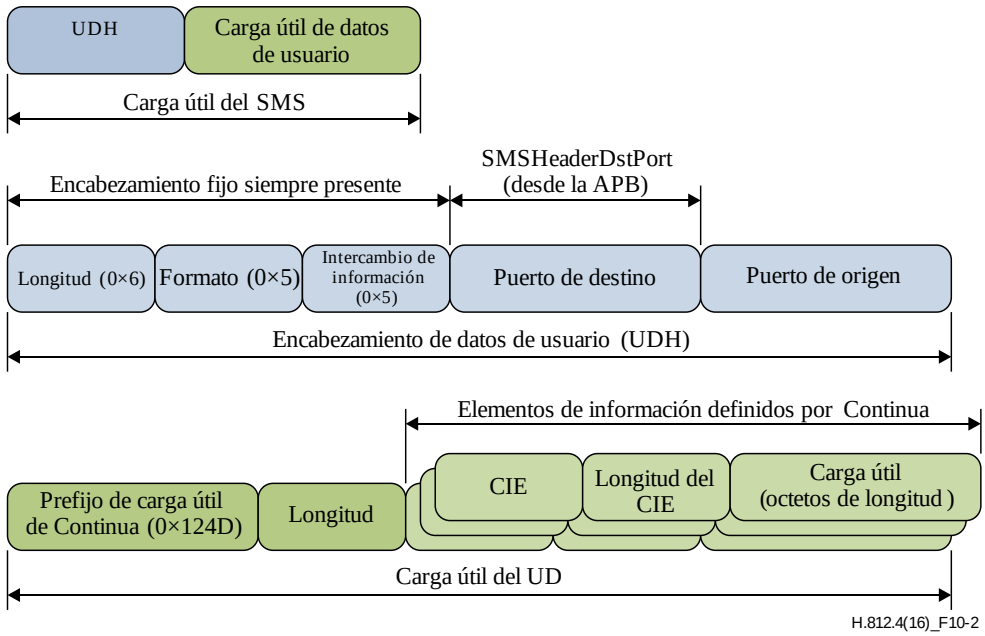

Figura 10-2 – Carga útil del mensaje SMS binario

El UDH tiene una longitud de seis octetos y la información del encabezamiento tiene formato hexadecimal (0x05). El encabezamiento contiene un elemento de información (valor 0x05 – Plan de direccionamiento de puertos de la aplicación, direccionamiento de 16 bits).

La carga útil contiene un valor de prefijo definido por Continua de 0x124D y la secuencia de repetición de los elementos de información de Continua (CIE) de acuerdo con el Cuadro 10-2.

Cuadro 10-1 – Estructura de la carga útil

Campo	Longitud
Prefijo de Continua '0001001001001101'b'0001001001001101'b =0x124D	2 octetos
Longitud de la carga útil de la interrupción, sin los tres primeros octetos	1 octeto
Tipo del elemento de información "A"	1 octeto
Longitud del elemento de información "A"	1 octeto
Valor del elemento de información "A"	0 a "n" octetos
(repetido para los demás elementos de información según sea necesario)	

Cuadro 10-2 – Elementos de información de Continua

Tipo del CIE	Longitud	Requisito	Significado
00	1-148	opcional	Identificador de aplicación de la interrupción: Este valor se comunica a la aplicación HFS a través del elemento de APB <SMSApplicationId>. En el mensaje SMS, está codificado con UTF-8.

Cuadro 10-2 – Elementos de información de Continua

Tipo del CIE	Longitud	Requisito	Significado
01	1	opcional	Semántica de la interrupción: Este valor indica la acción que debería ejecutar la aplicación PHG al recibir la interrupción. Los valores actuales definidos son: 0x01: Restablecer la conectividad en el nivel del transporte – La aplicación HFS quiere enviar un mensaje a la aplicación PHG y está esperando a que se restablezca la conectividad en el nivel del transporte.

10.6 Requisitos de la aplicación PHG

Cuando la aplicación PHG se está ejecutando en una plataforma de SO que procesa el mensaje SMS entrante, la plataforma tendrá que proporcionar a la aplicación PHG una interfaz que permita informar a dicha aplicación de la llegada del mensaje SMS binario. En las presentes directrices no se especifican los mecanismos utilizados para notificar la llegada del mensaje a la aplicación PHG.

10.7 Comportamiento semántico de la aplicación PHG tras recibir la interrupción

Al recibir una interrupción con el motivo "Re-establish connection to message exchange server", la aplicación PHG debe restablecer su conexión TCP con el servidor HFS MQTT y enviar un mensaje CONNECT. Es posible que, para aplicar este procedimiento, sea necesario restablecer la conexión con la red con conmutación de paquetes.

Anexo A

Directrices normativas para la CCC APS

(Este Anexo forma parte integrante de la presente Recomendación.)

Los cuadros del presente anexo enumeran las especificaciones de directrices aplicables a la certificación Continua de una aplicación PHG y de una aplicación HFS que admiten sesiones persistentes autenticadas.

A.1 Directrices para los componentes de la APS del intercambio de capacidades

Las aplicaciones HFS que admiten una sesión persistente autenticada (APS-CCC-Services) **deberán** proporcionar un fichero root.xml de conformidad con el Cuadro A-1. Las aplicaciones PHG que admiten una sesión persistente autenticada (APS-CCC-PHG) también **deberán** ser compatibles con el Cuadro A-1.

Cuadro A-1 – Elementos de la APS para el intercambio de capacidades

Nombre	Descripción	Observaciones
APS-CCC-Services _Root_Support	Para indicar que admite APS-CCC-Services, la aplicación HFS proporcionará un perfil cuyo valor del elemento de identificación figure como APS-CCC-Services en el fichero root.xml	Véase el Cuadro 8-1
APS-CCC-PHG_Root_Support	La aplicación PHG que ejecuta una operación POST en un fichero root.xml para una aplicación HFS durante el intercambio de capacidades proporcionará un perfil cuyo valor del elemento de identificación figure como APS-CCC-PHG en el fichero root.xml.	Véase la Figura 8-1. Nótese que APS-CCC- Services ha sido sustituido por APS-CCC-PHG.
APS-CCC- Services _Description_Information	Para describir el contenido del recurso de APB, una aplicación HFS utilizará una entrada <resourceType> del fichero root.xml de conformidad con la Figura 8-2.	Esta entrada de root.xml describe el contenido del recurso de APB y establece una referencia a un validador para el formateo del recurso de APB.
APS-CCC- Services POST_Location	La aplicación HFS proporcionará el URL en el que la aplicación PHG debe realizar el POST inicial a fin de establecer una APS en una entrada <section> del fichero root.xml de conformidad con la Figura 8-3.	
APS-CCC- Services _Resource_Prefix	El elemento de nivel inferior <resourcePrefix> de la entrada <section> estará presente y el valor se definirá como true.	El prefijo de recurso debe estar presente y ser true en esta especificación, aunque es opcional en la especificación hData.

