International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

H.812

(07/2016)

SERIES H: AUDIOVISUAL AND MULTIMEDIA SYSTEMS

E-health multimedia services and applications – Personal health systems

Interoperability design guidelines for personal health systems: Services interface: Common certified capability class

Recommendation ITU-T H.812

ITU-T H-SERIES RECOMMENDATIONS

AUDIOVISUAL AND MULTIMEDIA SYSTEMS

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

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

Recommendation ITU-T H.812

Interoperability design guidelines for personal health systems: Services interface: Common certified capability class

Summary

The Continua Design Guidelines (CDG) defines a framework of underlying standards and criteria that ensure the interoperability of devices and data used for personal connected health services.

Recommendation ITU-T H.812 contains an overview of the Services interface (Services-IF), common design guidelines for all Services-IF Certified Capability Classes (CCC) and the design guidelines for Consent Enabled Personal Health Gateway (PHG) and Services CCCs.

The design guidelines which support the following Certified Capability Classes (CCC) are defined in separate Recommendations, as follows:

– Observation Upload capability in [ITU-T H.812.1]

– Questionnaires capability in [ITU-T H.812.2]

– Capability Exchange capability in [ITU-T H.812.3]

– Authenticated Persistent Session capability in [ITU-T H.812.4]

Recommendation ITU-T H.812 is part of the "ITU-T H.810 interoperability design guidelines for personal connected health systems" subseries that covers the following areas:

– ITU-T H.810 – Interoperability design guidelines for personal connected health systems: System overview

– ITU-T H.811 – Interoperability design guidelines for personal connected health systems: Personal Health Devices interface design guidelines

– ITU-T H.812 – Interoperability design guidelines for personal connected health systems: Services interface design guidelines

– ITU-T H.812.1 – Interoperability design guidelines for personal connected health systems: Services interface: Observation Upload capability

– ITU-T H.812.2 – Interoperability design guidelines for personal connected health systems: Services interface: Questionnaires capability

– ITU-T H.812.3 – Interoperability design guidelines for personal connected health systems: Services interface: Capability Exchange capability

– ITU-T H.812.4 – Interoperability design guidelines for personal connected health systems: Services interface: Authenticated Persistent Session capability

– ITU-T H.813 – Interoperability design guidelines for personal connected health systems: Healthcare Information System interface design guidelines

History

Edition	Recommendation	Approval	Study Group	Unique ID*
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

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

FOREWORD

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

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

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

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

NOTE

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

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

INTELLECTUAL PROPERTY RIGHTS

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

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

Table of Contents

Page

Page

List of Tables

Page

List of Figures

Page

0 Introduction

The Continua Design Guidelines (CDG) defines a framework of underlying standards and criteria that ensure the interoperability of devices and data used for personal connected health services.

This Recommendation contains additional design guidelines (DGs) for interoperability that further clarify or reduce the options or add features missing from underlying standards or specifications.

This Recommendation contains a Services-IF overview, common design guidelines for all Services-IF Certified Capability Classes (CCC) and the design guidelines for Consent Enabled Personal Health Gateway (PHG) and Health and Fitness Service CCCs.

The design guidelines which support the following Certified Capability Classes (CCC) are defined in separate Recommendations as follows:

– [ITU-T H.812.1] *Interoperability design guidelines for personal health systems: Services interface: Observation upload certified capability class.*

– [ITU-T H.812.2] *Interoperability design guidelines for personal health systems: Services interface: Questionnaires.*

– [ITU-T H.812.3] *Interoperability design guidelines for personal health systems: Services interface:Capability exchange certified capability class.*

– [ITU-T H.812.4] *Interoperability design guidelines for personal health systems: Services interface: Authenticated persistent session capability.*

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

0.1 Organization

This Recommendation is organized in the following manner.

Clauses 0-5: Introduction and terminology – These clauses provide Services-IF specific information to help understand the structure of the design specifications.

Clause 6: Services-IF overview – This clause provides an overview of the Services-IF CCCs.

Clause 7: Use cases – This clause provides practical examples.

Clause 8: Behavioural model – This clause provides an overview of sequences of interactions under Services interface common CCCs and summarizes typical interactions, constraints and exceptions.

Clause 9: Implementation – This clause details the use of common payload content and simple object access protocol (SOAP) vs representational state transfer (REST) based transport methodology in the common Services-IF Certified Capability Classes.

0.2 Guideline releases and versioning

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

0.3 What's new

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

Recommendation ITU-T H.812

Interoperability design guidelines for personal health systems: Services interface: Common certified capability class

1 Scope

This Recommendation focuses on the following interface:

– **Services-IF** The interface between a personal health gateway (PHG) and Services.

This interface is defined in the Continua architecture as described in clause 6 of [ITU-T H.810] and is shown in Figure 1-1.

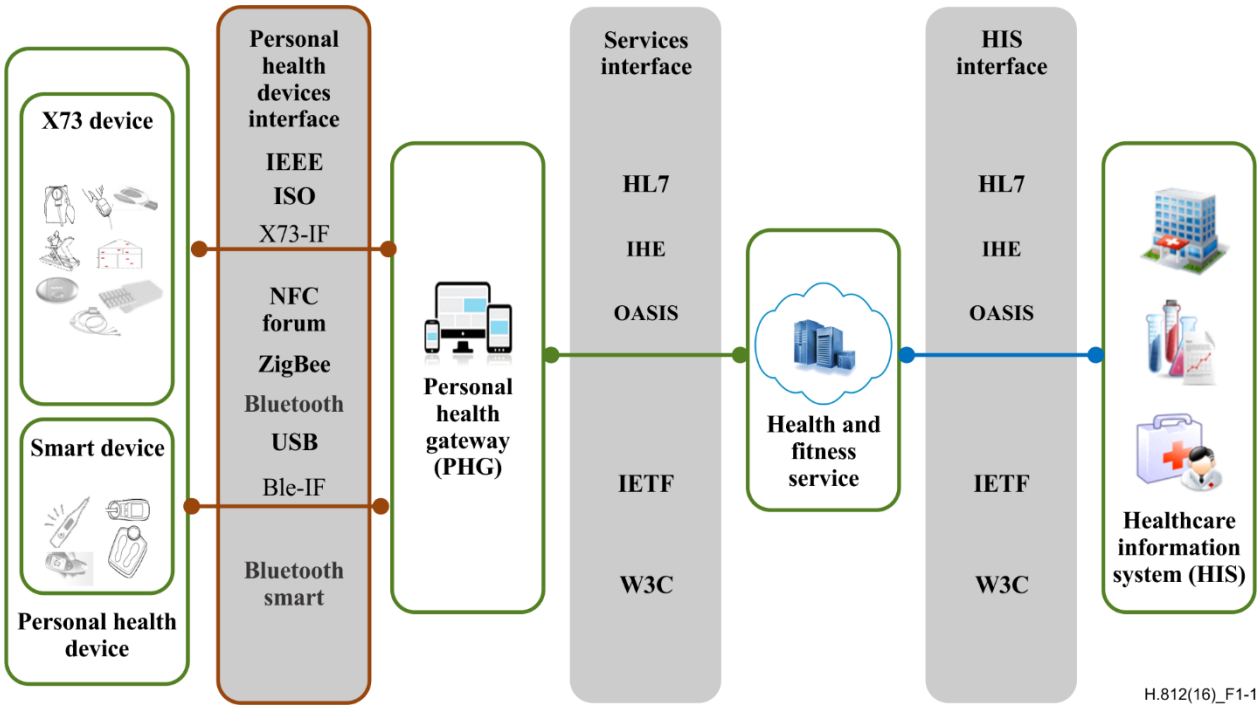

Figure 1-1 – Services interface in the Continua architecture

There are a number of Certified Capability Classes (CCCs) related to the Services-IF. This Recommendation contains interoperability design guidelines that are applicable to several CCCs. Security interoperability design guidelines are one such example. In addition, this Recommendation contains the design guidelines for the Consent Enabled PHG and Services interface CCCs. These CCCs may be grouped with multiple other Services-IF related CCCs, such as for example, Services Observation Upload CCCs or Questionnaire enabled CCCs.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T H.810] Recommendation ITU-T H.810 (2016), *Interoperability design guidelines for personal health systems*.

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

3 Definitions

This Recommendation uses terms defined in [ITU-T H.810].

4 Abbreviations and acronyms

This Recommendation uses abbreviations and acronyms defined in [ITU-T H.810].

5 Conventions

This Recommendation follows the conventions defined in [ITU-T H.810].

6 Architecture

In this end-to-end (E2E) reference architecture, the Services interface (Services-IF) connects a personal health gateway (PHG) to a health and fitness service. Figure 6-1 shows the Services interface in the Continua E2E architecture and Figure 6-2 shows an example of a Services-IF.

