Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

H.812

(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 servicio

Recomendación UIT-T H.812

Unión Internacional de Telecomunicaciones

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 APPLICACIONES 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.849
Servicios multimedios de intercambios de datos de cibersalud	H.860–H.869
Escucha segura	H.870–H.879

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

Recomendación UIT-T H.812

Directrices de diseño para la interoperabilidad de sistemas de salud personal conectados: Interfaz de servicio

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.

La Recomendación UIT-T H.812 comprende una visión general de la interfaz de servicios, las directrices de diseño comunes para todas las clases de capacidades certificadas (CCC) de la interfaz de servicios y las directrices de diseño para la pasarela de salud personal (PHG) con consentimiento habilitado y las CCC de servicios.

Las directrices de diseño que soportan las siguientes CCC se definen en diversas Recomendaciones independientes, a saber:

– capacidad de carga de observaciones en UIT-T H.812.1 (2017);

– capacidad de cuestionario en UIT-T H.812.2 (2017);

– capacidad de intercambio de capacidades en UIT-T H.812.3 (2017); y

– capacidad de sesión persistente autenticada en UIT-T H.812.4 (2017).

La Recomendación UIT-T H.812 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:

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

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

– UIT-T H.812 – Directrices de diseño para la interoperabilidad de sistemas de salud personal conectados: interfaz de servicios (o sea, las presentes directrices de diseño);

– UIT-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;

– UIT-T H.812.2 – Directrices de diseño para la interoperabilidad de sistemas de salud personal conectados: interfaz de servicios: cuestionarios;

– UIT-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;

– 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;

– UIT-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	2015-11-29	16	11.1002/1000/12653
2.0	ITU-T H.812	2016-07-14	16	11.1002/1000/12913
3.0	ITU-T H.812	2017-11-29	16	11.1002/1000/13415

Palabras clave

CDG, directrices de diseño continuas, dispositivos de salud personal, servicios, sistemas de información sanitaria, sistemas de salud personal conectados.

* 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 propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB en la dirección 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 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.

El presente documento también comprende directrices de diseño para la interoperabilidad adicionales, que aclaran o reducen aún más las opciones o añaden características ausentes en las normas o especificaciones subyacentes.

Esta directrices de diseño contienen una visión general de la interfaz de servicios, las directrices de diseño comunes para todas las clases de capacidades certificadas (CCC) de la interfaz de servicios y las directrices de diseño para la pasarela de salud personal (PHG) con consentimiento habilitado y las CCC de los servicios de salud y aptitud física.

Las directrices de diseño que soportan las siguientes CCC se definen en diversas Recomendaciones independientes, a saber:

– [UIT-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*.

– [UIT-T H.812.2] *Directrices de diseño para la interoperabilidad de sistemas de salud personal conectados: interfaz de servicios: cuestionarios*.

– [UIT-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*.

– [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*.

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 la Recomendación UIT-T H.810.

0.1 Organización

Las presentes de directrices de diseño se articulan como sigue:

Apartados 0-5: Introducción y terminología – Estos apartados contienen información específica sobre la interfaz de servicios, que ayuda a comprender la estructura de las especificaciones de diseño.

Apartado 6: Visión general de la interfaz de servicios – En este apartado se reseñan las CCC de la interfaz de servicios.

Apartado 7: Casos de uso – Este apartado comprende ejemplos prácticos.

Apartado 8: Modelo de conducta – En este apartado se proporciona una visión general de las secuencias de interacciones relacionadas con las CCC comunes de la interfaz de servicios, junto con las interacciones, restricciones y excepciones típicas.

Apartado 9: Implementación – En este apartado se detalla el uso del contenido de carga útil común y del protocolo simple de acceso a objetos (SOAP) frente a la metodología de transporte basada en la transferencia de estado representativo (REST) en las CCC comunes de la interfaz de servicios.

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

Directrices de diseño para la interoperabilidad de sistemas de salud personal conectados: Interfaz de servicio

1 Alcance

Las presentes directrices de diseño se centran en la siguiente interfaz:

– **Interfaz de servicios:** Interfaz situada entre la pasarela de salud personal (PHG) y los servicios.

Esta interfaz se define en la arquitectura Continua, según se indica en el apartado 6 de la Recomendación UIT-T H.810 y se ilustra en la Figura 1-1.

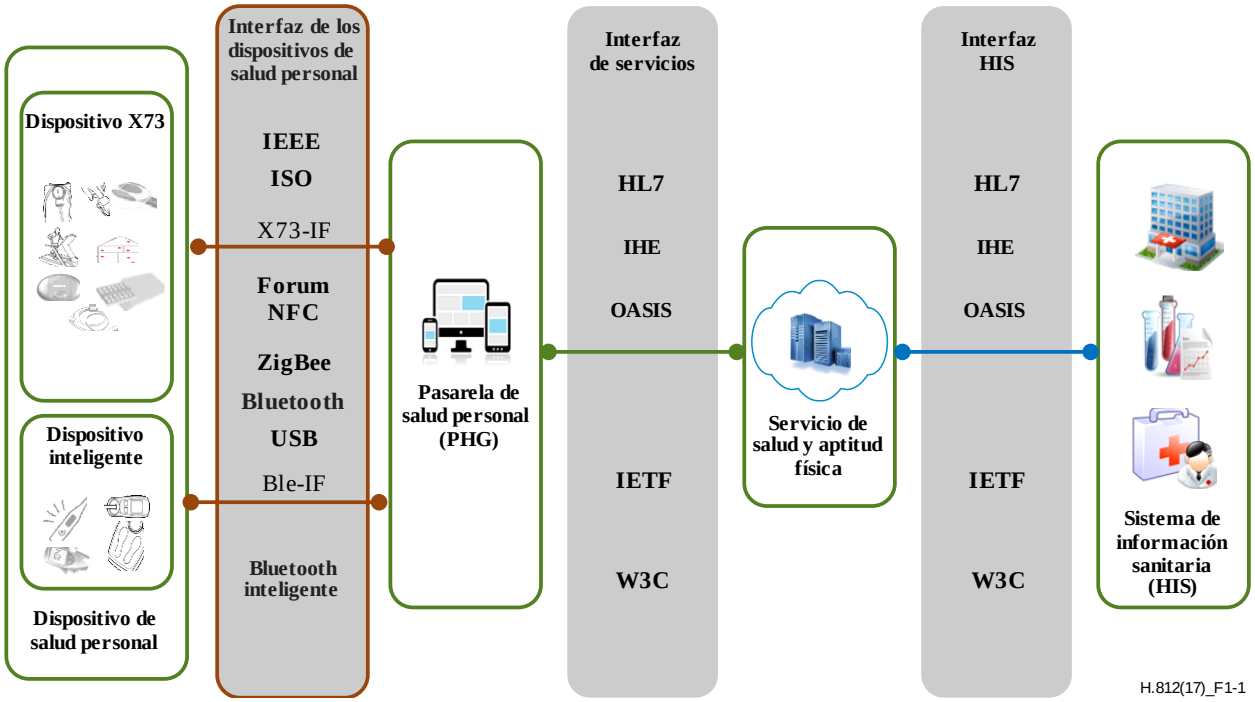

Figura 1-1 – Interfaz de servicios en la arquitectura Continua

Ciertas clases de capacidades certificadas (CCC) guardan relación con la interfaz de servicios. El presente documento contiene directrices de diseño para la interoperabilidad aplicables a varias CCC. Ejemplo de ello son las directrices de diseño para la interoperabilidad de la seguridad. Este documento también contiene las directrices de diseño de las CCC de las PHG con consentimiento habilitado y la interfaz de servicios. Estas CCC pueden agruparse con muchas otras CCC relacionadas con la interfaz de servicios, entre ellas, las CCC de carga de observaciones o las CCC con cuestionario habilitado.

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.*

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 los acrónimos y abreviaturas 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 Arquitectura

En el marco de esta arquitectura de referencia de extremo a extremo (E2E), la interfaz de servicios conecta una pasarela de salud personal (PHG) a un servicio de salud y aptitud física (HFS). La Figura 6-1 ilustra la interfaz de servicios de la arquitectura E2E Continua y la Figura 6-2 ejemplifica una interfaz de servicios.

El objetivo principal de las directrices de diseño de la interfaz de servicios es permitir el intercambio interoperable de información a través de dicha interfaz. En su marco se define un conjunto de clases de capacidades certificadas relacionadas con la interfaz de servicios para las PHG y los HFS, encaminadas a permitir la interoperabilidad de distintos casos de uso, incluidas la carga de datos de medición, la cumplimentación de cuestionarios y la ejecución de comandos.