Cuadro A-1 – Elementos de la APS para el intercambio de capacidades

Nombre	Descripción	Observaciones
APS-CCC- Services _Profile_ID	El valor <profileID> de <section> que se describe en la Figura 8-3 y el valor <id> de <profile> que se describe en la Figura 8-1 estará establecido en APS-CCC.	El valor del elemento profileID de la sección identifica el perfil al que está asociado.

A.2 Directrices de gestión de la APS en la PHG (APS-CCC-PHG)

Las aplicaciones PHG que admiten la clase de capacidad certificada de sesión persistente autenticada **deben** operar de conformidad con el Cuadro A-2.

Cuadro A-2 – PHG de gestión de la APS

Nombre	Descripción	Observaciones
APS-CCC-PHG_Initiate_APS_Establishment	Si la aplicación PHG indica que es compatible con una APS durante el intercambio de capacidades, debe iniciar el establecimiento de la APB mediante una operación POST sobre su recurso de APB.	En las presentes directrices no se define el momento exacto límite para establecer la APS. Sin embargo, los servicios de gestión de la CCC APS se deberían poner a disposición del HFS de manera oportuna.
_APS-CCC-PHG_POST_Location	Al establecer una sesión APS, la aplicación PHG debe ejecutar una operación POST sobre el recurso de APB con destino al URL especificado en el elemento de nivel inferior <path> de <section>, como se define en la Figura 8-3.	La aplicación PHG toma el URL para la acción POST de un elemento <section> del fichero root.xml. Dado que root.xml puede contener muchas secciones, el valor del elemento <profileID> identifica la <section> correcta.
APS-CCC-PHG_APB_POST_XML	Al establecer una sesión APS, la aplicación PHG debe ejecutar una operación POST sobre el recurso de APB como documento xml.	La APS viene descrita en un recurso de APB que se expresa como documento xml.
APS-CCC-PHG_APB_Schema	Al establecer una APS, la aplicación PHG siempre debe transmitir los recursos de APB de conformidad con el plan de recursos de APB del Apéndice II.	
APS-CCC-PHG_APB_FILL	Al establecer una sesión APS, la aplicación PHG debe cumplimentar todos los elementos del recurso de APB de conformidad con el Cuadro 8-1.	
APS-CCC-PHG_Supported_MH_List	Las entradas del elemento <supportedMH> se mostrarán como una lista separada por espacios.	La lista puede contener entradas patentadas.

Cuadro A-2 – PHG de gestión de la APS

Nombre	Descripción	Observaciones
APS-CCC-PHG_APS_MH	Las APS de la aplicación PHG deben contener la cadena "APS" como una de las entradas de lista del elemento supportedMH del recurso de APB.	Esto implica que todas las aplicaciones PHG responderán a los mensajes de gestión definidos por la CCC APS desde la aplicación HFS.
APS-CCC-PHG_Supported_MX_List	Las entradas de <exchangeMechanism> serán una lista separada por espacios, encabezada por el elemento más buscado por la PHG y en orden descendente (del más buscado al menos buscado).	En esta directriz se especifica el formato de la enumeración en el valor de elemento.
APS-CCC-PHG_MQTT_MX	La aplicación PHG especificará "MQTT" en su lista de mecanismos de intercambio admitidos.	Las aplicaciones PHG conformes con Continua que implementan la CCC APS deben ser compatibles con MQTT.
APS-CCC-PHG_Supported_ST_list	Las entradas de <shoulderTapMechanism> serán una lista separada por espacios, encabezada por el elemento más buscado por la PHG y en orden descendente (del más buscado al menos buscado).	En esta directriz se especifica el formato de la enumeración en el valor de elemento.
APS-CCC-PHG_ST_BASE	Si la aplicación PHG no admite un mecanismo de interrupción, la lista que proporcionará para shoulderTapMechanism estará vacía.	
APS-CCC-PHG_ST_SMS	Si la aplicación PHG admite el SMS como mecanismo de interrupción, debe incluir el elemento <SMS> del recurso de APB.	
APS-CCC-PHG_SMS_MSISDN	Si la aplicación PHG admite el SMS como mecanismo de interrupción, debe incluir el número para contactar con la aplicación PHG en el elemento de nivel inferior <MSISDN> que depende del elemento <SMS> del recurso de APB.	
APS-CCC-PHG_SMS_Destination_Port	Si la aplicación PHG admite el SMS como mecanismo de interrupción, debe incluir el puerto asociado con la aplicación PHG en el elemento de nivel inferior <SMSHeaderDstPort> que depende del elemento <SMS> del recurso de APB.	No es necesario especificar el puerto de origen y el número de origen en la APB ya que la aplicación PHG nunca envía mensajes SMS a la aplicación HFS.

Cuadro A-2 – PHG de gestión de la APS

Nombre	Descripción	Observaciones
APS-CCC-PHG_SMS_APP_ID	Si la aplicación PHG admite el SMS como mecanismo de interrupción, debe incluir el elemento de nivel inferior <SMSApplicationId> que depende del elemento <SMS> del recurso de APB.	Este mensaje contiene un identificador que puede utilizar la aplicación PHG para determinar si el mensaje SMS recibido está destinado a la propia aplicación PHG.
APS-CCC-PHG_SMS_APP_ID_Limit	La aplicación PHG no proporcionará ninguna cadena de <SMSApplicationId> que supere los 148 octetos en UTF-8.	
APS-CCC-PHG_SMS_APB_GET	Para obtener el recurso de APB completado, la aplicación PHG tendrá que invocar HTTP GET con el URL facilitado por la aplicación HFS en respuesta a una petición POST correcta de la aplicación PHG.	La aplicación PHG obtiene un URL en la devolución de POST. Este URL identifica la ubicación del recurso de APB que puede obtener la aplicación PHG mediante HTTP GET.
APS-CCC-PHG_Ignore_XML	La aplicación PHG ignorará todos los elementos XML que no entienda en el APB.	Admite la migración a versiones futuras de la APB.
APS-CCC-PHG_Process_HFS_Elements	Al recibir un recurso de APB de la aplicación HFS, la aplicación PHG solo debe procesar los elementos definidos en el Cuadro 8-2.	La aplicación PHG se ha configurado para proporcionar valores para elementos concretos de la APB. Si la aplicación HFS actualiza los valores de esos elementos de manera incorrecta, la PHG los omitirá.
APS-CCC-PHG_APS_ENABLE	La aplicación PHG invocará HTTP PUT del recurso de APB/APSState con el valor en ENABLED para indicar que está preparada para aceptar mensajes.	
APS-CCC-PHG_APS_Termination	La aplicación PHG indicará que se ha terminado la APS invocando HTTP PUT en el recurso de APB actual, con el valor del elemento <APSState> en TERMINATED.	Esta acción es el primer paso del proceso de terminación de la APS.
APS-CCC-PHG_immutable	Salvo el elemento <APSState>, no se modificará ningún recurso de APB obtenido de la aplicación HFS.	La PHG no puede modificar los campos del recurso de APB y los comunica de vuelta a la aplicación HFS.