The Services-IF design guidelines are focused on enabling the interoperable exchange of information across a Services interface. A set of Services-IF related Certified Capability Classes is defined for the PHG and the health and fitness service to enable interoperability for a number of different use cases, including the uploading of measurement data, completing of questionnaires and executing of commands.

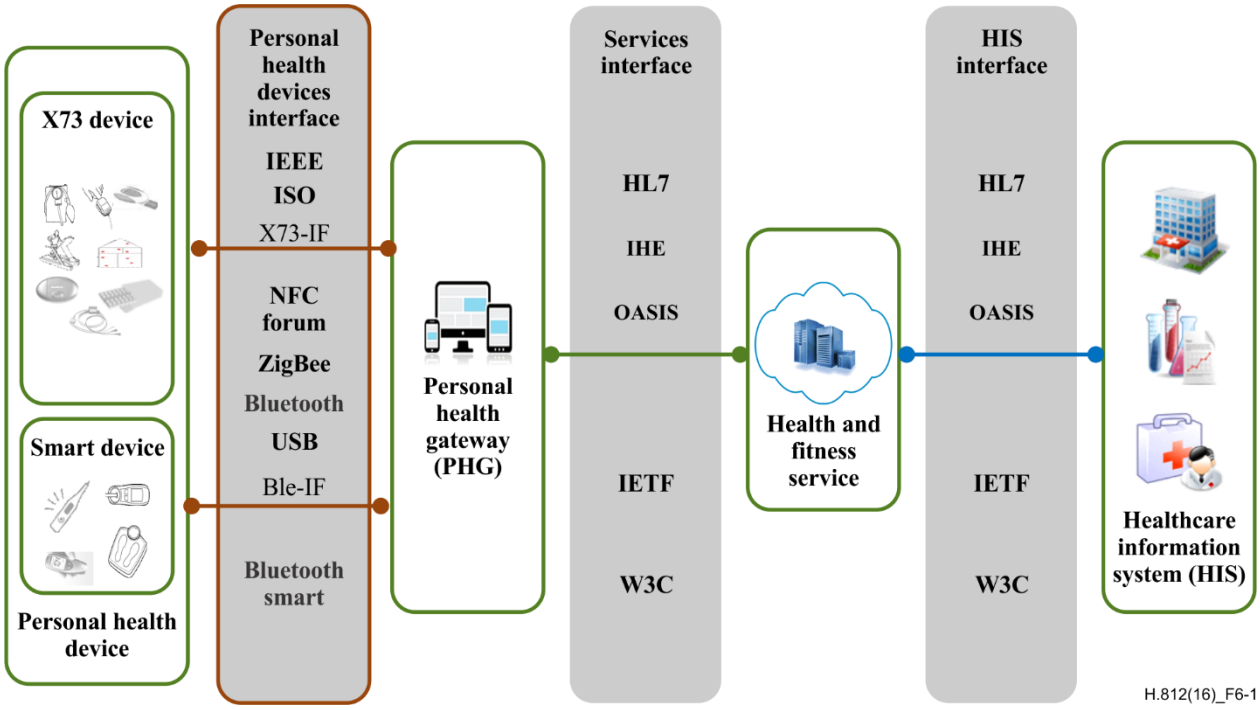

Figure 6-1 – Services interface in the Continua E2E architecture

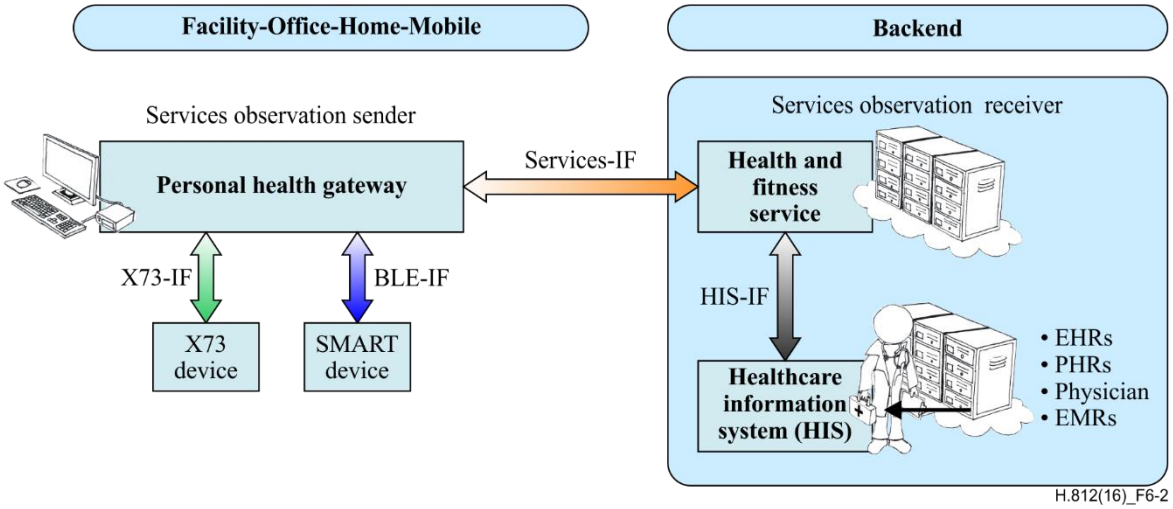

Figure 6-2 – Services-IF example

In addition to the Services-IF, the end-to-end reference architecture also defines the healthcare information system interface (HIS-IF). The Services-IF is designed to enable granular information exchange between a PHG (typically a PC, laptop, tablet, mobile phone or other type of embedded device), which is a device close to the user/patient and a health and fitness service (typically a backend cloud based service) which collects the information from such users and makes it available for further usage. In contrast the HIS-IF is designed to enable aggregated information exchange between two backend systems, e.g., a disease management system and an electronic health record (EHR)[1]. The HIS-IF is defined in [ITU-T H.813].

It is also expected that a PHG may be deployed to in-home or user-carried applications, which places a number of constraints on the Services-IF design. Due to the difficulty in maintaining and/or upgrading these devices "in the field", a PHG should be robust and stand-alone and simple enough to keep costs low and technical operational experience or expertise requirements to a minimum. Because of this focus, the Services-IF allows the majority of the contextual metadata associated with the exchange of observations to reside outside of the PHG.

On the other hand, it is expected that a health and fitness service will be hosted by a more capable system such as a server or personal computer. Therefore, the design of the Services-IF aims to push complexity and maintainability issues to the health and fitness service as this means that the issues can be avoided on the PHG.

The Services-IF is an abstract channel composed of one or more CCC pairs that connect a PHG application with a health and fitness service application. Each CCC pair has a component that resides in the health and fitness service application and a component that resides in the PHG application. Continua defines Certified Capability Classes on both sides of the Services-IF.

This version of the Services-IF guidelines enables the following Certified Capability Classes:

– the uploading of observations from the PHG to the health and fitness service in two different styles: web services (SOAP) and REST (data) [ITU-T H.812.1];

– the uploading of consent information from the PHG to the health and fitness service in two different styles: web services (SOAP) and REST (data) [ITU-T H.812];

[1] NOTE – Within the end-to-end architecture both the Services and the Healthcare Information System (HIS) interfaces can be implemented on a device close to the user/patient (PC, laptop, mobile phone, etc.) in order to exchange information with entities that are geographically distant from such devices. The guidelines place no restrictions on the deployment of certified capability classes on specific hardware.

– the downloading of to-be-completed questionnaires from the health and fitness Service to the PHG and the uploading of completed questionnaires from the PHG to the health and fitness service [[ITU-T H.812.2];

– the exchange of information (e.g., unsolicited commands) between the health and fitness service and the PHG over an authenticated persistent session [ITU-T H.812.4];

– the exchange of supported certified capability class information (capability exchange) between the PHG and the health and fitness service as an enabler for the other use cases [ITU-T H.812.3].

A PHG can support one or more applications that each implement one or more Continua Certified Capability Classes. Figure 6-3 depicts the Continua Services-IF, showing a PHG application and a health and fitness service application in which all of the possible Services-IF Certified Capability Classes are implemented.