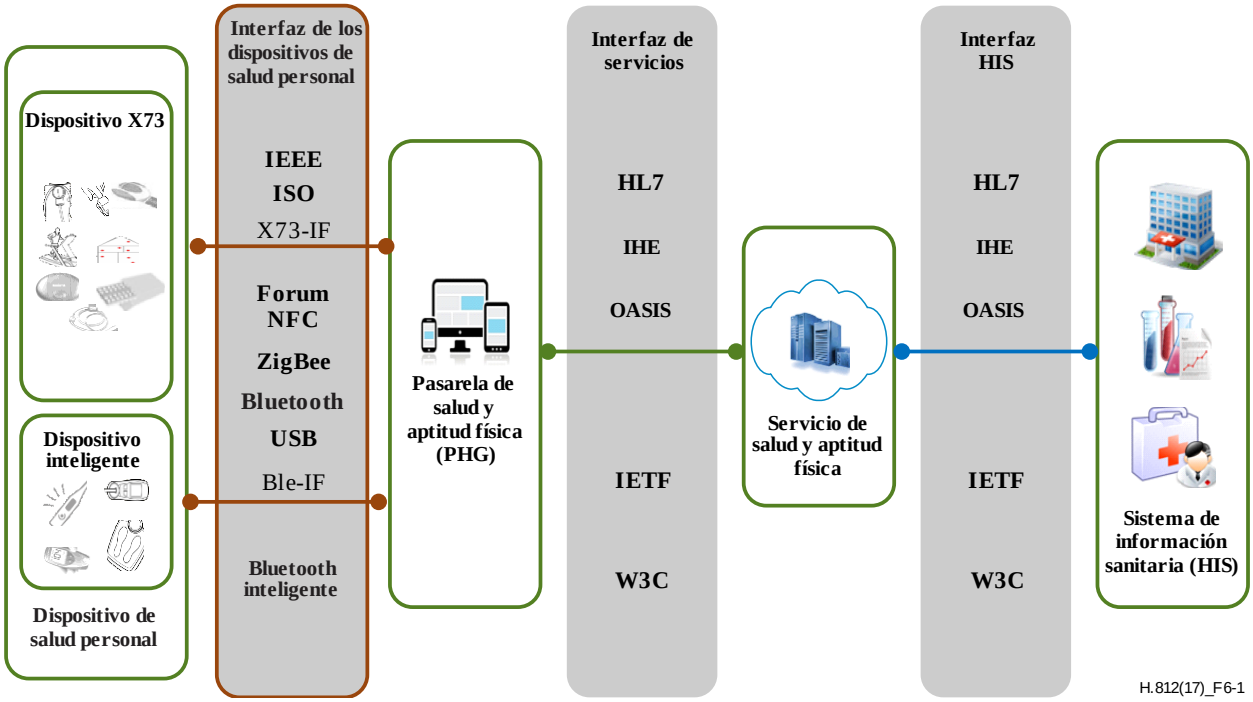

Figura 6-1 – Interfaz de servicios en la arquitectura E2E Continua

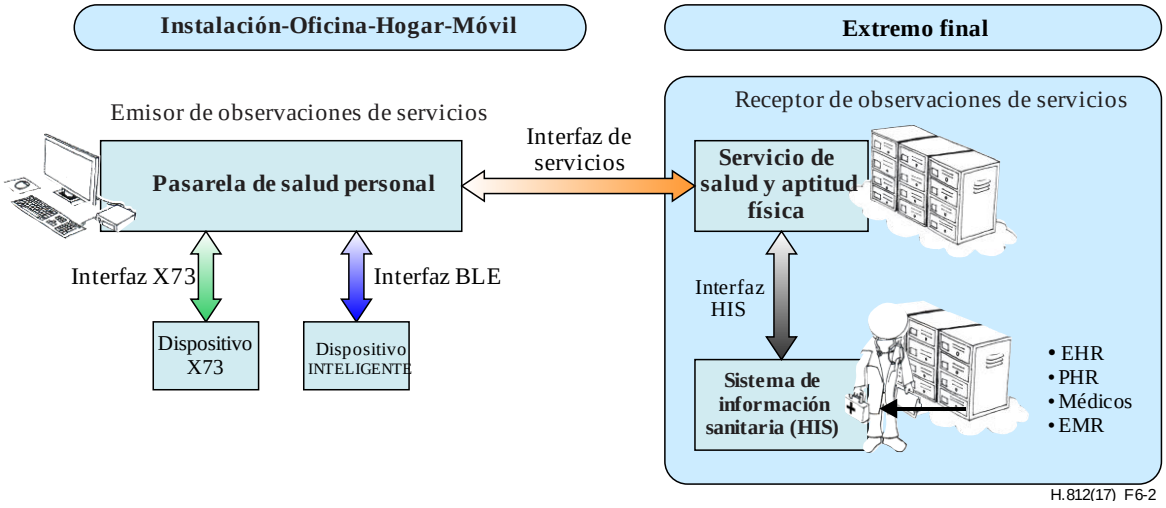

Figura 6-2 – Ejemplo de interfaz de servicios

Además de la interfaz de servicios, en el marco de la arquitectura de referencia de extremo a extremo también se define la interfaz del sistema de información sanitaria (interfaz HIS). El diseño de la interfaz de servicios permite el intercambio de información granular entre una PHG (normalmente, un ordenador personal, un portátil, una tableta, un teléfono móvil u otro tipo de dispositivo integrado), que es un dispositivo cercano al usuario/paciente, y un servicio de salud y aptitud física (normalmente, un servicio de extremo final basado en la nube), que compila información sobre dicho usuario y la pone a disposición para su uso posterior. En cambio, el diseño de la interfaz HIS permite el intercambio de información agregada entre dos sistemas de extremo final, por ejemplo, un sistema de gestión de patologías y una historia clínica electrónica (EHR)[1]. La interfaz HIS viene definida en [UIT-T H.813].

También es previsible que las PHG puedan implantarse en aplicaciones fijas en el hogar o móviles de usuario, lo que impone una serie de restricciones al diseño de la interfaz de servicios. Dadas las dificultades inherentes al mantenimiento y/o la actualización de estos dispositivos "sobre el terreno", las PHG deben ser lo suficientemente robustas, autónomas y sencillas para mantener los costes bajos y reducir al mínimo los requisitos en materia de conocimientos operativos de orden teórico o práctico. A la luz de lo anterior, la interfaz de servicios permite que la mayor parte de los metadatos de contexto asociados al intercambio de observaciones resida fuera de la PHG.

Por otro lado, cabe prever que los servicios de salud y aptitud física sean albergados en sistemas dotados de mayor capacidad, como servidores u ordenadores personales. Por tanto, el objetivo del diseño de la interfaz de servicios es traspasar la complejidad y los aspectos de mantenimiento al servicio de salud y aptitud física, a fin de liberar de esa carga a la PHG.

La interfaz de servicios es un canal abstracto compuesto por uno o más pares de CCC que conectan una aplicación PHG a una aplicación HFS. Cada par de CCC posee un componente que reside en la aplicación HFS y un componente que reside en la aplicación PHG. Continua define clases de capacidades certificadas en ambos lados de la interfaz de servicios.

---

[1] NOTA – En el marco de la arquitectura de extremo a extremo, las interfaces tanto de servicios como de sistemas de información sanitaria (HIS) pueden implantarse en un dispositivo cercano al usuario/paciente (PC, ordenador portátil, teléfono móvil, etc.), a fin de intercambiar información con entidades que se encuentran a una cierta distancia geográfica de dichos dispositivos. Las directrices no imponen restricciones a la implantación de clases de capacidades certificadas en soportes físicos específicos.

Esta versión de las directrices de la interfaz de servicios permite las siguientes clases de capacidad certificada:

– la carga de observaciones de la PHG al servicio de salud y aptitud física en dos estilos distintos: servicios web (SOAP) y REST (datos) [UIT-T H.812.1];

– la carga de información de consentimiento de la PHG al servicio de salud y aptitud física en dos estilos distintos: servicios web (SOAP) y REST (datos) [UIT-T H.812];

– la descarga de cuestionarios que deben cumplimentarse del servicio de salud y aptitud física a la PHG y la carga de los cuestionarios cumplimentados de la PHG al servicio de salud y aptitud física [UIT T H.812.2];

– el intercambio de información (por ejemplo, comandos no solicitados) entre el servicio de salud y aptitud física y la PHG a través de una sesión persistente autenticada [UIT-T H.812.4]; y

– el intercambio de información sobre la clase de capacidad certificada soportada (intercambio de capacidad) entre la PHG y el servicio de salud y aptitud física, como elemento habilitador de los demás casos de uso [UIT-T H.812.3].

Una PHG puede soportar una o más aplicaciones capaces de implementar una o más clases de capacidades certificadas Continua. La Figura 6-3 ilustra la interfaz de servicios Continua y muestra una aplicación PHG y una aplicación HFS en las que se implementan todas las clases de capacidades certificadas posibles de la interfaz de servicios.

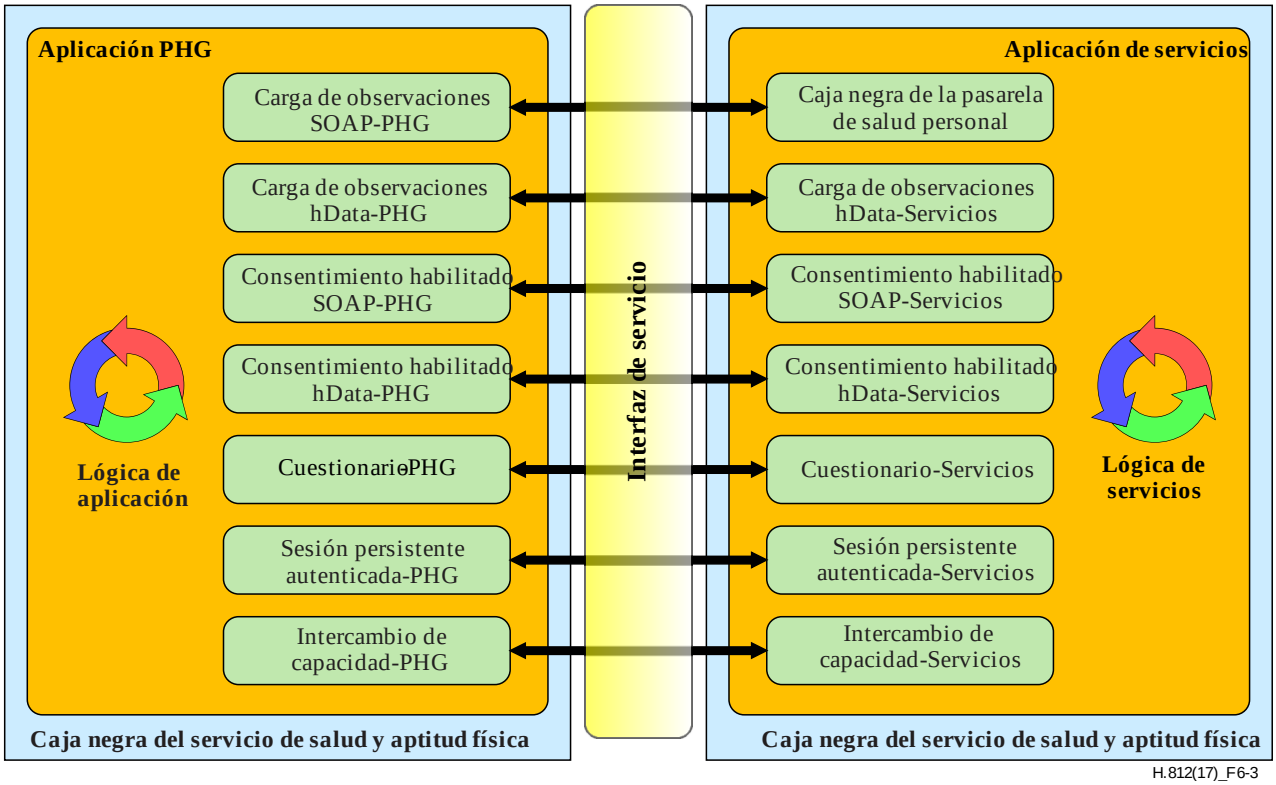

Figura 6-3 – Interfaz de servicios Continua y clases de capacidades certificadas conexas

Las presentes directrices tienen por objeto especificar la conducta del sistema con suficiente detalle como para lograr un nivel aceptable de interoperabilidad en casos de uso concretos. Los casos de uso se encapsulan en clases de capacidades certificadas (CCC). Las directrices formulan declaraciones normativas sobre el funcionamiento de la interfaz de red de los componentes de las funciones de las CCC. En el contexto de la interfaz de servicios, estos componentes se enmarcan en aplicaciones o servicios que residen en una PHG o en un servicio de salud y aptitud física.

Las plataformas comunes suelen limitar la forma en que las aplicaciones pueden comunicarse entre sí, a fin de garantizar la estabilidad de la plataforma en general. Esta interacción limitada entre aplicaciones se produce en un entorno aislado (sandbox). A fin de soportar aplicaciones en entornos aislados, esta versión de la interfaz de servicios utiliza un modelo de referencia que define las aplicaciones como "contenedores" para uno o más componentes de las CCC. Las interacciones entre los componentes dentro de estos contenedores no están sujetas a requisitos normativos y dependen por completo del desarrollador de la aplicación. En la interfaz de servicios, las interacciones entre las CCC de la aplicación PHG y las CCC correspondientes del servicio de salud y aptitud física son visibles y están sujetas a requisitos normativos a efectos de certificación.

El modelo de referencia permite la existencia de múltiples aplicaciones en una PHG o un servicio de salud y aptitud física, sin embargo, las aplicaciones no interactúan con otras aplicaciones si no es a través de una interfaz de red. En las presentes directrices, las aplicaciones que se ejecutan en un servicio de salud y aptitud física se denominan con frecuencia servicios, ya que los servicios de salud y aptitud física suelen ser plataformas de servicios web. En términos conceptuales, un servicio de salud y aptitud física es lo mismo que una aplicación PHG.

Las presentes directrices documentan mecanismos que permiten la comunicación entre componentes a través de una interfaz interna de programación de aplicaciones (API). Cabe la posibilidad de que, en versiones futuras de la interfaz de servicios, estos mecanismos se utilicen para propiciar la interoperabilidad entre componentes dentro de una aplicación.

En la Figura 6-4 se utilizan los conceptos del modelo de referencia de interfaz de servicios para representar una PHG con dos aplicaciones independientes que se comunican con una aplicación de servicios. Una de las aplicaciones PHG soporta tres CCC y la otra soporta una única CCC. Los requisitos normativos se establecen en las interfaces de red situadas entre la PHG y el servicio de salud y aptitud física. Las interacciones entre los componentes de las CCC dentro de un contenedor de aplicación no revisten un carácter normativo, se muestran como líneas rojas discontinuas coordinadas por el procesamiento interno de la aplicación y se hallan fuera del alcance de las presentes directrices.