A.3 Directrices de interacción de una aplicación PHG con el servidor MQTT

En el Cuadro A-3 se presenta la interacción de la aplicación PHG respecto de los intercambios MQTT. Las aplicaciones PHG que implementan APS-CCC-PHG funcionarán de conformidad con el Cuadro A-3.

Cuadro A-3 – Intercambios PHG-MQTT

Nombre	Descripción	Observaciones
APS-CCC-PHG_Message_Exchange	La aplicación PHG admitirá el uso de MQTT como método de intercambio de mensajes.	Es posible que las versiones futuras de estas directrices permitan otros métodos de intercambio de mensajes.
APS-CCC-PHG_MQTT_conformance	La aplicación PHG será conforme con el requisito de cliente que se especifica en MQTT.	
APS-CCC-PHG_MQTT_Connect_URL	El cliente MQTT de una aplicación PHG utilizará la información identificada en el elemento <APS_ExchangeURL> del recurso de APB para establecer la conexión de transporte con el servidor MQTT.	La aplicación HFS especifica en el valor del elemento <APS_ExchangeURL> el URL que permite que la aplicación PHG conecte con el servidor MQTT. Véase el Cuadro 8-2.
APS-CCC-PHG_MQTT APS_Connect_Setup	El componente de cliente MQTT de la aplicación PHG emitirá el paquete de control MQTT CONNECT de conformidad con el Cuadro 9-2.	La APS exige que se utilicen parámetros de MQTT específicos en un paquete de control CONNECT.
APS-CCC-PHG_MQTT Connect_User _Name	La aplicación PHG utilizará el valor del elemento <PHGAPBI> facilitado por la aplicación HFS en el recurso de APB como nombre de usuario en el mensaje de conexión MQTT.	Véase el Cuadro 8-2
APS-CCC-PHG_MQTT_Connect _Password	La aplicación PHG utilizará el valor del elemento <PHGCredential> facilitado por la aplicación HFS en el recurso de APB como contraseña en el mensaje de conexión MQTT.	Véase el Cuadro 8-2
APS-CCC-PHG_MQTT_Client_Identifier	La aplicación PHG utilizará el valor del elemento <clientId> facilitado por la aplicación HFS en el recurso de APB como identificador de cliente en el mensaje de conexión MQTT.	Véase el Cuadro 8-2

Cuadro A-3 – Intercambios PHG-MQTT

Nombre	Descripción	Observaciones
APS-CCC-PHG_MQTT_Connect_Will_Topic	La aplicación PHG debe establecer el tema Will del mensaje de conexión en el tema de estado de esta APS, conforme al Cuadro 7-1.	La configuración indica al servidor MQTT que debe publicar el mensaje Will en el tema de estado cuando se pierda la conexión con la aplicación PHG.
APS-CCC-PHG_MQTT APS_Connect_Will_Message	La aplicación PHG definirá el mensaje Will del mensaje de conexión como "LOST".	Si se pierde la conexión con la aplicación PHG, se enviará un mensaje LOST a la aplicación HFS.
APS-CCC-PHG_MQTT_Normal_Connect_Flags	La aplicación PHG definirá el campo de banderas del paquete de control de conexión de manera que indique que el nombre de usuario y la contraseña están presentes, que NO se solicita una sesión limpia y que se solicita un mensaje Will retenido.	La conexión MQTT requerirá un inicio de sesión con nombre de usuario y contraseña y un mensaje Will retenido, sin sesión limpia. Esto indica que los mensajes de la aplicación PHG no se recibirán hasta que se haya completado la conexión y la aplicación PHG haya completado su suscripción al tema de instrucción.
APS-CCC-PHG_PHG_Command_Subscribe	La aplicación PHG se suscribirá a los temas de mensaje conforme al Cuadro 7-1.	
APS-CCC-PHG_Subscribe_QoS	La aplicación PHG establecerá el valor 2 para la calidad de servicio de las peticiones de suscripción al tema de mensaje de conformidad con el Cuadro 9-3.	
APS-CCC-PHG_PHG Subscribe_All_Supported_mh	La aplicación PHG se suscribirá a todos los temas de mensaje de los manejadores de mensajes que ha especificado como admitidos en el valor de su elemento <supportedMH>.	Dado que la aplicación PHG no sabe qué CCC están admitidas por la aplicación HFS, debe suscribirse a todas ellas.
APS-CCC-PHG_Publish_Status_Topic	Una aplicación PHG publicará el tema de estado de esta APS de acuerdo con el Cuadro 7-1.	
APS-CCC-PHG_Status Publish_Retain	Al grabar los valores en el tema de estado, la aplicación PHG emitirá un paquete de control PUBLISH de conformidad con el Cuadro 9-4.	Si la PHG está reteniendo la APS en estado ENABLED, la publicación se ejecuta con la bandera de retención en true.