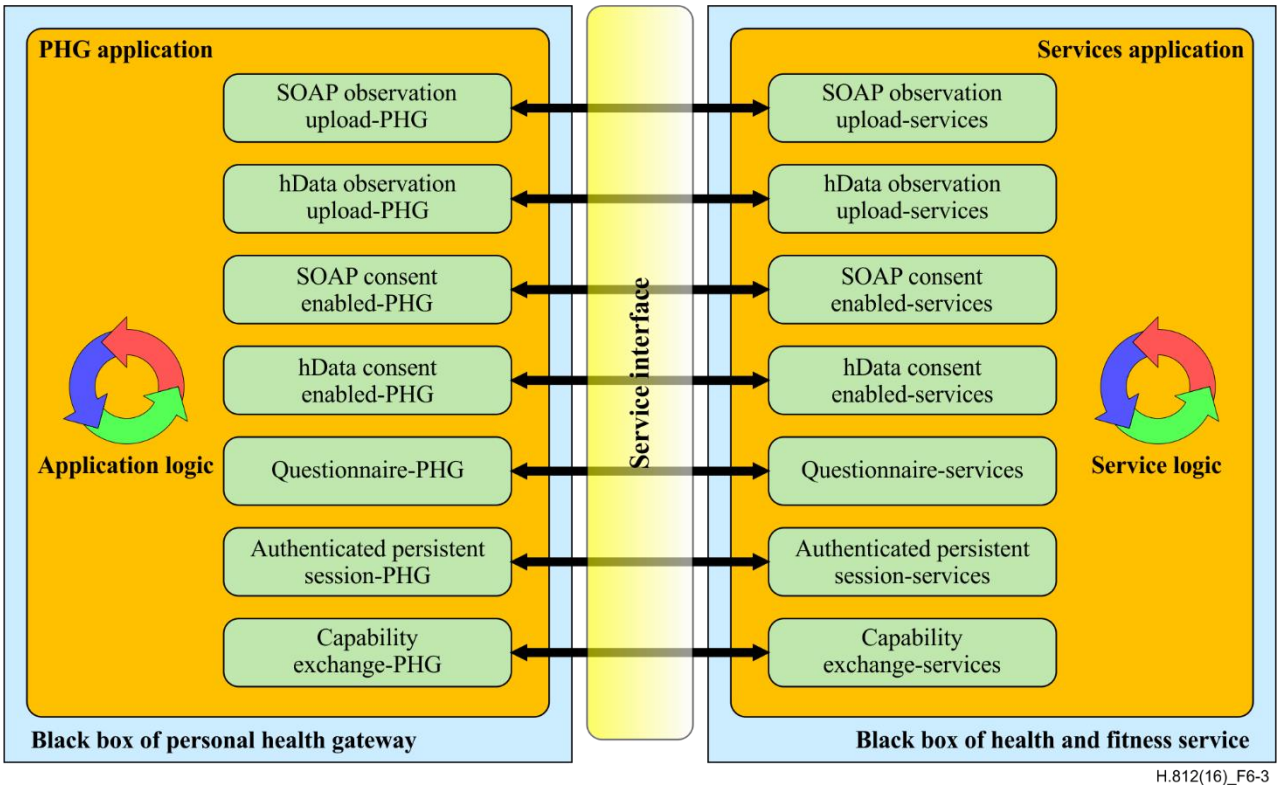

Figure 6-3 – Continua Services-IF showing the Services-IF Certified Capability Classes

The intent of these guidelines is to specify system behaviour in enough detail to achieve an acceptable level of interoperability for a particular use case. A use case is encapsulated in a certified capability class (CCC). The guidelines make normative statements about how the network interface of the components of the CCC functions. For the Services-IF these components exist in the context of applications or services that reside on a PHG or on a health and fitness service.

Common platforms often limit the manner in which applications can communicate with each other to ensure the stability of the overall platform. This limited interaction between applications is called sandboxing. In order to support sandboxed applications this version of the Services-IF uses a reference model that defines an application as a container for one or more CCC components. Interactions between the components within the application container do not have normative requirements and are fully up to the developer of the application. Interactions on the Services-IF between the application's CCCs on the PHG and the corresponding CCCs on the health and fitness service are visible and do have normative requirements in order to pass certification.

The reference model allows multiple applications to exist in a PHG or a health and fitness service, but applications do not interact with other applications except through network interfaces. In these guidelines applications that run on a health and fitness service are often referred to as services since health and fitness services are commonly web service platforms. A health and fitness service is conceptually the same as a PHG application.

These guidelines document mechanisms by which components may communicate with each other through an internal application programming interface (API). Future versions of the Services-IF may use these mechanisms to enable interoperability between components within an application.

In Figure 6-4 the concepts of the Services-IF reference model are used to depict a PHG with two independent applications communicating with a Services application. One PHG application supports three CCCs and the other supports a single CCC. Normative requirements are made on the network interfaces between the PHG and the health and fitness service. The interactions between the CCC components within an application container are not normative and are shown as red dashed lines coordinated by application internal processing that are out of the scope of these guidelines.

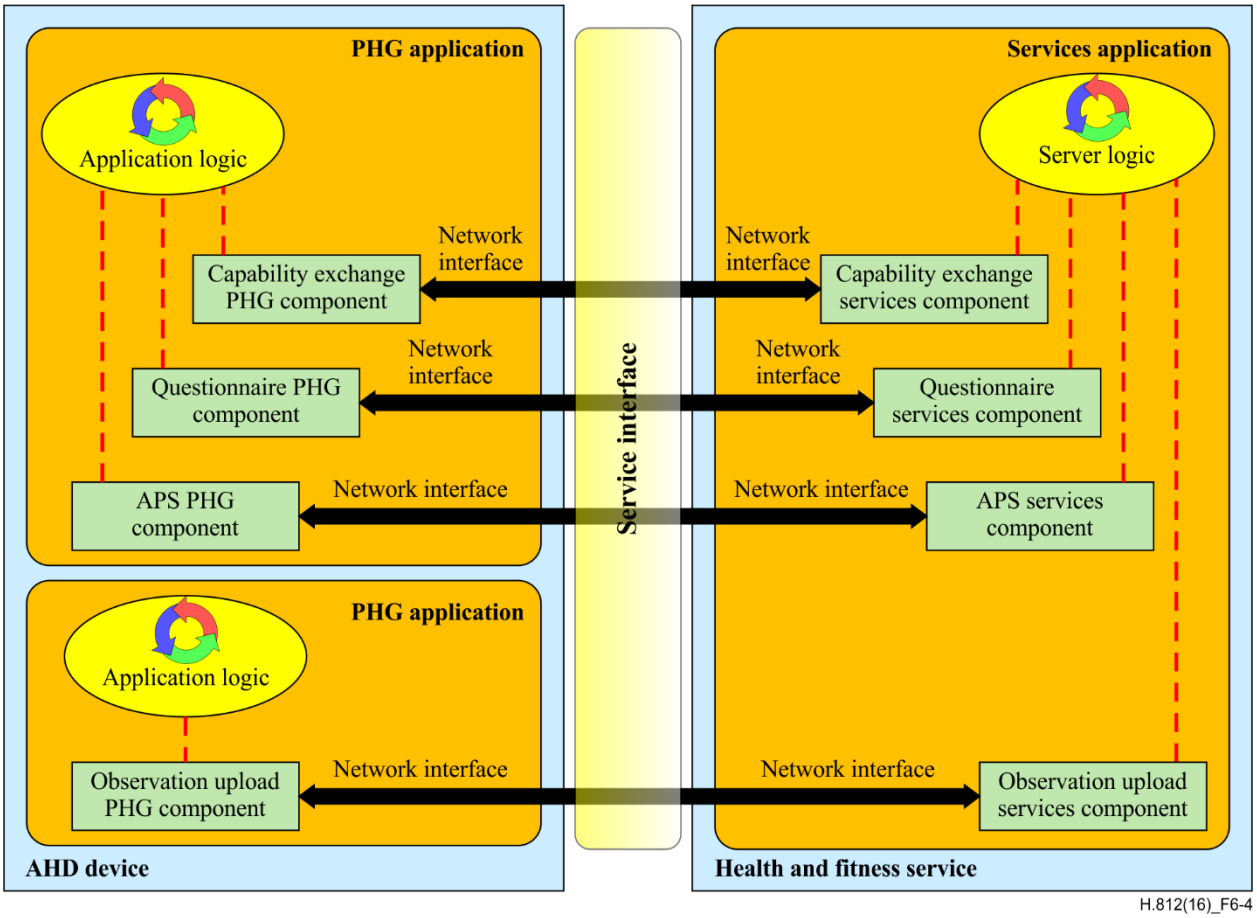

Figure 6-4 – Services-IF reference model

Communications that use the Services-IF start with the PHG's Capability Exchange component. This component sends a request to its peer component on the health and fitness service. The request asks the health and fitness service to specify the different Certified Capability Classes that it supports. In common language the PHG application is asking "What things can you do?" The health and fitness service application answers this in terms of the CCCs it supports. In the case of Figure 6-4 the health and fitness service application would say "I support Capability Exchange, Questionnaires, SOAP Observation Upload and Authenticated Persistent Sessions (APSs)". When the Capability Exchange component of the services application answers the PHG application, it will typically provide the PHG with additional information, such as an URL, which enables the PHG application to take the next step in communication with a particular CCC. A PHG that only supports observation uploading

using SOAP does not need to implement Capability Exchange. Capability Exchange does not need to be invoked if the PHG is already aware of the capabilities of the health and fitness service.