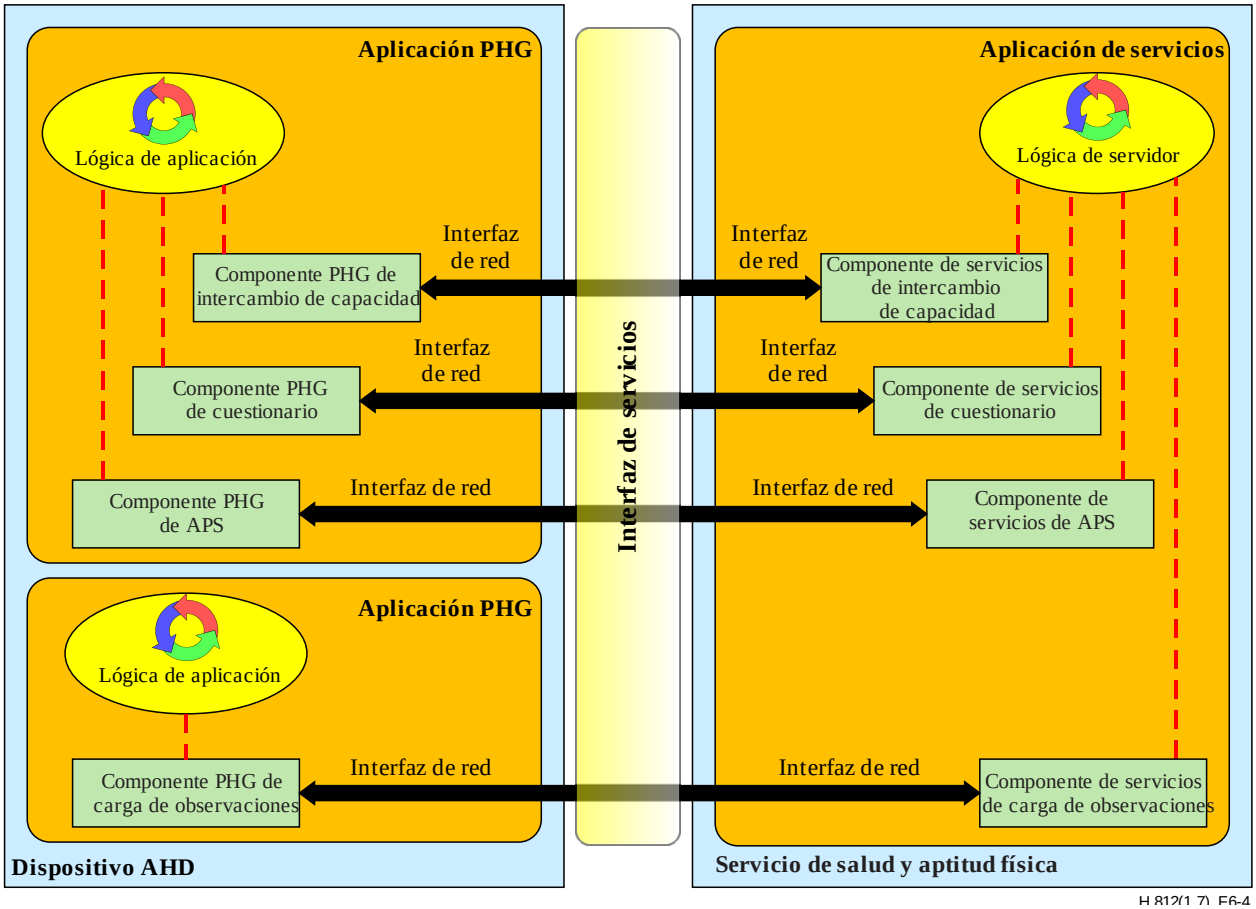

Figura 6-4 – Modelo de referencia de interfaz de servicios

Las comunicaciones que utilizan la interfaz de servicios se inician en el componente de intercambio de capacidad de la PHG. Este componente envía una solicitud a su componente homólogo del servicio de salud y aptitud física. En virtud de dicha solicitud se pide a este último servicio que especifique las clases de capacidades certificadas que soporta. En palabras llanas, la aplicación PHG le pregunta: "¿Qué puedes hacer?". La aplicación de salud y aptitud física responde en términos de las CCC que soporta. En el caso de la Figura 6-4, la aplicación del servicio de salud y aptitud física diría: "Soporto el intercambio de capacidades, los cuestionarios, la carga de observaciones SOAP y las sesiones persistentes autenticadas". Normalmente, cuando el componente de intercambio de capacidades de la aplicación de servicios responde a la aplicación PHG, proporciona información adicional a la pasarela (por ejemplo, una URL), que permite a la aplicación PHG pasar a la siguiente fase de comunicación con una CCC concreta. Una PHG que sólo soporta la carga de observaciones SOAP no necesita implementar el intercambio de capacidades. Tampoco es necesario invocar el intercambio de capacidades si la PHG ya conoce las capacidades del servicio de salud y aptitud física.

7 Casos de usos

7.1 Caso de uso relacionado con la gestión del consentimiento

Una directiva de consentimiento es un registro de la política de privacidad de un cliente de servicios sanitarios que concede o retira el permiso de acceso a información individualmente identificable sobre la salud (IIHI) [HL7 CDA IG].

El requisito de obtención del consentimiento del usuario es consecuencia de diversas reglamentaciones como la *Health Information and Portability Accountability Act* (HIPAA), la Directiva 95/46 de la Unión Europea, etc. En estas normas sobre privacidad se definen y asignan derechos específicos a los pacientes en relación con la recopilación, el acceso, el uso y la revelación

de información sobre su salud. Las leyes obligan a obtener el consentimiento del paciente antes de consultar, utilizar o compartir su información. Por ejemplo, cuando un paciente se registra en una organización especializada en la gestión de patologías (DMO), se le puede solicitar que rellene un formulario de consentimiento. En dicho formulario, el paciente reconoce y/o firma un conjunto predefinido de políticas que especifican quién está autorizado a acceder a su IIHI y con qué fin, y cómo puede utilizarla. En el presente apartado se describen la captura y transferencia electrónica de las políticas de consentimiento en la interfaz de servicios. El consentimiento electrónico contribuye a reforzar la autonomía del paciente y la eficacia en la gestión del cumplimiento de la normativa sobre consentimiento. Son ejemplos de consentimiento del paciente las alterativas de aceptación (opt-in) y rechazo (opt-out) de la IIHI, el permiso de cancelación de emergencia, la limitación del acceso a determinadas funciones o responsabilidades (por ejemplo, a proveedores de asistencia directa), la utilización de documentos específicos para proyectos de investigación concretos, etc.

En un contexto básico, el paciente definirá sus pautas de consentimiento durante o después de registrarse en la aplicación del servicio de salud y aptitud física. La forma precisa en que el paciente especifica su consentimiento queda fuera del alcance de las presentes directrices, no obstante, podría implicar la selección, y posiblemente la adaptación, de una política de consentimiento predefinida por conducto de una interfaz de usuario en su PHG, que la traduciría en una representación de política de consentimiento legible por una máquina. Dichas políticas incluyen, por lo general, una referencia a las partes que participan, a los objetos de datos y a las posibles actuaciones, estén o no autorizadas. Cuando una aplicación del servicio de salud y aptitud física recibe el consentimiento de un paciente en concreto, lo almacena y exige su cumplimiento en relación con los datos sanitarios que reciba del paciente.

Los siguientes casos de uso se centran en una serie de necesidades definidas con respecto a la gestión del consentimiento del paciente.

7.1.1 Carga del consentimiento en el servidor

Adam Everyman se registra en una organización, véase una DMO, que realiza un seguimiento a distancia de los pacientes en el hogar y recopila información sobre su salud a partir de dispositivos de medición sanitaria instalados en sus propios hogares. Al registrarse, Adam rellena un formulario de consentimiento electrónico en la aplicación PHG. El formulario de consentimiento comprende en una serie de opciones relacionadas con quién estará autorizado a consultar, utilizar, actualizar y revelar los distintos tipos de signos vitales recopilados a través del sistema de seguimiento del paciente a distancia. Una vez especificadas sus preferencias, Adam pulsa el botón "enviar" en su plataforma de telesalud. La plataforma recopila dichas preferencias en un documento de directivas de consentimiento de privacidad, basado en la norma HL7 CDA R2, que a continuación envía desde su PHG a la DMO que proporciona el servicio de seguimiento de pacientes a distancia. A partir de ese momento, la directiva de consentimiento regula el acceso a los datos del paciente en la DMO y el posible envío a terceras partes de dichos datos, lo que, en caso de estar permitido, podría incluir la historia clínica personal del paciente (PHR), el registro de salud electrónico (EHR) y el expediente clínico electrónico (EMR). La directiva de consentimiento de privacidad de Adam se asocia a los datos a través del identificador del paciente.

7.1.2 Recuperación del consentimiento definido por el paciente en el servidor

Cabe la posibilidad de que Adam desee actualizar sus preferencias de privacidad, por ejemplo, para permitir que su entrenador tenga acceso a sus datos, ya que recientemente se ha inscrito en un servicio de entrenamiento físico, tal y como le sugirió un miembro del personal de enfermería de la DMO. Su PHG le facilita un enlace a la última versión del correspondiente documento de directivas de consentimiento de privacidad. Adam accede a dicho enlace y la PHG recupera la última versión de sus directivas de consentimiento de privacidad del servidor y se la remite.

7.1.3 Carga del consentimiento actualizado en el servidor

Adam revisa sus preferencias de consentimiento en materia de privacidad y, si su entrenador no puede acceder a los datos, las actualiza. Una vez actualizadas las preferencias de consentimiento, pulsa el botón "enviar" de su PHG, que compila dichas preferencias en un documento de directivas de consentimiento de privacidad dirigido a la DMO. Acto seguido, la DMO reemplaza el consentimiento antiguo por el documento de directivas de consentimiento de privacidad actualizado.

7.2 Caso de uso relacionado con la observancia del consentimiento

La observancia del consentimiento a través de la encriptación protege la privacidad del paciente de manera eficiente y garantiza que el contenido (por ejemplo, observaciones o respuestas a un cuestionario) sólo esté disponible para el destinatario previsto. Ello evita que otros individuos que podrían trabajar en la misma organización, por ejemplo, personal administrativo, puedan visualizar el contenido. El servicio de salud y aptitud física con consentimiento habilitado debe evaluar el consentimiento antes de desencriptar el contenido. La evaluación del consentimiento permite determinar si el destinatario puede acceder al contenido. Por ejemplo, la conclusión de la evaluación del consentimiento puede ser positiva ("Sucess-1") o negativa ("Failure-0"). El servicio de salud y aptitud física con consentimiento habilitado debe procurar la observancia de las preferencias de consentimiento expresadas en el documento de consentimiento.

7.2.1 Encriptación del contenido antes de la carga

Adam Everyman se registra en la DMO que realiza un seguimiento a distancia de su estado en el hogar y recopila información sobre su salud a partir de los dispositivos de medición sanitaria instalados en su propia casa. Además, ha contratado los servicios de un entrenador, tal y como sugirió un miembro del personal de enfermería de la DMO. Adam Everyman quiere que su entrenador visualice los datos relativos a su actividad y no así los de otros dispositivos de medición, como podría ser un tensiómetro. Así, Adam puede configurar su PHG de tal manera que los miembros del personal de enfermería de la DMO tengan acceso a los datos del tensiómetro y de los dispositivos de seguimiento de actividad, y su entrenador sólo pueda acceder a estos últimos. A tal efecto se utiliza la encriptación.

7.3 Otros casos de uso relacionados con las CCC

Véase el apartado 6 de las siguientes directrices de diseño para consultar otros casos de uso relacionados con las CCC:

– [UIT-T H.812.1] Carga de observaciones
– [UIT-T H.812.2] Cuestionario
– [UIT-T H.812.3] Intercambio de capacidad
– [UIT-T H.812.4] Sesión persistente autenticada

8 Modelos de conducta

El presente apartado versa sobre conductas en términos de:

– intercambio de mensajes de la interfaz de servicios;
– seguridad de las CCC basadas en REST; y
– gestión y observancia del consentimiento de las CCC.