Cuadro A-3 – Intercambios PHG-MQTT

Nombre	Descripción	Observaciones
APS-CCC-PHG_Clear_Queue	Al definir la carga útil en un mensaje de longitud cero, la aplicación PHG establecerá el paquete de control PUBLISH en true.	Si la PHG está terminando la APS, la publicación se ejecuta con la bandera de retención en true ya que su objetivo es eliminar los mensajes de estado pendientes. Véase el apartado 9.1.1.
APS-CCC-PHG_Status_Publish_QoS	La aplicación PHG establecerá en 2 el nivel de calidad de servicio del paquete de control PUBLISH que corresponde al mensaje de tema de estado.	La calidad de servicio 2 se aplica a todos los paquetes de control PUBLISH.
APS-CCC-PHG_Status_Publish_Payload_Values	La aplicación PHG establecerá que el valor de la carga útil del paquete de control PUBLISH correspondiente al tema de estado sea "CONNECTED", "CLOSED" o de longitud cero.	En las presentes directrices, la carga útil del mensaje de estado publicada por la aplicación PHG puede adoptar uno de los valores siguientes: "CONNECTED", "CLOSED" o longitud cero; este último solo se utiliza cuando se limpia el MQTT después de que la aplicación PHG haya terminado la APS.
APS-CCC-PHG_Response_Publish_Topic	La aplicación PHG ejecutará una operación PUBLISH en el tema de respuesta de conformidad con el Cuadro 9-4.	El tema de respuesta está especificado en el Cuadro 7-1. Se deben sustituir los elementos que proceda.
APS-CCC-PHG_Response_Publish_Retain	Al publicar un tema de respuesta, la aplicación PHG establecerá la bandera de retención en false.	No es necesario que el mensaje esté retenido ya que se ha entregado a la aplicación HFS. El servidor MQTT es interno a la aplicación HFS.
APS-CCC-PHG_Response_Publish_QoS	La aplicación PHG definirá en 2 el nivel de calidad de servicio del paquete de control PUBLISH que corresponde al mensaje de tema de respuesta.	La calidad de servicio 2 se aplica a todos los paquetes de control PUBLISH.
APS-CCC-PHG_ECHO_Support	La aplicación PHG admitirá la instrucción ECHO del mensaje de diagnóstico de APS-CCC-HFS como se describe en el apartado 8.2.6.	

Cuadro A-3 – Intercambios PHG-MQTT

Nombre	Descripción	Observaciones
APS-CCC-PHG_Status_Behaviour	La aplicación PHG gestionará el tema de estado de conformidad con el Cuadro 9-5.	
APS-CCC-PHG_Status_Publish_Clear_MQTT	La aplicación PHG establecerá el tema de estado en INACTIVE cuando establezca correctamente una conexión con el servidor MQTT, siempre y cuando haya definido tanto la bandera de sesión limpia como la bandera de retención en true y la carga útil tenga una longitud cero.	En esta directriz se define la acción de publicación de la PHG tras conectar con el servidor MQTT para borrarle sus recursos. La actualización de estado forma parte de una secuencia de eventos que se producen cuando la PHG ha terminado la APS.
APS-CCC-PHG_Graceful_APS_Termination_Procedure	La aplicación PHG terminará una APS de acuerdo con el procedimiento descrito en el apartado 9.1.1.	Con esta directriz se pretende verificar que el procedimiento de terminación correcta de la APS sigue todos los pasos del apartado 9.1.1 de manera ordenada: terminar la APS en la conexión de gestión de la APS, cambiar el servidor MQTT al estado LOST o CLOSED si no lo tiene ya, conectar mediante la configuración de conexión limpia, publicar mediante la configuración de estado limpio y cerrar la conexión MQTT.

A.4 Directrices de gestión de la APS en la aplicación HFS

La aplicación HFS configura varios elementos del recurso de APB para la APS. También es responsable de garantizar que una APS concreta se asocia a una credencial de seguridad dada que identifica la PHG autenticada para utilizar la APS. Al implementar APS-CCC-HFS, la aplicación HFS funcionará de conformidad con el Cuadro A-4.

Cuadro A-4 – Requisitos de gestión de la APS para la aplicación HFS

Nombre	Descripción	Observaciones
APS-CCC-Services_Enforce_Authorized_APB_Access	La aplicación HFS garantizará que sólo pueden acceder al recurso de APB creado para representar una APS específica aquellas entidades que posean la credencial de seguridad utilizada para establecer la APS.	De acuerdo con esta directriz, la aplicación HFS debe garantizar que cualquier reconexión ejecutada por la aplicación PHG para la gestión de la APS solo puede operar dentro de la APS autorizada para la aplicación PHG.
APS-CCC-Services_Enforce_Topic_Space_Access	La aplicación HFS aplicará el control de acceso al espacio de tema conforme al apartado 7.2.	
APS-CCC-Services_XPath	La aplicación HFS admitirá una referencia al elemento <APSState> definido en APB cuando la referencia está expresada de conformidad con [XPath 2.0].	
APS-CCC-Services_MQTT_Support	La aplicación HFS admitirá el uso de MQTT como mecanismo de intercambio de mensajes de APS.	La manera en que la aplicación HFS interactúa con el servidor MQTT depende de la implementación, pero la interfaz expuesta a la aplicación PHG viene definida por la norma de MQTT.
APS-CCC-Services_APS_Management_Support	La aplicación HFS compatible con la CCC APS admitirá los mensajes de gestión de la APS definidos en el apartado 8.2.6.1.1.	
APS-CCC-Services_APB_POST_RESPONSE_APB_CREATED	Si la aplicación HFS crea una APS con la aplicación PHG, establecerá el código de retorno en 201.	
APS-CCC-Services_APB_POST_RESPONSE_APB_NOT_CREATED	Si la aplicación HFS no crea ni actualiza una APB tras recibir una petición de cliente para hacerlo, devolverá un código de estado adecuado del grupo 400 ó 500.	
APS-CCC-Services_Process_Services_Elements	Al recibir un recurso de APB de la aplicación PHG, la aplicación HFS solo procesará los elementos definidos en el Cuadro 8-1.	
APS-CCC-Services_Ignore_XML	La aplicación HFS ignorará todos los elementos XML que no entienda en el APB.	Admite la migración a versiones futuras de la APB.