7 Use cases

7.1 Consent management use cases

A consent directive is a record of a healthcare client's privacy policy that grants or withholds consent to the individually identifiable health information (IIHI) [HL7 CDA IG].

The user consent requirement is derived from different regulations such as the Health Information and Portability Accountability Act (HIPAA), EU Directives 95/46, etc. These privacy laws define and assign specific rights to patients with respect to the collection, access, use and disclosure of their health information. The laws mandate that the patient consent must be obtained before his/her health information may be accessed, used or shared. For example, a patient during registration with a disease management organization (DMO) may be required to fill in a consent form. This consent form captures the patient's acknowledgment and/or signature for a predefined set of policies that specify who is allowed to access his/her IIHI, for what purpose and how they can use it. This clause introduces the capturing and transferring of consent policy in electronic form on the Continua Services-IF. Digital consent contributes to improved patient empowerment and efficient handling to comply with consent. Examples of patient consent include basic opt-in/opt-out to IIHI, allowing emergency override, limiting access to functional roles (e.g., direct care providers), specific documents to be used for specific research projects, etc.

In a basic scenario a patient will define his consent during or after registering with the health and fitness service application. How he precisely specifies his consent is out-of-scope for the Continua guidelines, but it could involve selection and possibly adaptation of a default policy using a user interface on his PHG which translates it to a machine readable consent policy representation. Such policies typically contain a reference to the parties involved, data objects and actions that are authorized or not. A health and fitness service application that receives consent for a particular patient will store it and enforce it for health data that it receives for the patient.

The use cases below are focused on the needs identified for patient consent management.

7.1.1 Upload consent to the server

Adam Everyman registers with an organization e.g., a disease management organization (DMO) which remotely monitors patients at home and collects health information from health measurement devices installed at Adam's home. At the time of registration, Adam fills in an eConsent form on the personal health gateway (PHG) application. The eConsent form consists of options regarding who will be able to access, use, update and disclose different types of vital signs that are collected through a remote patient monitoring system. After specifying preferences, Adam then hits the "submit" button on his telehealth hub. The hub compiles his preferences into a privacy consent directives document which is based on the HL7 CDA R2 standard and is then sent from his PHG to the DMO which provides a remote patient monitoring service. The consent directive then governs access to patient data at the DMO and if Adam's data is sent to third parties which assuming that this is allowed may include the patient's personal health record (PHR), electronic health records EHRs and electronic medical records (EMRs). Adam's privacy consent directive will then be associated with the data via the patient identifier.

7.1.2 Retrieve the already completed patient consent from the server

Adam may want to update his privacy preferences e.g., allowing his fitness coach to get access to his data as he has recently registered with a fitness service as suggested by a nurse at the DMO. His PHG provides a link to his latest version of the privacy consent directive document. Adam clicks on the link and PHG then retrieves the latest version of his privacy consent directives from the server and renders it to Adam.

7.1.3 Upload updated consent to the server

Adam reviews his privacy consent preferences and updates them if his fitness coach does not have access to his data. After updating consent preferences, he hits the "submit" button on his PHG which then compiles his preferences into a privacy consent directive document that is sent to the DMO. The DMO replaces the old consent with the updated privacy consent directive document.

7.2 Consent enforcement use case

Consent enforcement through encryption protects the privacy of the patient in an efficient manner and makes sure that the content (e.g., observations or response to a Questionnaire) is viewed only by the intended recipient. This prevents viewing of the content by other individuals who may be working in the same organization e.g., administrative staff. The Consent Enabled health and fitness service should evaluate consent before decrypting the content. Consent is evaluated in order to determine whether the recipient is able to view the content. For example, the process of consent evaluation results in "Success-1" or "Failure-0". The Consent enabled health and fitness service should enforce the consent preferences expressed in a consent document.

7.2.1 Content encryption before upload

Adam Everyman registers with the DMO which remotely monitors him at home and collects health information from health measurement devices installed at his home. Adam Everyman has also registered with a fitness coach as suggested by a nurse at the DMO. Adam Everyman wants his fitness coach to view his activity data and not data from other measurement devices such as a blood pressure monitor (BPM). Adam configures his PHG such that now only the nurse at the DMO organization has access to the data from the BPM and activity monitors while the fitness coach only has access to the data from the activity monitors. This is enabled through encryption.

7.3 Other CCC use cases

See clause 6 in the following design guidelines for their respective CCC use cases:

– [ITU-T H.812.1] Observation Upload
– [ITU-T H.812.2] Questionnaire
– [ITU-T H.812.3] Capability Exchange
– [ITU-T H.812.4] Authenticated Persistent Session

8 Behavioural models

This clause includes:

– Services-IF message exchange behaviour
– Security behaviour of REST based CCCs
– Consent management and enforcement of CCC behavior

8.1 Common Services-IF message exchange behaviour

Due to security and privacy concerns, as well as the technical feasibility of the overall system, the Services-IF requires that all connections be initiated from the PHG. This is illustrated in Figure 8-1. See each design guideline for its message payload and other specifics.

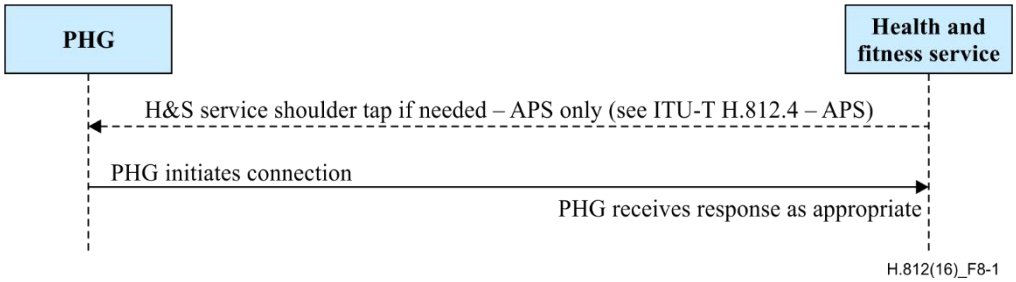

Figure 8-1 – All connections are initiated from PHG

When transport level security (TLS) is required for point to point content security, the use of mutual certificate validation in the TLS handshake is up to the security policy of the health and fitness service.

When authentication is required:

– in the SOAP case, the authentication is a SAML 2.0 token and

– for data, an OAuth 2.0 bearer token.

How the PHG obtains these tokens is not specified by Continua and it depends upon the trust relationship established between the parties. The health and fitness service application may support one or more WS-Trust options to obtain SAML 2.0 tokens or it may support an OAuth 2.0 authorization framework server using one or more grant types, for example the resource owner password credentials grant type. The health and fitness service may support both services if it supports both data and SOAP uploads. In either of these cases, an out-of-band operation must take place where the user of the PHG establishes some type of account on the health and fitness service application allowing the client to obtain these tokens. The health and fitness service token service generates these tokens customized for the recipient which it can validate when it receives the content. On the other hand, the health and fitness service may require that these tokens be obtained from a third party authorization service (such as a CA) with which the PHG has established a trust relationship. In this case, the health and fitness service is letting the third party authorization service validate the client. The health and fitness service may then choose to accept any token that comes from this third party service, or it may additionally choose to pass any received token to the third party authorization service for confirmation before acceptance. The trust relationship details are determined by the security policy of the health and fitness service.

8.2 Common security model for REST based CCC implementations

Figure 8-2 provides an interaction diagram for authorized RESTful transactions based on data (REST) over HTTP. The authorization is realized using OAuth 2.0 authorization framework using resource owner password credentials as the authorization grant type. Resource owner password credentials are usually used when there is a high degree of trust between the resource owner (patient) and client (for example, a trusted application running on the application hosting device). In future versions of design guidelines other credential types may be needed based on the use cases where third party applications (less privileged) may be used to get access to patient's data. The resource owner credentials are used for a single request and are exchanged for an access token. The access token is then used to perform a RESTful transaction on a resource. All interactions with the authorization and resource server are performed in a secure session using [IETF RFC 4346].