8.1 Conducta en términos de intercambio de mensajes de la interfaz de servicios comunes

Dadas las inquietudes existentes en relación con la seguridad y la privacidad, así como con la viabilidad técnica del sistema en general, la interfaz de servicios requiere que todas las conexiones se

inicien en la PHG. La Figura 8-1 ilustra este particular. Consúltese cada directriz de diseño para conocer la carga útil de mensajes y otros detalles específicos.

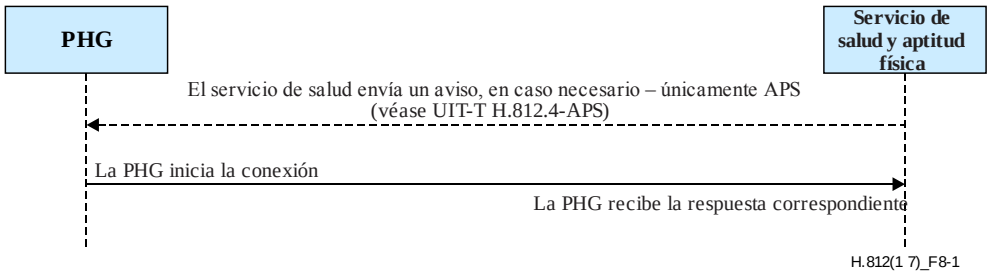

Figura 8-1 – Todas las conexiones se inician en la PHG

Cuando se requiere la seguridad del nivel de transporte (TLS) para la seguridad del contenido de punto a punto, el recurso a la validación mutua de certificados en la toma de contacto TLS depende de la política de seguridad del servicio de salud y aptitud física.

En los casos en que se requiere autenticación:

– en el contexto SOAP, se utiliza un testigo SAML 2.0; y

– para los datos, se utiliza un testigo "portador" OAuth 2.0.

En las presentes directrices no se especifica el modo en que la PHG obtiene dichos testigos, pues ello depende de la relación de confianza existente entre las partes. La aplicación del servicio de salud y aptitud física puede soportar una o más opciones de WS-Trust para obtener testigos SAML 2.0 o un servidor marco de autorización OAuth 2.0 que utilice uno o más tipos de concesiones, entre ellos el de "credenciales contraseña de propietario del recurso". El servicio de salud y aptitud física puede soportar ambos servicios si soporta cargas tanto de datos como de SOAP. En cualquiera de estos casos, debe realizarse una operación fuera de banda, a través de la cual el usuario de la PHG crea una cuenta en la aplicación del servicio de salud y aptitud física que permite al cliente obtener esos testigos. El servicio de testigos del servicio de salud y aptitud física genera testigos personalizados para el destinatario, que este puede validar cuando recibe el contenido. Por otro lado, el servicio de salud y aptitud física puede requerir que dichos testigos procedan de un servicio de autorización de un tercero (véase una CA), con el que la PHG haya establecido una relación de confianza. En ese caso, el servicio de salud y aptitud física permite que el servicio de autorización en cuestión valide al cliente. El servicio de salud y aptitud física puede entonces optar por aceptar cualquier testigo procedente de ese servicio de un tercero, o transmitir cualquier testigo recibido a dicho servicio de autorización con miras a una confirmación previa a su aceptación. Los detalles de la relación de confianza se rigen por la política de seguridad del servicio de salud y aptitud física.

8.2 8.2 Modelo de seguridad común para implementaciones de CCC basadas en REST

La Figura 8 2 ilustra un diagrama de interacción para transacciones RESTful autorizadas basadas en datos (REST) sobre HTTP. A efectos de la autorización se utiliza el marco de autorización OAuth 2.0, que emplea credenciales de contraseña de propietario del recurso, tales como el tipo de concesión de autorización. Se suele recurrir a las credenciales de contraseña de propietario del recurso en los casos en que existe una sólida relación de confianza entre el propietario del recurso (paciente) y el cliente (por ejemplo, una aplicación fidedigna que se ejecuta en el dispositivo que aloja la aplicación). Cabe la posibilidad de que, en futuras versiones de las directrices de diseño, se necesiten otros tipos de credenciales en función de los casos de uso en que pueden utilizarse aplicaciones de terceros (menos privilegiadas) para acceder a los datos del paciente. La utilización de las credenciales de propietario del recurso se limita a una única solicitud, en cuyo marco se intercambian por un testigo de acceso que permite realizar una transacción RESTful en un recurso. Todas las interacciones con

los servidores de autorización y de recursos se efectúan en una sesión segura, conforme a la norma IETF RFC 4346.

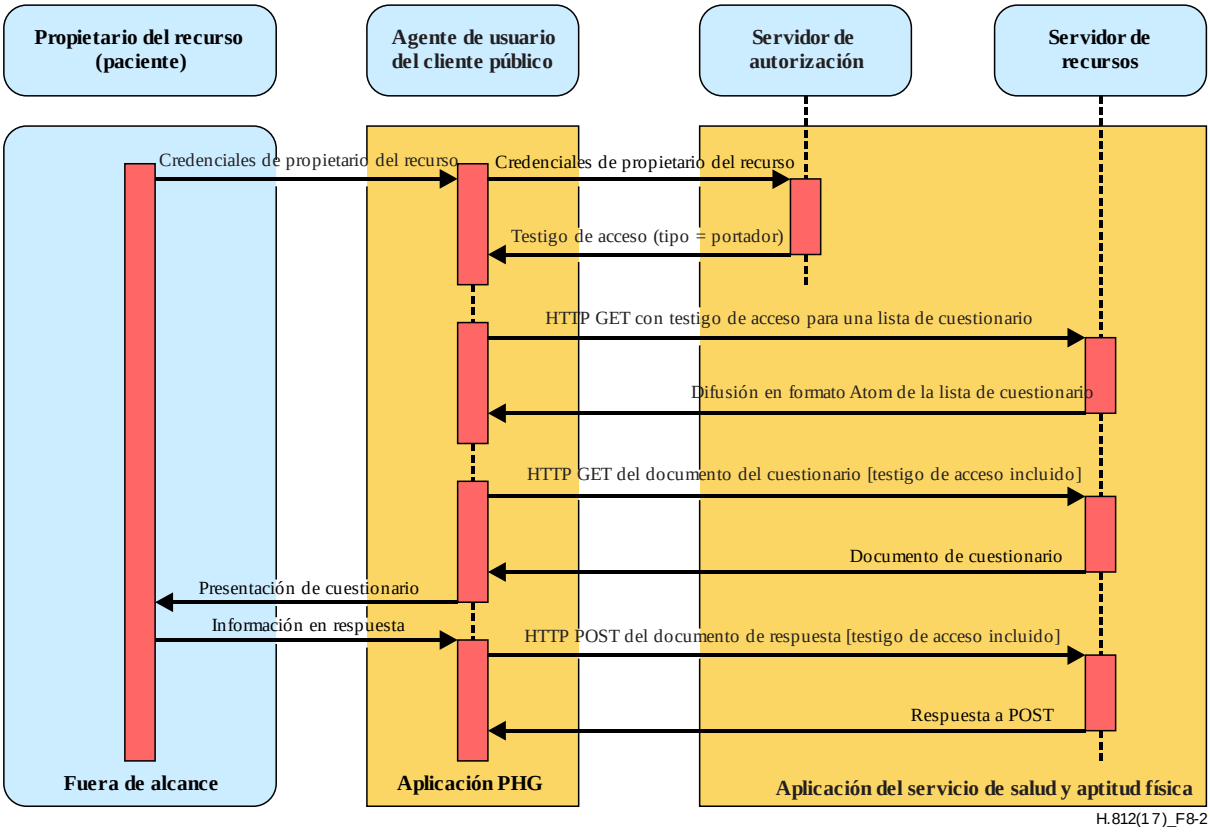

Figura 8-2 – Conducta en términos de seguridad de una CCC RESTful autorizada (se toma como ejemplo el caso de uso del cuestionario)

Las directrices de seguridad relativas a la CCC REST figuran en el Cuadro B.1 y el Cuadro B.2

8.3 Modelo de conducta en términos de gestión del consentimiento

A continuación se especifican los siguientes mecanismos de intercambio del servicio de gestión del consentimiento:

– creación de un *nuevo* documento de consentimiento en el servidor;

– recuperación del documento de consentimiento *ya* especificado del servidor; y

– carga del documento de consentimiento *actualizado* en el servidor.

La Figura 8-3 ilustra las transacciones relacionadas con los casos de uso de gestión del consentimiento descritos en este perfil de contenido.

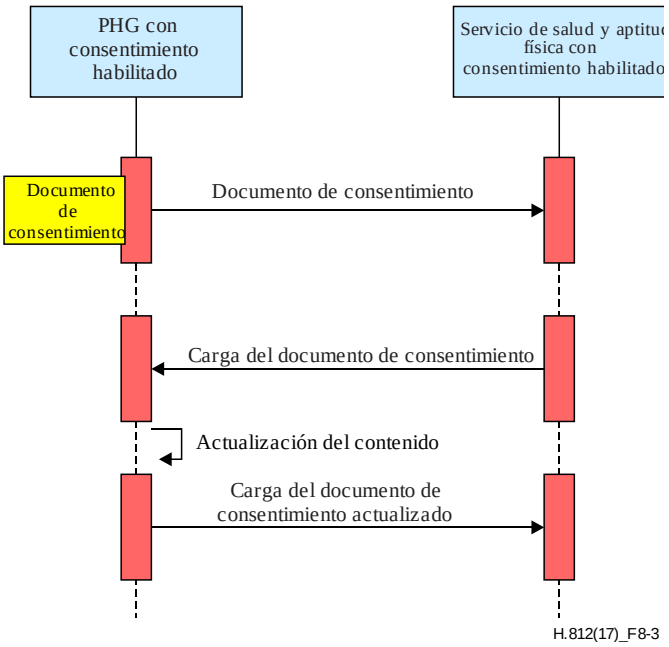

Figura 8-3 – Transacciones entre la PHG y el servicio de salud y aptitud física relacionadas con la gestión del consentimiento

Las directrices relativas a la gestión del consentimiento figuran en el Cuadro C.1 y el Cuadro C.2.

8.4 Modelo de conducta en términos de observancia del consentimiento

A continuación se especifica la siguiente función relacionada con la observancia del consentimiento:

– encriptación del contenido que se va a cargar.

La Figura 8-4 ilustra la funcionalidad de observancia del consentimiento.

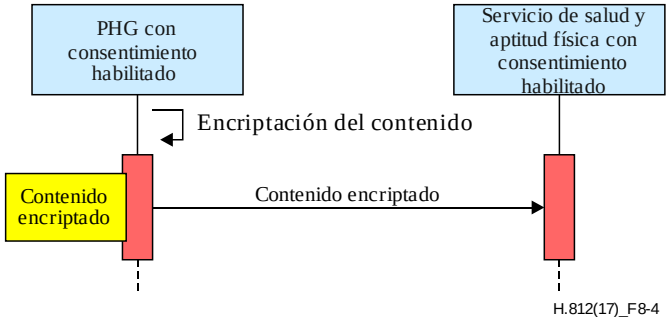

Figura 8-4 – Observancia del consentimiento en la interfaz de servicios

Las directrices relativas a la observancia del consentimiento figuran en el Cuadro C.3 y cuadro C.4.

9 Implementación

9.1 Representación del consentimiento

Las preferencias de consentimiento se representan de conformidad la especificación HL7 *Implementation Guide for CDA Release 2.0* (véase la directiva de consentimiento en [HL7 CDA IG]).

El paquete de presentación de la norma antes mencionada contiene ejemplos de archivos para un documento de consentimiento.

9.2 Protocolos de transporte

9.2.1 Protocolos de transporte que utilizan datos a través de HTTP

En este contexto, los datos a través de HTTP se utilizan como protocolo de transporte para el intercambio de documentos de consentimiento en el marco de la interfaz de servicios y soportan todos los casos de uso evocados en los apartados 7.1 y 7.2. Para conocer los requisitos detallados de la utilización de datos a través del protocolo HTTP entre las PHG y los servicios de salud y aptitud física, consúltese el Anexo A, el Cuadro C.1, el Cuadro C.2, el Cuadro C.3 y el Cuadro C.4.