Cuadro A-4 – Requisitos de gestión de la APS para la aplicación HFS

Nombre	Descripción	Observaciones
APS-CCC-Services_No_Modify	La aplicación HFS no modificará ningún elemento del Cuadro 8-1 al presentar o procesar los elementos de la APB.	
APS-CCC-Services_APB_Schema	Al establecer una sesión APS, la aplicación HFS siempre debe transmitir los recursos de APB de conformidad con el plan de recursos de APB del Apéndice II.	
APS-CCC-Services_Unique_PHGAPBI	La aplicación HFS creará un valor para el elemento <PHGAPBI> que sea único para todas las APS conocidas válidas para la aplicación HFS.	En todo momento, si la aplicación HFS tiene N APS, el valor <PHGAPBI> de cada uno de los N recursos asociados debe ser único. Este requisito no excluye la posibilidad de reutilizar un valor de una APS terminada.
APS-CCC-Services_PHGAPBI_Constraints	La aplicación HFS restringirá el valor del elemento <PHGAPBI> de acuerdo con la entrada PHGAPBI del Cuadro 8-2.	
APS-CCC-Services_HFSAPBI_Constraints	La aplicación HFS restringirá el valor del elemento <HFSAPBI> de acuerdo con la entrada HFSAPBI del Cuadro 8-2.	
APS-CCC-Services_Unique_ClientId	La aplicación HFS creará un valor <clientId> que sea único para todas las APS que están en servicio actualmente.	Cabe recordar que este valor se utiliza como identificador de cliente MQTT PHG.
APS-CCC-Services_ClientId_Constraints	La aplicación HFS restringirá el valor de <clientId> de acuerdo con la entrada clientId del Cuadro 8-2.	La especificación MQTT actual limita la longitud de la cadena a 23 caracteres UTF-8.
APS-CCC-Services_NEW_APSState	La aplicación HFS establecerá el valor de <APSState> en NEW si la aplicación PHG ejecuta una operación HTTP POST y no existe ninguna APS para la credencial de seguridad indicada.	Cuando la aplicación HFS gestiona una operación POST procedente de la aplicación PHG y no existe ninguna APS para esa credencial de seguridad, tiene que completar el recurso de APB objeto de la acción POST de la PHG y establecer el estado en NEW.

Cuadro A-4 – Requisitos de gestión de la APS para la aplicación HFS

Nombre	Descripción	Observaciones
APS-CCC-Services_ExpirationTime	La aplicación HFS proporcionará un plazo de expiración en el valor del elemento <expirationTime>, que representa el periodo durante el cual la aplicación HFS permitirá la inactividad.	Este valor representa el periodo de tiempo durante el cual la aplicación HFS no aceptará actividad de la aplicación PHG en la APS antes de comprobar si la aplicación PHG continúa implicada. Una vez vencido ese plazo, si la aplicación HFS no recibe una respuesta oportuna a un mensaje "ECHO" de la APS tras la activación de la interrupción de una interrupción O si la aplicación PHG no responde a la activación de la interrupción, la aplicación HFS puede terminar la APS.
APS-CCC-Services_ResponseTime	La aplicación HFS indicará un tiempo de respuesta obligatorio a un mensaje de gestión "ECHO" de la APS en el valor del elemento <requiredResponseTime>, que representa el periodo temporal durante el cual puede esperar una respuesta a ECHO.	Este valor representa el periodo de tiempo del que dispone una aplicación PHG para responder a un mensaje "ECHO" UC hasta que la aplicación HFS considera que la aplicación PHG está fuera de servicio y, por tanto, puede terminar la APS.
APS-SUPPORT-TERMINATE	La aplicación HFS admitirá la terminación de una APS conforme al apartado 8.2.5.	
APS-CCC-Services_ MQTT_URL	La aplicación HFS especificará en el valor del elemento <APSExchangeURL> el URL al punto extremo MQTT del HFS.	

Cuadro A-4 – Requisitos de gestión de la APS para la aplicación HFS

Nombre	Descripción	Observaciones
APS-CCC-Services_APB_EXISTS	Si la aplicación PHG invoca HTTP POST y ya existe una APS para la credencial de seguridad, la aplicación HFS omitirá el contenido de POST y devolverá el URL a la APB existente.	La aplicación PHG que ejecuta POST para recuperar una APB utilizando una credencial de seguridad asociada a una APB existente obtendrá el recurso de APB que ya existe. En este caso, el valor del elemento APSState se establecerá en ENABLED. Es recomendable comprobar el estado de APSState para garantizar que se devuelve el valor esperado. Conviene destacar que, cuando ya existe una APB en el dispositivo HFS, omitirá toda la información de APB POST definida por la PHG. Por tanto, cuando la PHG recibe una APB con APSState en ENABLED, debería comprobar que toda la información de la APB relativa a la PHG continúa siendo correcta. Si la información relativa a la PHG ya no es correcta, la PHG tendrá que terminar la APB existente y, posteriormente, crear una APB nueva con información actualizada.
APS-CCC-Services_APB_URL	La aplicación HFS responderá a una operación HTTP POST que haya creado correctamente un recurso de APB con un URL que apunte al recurso de APB.	
APS-CCC-Services_Provide_APB	La aplicación HFS proporcionará el recurso de APB completado cuando la aplicación PHG realice una operación GET con POST URL. POST URL es el URL devuelto por la aplicación HFS en respuesta a la operación POST de las aplicaciones PHG.	Cuando la aplicación PHG ejecuta HTTP GET para el recurso de APB, la aplicación HFS entrega el recurso de APB autenticado para la aplicación PHG.
APS-CCC-Services_NO_APB_GET	Si la PHG ejecuta HTTP GET para el recurso de APB pero la aplicación HFS no encuentra ningún recurso de APB autorizado para su uso por esta aplicación PHG, la aplicación HFS responderá con el código 404, que indica que no se ha encontrado el recurso.	Esto podría suceder, por ejemplo, si una PHG fiable no ha ejecutado una operación POST pero sigue teniendo el URL correcto para apuntar al recurso.

Cuadro A-4 – Requisitos de gestión de la APS para la aplicación HFS

Nombre	Descripción	Observaciones
APS-CCC-Services_APSState_Update	La aplicación HFS actualizará el valor del elemento <APSState> del recurso de APB con el valor del elemento <APSState> enviado por la aplicación PHG en una transacción HTTP PUT si el valor es ENABLED o en TERMINATED; en caso contrario, devolverá el código de estado 403.	
APS-CCC-Services_APSState_Only	La aplicación HFS omitirá todos los valores del recurso de APB, a excepción del valor del elemento <APSState> enviado por la aplicación PHG en una transacción HTTP PUT.	
APS-CCC-Services_NO_APB_PUT	Si la aplicación PHG ejecuta HTTP PUT de un recurso de APB pero la aplicación HFS no encuentra ningún recurso de APB autenticado para su uso por la aplicación PHG, la aplicación HFS responderá con el código 404, que indica que no se ha encontrado el recurso.	
APS-CCC-Services_WAIT_FOR_ENABLE	La aplicación HFS se abstendrá de enviar mensajes a una aplicación PHG hasta que <APSState> esté definido en ENABLED	Aunque, técnicamente, la aplicación PHG puede recibir mensajes en cuanto se ha conectado y suscrito al tema del mensaje, no se envía ningún mensaje hasta que el estado de la APS está establecido en ENABLED. Solo la aplicación PHG puede definir el estado. La aplicación PHG no establece el estado en ENABLED hasta estar preparada para manejar los mensajes.
APS-CCC-Services_APB_Remove_On_Terminate	La aplicación HFS terminará la APS asociada a la APB cuando la PHG establezca <APSState> en TERMINATED. La aplicación HFS se asegurará de que fallen las conexiones MQTT basadas en el recurso de APB.	
APS-CCC-Services_ExpirationTime	En lo que respecta a un tiempo de inactividad mayor a <expirationTime>, la aplicación HFS operará de conformidad con el Cuadro 8-2.	Véase <expirationTime> en el Cuadro 8-2.