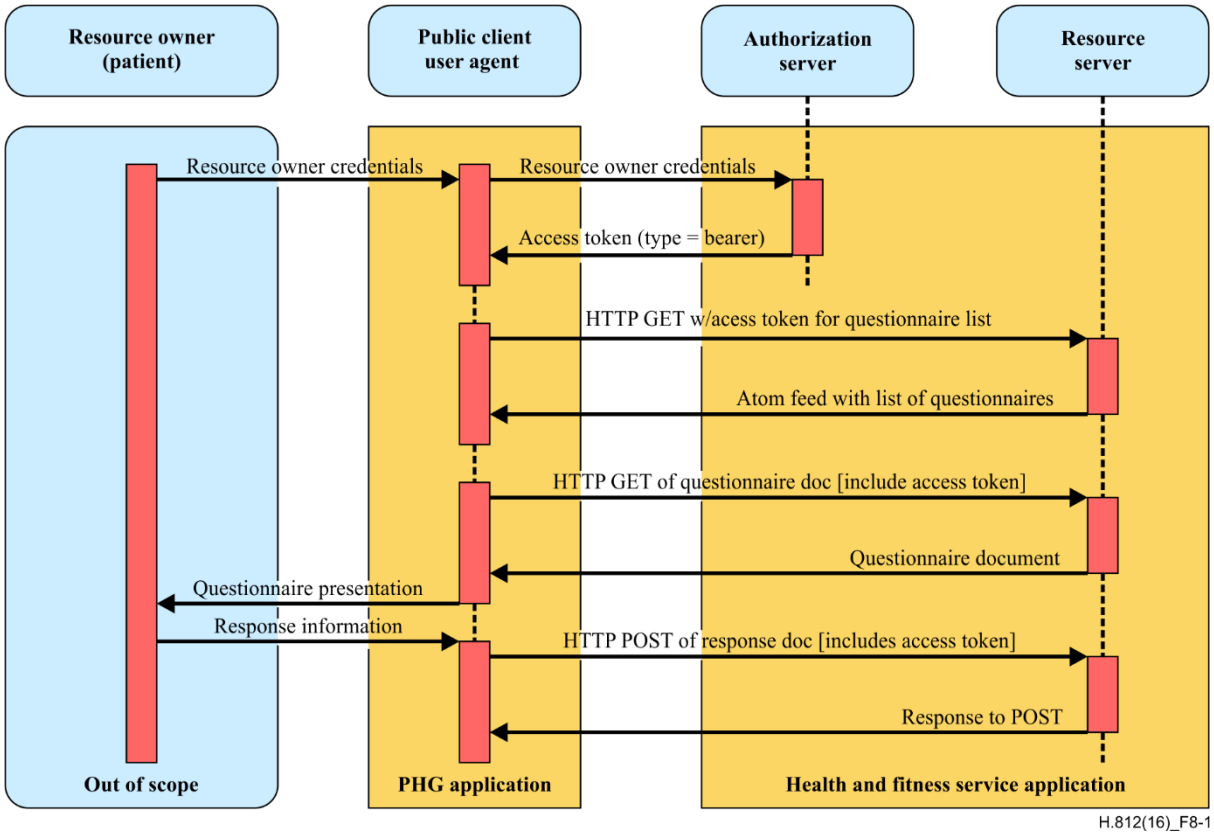

Figure 8-2 – Security behaviour for authorized RESTful CCC behaviour (Questionnaire use case is taken as an example)

See Table B.1 and Table B.2 for REST CCC security guidelines.

8.3 Consent management behavioural model

The following exchange mechanisms are specified for the consent management service:

– Create a *new* consent document on the server.

– Retrieve *already* specified consent document from the server.

– Upload *updated* consent document to the server.

Figure 8-3 illustrates transactions related to the consent management use cases described in this content profile.

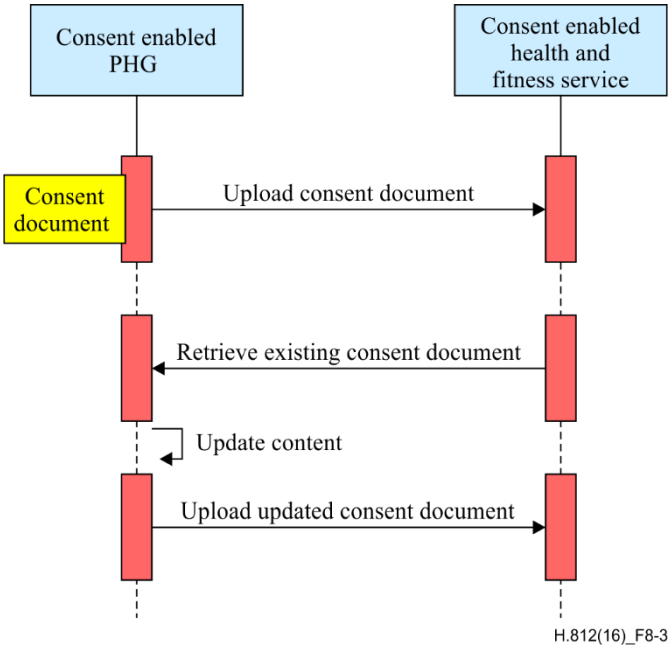

Figure 8-3 – Transactions between PHG and health and fitness service related to consent management

See Table C.1 and Table C.2 for consent management guidelines.

8.4 Consent enforcement behavioural model

The following function is specified for the consent enforcement:

– Encrypt to-be uploaded content

Figure 8-4 illustrates consent enforcement functionality.

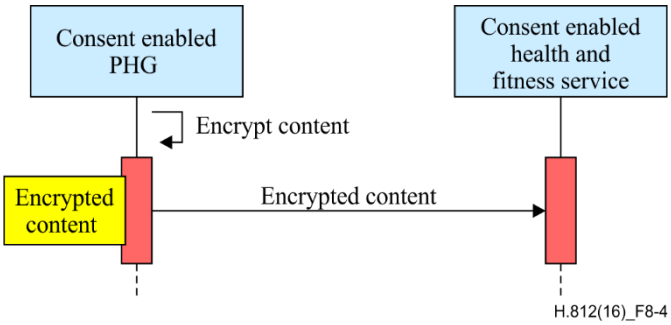

Figure 8-4 – Consent enforcement at the Services-IF

See Table C.3 and Table C.4 for consent enforcement guidelines.

9 Implementation

9.1 Consent representation

The consent preferences are represented according to the HL7 Implementation Guide for CDA Release 2.0: Consent Directive in [HL7 CDA IG].

The sample files for a consent document can be found in the submission package for the above mentioned standard.

9.2 Transport protocols

9.2.1 Transport protocol using data over HTTP

In this case, data over HTTP is used as the transport protocol for the exchange of consent documents across the Services-IF and it supports all use cases that are mentioned in clauses 7.1 and 7.2. For the detailed requirements on the use of data over HTTP protocol between PHG and health and fitness services consult Annex A, Table C.1, Table C.2, Table C.3 and Table C.4.

9.2.2 Transport protocol using IHE XDR

In this case, [IHE ITI TFS XDR] is used as transport protocol for the exchange of consent documents across the Services-IF and supports only uploading consent to the server use case. Consent documents are linked to the health information (PCD-01 message) via the patient identifier. This way the consent is associated to the health information and thereby controls its use.

9.3 Consent enforcement

9.3.1 Consent enforcement using XML encryption

In the case of the transport protocol using [IHE ITI TFS XDR], XML encryption standard [W3C XMLENC] is used to enable the consent enforcement through encryption. The XML encryption standard enables encryption of the payload of the PCD-01 transaction for a specific recipient (e.g., doctor or nurse) at the Consent Enabled health and fitness service.

The XML encryption standard is used to enable consent enforcement through encryption.

9.3.2 Consent enforcement using IHE DEN

In the case of the transport protocol using data over HTTP, consent enforcement is enabled through the use of the IHE DEN profile [IHE ITI DEN].

Annex A

Normative guidelines overview

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

The services Certified Capability Classes are listed in Table A.1.

Table A.1 – Certified Capability Classes

Name of certified capability classes	Certified Capability Classes	Logo-ed capability classes
SOAP Observation Upload - PHG	Yes	Yes
SOAP Observation Upload - Health and fitness service	Yes	Yes
data Observation Upload - PHG	Yes	Yes
data Observation Upload - Health and fitness service	Yes	Yes
SOAP Consent Enabled - PHG	Yes	Yes
SOAP Consent Enabled - Health and fitness service	Yes	Yes
data Consent Enabled - PHG	Yes	Yes
data Consent Enabled - Health and fitness service	Yes	Yes
Questionnaire -PHG	Yes	Yes
Questionnaire - Health and fitness service	Yes	Yes
Capability Exchange - PHG	Yes	Yes
Capability Exchange - Health and fitness service	Yes	Yes
Authenticated Persistent Session - PHG	Yes	*
Authenticated Persistent Session - Health and fitness service	Yes	*[2]

The guidelines that are applicable for each of the Certified Capability Classes are referenced in Table A.2 below.