9.2.2 Protocolos de transporte que utilizan IHE XDR

En este contexto, la especificación [IHE ITI TFS XDR] se utiliza como protocolo de transporte para el intercambio de documentos de consentimiento en el marco de una interfaz de servicios y sólo admite la carga del consentimiento en el caso de uso del servidor. Los documentos de consentimiento se vinculan a la información sanitaria (mensaje PCD-01) a través del identificador del paciente. De esta forma, el consentimiento queda asociado a la información sanitaria y rige su utilización.

9.3 Observancia del consentimiento

9.3.1 Observancia del consentimiento mediante encriptación XML

En el caso de los protocolos de transporte que utilizan la especificación [IHE ITI TFS XDR], la norma de encriptación XML [W3C XMLENC] se aplica a efectos de la observancia del consentimiento mediante encriptación. La norma de encriptación XML permite encriptar la carga útil de la transacción PCD-01 para un destinatario específico (véanse doctores o enfermeros) en el servicio de salud o aptitud física.

La norma de encriptación XML se utiliza a efectos de la observancia del consentimiento mediante encriptación.

9.3.2 Observancia del consentimiento mediante IHE DEN

En el caso de los protocolos de transporte que utilizan datos a través de HTTP, la observancia del consentimiento se habilita mediante la utilización del perfil IHE DEN de la especificación [IHE ITI DEN].

Anexo A

Reseña de las directrices normativas

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

En el Cuadro A.1 se enumeran las clases de capacidades certificadas de los servicios.

Cuadro A.1 – Clases de capacidades certificadas

Nombres de las clases de capacidades certificadas	Clases de capacidades certificadas	Clases de capacidades de logotipo
Carga de observaciones SOAP – PHG	Sí	Sí
Carga de observaciones SOAP – Servicio de salud y aptitud física	Sí	Sí
Carga de observaciones de datos – PHG	Sí	Sí
Carga de observaciones de datos – Servicio de salud y aptitud física	Sí	Sí
Consentimiento habilitado SOAP – PHG	Sí	Sí
Consentimiento habilitado SOAP – Servicio de salud y aptitud física	Sí	Sí
Consentimiento habilitado de datos – PHG	Sí	Sí
Consentimiento habilitado de datos – Servicio de salud y aptitud física	Sí	Sí
Cuestionario – PHG	Sí	Sí
Cuestionario – Servicio de salud y aptitud física	Sí	Sí
Intercambio de capacidades – PHG	Sí	Sí
Intercambio de capacidades – Servicio de salud y aptitud física	Sí	Sí
Sesión persistente autenticada – PHG	Sí	*
Sesión persistente autenticada – Servicio de salud y aptitud física	Sí	*[2]

Las directrices aplicables a cada clase de capacidad certificada figuran el Cuadro A.2 infra.

Cuadro A.2 – Directrices aplicables a las clases de capacidades certificadas

Clases de capacidades certificadas	Directrices pertinentes
Carga de observaciones SOAP – PHG	Véanse [UIT-T H.812.1] y [UIT-T H.812], Cuadro A.3 y Cuadro B.3
Carga de observaciones SOAP – Servicio de salud y aptitud física	Véanse [UIT-T H.812.1] y [UIT-T H.812], Cuadro A.3 y Cuadro B.3
Carga de observaciones de datos – PHG	Véanse [UIT-T H.812.1] y [UIT-T H.812], Cuadro A.3 y Cuadro B.1
Carga de observaciones de datos – Servicio de salud y aptitud física	Véanse [UIT-T H.812.1] y [UIT-T H.812], Cuadro A.3 y Cuadro B.2

[2] * Estos recuadros se han dejado intencionalmente en blanco.

Cuadro A.2 – Directrices aplicables a las clases de capacidades certificadas

Clases de capacidades certificadas	Directrices pertinentes
Consentimiento habilitado SOAP – PHG	Véanse [UIT-T H.812.1] y [UIT-T H.812], Cuadro A.3, Cuadro B.3, Cuadro C.5 y Cuadro C.7
Consentimiento habilitado SOAP – Servicio de salud y aptitud física	Véanse [UIT-T H.812.1] y [UIT-T H.812], Cuadro A.3, Cuadro B.3, Cuadro C.6 y Cuadro C.8
Consentimiento habilitado de datos – PHG	Véase [UIT-T H.812], Cuadro A.3, Cuadro C.1, Cuadro C.3 y Cuadro B.1
Consentimiento habilitado de datos – Servicio de salud y aptitud física	Véase [UIT-T H.812], Cuadro A.3, Cuadro C.2, Cuadro C.4 y Cuadro B.2
Cuestionario – PHG	Véanse [UIT-T H.812.2], Cuadro A.1, y [UIT-T H.812], Cuadro A.3 y Cuadro B.1
Cuestionario – Servicio de salud y aptitud física	Véanse [UIT-T H.812.2], Cuadro A.2, y [UIT-T H.812] y Cuadro A.3 y Cuadro B.2
Intercambio de capacidades – PHG	Véanse [UIT-T H.812.3], Cuadro A.2, y [UIT-T H.812], Cuadro A.3 y Cuadro B.1
Intercambio de capacidades – Servicio de salud y aptitud física	Véanse [UIT-T H.812.3], Cuadro A.1, y [UIT-T H.812], Cuadro A.3 y Cuadro B.2
Sesión persistente autenticada – PHG	Véanse [UIT-T H.812.4], Cuadros A.1, A.2, A.3 y A.5, y [UIT T H.812], Cuadro A.3 y Cuadro B.1
Sesión persistente autenticada – Servicio de salud y aptitud física	Véanse [UIT-T H.812.4], Cuadros A.1, A.4 y A.6, y [UIT T H.812], Cuadro A.3 y Cuadro B.2

Cuadro A.3 – Requisitos comunes de todas las CCC

Nombre	Descripción	Observaciones
CapX-HFS-Universality	Todos los servicios de salud y aptitud físicas **deberán** soportar el intercambio de capacidades, salvo las CCC de carga de observaciones SOAP y de servicio de salud y aptitud física con consentimiento habilitado.	No es necesario que los servicios de salud y aptitud física que sólo implementan CCC de servicios de salud y aptitud física con consentimiento habilitado o carga de observaciones SOAP soporten la CCC de intercambio de capacidades de dichos servicios.
HFS-Transport_Connection_Initiation	Las conexiones de todos los servicios de salud y aptitud física **deberán** iniciarse en la aplicación PHG de dichos servicios y **no deberán** iniciarse en los propios servicios.	

Anexo B

Directrices generales de seguridad para las CCC de la interfaz de servicios

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

Cuadro B.1 – Directrices de seguridad para las PHG que utilizan REST

Nombre	Descripción	Observaciones
PHG-Grant_Type	Las PHG pueden utilizar credenciales de contraseña de propietario del recurso, tales como el tipo de concesión de autorización, según se indica en el apartado 1.3.3 de OAuth v2.0 [IETF RFC 6749].	Las PHG pueden valerse de otros medios para obtener el testigo de autorización del servidor de autorización.
PHG-authorization_request	Las PHG pueden obtener un testigo de autorización del servidor de autorización, según se indica en los apartados 4.3 y 4.3.2 de OAuth v2.0 [IETF RFC 6749].	El Apéndice III contiene ejemplos de formatos de transferencia de solicitudes de autorización. Para la respuesta, véase la directriz HFS-authorization_request_response.
PHG-bearer_token	Las PHG **deberán** utilizar un testigo "portador", de conformidad con [IETF RFC 6750], cuando soliciten acceso a un recurso protegido del servicio de salud y aptitud física [IETF RFC 6750].	Véase la directriz conexa HFS – authorization_request_response.
PHG-Token_Transmit	Las PHG **deberán** utilizar el método de campo de encabezamiento de solicitud de autorización cuando envíen el testigo portador, según se indica en el apartado 2.1 de [IETF RFC 6750].	
PHG-Confidentiality	Las PHG **deberán** utilizar como mínimo la versión 1.1 del protocolo TLS en aras de la seguridad de la comunicación punto a punto con el servidor de autorización y el servicio de salud y aptitud física [IETF RFC 4346].	
PHG-Cipher	Las PHG **deberían** utilizar una serie de cifras de encriptación de TLS_RSA_WITH_AES_128_CBC_SHA.	

Cuadro B.2 – Directrices de seguridad para los servicios de salud y aptitud física que utilizan REST

Nombre	Descripción	Observaciones
HFS-authorization_request_response	Los servicios de salud y aptitud física que implementan el servidor de autorización **deberán** devolver el testigo de autorización de tipo "portador" después de validar la solicitud de testigo de acceso, según se indica en el apartado 4.3.3 de OAuth v2.0 [IETF RFC 6749].	Para el formato de las solicitudes, véase la directriz PHG-authorization_request. La autorización podría corresponder a una entidad independiente y no tiene por qué formar parte del servicio de salud y aptitud física.
HFS-refresh_token	Los servicios de salud y aptitud física que implementan el servidor de autorización **deberán** devolver el testigo de actualización.	
HFS-Token_Evaluation	Los servicios de salud y aptitud física **deberán** evaluar el testigo de autorización y su alcance antes de conceder acceso a un registro del servicio de salud y aptitud física.	

Cuadro B.3 – Directrices de seguridad para el transporte en la interfaz de servicios

Nombre	Descripción	Observaciones
HFS-Security_Transport	Las aplicaciones de los servicios de salud y aptitud física y las aplicaciones de las PHG **deberán** soportar, como mínimo, la versión 1.1 del protocolo TLS [IETF RFC 4346] de la versión 1.0 de WS-I BSP para ofrecer una comunicación segura.	Esta directriz es consistente con el perfil IHE ATNA cuando la encriptación está habilitada. Las directrices Continua dependen de la directriz de la versión 1.1 de TLS [IETF RFC 4346] para la autenticación mutua.
HFS-Security_Transport_Cipher	Las aplicaciones de los servicios de salud y aptitud física y las aplicaciones de las PHG **deberán** soportar el cifrado AES, según se indica en [IETF RFC 3268].	El perfil IHE ATNA requiere el uso opcional de la siguiente serie de cifrado: TLS_RSA_WITH_AES_128_CBC_SHA Las directrices HIS utilizan la siguiente serie de cifrado para la seguridad: TLS_RSA_WITH_AES_128_CBC_SHA Se permiten otras series de cifrado, no obstante, estas han de ser negociadas entre la PHG y el servicio de salud y aptitud física.

Cuadro B.3 – Directrices de seguridad para el transporte en la interfaz de servicios

Nombre	Descripción	Observaciones
HFS-Confidentiality	Los servicios de salud y aptitud física **deberán** utilizar la versión 1.1 del protocolo TLS para unas comunicaciones de punto a punto seguras con el servidor de autorización y el servicio de salud y aptitud física con cuestionario habilitado [IETF RFC 4346].	
HFS-Cipher	Los servicios de salud y aptitud física **deberían** soportar series de cifras de encriptación TLS_RSA_WITH_AES_128_CBC_SHA.	