A.5 Directrices para la interrupción SMS de la aplicación PHG

Las aplicaciones PHG que implementan APS-CCC-PHG **deben** funcionar de conformidad con el Cuadro A-5.

Cuadro A-5 – PHG con interrupción SMS

Nombre	Descripción	Observaciones
APS-CCC-PHG_ST_Missing_ID	Si la aplicación PHG admite la interrupción mediante SMS y proporciona un valor de SMSApplicationId, omitirá todos los mensajes que no contengan el identificador de aplicación definido por ella misma en el recurso de APB.	El identificador es un número creado por la aplicación PHG para identificar que el mensaje SMS está destinado a la propia aplicación PHG.
APS-CCC-PHG_ST_Reestablish	Si la aplicación PHG admite la interrupción mediante SMS, intentará restablecer la conectividad TCP con la aplicación HFS cuando se reciba un mensaje SMS que contenga el CEI de 01 (Restablecer la conectividad en el nivel del transporte).	En la presente directriz se asume que el mensaje está dirigido a la dirección y el puerto especificados en el recurso de APB.

A.6 Directrices para la interrupción SMS de la aplicación HFS

Las aplicaciones HFS que implementan APS-CCC-Services funcionarán de conformidad con el Cuadro A-6.

Cuadro A-6 – Aplicación HFS con interrupción SMS

Nombre	Descripción	Observaciones
APS-CCC- Services _ST_Send_Contents	Si la aplicación HFS admite la interrupción mediante SMS, al generar el mensaje de interrupción **debe**: a) utilizar los elementos MSISDN y SMSHeaderDstPort en el recurso de APB, y b) incluir la carga útil de la interrupción.	
APS-CCC- Services _ST_Format	La aplicación HFS **debe** formatear la carga útil de la interrupción conforme al apartado 10-5.	En esta directriz se abordan diferentes cuestiones, como la presencia del encabezamiento de Continua y los mensajes TLV.
APS-CCC- Services _ST_Include_APP_ID	La aplicación HFS **debe** incluir el valor del elemento <SMSApplicationId> del recurso de APB en la carga útil del SMS de conformidad con el apartado 10.5.	Este valor permite que la aplicación PHG determine que el mensaje SMS está destinado a la propia aplicación PHG.

Anexo B

Esquema XML para el recurso de APB

(Este Anexo forma parte integrante de la presente Recomendación.)

La aplicación PHG que ejecuta la operación GET de la APB visualiza la estructura XML siguiente.

```
<?xml version="1.0" encoding="UTF-8"?>
<schema xmlns="http://www.w3.org/2001/XMLSchema"

targetNamespace="http://handle.itu.int/11.1002/3000/hData/APS/2017/01/H.812.4.pdf"
    xmlns:tns="http://handle.itu.int/11.1002/3000/hData/APS/2017/01/H.812.4.pdf"
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:HFSServerFields" 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="HFSServerFields">
 <sequence>
  <element name="HFSAPBI" 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>
```

Apéndice I

Información detallada de la APS

(Este Apéndice no forma parte integrante de la presente Recomendación.)

I.1 Información de la APS en root.xml

Para obtener la información sobre las capacidades admitidas por una aplicación HFS, la PHG examina la disposición del recurso definida en hData de la aplicación HFS. Esta información se obtiene con el fichero root.xml facilitado por la aplicación HFS por medio de la facilidad de intercambio de capacidades documentada en [UIT-T H.812.3].

El fichero root.xml de la aplicación HFS que admite la APS contiene tres entradas relacionadas con la APS. La primera de ellas indica a la aplicación PHG que se admite la capacidad de APS. Esta entrada se incluye en un elemento profile y tiene el aspecto que se muestra en la Figura 8-1.

La segunda entrada proporciona tanto una referencia al descriptor APB (por ejemplo, un esquema xml) como un validador (por ejemplo, un esquema xml) de ese descriptor. Esta entrada se incluye en un elemento resourceType y tiene el aspecto que se muestra en la Figura 8-2.

La tercera entrada proporciona el URL que debe utilizar la aplicación PHG cuando quiera establecer una APS en la aplicación HFS. Es en este URL donde la aplicación PHG ejecuta un POST de la descripción de sus capacidades relacionadas con la APS. Esta entrada se incluye en un elemento section y tiene el aspecto que se muestra en la Cuadro 8-3.

NOTA – Las clases de capacidad certificada (CCC) Continua documentadas en root.xml no son los manejadores de mensajes admitidos por la aplicación PHG. Estos manejadores figuran en el recurso de APB. La aplicación HFS no muestra qué protocolos utilizará el servicio de APS.

I.2 Autenticación de APS: Enfoque de las credenciales de contraseña de propietario del recurso

Se pueden emplear diferentes técnicas para asociar una APS con una credencial de seguridad. En la descripción siguiente se muestra el uso de las credenciales de contraseña de propietario del recurso como método para obtener acceso al recurso de APB asociado con la APS. Para obtener más información, véase el Anexo B de [UIT-T H.812].

Cuando la aplicación PHG ha determinado que la aplicación HFS admite la creación de una APS mediante el intercambio de capacidades, puede iniciar el proceso de establecimiento de la APS. En el primer paso del proceso, la aplicación PHG valida la aplicación HFS mediante el establecimiento de una conexión TLS con ella. La aplicación PHG puede conocer la existencia de varios URL diferentes asociados a la aplicación HFS. En este caso, se presupone que la aplicación PHG y la aplicación HFS han intercambiado información sobre un servicio de autenticación. El servicio de inicio de sesión acepta un nombre de usuario y una contraseña (credenciales de propietario del recurso) procedentes de la aplicación PHG y, si coinciden, devuelve un testigo de acceso OAUTH de tipo portador. Con este testigo de acceso, la aplicación PHG puede ejecutar operaciones HTTPS para obtener el recurso de APB asociado al servicio de APS indicado en el fichero root.xml.