Table A.2 – Guidelines for Certified Capability Classes

Certified Capability Classes	Relevant guidelines
SOAP Observation Upload - PHG	See [ITU-T H.812.1], and [ITU-T H.812] Table A.3, Table B.3
SOAP Observation Upload - Health and fitness service	See [ITU-T H.812.1], and [ITU-T H.812] Table A.3, Table B.3
data Observation Upload - PHG	See [ITU-T H.812.1], and [ITU-T H.812] Table A.3, Table B.1

[2] * These cells are intentionally blank.

Table A.2 – Guidelines for Certified Capability Classes

Certified Capability Classes	Relevant guidelines
data Observation Upload - Health and fitness service	See [ITU-T H.812.1] and [ITU-T H.812] Table A.3, Table B.2
SOAP Consent Enabled - PHG	See [ITU-T H.812.1] and [ITU-T H.812] Table A.3, Table B.3, Table C.5, Table C.7
SOAP Consent Enabled - Health and fitness service	See [ITU-T H.812.1], and [ITU-T H.812] Table A.3, Table B.3, Table C.6, Table C.8
data Consent Enabled - PHG	See [ITU-T H.812] Table A.3, Table C.1,Table C.3, Table B.1
data Consent Enabled - Health and fitness service	See [ITU-T H.812] Table A.3, Table C.2, Table C.4, Table B.2
Questionnaire - PHG	See [ITU-T H.812.2] Table A.1 and [ITU-T H.812] Table A.3, Table B.1
Questionnaire - Health and fitness service	See [ITU-T H.812.2] Table A.2 and [ITU-T H.812] Table A.3, Table B.2
Capability Exchange - PHG	See [ITU-T H.812.3] Table A.2 and [ITU-T H.812] Table A.3, Table B.1
Capability Exchange - Health and fitness service	See [ITU-T H.812.3] Table A.1, and [ITU-T H.812] Table A.3, Table B.2
Authenticated Persistent Session - PHG	See [ITU-T H.812.4] Tables A.1, A.2, A.3, A.5 and [ITU-T H.812] Table A.3, Table B.1
Authenticated Persistent Session - Health and fitness service	See [ITU-T H.812.4], Tables A.1, A.4, A.6 and [ITU-T H.812] Table A.3, Table B.2

Table A.3 – Requirements common to all CCCs

Name	Description	Comments
CapX-Health and fitness service-Universality	All health and fitness services **shall** support Capability Exchange except SOAP based Observation Upload or Consent Enabled -health and fitness service CCCs	A Health and Fitness Service that implements only SOAP based Observation Upload or Consent Enabled -health and fitness service CCCs is not required to support the Capability Exchange-Health and fitness service CCC.
Health and fitness service-Transport_Connection_Initiation	All Continua health and fitness service connections **shall** be initiated from the health and fitness service PHG application and **shall not** be initiated from the health and fitness Service	

Annex B

General security guidelines for Services-IF CCCs

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

Table B.1 – PHG security guidelines using REST

Name	Description	Comments
PHG-Grant_Type	A PHG may use Resource Owner Password Credential as Authorization Grant Type as defined in section 1.3.3 of OAuth v2.0 [IETF RFC 6749].	A PHG may use other means to get authorization token from the authorization server.
PHG-authorization_request	A PHG may obtain authorization token from the authorization server according to sections 4.3 and 4.3.2 of OAuth v2.0 [IETF RFC 6749].	See examples in Appendix III for the wire format of the authorization request. See guideline Health and fitness service-authorization_ request_response for the response
PHG-bearer_token	A PHG **shall** use "bearer" token according to [IETF RFC 6750] when requesting access to a protected resource on the health and fitness service [IETF RFC 6750].	See the related guideline Health and fitness service-authorization_ request_response.
PHG-Token_Transmit	A PHG **shall** use the Authorization Request Header Field Method when sending the bearer token as defined in section 2.1 of [IETF RFC 6750].	
PHG-Confidentiality	A PHG **shall** at minimum use TLS protocol v1.1 for secure point-to-point communication with the authorization server and health and fitness service [IETF RFC 4346].	
PHG-Cipher	A PHG **should** use an encryption cipher suite of TLS_RSA_WITH_AES_128_ CBC_SHA	

Table B.2 – Health and fitness service security guidelines using REST

Name	Description	Comments
Health and fitness service-authorization_ request_response	A health and fitness service implementing the authorization server **shall** return authorization token of type "bearer" after validating the access token request according to the section 4.3.3 of the OAuth v2.0 [IETF RFC 6749].	See the guideline PHG-authorization_request for the request format. Authorization could be a separate entity and does not need to be the part of the health and fitness service.
Health and fitness service-refresh_token	A health and fitness service implementing the authorization server **shall** return refresh token.	
Health and fitness service-Token_Evaluation	A health and fitness service **shall** evaluate the authorization token and its scope before granting access to a record on the health and fitness service.	

Table B.3 – Services-IF transport security guidelines

Name	Description	Comments
Health and fitness service-Security_Transport	A health and fitness service application and PHG applications **shall** at minimum support the TLS protocol v1.1 [IETF RFC 4346] from WS-I BSP v1.0 for secure communication	This guideline is consistent with the IHE ATNA profile when encryption is enabled. Continua guidelines depend on the guidance in TLS v1.1 [IETF RFC 4346] for mutual authentication
Health and fitness service-Security_ Transport_Cipher	A health and fitness service application and PHG applications **shall** support AES cipher as specified in [IETF RFC 3268]	IHE ATNA requires the optional use of the following cipher suit: TLS_RSA_WITH_AES_128_CBC_SHA Continua HIS guidelines use the following cipher suite for security: TLS_RSA_WITH_AES_128_CBC_SHA Other cipher suites are allowed but would need to be negotiated between PHG and health and fitness service
Health and fitness service-Confidentiality	A health and fitness service **shall** use TLS protocol v1.1 for secure point-to-point communication with the authorization server and Questionnaire enabled health and fitness service [IETF RFC 4346].	
Health and fitness service-Cipher	A health and fitness service **should** support TLS_RSA_WITH_AES_128_CBC_SHA encryption cipher suite.	

Annex C

Normative guidelines for consent management

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

Table C.1 – Consent management guidelines using REST for the Consent Enabled PHG

Name	Description	Comments
PHG-Consent_Enabled	Consent Enabled PHG shall comply with HL7 CDA R2 Consent Directive standard for the representation of patient consent preference [HL7 CDA IG].	
PHG-Consent_Enabled_ Transport_Standards	Consent Enabled PHG shall comply to the following transport standards: 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	Consent Enabled PHG shall use HTTP POST with the following URL for posting consent to the health and fitness service: *baseURL/continua/consent*	See the use case in clause 7.1 For retrieve, locate and update service (RLUS) data over REST transport, this is performed by performing an HTTP POST request without query parameters at this URL with the privacy consent document in the body of the request.
Consent_Enabled-PHG-Observation_Association	The consent document transmitted by the Consent Enabled PHG shall contain the same patient identifier as the health and fitness service observation measurement message(s).	This is to associate the consent document to the health and fitness service observation measurement messages.
Consent_Enabled-PHG-Observation-Association_ Value	The "Patient ID" field in the consent document header shall be set to the PID-3 value. Subfields CX-1 and CX-4 shall be present and subfield CX-5 shall not be present.	
Consent_Enabled-PHG-Questionnaire Response_Confidentilality	Consent Enabled PHG shall set the confidentiality code value to "R" in the header of the Questionnaire response document.	

Table C.1 – Consent management guidelines using REST for the Consent Enabled PHG

Name	Description	Comments
Consent_Enabled-PHG-Questionnaire Response_Association_Value	To associate Questionnaire response documents(s) with a patient consent document, Consent Enabled PHG shall use the translation element of the confidentiality code system as defined in Table IV.3	See (This appendix does not form an integral part of this Recommendation.) Table IV.1, Table IV.2, and Table IV.4
Retrieving_Consent	Consent Enabled PHG shall use HTTP GET with the following URL for retrieving consent from the health and fitness service: *baseURL/continua/consent* Consent Enabled PHG shall use HTTP GET with the value of the link element from the ATOM feed entry for retrieving actual consent document from the Health & Fitness Service and shall validate that it is a valid HL7 CDA R2 Consent Directive document [HL7 CDA IG].	See the use case in clause 7.1 For RLUS data over REST transport, this is performed by performing an HTTP GET request without query parameters at the URL representing patient's consent data section path which returns the ATOM feed entry. For further information on the Atom feed entry element consult Table I.1

Table C.2 – Consent management guidelines using REST for Consent Enabled health and fitness service