Anexo C

Directrices normativas para la gestión del consentimiento

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

Cuadro C.1 – Directrices de gestión del consentimiento que utilizan REST para las PHG con consentimiento habilitado

Nombre	Descripción	Observaciones
PHG-Consent_Enabled	Las PHG con consentimiento habilitado deberán cumplir la norma de la directiva de consentimiento HL7 CDA R2 para la representación de las preferencias de consentimiento del paciente [HL7 CDA IG].	
PHG-Consent_Enabled_Transport_Standards	Las PHG con consentimiento habilitado deberán cumplir las siguientes normas de transporte: *HL7 Version 3 Specification: data Record Format, Release 1* [HL7 hRF] *OMG data REST Binding for RLUS* [OMG/data BIND] *OMG Retrieve, Locate, and Update Service (RLUS) Specification 1.0.1* [OMG/data RLUS]	
PHG-Post_Consent	Las PHG con consentimiento habilitado deberán utilizar HTTP POST con la siguiente URL para publicar el consentimiento en el servicio de salud y aptitud física: *baseURL/continua/consent*	Véase el caso de uso en el apartado 7.1. A fin de recuperar, localizar y actualizar los datos del servicio (RLUS) utilizando el transporte REST, se realiza una petición HTTP POST sin parámetros de consulta en esta
PHG-Post_Consent		URL con el documento de consentimiento de privacidad en el cuerpo de la petición.
Consent_Enabled-PHG-Observation_Association	Los documentos de consentimiento transmitidos por las PHG con consentimiento habilitado deberán contener el mismo identificador de paciente que el mensaje o mensajes de medición de observaciones de los servicios de salud y aptitud física.	El objetivo es asociar el documento de consentimiento a los mensajes de mediciones de observaciones de los servicios de salud y aptitud física.

Cuadro C.1 – Directrices de gestión del consentimiento que utilizan REST para las PHG con consentimiento habilitado

Nombre	Descripción	Observaciones
Consent_Enabled-PHG-Observation-Association_Value	El campo "identificador de paciente" (*Patient ID*) del encabezamiento del documento de consentimiento deberá tomar el valor PID-3. Lo subcampos CX-1 y CX-4 deberán estar presentes y el subcampo CX-5 no deberá estarlo.	
Consent_Enabled-PHG-Questionnaire Response_Confidentiality	Las PHG con consentimiento habilitado deberán fijar el valor del código de confidencialidad a "R" en el encabezamiento del documento de respuesta al cuestionario.	
Consent_Enabled-PHG-Questionnaire Response_Association_Value	Para asociar uno o varios documentos de respuesta a cuestionarios al documento de consentimiento del paciente, las PHG con consentimiento habilitado deberán utilizar el elemento de traducción del sistema del código de confidencialidad definido en el Cuadro IV.3.	Véanse los Cuadros IV.1, IV.2 y IV.4
Retrieving_Consent	Las PHG con consentimiento habilitado deberán utilizar HTTP GET con la siguiente URL para recuperar el consentimiento del servicio de salud y aptitud física: *baseURL/continua/consent* Las PHG con consentimiento habilitado deberán utilizar HTTP GET con el valor del elemento de enlace de la entrada de difusión Atom para recuperar el documento de consentimiento real del servicio de salud y aptitud física y deberán confirmar que es un documento de directiva de consentimiento HL7 CDA R2 [HL7 CDA IG] válido.	Véase el caso de uso en el apartado 7.1. A fin de recuperar, localizar y actualizar los datos del servicio (RLUS) utilizando el transporte REST, se realiza una petición HTTP GET sin parámetros de consulta en la URL que representa el trayecto de la sección de datos de consentimiento del paciente que devuelve la entrada de difusión Atom. Para más información sobre el elemento de entrada de difusión Atom, consúltese el Cuadro I.1.

Cuadro C.2 – Directrices de gestión del consentimiento que utilizan REST para los servicios de salud y aptitud física con consentimiento habilitado

Nombre	Descripción	Observaciones
Consent_Enabled-Health-&-Fitness-Service	Los servicios de salud y aptitud física con consentimiento habilitado deberán poder recuperar uno o varios documentos de consentimiento acordes a la directiva de consentimiento HL7 CDA R2 [HL7 CDA IG].	
Health-&-Fitness Service-Consent_Enabled_Transport_Standards	Las PHG con consentimiento habilitado deberán cumplir las siguientes normas de transporte: *HL7 Version 3 Specification: data Record Format, Release 1* [HL7 hRF] *OMG data REST Binding for RLUS* [OMG/data BIND] *OMG Retrieve, Locate, and Update Service (RLUS) Specification 1.0.1* [OMG/data RLUS]	
HFS-Consent_Root	Los servicios de salud y aptitud física con consentimiento habilitado deberán incluir los siguientes elementos en el contenido del cuestionario en root.xml: 1) Perfil (*profile*): a) id="consent" b) reference="http://handle.itu.int/11.1002/3000/hData/Consent/2017/01/H.812.pdf" 2) Sección (*section*): a) path="consent" b) profileID= "consent" c) resourceTypeId="consent" 3) Tipo de recurso (*resourceType*): a) resourceTypeId="consent" b) reference="http://www.hl7.org/dstucomments/showdetail.cfm?dstuid=63" c) representation d) mediaType="application/xml2	Nota: En la referencia 1.b figura una URL a título de ejemplo.
HFS-Consent_Validate	Los servicios de salud y aptitud física con consentimiento habilitado deberán verificar que el documento de consentimiento sea un documento de directiva de consentimiento HL7 CDA R2 válido y, en caso afirmativo, enviar HTTP 200 como respuesta.	
HFS-Post_Consent-Response	Una vez recibido el mensaje POST de la PHG con consentimiento habilitado, los servicios de salud y aptitud física con consentimiento habilitado deberán crear un registro de documentos de consentimiento y enviar HTTP 201 como respuesta.	Véase la *PHG-Post_Consent supra*.

Cuadro C.2 – Directrices de gestión del consentimiento que utilizan REST para los servicios de salud y aptitud física con consentimiento habilitado

Nombre	Descripción	Observaciones
PHG-Delete_Consent_Response	Los servicios de salud y aptitud física con consentimiento habilitado no deberán soportar la eliminación de un registro de documentos de consentimiento existente y deberán devolver HTTP 405 Method Not Allowed como respuesta a la petición HTTP DELETE en una URL de consentimiento.	

Cuadro C.3 – Directrices de observancia del consentimiento que utilizan datos para las PHG con consentimiento habilitado

Nombre	Descripción	Observaciones
Consent_Enabled-PHG-Content-Encryption_Actor	Las PHG con consentimiento habilitado deberán encriptar el contenido de acuerdo con el Perfil de Encriptación de Documentos (DEN) del IHE [IHE ITI DEN].	En este caso, el contenido podría ser la carga útil de la transacción PCD-01 o el documento de respuesta al cuestionario.
Consent_Enabled-PHG-Questionnaire-Response_MIMEtype_	Las PHG con consentimiento habilitado deberán fijar el tipo MIME a "application/xml" en los casos en que el contenido encriptado sea la respuesta al cuestionario.	El objetivo es indicar el tipo de carga útil encriptada.
Consent_Enabled-PHG-Observation-Upload_MIMEtype_	Las PHG con consentimiento habilitado deberán fijar el tipo de MIME a "application/txt" en los casos en que el contenido encriptado sea la carga de observaciones.	El objetivo es indicar el tipo de carga útil encriptada.
Consent_Enabled-PHG-Content-Encryption_Algorithm	Las PHG con consentimiento habilitado deberán utilizar AES-128 CBC para encriptar el contenido.	El algoritmo utilizado se identifica mediante el ContentEncryptionAlgorithmIdentifier en la norma de sintaxis de mensajes criptográficos (CMS), en cuyo perfil ahonda el IHE DEN.
Consent_Enabled-PHG-Encryption-Recipient_Binding_PKI	Las PHG con consentimiento habilitado deberán utilizar el método de gestión de claves PKI del perfil IHE DEN [IHE ITI DEN].	El método de gestión de clave PKI utiliza KeyTransRecipientInfo como RecipientInfoType de la CMS, lo que hace referencia a la clave pública o al certificado X.509 v3 del receptor.

Cuadro C.4 – Directrices de observancia del consentimiento que utilizan datos para los servicios de salud y aptitud física con consentimiento habilitado

Nombre	Descripción	Observaciones
HFS-Device_HTTP_Ack	Los servicios de salud y aptitud física con consentimiento habilitado deberán enviar HTTP 202 como respuesta tras recibir satisfactoriamente del contenido encriptado.	
Consent_Enabled-HFS-Content-Decryption_Actor_XDR	Los servicios de salud y aptitud física con consentimiento habilitado deberán ajustarse al perfil IHE DEN para desencriptar el contenido encriptado [IHE ITI DEN].	
Consent_EnabledKey_ Management	Los servicios de salud y aptitud física con consentimiento habilitado deberán utilizar el método de gestión de claves basado en PKI del perfil IHE DEN [IHE ITI DEN].	
Consent_Enabled-HFS-Decryption-Algorithm	Los servicios de salud y aptitud física con consentimiento habilitado deberán utilizar el algoritmo de desencriptación AES.128 CBC para desencriptar la carga útil.	El algoritmo utilizado se identifica mediante el *ContentEncryptionAlgorithmIdentifier* de la norma de sintaxis de mensajes criptográficos (CMS).
Consent_Enabled-HFS-Consent_Enforcement_	Los servicios de salud y aptitud física con consentimiento habilitado deberán observar las preferencias de consentimiento expresadas en el documento de consentimiento.	Ello impide, por ejemplo, que se siga revelando contenido a entidades no autorizadas.

Cuadro C.5 – Directrices de gestión del consentimiento que utilizan SOAP para las PHG con consentimiento habilitado

Nombre	Descripción	Observaciones
Services-Observation-PHG-Consent	Las PHG de observación de servicios con consentimiento habilitado **deberán** cumplir la directiva de consentimiento [HL7 CDA IG] para representar el consentimiento del paciente en un documento de consentimiento.	
Services-Observation-PHG-Consent-Transport	Las PHG de observación de servicios con consentimiento habilitado **deberán** implementar el agente fuente de documento del IHE XDR para enviar un documento de consentimiento utilizando la transacción ITI-41 Conjunto-b de provisión y registro de documento (*Provider and Register document Set-b*).	

Cuadro C.5 – Directrices de gestión del consentimiento que utilizan SOAP para las PHG con consentimiento habilitado

Nombre	Descripción	Observaciones
Services-Observation-PHG-Consent-Frequency	Las PHG de observación de servicios con consentimiento habilitado **deberán** enviar el documento de consentimiento al menos una vez al servicio de salud y aptitud física de observación.	Por ejemplo, el documento de consentimiento podría enviarse al efectuar el registro en el servicio. Es recomendable enviar el consentimiento al menos una vez durante la vida de la conexión al servicio de salud y aptitud física de observación. El documento también soporta casos de uso, tales como la actualización de las preferencias de consentimiento.
Services-Observation-PHG-Consent-Frequency		El documento de consentimiento actualizado sustituye al existente en el servicio de salud y aptitud física de observación.
HFS-Observation_Measurement_Consent_Document_Association	El documento de consentimiento transmitido por las PHG de observación de servicios con consentimiento habilitado **deberá** incluir el mismo identificador de paciente que el mensaje o mensajes de medición de observaciones de servicios.	El objetivo es asociar el documento de consentimiento a los mensajes de mediciones de observaciones de los servicios de salud y aptitud física.
HFS-Observation_Measurement_Consent_Document_Association_Value	El campo "identificador de paciente" (*Patient ID*) del encabezamiento del documento de consentimiento **deberá** tomar el valor PID-3. Lo subcampos CX-1 y CX-4 **deberán** estar presentes y el subcampo CX-5 **no deberá** estarlo.	

Cuadro C.6 – Directrices de gestión del consentimiento que utilizan SOAP para los servicios de salud y aptitud física con consentimiento habilitado

Nombre	Descripción	Observaciones
Observation-Health-&-Fitness-Service-Consent	Los servicios de salud y aptitud física de observación con consentimiento habilitado **deberán** poder recibir el documento o documentos de consentimiento de la directiva de consentimiento [HL7 CDA IG].	
Observation-HFS-Consent_Transport	Los servicios de salud y aptitud física de observación con consentimiento habilitado **deberán** implementar el agente receptor de documentos del IHE XDR para recibir un documento de consentimiento utilizando la transacción ITI-41 Conjunto-b de provisión y registro de documento (*Provider and Register document Set-b*).	Los servicios de salud y aptitud física de observación sustituyen el documento de consentimiento existente si reciben una nueva versión, conforme a lo indicado en los metadatos XDS del documento de consentimiento.