I.3 Establecimiento de la APS: POST de la aplicación PHG con APB parcial

Una vez establecida la conexión, la aplicación PHG ejecuta una operación POST al URL proporcionado en el fichero root.xml de la aplicación HGS. La operación POST contiene un documento xml que describe las capacidades de APS de la aplicación PHG (Cuadro 8-1), como se muestra en la Figura I-1.

```
<?xml version="1.0" encoding="UTF-8"?>
 <aps:APB
xmlns:aps="http://handle.itu.int/11.1002/3000/hData/APS/2017/01/H.812.4.pdf"
xmlns:xsi = "http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation =
"http://handle.itu.int/11.1002/3000/hData/APS/2017/01/APBConfigResource.xsd">
 <!-- La PHG cumplimenta estos campos -->
 <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>
```

Figura I-1 – APB de ejemplo publicada por la aplicación PHG

La aplicación HFS puede examinar la lista separada por espacios de manejadores de mensajes admitidos del elemento <supportedMH> para determinar si la aplicación PHG admite servicios para los que la aplicación HFS puede emitir mensajes. La aplicación HFS también puede inspeccionar la lista separada por espacios de mecanismos de intercambio y la lista separada por espacios de mecanismos de interrupción. Si la aplicación HFS admite un mecanismo de transferencia mostrado por la aplicación PHG, podrá establecer una APS. En este caso, la aplicación HFS responde con un código HTTP adecuado, como 201 CREATED, y proporciona un URL al recurso de APB. Si la aplicación PHG no admite ninguna de las CCC o mecanismos de transferencia soportados por la aplicación HFS, esta responde con un código de error HTTP, por ejemplo, 501 (Not Implemented).

I.3.1 Establecimiento de la APS: PHG GET para APB completada

A continuación, la aplicación PHG puede emitir una petición GET para el recurso de APB. La aplicación PHG debe formatear correctamente el trayecto del recurso de acuerdo con la entrada <resourcePrefix> de root.xml. La aplicación HFS crea el recurso de APB para la APS. El recurso de APB creado está asociado con las credenciales de autenticación de la aplicación PHG. La aplicación HFS cumplimenta los elementos restantes del documento xml que describe el recurso de APB de conformidad con el Cuadro 8-2.

La APB resultante, tal y como la obtendría la PHG con la operación GET, está descrita en la Figura I-2.

```
<?xml version="1.0" encoding="UTF-8"?>
<aps:APB
xmlns:aps="http://handle.itu.int/11.1002/3000/hData/APS/2017/01/H.812.4.pdf"
     xmlns:xsi = "http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation =
"http://handle.itu.int/11.1002/3000/hData/APS/2017/01/APBConfigResource.xsd">


 <!-- La PHG cumplimenta estos campos -->
 <supportedMH>APS lampreynetworks.com/private</supportedMH>
 <exchangeMechanism>MQTT privateMessageProtocol</exchangeMechanism>
 <shoulderTapMechanism>SMS</shoulderTapMechanism>
 <SMS>
 <MSISDN>441111223344</MSISDN>
 <SMSHeaderDstPort>1234</SMSHeaderDstPort>
 <SMSApplicationId>4827351</SMSApplicationId>
 </SMS>

 <!-- escogido por la aplicación HFS; puede ser igual en todas las APS -->
 <HFSAPBI>HFSAPBI</HFSAPBI>
 <!-- escogido por la aplicación HFS; debe ser unívoco en todas las APS de la
aplicación HFS
  Se utiliza como nombre de usuario de MQTT -->
 <PHGAPBI>PHGAPBI</PHGAPBI>
 <!-- Dirección del servidor MQTT -->
 <APSExchangeURL>address to the MQTT server</APSExchangeURL>
 <!-- Estado de la APS, que es NEW al ser creada por primera vez -->
 <APSState>NEW</APSState>
 <!-- Escogido por la aplicación HFS; periodo de tiempo que la PHG puede
permanecer silenciosa
  hasta que la aplicación HFS intente cerrarla (después de un sondeo) -->
 <expirationTime>expirationTime</expirationTime>
 <!-- Escogido por la aplicación HFS; periodo de tiempo del que dispone la PHG
para
  responder a una operación ECHO -->
 <requiredResponseTime>requiredResponseTime</requiredResponseTime>
 <!-- escogido por la aplicación HFS; actúa como identificador de cliente para
el servidor MQTT -->
 <clientId>clientId</clientId>
 <!-- escogido por la aplicación HFS; actúa como contraseña del servidor MQTT --
>
  Por ejemplo, la huella dactilar del certificado de PHG -->
 <PHGCredential>PHGCredential</PHGCredential>
</aps:APB>
```

NOTA – Este ejemplo incluye un manejador de mensajes privado (lampreynetworks.com/private) así como el manejador de mensajes de APS requerido.

Figura I-2 – APB creada por la aplicación HFS

Es posible que la aplicación HFS quiera configurar el componente de software MQTT en este momento. En esta norma no se especifica la manera en que la aplicación HFS interactúa con el servidor MQTT. La aplicación PHG publicará en los temas de respuesta y estado. El método que utiliza la aplicación HFS para obtener esta información queda fuera del alcance de este documento de directrices de diseño.

I.3.2 Establecimiento de la APS: Configuración de la PHG con servidor MQTT

Tras recibir el recurso de APB, la aplicación PHG debe establecer una conexión segura con el servidor MQTT. La dirección del servidor MQTT está disponible en el recurso de APB.

Se utilizan las banderas de la instrucción MQTT CONNECT para indicar que el nombre de usuario y la contraseña están presentes, que se retendrá el mensaje Will y que no se debe limpiar la sesión (es decir, los mensajes no entregados serán persistentes en las supresiones de la conexión TCP), conforme al Cuadro 9-2. Con estos parámetros, se puede recibir un mensaje publicado previamente en un tema después de que la aplicación PHG se haya suscrito a ese tema. El nombre de usuario y la contraseña son PHGAPBI y PHGCredential respectivamente, que se indican en el recurso de APB. El protocolo MQTT requiere que la aplicación PHG proporcione un identificador de cliente. El identificador de cliente se indica en el elemento clientID del recurso de APB. La aplicación PHG también especifica un periodo de tiempo de mantener vigente (keep alive), que establece el periodo de tiempo durante el cual la aplicación puede permanecer inactiva antes de emitir un MQTT PING. El valor 0 indica que la aplicación PHG no enviará paquetes PING. La aplicación PHG también establece la bandera de mensaje WILL. Este parámetro indica cómo actuará el servidor MQTT cuando se pierda la conexión con la aplicación PHG. La aplicación PHG define los parámetros WILL para que utilicen el tema de estado con una carga útil "LOST". Por tanto, cuando se pierde la conexión con la aplicación PHG, el servidor MQTT publica un mensaje en el tema de estado con la carga útil "LOST".