Name	Description	Comments
Consent_Enabled-Health-&-Fitness-Service	Consent Enabled health and fitness service shall be able to receive, HL7 CDA R2 Consent Directive consent document(s) [HL7 CDA IG].	
Health-&-Fitness Service-Consent_Enabled_Transport_Standards	Consent Enabled PHG shall comply to the following transport standards: 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]	

Table C.2 – Consent management guidelines using REST for Consent Enabled health and fitness service

Name	Description	Comments
Health-&-Fitness Service-Consent_Root	Consent Enabled health and fitness service shall include the following elements for Questionnaire content in the root.xml file: 1. profile a. id="consent" b. reference=<http://handle.itu.int/11.1002/3000/hData/Consent/2016/01/H.812.pdf> 2. section a. path="consent" b. profileID= "consent" c. resourceTypeId="consent" 3. resourceType a. resourceTypeId="consent" b. reference="http://www.hl7.org/dstucomments/showdetail.cfm?dstuid=63" c. representation d. mediaType="application/xml2	Note: The URL given for 1.b reference is an example only
Health-&-Fitness Service-Consent_Validate	Consent Enabled health and fitness service shall validate the consent document that it is a valid HL7 CDA R2 Consent Directive document and send the HTTP 200 as a response if it is a valid document.	
Health-&-Fitness Service-Post_Consent-Response	Consent Enabled health a fitness service shall create a consent document record after receiving POST message from the Consent Enabled PHG and send the HTTP 201 as a response.	See the PHG-Post_Consent above
PHG-Delete_Consent_Response	Consent Enabled health and fitness service shall not support the deletion of an existing consent document record and shall return HTTP 405 Method Not Allowed as a response to HTTP DELETE request on a consent URL.	

Table C.3 – Consent enforcement guidelines using data for the Consent Enabled PHG

Name	Description	Comments
Consent_Enabled-PHG-Content-Encryption_Actor	Consent Enabled PHG shall encrypt the content in compliance with IHE Document Encryption (DEN) Profile [IHE ITI DEN].	The content here could be the payload of the PCD-01 transaction or Questionnaire response document.
Consent_Enabled-PHG-Questionnaire-Response_MIMEtype_	Consent Enabled PHG shall set the MIME type to "application/xml" in case the encrypted content is Questionnaire response.	The purpose is to indicate the type of the payload that is encrypted.
Consent_Enabled-PHG-Observation - Upload_MIMEtype_	Consent Enabled PHG shall set the MIME type to "application/txt" in case the encrypted content is Observation Upload.	The purpose is to indicate the type of the payload that is encrypted.

Table C.3 – Consent enforcement guidelines using data for the Consent Enabled PHG

Name	Description	Comments
Consent_Enabled-PHG-Content-Encryption_Algorithm	Consent Enabled PHG shall use AES-128 CBC for encryption of the content.	The algorithm used is identified through the ContentEncryptionAlgorithmIdentifier in CMS (cryptographic message syntax) which is further profiled by IHE DEN.
Consent_Enabled-PHG-Encryption-Recipient_Binding_PKI	Consent Enabled PHG shall use PKI based key management method from IHE DEN Profile [IHE ITI DEN].	PKI based content key management method uses KeyTransRecipientInfo as CMS RecipientInfoType. This point to the public key or x.509 v3 certificate of the recipient

Table C.4 – Consent enforcement guidelines using data for Consent Enabled health and fitness service

Name	Description	Comments
Health-&-Fitness-Service-Device_HTTP_Ack	Consent Enabled health and fitness service shall send the HTTP 202 as a response after successful reception of the encrypted content.	
Consent_Enabled-Health-&-Fitness-Service-Content-Decryption_Actor_XDR	Consent Enabled health and fitness service shall comply with IHE DEN Profile to decrypt the encrypted content [IHE ITI DEN].	
Consent_EnabledKey_Management	Consent Enabled health and fitness service shall use PKI based key management method as specified by the IHE DEN Profile [IHE ITI DEN].	
Consent_Enabled-Health-&-Fitness-Service-Decryption-Algorithm	Consent Enabled health and fitness service shall use AES.128 CBC decryption algorithm for the decryption of the payload.	The algorithm used is identified through the ContentEncryptionAlgorithmIdentifier in CMS (cryptographic message syntax)
Consent_Enabled-Health-&-Fitness-Service-Consent_Enforcement_	Consent Enabled health and fitness service shall enforce consent preferences expressed in consent document.	For example prevents further disclosure of the content to the unauthorized entities

Table C.5 – Consent management guidelines using SOAP for the Consent Enabled PHG

Name	Description	Comments
Services-Observation-PHG-Consent	Consent Enabled services observation PHG **shall** comply with [HL7 CDA IG] Consent Directive to represent patient consent in a consent document	
Services-Observation-PHG-Consent-Transport	Consent Enabled services observation PHG **shall** implement the Document Source actor of IHE XDR to send a consent document using the ITI 41 Provide and Register Document Set-b transaction	
Services-Observation-PHG-Consent-Frequency	Consent Enabled services observation PHG **shall** send the consent document at least once to the Observation health and fitness service	The consent document is e.g., first sent during registration with the service. It is recommended to send consent at least once during the lifetime of connection to observation health and fitness service. Also supports the use cases such as updating consent preferences. The updated consent document is a replacement of the existing consent document at the Consent Enabled observation health and fitness service
Health-&-Fitness-Services-Observation_Measurement_Consent_Document_Association	The consent document transmitted by the Consent Enabled services observation PHG **shall** contain the same patient identifier as the services observation measurement message(s)	This is to associate the consent document to the Health-&-Fitness-Services observation measurement messages
Health-&-Fitness-Services-Observation_Measurement_Consent_Document_Association_Value	The "Patient ID" field in the consent document header **shall** be set to the PID-3 value. Subfields CX-1 and CX-4 **shall** be present and subfield CX-5 **shall not** be present	

Table C.6 – Consent management guidelines using SOAP for Consent Enabled health and fitness service

Name	Description	Comments
Observation-Health-&-Fitness-Service-Consent	Consent Enabled observation health and fitness service **shall** be able to receive, [HL7 CDA IG] Consent Directive consent document(s)	
Observation-Health-&-Fitness-Service-Consent_Transport	Consent Enabled observation health and fitness service **shall** implement the Document Recipient actor of IHE XDR to receive a consent document using the ITI 41 Provide and Register Document Set-b transaction	The Observation health and fitness service replaces the existing consent document if a new version was received as indicated by XDS metadata of the consent document

Table C.7 – Consent enforcement guidelines using SOAP for the Consent Enabled PHG

Name	Description	Comments
Health-&-Fitness-Services-PHG-Content_ Encryption_Actor	Consent Enabled health and fitness services observation PHG **shall** encrypt the payload (Annex D of [ITU-T H.812.1]) of the PCD-01 transaction in compliance with the encryption processing rules defined in clause 4.1 of the XML Encryption Specification [W3C XMLENC]	
Health-&-Fitness-Services-PHG-Content_ Encryption_MIMEtype	Consent Enabled health and fitness services observation PHG **shall** set the MIME type to "application/hl7-v2+xml"	The purpose is to indicate the type of payload that is encrypted
Health-&-Fitness-Services-Services-PHG-Content_ Encryption_Algorithm	Consent Enabled health and fitness services observation PHG **shall** use AES-128 CBC as the payload encryption algorithm from the XML Encryption Specification.	The AES-128 CBC algorithm is identified through the use of the following identifier: http://www.w3.org/2001/04/xmlenc#aes128-cbc [W3C XMLENC]
Health-&-Fitness-Services-PHG-Encryption_ Recipient_Binding_PKI	For the content key transport, Consent Enabled health and fitness services observation PHG **shall** support RSA Version 1.5 from the XML Encryption Specification	The key transport based on RSA v1.5 is identified through the use of the following identifier [W3C XMLENC]: http://www.w3.org/2001/04/xmlenc#rsa-1_5 . For detailed information about RSA v1.5, consult [b-RFC 2437] RSA v1.5 based key transport is also used in CMS (cryptographic message syntax) standard used on the HIS-IF. To find out more, consult [b-RFC 3370] and the consent enforcement guidelines for the HIS-IF

Table C.7 – Consent enforcement guidelines using SOAP for the Consent Enabled PHG