Cuadro C.7 – Directrices de observancia del consentimiento que utilizan SOAP para las PHG con consentimiento habilitado

Nombre	Descripción	Observaciones
HFS-PHG-Content_Encryption_Actor	Las PHG de observación de los servicios de salud y aptitud física con consentimiento habilitado **deberán** encriptar la carga útil (Anexo D a [UIT-T H.812.1]) de la transacción PCD-01 de conformidad con las reglas de procesamiento de encriptación definidas en el apartado 4.1 de la especificación de encriptación de XML [W3C XMLENC]	
HFS-PHG-Content_Encryption_MIMEtype	Las PHG de observación de los servicios de salud y aptitud física con consentimiento habilitado **deberán** fijar el tipo de MIME a "application/hl7-v2+xml"	El objetivo es indicar el tipo de carga útil encriptada.
HFS-Services-PHG-Content_Encryption_Algorithm	Las PHG de observación de los servicios de salud y aptitud física con consentimiento habilitado **deberán** usar el algoritmo de encriptación de carga útil AES-128 CBC incluido en la especificación de encriptación XML.	El algoritmo AES-128 CBC se identifica mediante el siguiente identificador: http://www.w3.org/2001/04/xmlenc#aes128-cbc [W3C XMLENC]

Cuadro C.7 – Directrices de observancia del consentimiento que utilizan SOAP para las PHG con consentimiento habilitado

Nombre	Descripción	Observaciones
HFS-PHG-Encryption_Recipient_Binding_PKI	Para el transporte de la clave de contenidos, las PHG de observación de los servicios de salud y aptitud física con consentimiento habilitado **deberán** soportar la versión 1.5 del algoritmo RSA icnluido en la especificación de encriptación XML.	El transporte de claves basado en la versión 1.5 de RSA se identifica mediante el siguiente identificador [W3C XMLENC]: http://www.w3.org/2001/04/xmlenc#rsa-1_5. Para obtener información detallada sobre la versión 1.5 del algoritmo RSA, consúltese [b-RFC 2437]. El transporte de claves basado la versión 1.5 de RSA también se utiliza en la norma de sintaxis de mensajes criptográficos (CMS) aplicada en la HRN-IF. Para más información, véase [b-RFC 3370] y las directrices sobre la observancia del consentimiento para la HRN-IF.
HFS-PHG-Encryption_Recipient_Binding_Symmetric	Para el transporte de la clave de contenido, las PHG de observación de los servicios de salud y aptitud física con consentimiento habilitado **deberían** utilizar el algoritmo de encriptación de clave (key wrap) simétrica AES-128 de la especificación de encriptación XML. En caso de encriptación basada en contraseña, las PHG de observación de los servicios de salud y aptitud física con consentimiento habilitado **podrían** utilizar PBKDF2 como algoritmo de derivación de claves de [IETF RFC 3211].	El identificador utilizado para la encriptación de clave simétrica AES-128 es: http://www.w3.org/2001/04/xmlenc#kw-aes128 [W3C XMLENC]. La clave utilizada para la encriptación de claves se denomina KEK y puede obtenerse a partir de una contraseña o de una clave secreta compartida a largo plazo.
HFS-PHG-Integrity_Payload_PCD-01_Create	Las PHG de observación de los servicios de salud y aptitud física con consentimiento habilitado **deberán** calcular el resumen (digest) de la carga útil encriptada utilizando el algoritmo SHA256 (apartado 5.7.2), de conformidad con la especificación de encriptación XML.	El algoritmo SHA256 se identifica mediante la siguiente URL: http://www.w3.org/2001/04/xmlenc#sha256 [W3C XMLENC].

Cuadro C.7 – Directrices de observancia del consentimiento que utilizan SOAP para las PHG con consentimiento habilitado

Nombre	Descripción	Observaciones
HFS-Encrypted_Payload_PCD-01_transaction	Las PHG de observación de los servicios de salud y aptitud física con consentimiento habilitado **deberán** cifrar con una clave la carga útil encriptada dentro del elemento <CommunicateEncPCDData xmlns= "urn:ihe:continua:enc:pcd:dec:2012">	Si la carga útil no está encriptada, el contenido es cifrado con clave en el elemento <CommunicatePCDData xmlns="urn:ihe:pcd:dec: 2010">. Véase el ejemplo de la Figura II.1
HFS-Encrypted_Payload_PCD-01_Transaction_Header	Si la carga útil está encriptada, el encabezamiento SOAP **deberá** contener "urn:ihe:continua:enc:pcd:dec:2012:CommunicateEncPCDData" en lugar de "urn:ihe: pcd:dec:2010: CommunicatePCDData".	La transacción PCD-01 simple contiene "urn:ihe: pcd:dec:2010:CommunicatePCDData". Véanse los ejemplos de las Figuras II.1, II.2 y II.3.

Cuadro C.8 – Directrices de observancia del consentimiento que utilizan SOAP para los servicios de salud y aptitud física con consentimiento habilitado

Nombre	Descripción	Observaciones
HFS-HTTP-Ack	Los servicios de salud y aptitud física de observación con consentimiento habilitado **deberán** enviar la respuesta HTTP SOAP con el código de estado 202 tras recibir correctamente el mensaje encriptado. Los servicios de salud y aptitud física de observación con consentimiento habilitado **no deberían** enviar el acuse de recibo a nivel de aplicación PCD-01.	Ello se debe a que el servicio de salud y aptitud física de observación puede no disponer de la clave de desencriptación, ya que el contenido puede haber sido encriptado para un destinatario específico en dicho servicio.
HFS-Payload-PCD-01-Verify-Integrity	Los servicios de salud y aptitud física de observación con consentimiento habilitado **deberán** verificar el resumen del mensaje de la carga útil encriptada.	
HFS-Payload-PCD-01-Verify-Integrity-Algorithm	Los servicios de salud y aptitud física de observación con consentimiento habilitado **deberán** soportar el algoritmo SHA256.	
HFS-Content-Decryption-Actor	Los servicios de salud y aptitud física de observación con consentimiento habilitado **deberán** cumplir las normas de desencriptación especificadas en el apartado 4.2 de la especificación de encriptación de XML [W3C XMLENC].	
HFS-Key-Transport-RSA	Los servicios de salud y aptitud física de observación con consentimiento habilitado **deberán** soportar la versión 1.5 de RSA de la especificación de encriptación de XML [W3C XMLENC].	

Cuadro C.8 – Directrices de observancia del consentimiento que utilizan SOAP para los servicios de salud y aptitud física con consentimiento habilitado

Nombre	Descripción	Observaciones
HFS-Key-Transport-Symmetric	Los servicios de salud y aptitud física de observación con consentimiento habilitado **deberán** soportar el algoritmo de encriptación de clave simétrico AES-128 de la especificación de encriptación de XML [W3C XMLENC]. Los servicios de salud y aptitud física de observación con consentimiento habilitado **deberán** soportar PBKDF2 como algoritmo de derivación de claves de [IETF RFC 3211].	El identificador utilizado para la encriptación simétrica de clave AES-128 es: http://www.w3.org/2001/04/xmlenc#kw-aes128 [W3C XMLENC]. La clave utilizada para la encriptación de la clave se denomina KEK y puede obtenerse a partir de una contraseña o de una clave secreta compartida a largo plazo.
HFS-Content-Decryption-Algorithm	Los servicios de salud y aptitud física de observación con consentimiento habilitado **deberán** utilizar el algoritmo de desencriptación AES-128 CBC de la especificación de encriptación de XML [W3C XMLENC].	El algoritmo AES-128 CBC se identifica mediante el siguiente identificador: http://www.w3.org/2001/04/xmlenc#aes128-cbc [W3C XMLENC].

Apéndice I

Elementos de difusión en formato Atom para la gestión del consentimiento

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

A los siguientes elementos secundarios de difusión en formato Atom del elemento de entrada se les confiere un uso específico a efectos de los documentos de consentimiento.

Cuadro I.1 – Elementos secundarios de difusión Atom para la gestión del consentimiento

Elemento	Utilización
Autor	Constructo de persona que indica quién proporcionó la información en el documento de consentimiento, es decir, quién lo cumplimentó.
Título	Título del documento de consentimiento del paciente (por ejemplo, autorización de consentimiento de Adam).
Enlace	Referencia al documento de directiva de consentimiento de Adam, que deberá ser un documento de directiva de consentimiento HL7 CDAR2 válido. El enlace deberá ser relativo y el documento de consentimiento de privacidad deberá hallarse en la sección de consentimiento del registro de datos.
Publicado	El elemento publicado deberá ajustarse a la fecha y hora en que se publicó el documento de consentimiento de privacidad en el servidor.

I.1 Información para el consentimiento en root.xml

```
<profile>
   <id>consent</id>

<reference><http://handle.itu.int/11.1002/3000/hData/Consent/2017/01/H.812.pdf></reference>
</profile>
<section>
  <path>consent</path>
  <profileID>consentId</profileID>
  <resourceTypeID>consent</resourceTypeID>
</section>
<resourceType>
  <resourceTypeID>consent</resourceTypeID>
  <reference>
    http://www.hl7.org/dstucomments/showdetail.cfm?dstuid=63
  </reference>
  <representation>
     <mediaType>application/xml</mediaType>
  </representation>
</resourceType>
```

Apéndice II

Ejemplos de gestión de consentimiento con SOAP

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

```
<html version="1.0" encoding="UTF-8" ?>
<soapenv:Envelope xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope">
   <soapenv:Header xmlns:wsa="http://www.w3.org/2005/08/addressing" >
      <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd"
soapenv:mustUnderstand="true" >
      <wsa:To
soapenv:mustUnderstand="true">
https://localhost:8443/WanReceiver/services/DeviceObservationConsumer_Service>/wsa:To>
      <wsa:ReplyTo soapenv:mustUnderstand="true">
         <wsa:Address>http://www.w3.org/2005/08/addressing/anonymous</wsa:Address>
      </wsa:ReplyTo>
      <wsa:MessageID
soapenv:mustUnderstand="true">urn:uuid:BC4B55779CD53E3F0C1333967505413</wsa:MessageID>
      <wsa:Action soapenv:mustUnderstand="true">urn:ihe:pcd:2010:CommunicatePCDData</wsa:Action>
      </soapenv:Header>
      <soapenv:Body>
         <CommunicatePCDData xmls="urn:ihe:pcd:dec:2010">
            MSH|^~\&|AT4_PHG^123456789ABCDEF^EUI-
            64|||20120409103145+0000||ORU^R01^ORU_R01|MSGID2848518|P|2.6|||NE|AL|||||IHE PCD ORU-
            R012006^HL7^2.16.840.1.113883.9.n.m^HL7 PID|||789567^^^Imaginary
            Hospital^PI||Doe^John^Joseph^^^^L
            OBR|1|POTest^AT4_PHG^1234567890ABCDEF^EUI-64|POTest^AT4_PHG*1234567890ABCDEF^EUI-
            64|182777000^monitoring of patient^SNOMED-CT|||20100903124015+0000
            OBX|1|CWE|68220^MDC_TIME_SYNC_PROTOCOL^MDC|0.0.0.1|532224^MDC_Time_SYNC_NONE^MDC||||||
            R
            OBX|2|CWE|68220^MDC_REG_CERT_DATA_AUTH_BODY^MDC|0.0.0.2|1^auth-body-continua(2)||||||R
            OBX|3|ST|588800^MDC_REG_CERT_DATA_CONTINUA_VERSION^MDC|0.0.0.3|1.5||||||R
            OBX|4||528388^MDC_DEV_SPEC_PROFILE_PULS_OXIM^MDC|1||||||X||||||1234567890ABCDEF^EUI-64
            OBX|5|ST|531696^MDC_ID_MODEL_NUMBER^MDC|PulseOx v1.5||||||R
            OBX|6|ST|531970^MDC_ID_MANUFACTURER^MDC|1.0.0.2|AT4 Wireless||||||R
            OBX|7|DTM|67975|^MDC_ATTR_TIME_ABS^MDC|1.0.0.3|20100903124015+0000||||||R2010090312401
            5+0000
            OBX|8|CWE|68218^MDC_CERT_DATA_AUTH_BODY^MDC|1.0.0.4|1^auth-body-continua(2)||||||R
            OBX|9|ST|588800^MDC_REG_CERT_DATA_CONTINUA_VERSION^MDC|1.0.0.5||||||R
            OBX|10|NA|588801^MDC_REG_CERT_DATA_CONTINUA_CERT_DEV_LIST^MDC|1.0.0.6|16388||||||R
            OBX|11|CWE|588802^MDC_REG_CERT_DATA_CONTINUA_REG_STATUS^MDC|1.0.0.7|0^unregulated-
            device(0)||||||R
            OBX|12|NM|150456^MDC_DIM_PERCENT^MDC|||||R|||20100903124015+0000
            OBX|13|NM|149520^MDC_PULS_OXIM_RATE^MDC|1.0.0.9|71|264864^MDC_DIM_BEAT_PER_MIN^MDC||||
            |R|||20100903124015+0000
         </soapenv:Body>
      </soapenv:Envelop>
```