I.3.3 MQTT: La aplicación PHG se suscribe a las instrucciones

Una vez conectada, la aplicación PHG se suscribe al tema de mensaje de cada CCC de la que quiere recibir mensajes. Un único tema de mensaje se especifica como sigue:

```
pcha/message/HFSAPBI/PHGAPBI/mh
```

donde HFSAPBI y PHGAPBI son los valores facilitados en el recurso de APB y el parámetro "mh" es la CCC que recibirá el mensaje. Un ejemplo de tema de mensaje posible es:

```
pcha/message/HFSAPBI/6d296e99-e5dc-43d0-b455-7c1f3eb35d83/APS
```

I.3.4 MQTT: La aplicación PHG publica "CONNECTED"

Una vez completadas todas las suscripciones, la aplicación PHG publica un mensaje en el tema de estado:

```
pcha/status/HFSAPBI/6d296e99-e5dc-43d0-b455-7c1f3eb35d83
```

con la carga útil "CONNECTED". En este momento, técnicamente la aplicación PHG puede recibir instrucciones de la aplicación HFS. Sin embargo, existe un requisito adicional según el cual la aplicación HFS debe abstenerse de enviar mensajes hasta que la aplicación PHG habilite la APS.

I.4 Establecimiento de la APS: La aplicación PHG habilita la APS

Para habilitar la APS, la aplicación PHG debe ejecutar una operación PUT en el URL proporcionado en la respuesta POST (response_URL) tras añadirle la representación XPath del elemento APSSTate. (Por ejemplo, created_APS_resource_URL/APSState). El tipo MIME está establecido en "application/text" y el cuerpo http contiene el texto ENABLED.

La aplicación HFS responde con éxito (200 OK) si es capaz de cambiar APSState.

I.5 Funcionamiento

En este momento, la aplicación PHG puede recibir mensajes de todas las cadenas de mensaje con manejadores suscritos para la recepción de mensajes. La aplicación PHG puede identificar a qué CCC corresponde la carga útil de mensaje examinando el componente "mh" del tema de mensaje.

Tras manejar el mensaje, la aplicación PHG responde a él publicando un mensaje de temas de respuesta con la carga útil devuelta de la CCC (si la hubiere).

La aplicación PHG tiene permiso para desconectarse del servidor MQTT manteniendo la sesión APS; la sesión APS continúa habilitada pero la aplicación PHG no podrá recibir mensajes. La aplicación HFS descubrirá que la conexión tiene el estado "CLOSED" al recibir un mensaje CLOSED en el tema de estado. La aplicación PHG puede restablecer la conexión en cualquier momento volviendo a invocar la secuencia de conexión de MQTT. La aplicación PHG publicará "CONNECTED"·en el tema de estado cuando haya establecido correctamente la conexión de cliente MQTT.

Sin embargo, en la situación de reconexión de la aplicación PHG más probable, la aplicación HFS activa la aplicación PHG con uno de los mecanismos de interrupción que ambas aplicaciones admiten porque necesita enviar un mensaje.

Si no se ha producido actividad del recurso de APB antes de que venza el plazo <expirationTime>, la aplicación PHG puede recibir un mensaje de gestión ECHO ("APS") de la aplicación FHS. La aplicación PHG comunica a la aplicación HFS que continúa activa y conectada publicando la respuesta a la instrucción "ECHO" en el tema de respuesta. La aplicación HFS espera que se le notifique esta respuesta dentro del plazo <requiredResponseTime> especificado en el recurso de APB. Si la aplicación PHG no está conectada en ese momento, la aplicación HFS puede optar por utilizar el proceso de interrupción para restablecer la conectividad en el nivel de transporte.

La aplicación PHG puede terminar una APS en cualquier momento realizando la misma operación PUT que cuando habilitó la APS pero, en este caso, con el valor del elemento <APSState> del recurso de APB en TERMINATED. La aplicación PHG termina la APS eliminando las instrucciones pendientes del servidor MQTT y ejecuta UNSUBSCRIBES para la respuesta y los temas de estado asociados. Ambos lados pueden terminar la APS por razones administrativas (fuera de banda).

Una vez terminada, la aplicación HFS elimina la información que asocia el recurso de APB con la credencial de autenticación de la aplicación PHG, de tal manera que, si la aplicación PHG inició otro procedimiento de establecimiento de APS con la misma credencial de autenticación, la aplicación HFS devolvería el valor del elemento APSState a NEW.

Apéndice II

Ejemplo de fichero root.xml del HFS

(Este Apéndice no forma parte integrante de la presente Recomendación.)

A continuación se proporciona un código XML de ejemplo de un fichero root.xml del HFS.

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

<resourceType>
 <resourceTypeId>APB</resourceTypeId>
 <!-- ubicación de referencia que describe la norma APS -->
 <reference>
 http://handle.itu.int/11.1002/3000/hData/APS/2017/01/H.812.4.pdf
 </reference>
 <representation>
 <mediaType>application/xml</mediaType>
 <!-- Esquema para el recurso xml de APB -->
 <validator>
 http://handle.itu.int/11.1002/3000/hData/APS/2017/01/APBConfigResource.xsd
 </validator>
 </representation>
<resourceType>

<section>
 <path>APB/</path>
 <profileId>APS-CCC-HFS</profileId>
 <!-- obligatorio en esta especificación; opcional pero recomendado en hData;
-->
 <resourcePrefix>true</resourcePrefix>
 <resourceTypeId>APB</resourceTypeId>
</section>
```

Bibliografía

Para obtener una lista de referencias no normativas y publicaciones que contienen más información de fondo, véase [UIT-T H.810].

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios de tarificación y contabilidad y cuestiones económicas y políticas de las telecomunicaciones/TIC internacionales
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	**Sistemas audiovisuales y multimedia**
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedia
Serie K	Protección contra las interferencias
Serie L	Medio ambiente y TIC, cambio climático, ciberdesechos, eficiencia energética, construcción, instalación y protección de los cables y demás elementos de planta exterior
Serie M	Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de la transmisión telefónica, instalaciones telefónicas y redes de líneas locales
Serie Q	Conmutación y señalización, y mediciones y pruebas asociadas
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	Redes de datos, comunicaciones de sistemas abiertos y seguridad
Serie Y	Infraestructura mundial de la información, aspectos del protocolo Internet, redes de próxima generación, Internet de las cosas y ciudades inteligentes
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2021