Name	Description	Comments
Health-&-Fitness-Services-PHG-Encryption_ Recipient_Binding_Symmetric	For the content key transport, the Consent Enabled health and fitness services observation PHG **should** use AES-128 symmetric key wrap algorithm from the XML Encryption Specification. In case of password based encryption, the Consent Enabled health and fitness services observation PHG **may** use PBKDF2 as the key derivation algorithm from [IETF RFC 3211]	The identifier used for AES-128 symmetric key wrap is http://www.w3.org/2001/04/xmlenc#kw-aes128 [W3C XMLENC]. The key used in wrapping is referred as KEK, which may be derived from a password or a long term shared secret key
Health-&-Fitness-Services-PHG-Integrity_ Payload_PCD-01_Create	Consent Enabled health and fitness services observation PHG **shall** compute the digest of the encrypted payload using SHA256 (clause 5.7.2) algorithm according to the XML Encryption Specification	The SHA256 algorithm is identified through the use of the following URL: http://www.w3.org/2001/04/xmlenc#sha256 [W3C XMLENC].
Health-&-Fitness-Services-Encrypted_ Payload_PCD-01_ transaction	Consent Enabled health and fitness services observation PHG **shall** wrap the encrypted payload inside the element <CommunicateEncPCDData xmlns= "urn:ihe:continua:enc:pcd:dec:2012">	In case of the un-encrypted payload the content is wrapped inside the element < CommunicatePCDData xmlns=" urn:ihe:pcd:dec:2010">. See the example in Figure II.1.
Health-&-Fitness-Services-Encrypted_ Payload_PCD-01_Transaction_ Header	In case of the encrypted payload, the SOAP header **shall** contain "urn:ihe:continua:enc:pcd:dec:2012:CommunicateEncPCDData" instead of "urn:ihe: pcd:dec:2010: CommunicatePCDData"	The plain PCD-01 transaction contains "urn:ihe: pcd:dec:2010:CommunicatePCDData". See the example in Figure II.1, Figure II.2, and Figure II.3

Table C.8 – Consent enforcement guidelines using SOAP for Consent Enabled health and fitness service

Name	Description	Comments
Health-&-Fitness-Service-HTTP-Ack	Consent Enabled observation health and fitness service **shall** send the SOAP HTTP response with the status code equal to 202 after the successful reception of the encrypted message. Consent Enabled observation health and fitness service **should not** send the PCD-01 application level acknowledgement	The reason is that the observation health and fitness service may not be in possession of the decryption key as the content may be encrypted for a specific recipient on the Health and Fitness Service
Health-&-Fitness-Service-Payload-PCD-01-Verify-Integrity	Consent Enabled observation health and fitness service **shall** verify the message digest of the encrypted payload	
Health-&-Fitness-Service-Payload-PCD-01-Verify-Integrity-Algorithm	Consent Enabled observation health and fitness service **shall** support the SHA256 algorithm	

Table C.8 – Consent enforcement guidelines using SOAP for Consent Enabled health and fitness service

Name	Description	Comments
Health-&-Fitness-Service-Content-Decryption-Actor	Consent Enabled observation health and fitness service **shall** comply with decryption rules specified in clause 4.2 of the XML Encryption Specification [W3C XMLENC].	
Health-&-Fitness-Service-Key-Transport-RSA	Consent Enabled observation health and fitness service **shall** support RSA Version 1.5 from the XML Encryption Specification [W3C XMLENC].	
Health-&-Fitness-Service-Key-Transport-Symmetric	Consent Enabled observation health and fitness service **shall** support AES-128 symmetric key wrap algorithm from the XML Encryption Specification [W3C XMLENC]. The Consent Enabled observation health and fitness service **shall** support PBKDF2 as the key derivation algorithm from [IETF RFC 3211]	The identifier used for AES-128 symmetric key wrap is http://www.w3.org/2001/04/xmlenc#kw-aes128 [W3C XMLENC]. The key used in wrapping is referred as KEK, which may be derived from a password or a long term shared secret key.
Health-&-Fitness-Services-Content-Decryption-Algorithm	Consent Enabled observation health and fitness serviceice **shall** use AES-128 CBC decryption algorithm from the XML Encryption Specification [W3C XMLENC].	The AES-128 CBC algorithm is identified through the use of the following identifier: http://www.w3.org/2001/04/xmlenc#aes128-cbc [W3C XMLENC].

Appendix I

ATOM feed elements for consent management

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

The following ATOM feed child elements of the entry element have a specific usage for the purpose of consent documents.

Table I.1 – ATOM feed child elements for consent management

Element	Usage
Author	Person construct that indicates who provided the information in the consent document. i.e., who filled consent
Title	Title of the patient consent document (e.g., Adam's consent authorization)
link	Reference to the Adam's consent directive document which shall be a valid HL7 CDAR2 Consent Directive IG document. The link shall be relative and the privacy consent document shall be in the consent section of the data record.
Published	The published element shall be set to the date and time at which the privacy consent document was posted to the server.

I.1 Information for consent in the root.xml

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

<reference><http://handle.itu.int/11.1002/3000/hData/Consent/2016/01/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>
```

Appendix II

Examples of consent management using SOAP

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

```
<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||||||R20100903124015+0
            000
            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>
```

Figure II.1 – The PCD-01 transaction with un-encrypted payload

```
<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/DeviceObservationCons
umer_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>
```

Figure II.2 – Encrypted PCD-01 transaction – public key based

In Figure II.2, PCD-01 transaction is shown with encrypted payload using XML encryption standard. The content key is encrypted with the public key of the recipient.

```
<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/DeviceObservationCons
umer_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>
```

Figure II.3 – Encrypted PCD-01 transaction – symmetric key based

Figure II.3 shows PCD-01 transaction with encrypted payload using XML encryption standard. In this example, the content key is assumed to be known to both the sender and recipient and is read only.

Appendix III

OAuth example

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

Example 1:

– Request for access token

In order to obtain an access token, Questionnaire enabled PHG makes the following HTTP POST request to the authorization server.

```
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
```

Where

– http://localhost:3000/oauth2/token is the URL for reaching authorization server and must be known to the Questionnaire enabled PHG.

– Authorization: Basic MTIwMDk0NTc0NjczNzY3OmI1NGRjODI0NzZhZjI4MTRlNjIwYjg2Nzc2YzQyYzBl

– This is a basic HTTP authorization header that is generated by Questionnaire enabled PHG using its given identifier and secret word by encoding them into Base64 hash string Base64("120094574673767:b54dc82476af2814e620b86776c42c0e") =

– "MTIwMDk0NTc0NjczNzY3OmI1NGRjODI0NzZhZjI4MTRlNjIwYjg2Nzc2YzQyYzBl"

– grant_type indicates the authorization code. In this authorization code is username and password.

– Access Token Response

The authorization server validates access token request and if authorized, it generates access token of type "bearer" and optional refresh token.

```
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":"789f3daf81a30
2e0636325114113e4b4","token_type":"bearer","expires_in":899}
```

Where

– "f779da766bfd1b9164b0fd6d280d52f1"is access token that would be used by PHG when accessing a resource on the server.

– "789f3daf81a302e0636325114113e4b4" is refresh token which can be used to obtain a new token.
– The token type in the above example is "bearer".
– The lifetime of the token is 899 seconds.
– Requesting a resource using access token of type "bearer".

Example 2:

In the example below the PHG uses a bearer token in order to request a protected resource e.g., Questionnaire.

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

Appendix IV

Consent Enabled PHG Questionnaire response association

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

Table IV.1 – The elements of the confidentiality code system

Name	Value	Comments
Code	"R"	
codeSystem	2.16.840.1.113883.5.25	
codeSystemName	"Confidentiality"	
displayName	"Restricted"	

Table IV.2 – The elements of the Continua Consent Directive code system

Name	Value	Comments
Code	The value **shall** be the same as specified by [HL7 CDA IG].	
codeSystem	2.16.840.1.113883.3.1817 .1.2.1	
codeSystemName	"Continua Consent Directive"	
displayName	ID of the consent document	

Table IV.3 – The translation of the confidentiality code system to the Continua Consent Directive code system

Name	Value	Comments
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	"<> " is a placeholder for the ID of the consent document. Consult Table IV.2 for the elements of the Continua Consent Directive code system.

Table IV.4 – OID distribution for Continua Health Alliance

OID	Description	Comments
2.16.840.1.113883.3.1817	Organization OID: Continua Health Alliance	
2.16.840.1.113883.3.1817.1	Root OID for the Continua E2E architecture	
2.16.840.1.113883.3.1817.1.2	Root OID for the E2E Security and Privacy	
2.16.840.1.113883.3.1817.1.3	Root OID for the PAN-IF	
2.16.840.1.113883.3.1817.1.4	Root OID for the LAN-IF	
2.16.840.1.113883.3.1817.1.5	Root OID for the TAN-IF	
2.16.840.1.113883.3.1817.1.6	Root OID for the Services-IF	
2.16.840.1.113883.3.1817.1.7	Root OID for the HIS-IF	
2.16.840.1.113883.3.1817.1.2.1	E2E Security and Privacy: OID for the Continua Consent Directive code system	

Bibliography

For a list of non-normative references and publications that contain further background information, see [ITU-T H.810].

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	**Audiovisual and multimedia systems**
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2017