Figura II.1 – Transacción PCD-01 con carga útil no encriptada

```
<html version="1.0" encoding="UTF-8" ?>
<soapenv:Envelope xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope">
   <soapenv:Header xmlns:wsa="http://www.w3.org/2005/08/addressing" >
      <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd"
   soapenv:mustUnderstand="true">
<wsa:To
soapenv:mustUnderstand="true"
>https://localhost:8443/WanReceiver/services/DeviceObservationConsumer_Services/DeviceObservationC
onsumer_Service</wsa:To>
      <wsa:ReplyTo soapenv:mustUnderstand="true">
         <wsa:Address>http://www.w3.org/2005/08/addressing/anonymous</wsa:Address>
      </wsa:ReplyTo>
      <wsa:MessageID
soapenv:mustUnderstand="true">urn:uuid:BC4B55779CD53E3F0C1333967505413</wsa:MessageID>
      <wsa:Action soapenv:mustUnderstand="true">urn:ihe:pcd:2010:CommunicatePCDData</wsa:Action>
      </soapenv:Header>
      <soapenv:Body>
         <CommunicateEncPCDData xmlns="urn:ihe:continuacenc:pcd:dec:2012">
<EncryptedData xmlns=http://www.w3.org/2001/04/xmlenc#    MimeType="applicationhl7-v2+xml">
      <EncryptionMethod Algorithm=http://www.w3.org/2001/04/xmlenc#aes128-cbc/>
      <KeyInfo xmlns+"http://www.w3.org/2000/09/xmldsig#">
            <EncryptedKey xmlns=http://www.w3.org/2001/04/xmlenc#">
<Encryption Method Algorithm=http://www.w3.org/2001/04/xmlenc#rsa-1_5/>
                     <KeyInfo xmlns=http://www.w3.org/2000/09/xmldsig#>
                        <KeyName>John Smith</KeyName>
                     </KeyInfo>
                     <CipherData>
                        <CipherValue>Encrypted Key…</CipherValue>
                     </CipherData>
                  </EncryptedKey>
            </KeyInfo>
            <CipherData>
                     <CipherValu>Enc.OBX Message goes here…</CipherValue>
            </CipherData>
            </EncrptedData>
         </CommunicateEncPCDData>
      </soapenv:Body>
   </soapenv:Envelop>
```

Figura II.2 – Transacción PCD-01 encriptada – con clave pública

La Figura II.2 ilustra una transacción PCD-01 cuya carga útil ha sido encriptada utilizando la norma de encriptación de XML. La clave del contenido se encripta con la clave pública del receptor.

```
<html version=”1.0” encoding=”UTF-8” ?>
<soapenv:Envelope xmlns:soapenv=”http://www.w3.org/2003/05/soap-envelope”>
   <soapenv:Header xmlns:wsa=”http://www.w3.org/2005/08/addressing” >
      <wsse:Security xmlns:wsse=”http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd”
   soapenv:mustUnderstand=”true”>
<wsa:To
soapenv:mustUnderstand=”true”
>https://localhost:8443/WanReceiver/services/DeviceObservationConsumer_Services/DeviceObservationC
onsumer_Service</wsa:To>
      <wsa:ReplyTo soapenv:mustUnderstand=”true”>
         <wsa:Address>http://www.w3.org/2005/08/addressing/anonymous</wsa:Address>
      </wsa:ReplyTo>
      <wsa:MessageID
soapenv:mustUnderstand=”true”>urn:uuid:BC4B55779CD53E3F0C1333967505413</wsa:MessageID>
      <wsa:Action soapenv:mustUnderstand=”true”>urn:ihe:pcd:2010:CommunicatePCDData</wsa:Action>
      </soapenv:Header>
      <soapenv:Body>
         <CommunicateEncPCDData xmlns=”urn:ihe:continuacenc:pcd:dec:2012”>
<EncryptedData xmlns=http://www.w3.org/2001/04/xmlenc#    MimeType=”applicationhl7-v2+xml”>
      <EncryptionMethod Algorithm=http://www.w3.org/2001/04/xmlenc#aes128-cbc/>
      <KeyInfo xmlns+”http://www.w3.org/2000/09/xmldsig#”>
            <EncryptedKey xmlns=http://www.w3.org/2001/04/xmlenc#”>
<Encryption Method Algorithm=http://www.w3.org/2001/04/xmlenc #rsa-1_5/>
                     <KeyInfo xmlns=http://www.w3.org/2000/09/xmldsig#>
                        <KeyName>John Smith</KeyName>
                     </KeyInfo>
                     <CipherData>
                        <CipherValue>Encrypted Key…</CipherValue>
                     </CipherData>
                  </EncryptedKey>
            </KeyInfo>
            <CipherData>
                     <CipherValu>Enc.OBX Message goes here…</CipherValue>
            </CipherData>
            </EncrptedData>
         </CommunicateEncPCDData>
      </soapenv:Body>
   </soapenv:Envelop>
```

Figura II.3 – Transacción PCD-01 encriptada – con clave simétrica

La Figura II.3 ilustra una transacción PCD-01 cuya carga útil ha sido encriptada utilizando la norma de encriptación de XML. En este ejemplo se asume que tanto el emisor como el receptor conocen la clave del contenido, que es sólo de lectura.

Apéndice III

Ejemplo de OAuth

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

Ejemplo 1:

– Solicitud de testigo de acceso

A fin de obtener un testigo de acceso, una PHG con cuestionario habilitado realiza la solicitud HTTP POST infra al servidor de autorización.

```
POST http://localhost:3000/oauth2/token HTTP/1.1
User-Agent: Fiddler
Host: localhost:3000
Authorization: Basic
MTIwMDk0NTc0NjczNzY3OmI1NGRjODI0NzZhZjI4MTRlNjIwYjg2Nzc2YzQyYzBl
Content-Type: application/x-www-form-urlencoded
Content-Length: 59

grant_type=password&username=john@example.com&password=test
```

Donde:

– http://localhost:3000/oauth2/token es la URL para llegar al servidor de autorización y debe hallarse en conocimiento de la PHG con cuestionario habilitado.

– Authorization: Basic MTIwMDk0NTc0NjczNzY3OmI1NGRjODI0NzZhZjI4MTRlNjIwYjg2Nzc2YzQyYzBl

– Se trata de una cabecera de autorización HTTP básica, que la PHG con cuestionario habilitado genera codificando su identificador dado y su palabra secreta en una cadena de troceo Base64: Base64("120094574673767:b54dc82476af2814e620b86776c42c0e") =

– "MTIwMDk0NTc0NjczNzY3OmI1NGRjODI0NzZhZjI4MTRlNjIwYjg2Nzc2YzQyYzBl"

– grant_type indica el código de autorización. Este código de autorización comprende el nombre de usuario y la contraseña.

– Respuesta del testigo de acceso.

El servidor de autorización verifica la solicitud de testigo de acceso y, de autorizarla, genera un testigo de acceso de tipo "portador" y un testigo de actualización opcional.

```
HTTP/1.1 200 OK
Content-Length: 141
Content-Type: application/json
X-Ua-Compatible: IE=Edge
X-Runtime: 0.273027
Server: WEBrick/1.3.1 (Ruby/1.9.3/2013-02-22)
Date: Wed, 03 Apr 2013 08:54:57 GMT
Connection: Keep-Alive

{"access_token":"f779da766bfd1b9164b0fd6d280d52f1","refresh_token":"789f3daf81
a302e0636325114113e4b4","token_type":"bearer","expires_in":899}
```

Donde:

– "f779da766bfd1b9164b0fd6d280d52f1" es el testigo de acceso que la PHG utilizaría para acceder a un recurso en el servidor.
– "789f3daf81a302e0636325114113e4b4" es un testigo de actualización que puede utilizarse para obtener un nuevo testigo.
– En el ejemplo anterior, el testigo es de tipo "portador".
– La vida útil del testigo es de 899 segundos.
– Se solicita un recurso mediante un testigo de acceso de tipo "portador".

Ejemplo 2:

En el siguiente ejemplo, la PHG utiliza un testigo portador para solicitar un recurso protegido, por ejemplo, el cuestionario.

```
GET http://localhost:3000/hdata/root.xml HTTP/1.1
User-Agent: Fiddler
Host: localhost:3000
Authorization: Bearer f779da766bfd1b9164b0fd6d280d52f1
```

Apéndice IV

Asociación de respuesta al cuestionario de la PHG con consentimiento habilitado

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

Cuadro IV.1 – Elementos del sistema de código de confidencialidad

Nombre	Valor	Observaciones
Code	"R"	
codeSystem	2.16.840.1.113883.5.25	
codeSystemName	"Confidentiality"	
displayName	"Restricted"	

Cuadro IV.2 – Elementos del sistema de código de la directiva de consentimiento Continua

Nombre	Valor	Observaciones
Code	El valor **deberá** ser igual al especificado en [HL7 CDA IG].	
codeSystem	2.16.840.1.113883.3.1817.1.2.1	
codeSystemName	"Continua Consent Directive"	
displayName	ID del documento de consentimiento	

Cuadro IV.3 – Traducción del sistema de código de confidencialidad al sistema de código de la directiva de consentimiento Continua

Nombre	Valor	Observaciones
Code	"R"	
codeSystem	2.16.840.1.113883.5.25	
codeSystemName	"Confidentiality"	
displayName	"Restricted"	
translation	code="<ID of the consent document>" codeSystem=2.16.840.1.113883.3.1817.1.2.1 codeSystemName="Continua Consent Directive" displayName=ID of the consent document	En "<>" se ubica el ID del documento de consentimiento. Véanse los elementos del sistema de código de la directiva de consentimiento Continua en el Cuadro IV.2.

Cuadro IV.4– Distribución OID para la Alianza Continua para la salud personal conectada

OID	Descripción	Observaciones
2.16.840.1.113883.3.1817	OID de la organización: Alianza para la salud personal conectada	
2.16.840.1.113883.3.1817.1	OID raíz para la Arquitectura E2E Continua V1.0	
2.16.840.1.113883.3.1817.1.2	OID raíz para la privacidad y seguridad E2E	
2.16.840.1.113883.3.1817.1.3	OID raíz para la interfaz del dispositivo de salud personal	

Cuadro IV.4– Distribución OID para la Alianza Continua para la salud personal conectada

OID	Descripción	Observaciones
2.16.840.1.113883.3.1817.1.4	OID raíz para la interfaz del dispositivo de salud personal ZigBee	
2.16.840.1.113883.3.1817.1.5	OID raíz para la interfaz del dispositivo de salud personal NFC	
2.16.840.1.113883.3.1817.1.6	OID raíz para la interfaz de servicios	
2.16.840.1.113883.3.1817.1.7	OID raíz para la interfaz HIS	
2.16.840.1.113883.3.1817.1.2.1	Seguridad y privacidad E2E: OID del sistema de código de la directiva de consentimiento Continua	

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, 2019