International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

H.812

(11/2015)

SERIES H: AUDIOVISUAL AND MULTIMEDIA SYSTEMS

E-health multimedia services and applications

Interoperability design guidelines for personal health systems: WAN interface: Common certified device 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: WAN interface: Common certified device class

Summary

The Continua Design Guidelines (CDG) define a framework of underlying standards and criteria which are required to ensure the interoperability of devices and data used for personal connected health.

This Recommendation contains a WAN-IF overview, common design guidelines for all WAN-IF certified device classes (CDC), and the design guidelines for consent enabled AHD and WAN device CDCs.

The design guidelines which support the following certified device classes (CDC) are defined in separate Recommendations as follows:

– H.812.1 Observation upload certified device class

– H.812.2 Questionnaires

– H.812.3 Capability exchange certified device class

– H.812.4 Authenticated persistent session device class

This Recommendation is part of the "ITU-T H.810 interoperability design guidelines for personal health systems" subseries, which is outlined in the table below:

Mapping of CDG 2013, ITU-T H.810 and restructured ITU-T H.810-series

Part	Elements	Clauses in the 2013 CDG "Endorphin"	Clauses in ITU-T H.810 (2013)	Restructured H.810-series (2015)
Part 0	System overview	Up to clause 3, plus Annex A and Appendix G	Up to clause 6, plus Annex A and Appendix V	ITU-T H.810 – System overview
Part 1	TAN/PAN/LAN	Clauses 4 to 7, Appendices C, D, M	Clauses 7 to 10, Appendices I, II, XI	ITU-T H.811 – TAN-PAN-LAN interface
Part 2	WAN	Clause 8, Appendices H, I, J, K	Clause 11; Appendices VI, VII, VIII, IX	ITU-T H.812 – WAN interface ITU-T H.812.1 – Observation upload ITU-T H.812.2 – Questionnaires ITU-T H.812.3 – Capability exchange ITU-T H.812.4 – Authenticated persistent session
Part 3	HRN	Clause 9, Appendices E, F, L	Clause 12, Appendices III, IV, X	ITU-T H.813 – HRN interface

History

Edition	Recommendation	Approval	Study Group	Unique ID[*]
1.0	ITU-T H.812	2015-11-29	16	11.1002/1000/12653

[*] 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

0 Introduction

The Continua design guidelines (CDG) define a framework of underlying standards and criteria which are required to ensure the interoperability of devices and data used for personal connected health.

This document contains a WAN-IF overview, common design guidelines for all WAN-IF certified device classes (CDC), and the design guidelines for consent enabled AHD and WAN device CDCs.

The design guidelines which support the following certified device classes (CDC) are defined in separate Recommendations as follows:

- ITU-T H.812.1 Observation upload certified device class
- ITU-T H.812.2 Questionnaires
- ITU-T H.812.3 Capability exchange certified device class
- ITU-T H.812.4 Authenticated persistent session device class

This Recommendation is part of the ITU-T H.810 subseries "ITU-T H.810 Interoperability design guidelines for personal health systems". 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 WAN-IF specific information which are helpful in comprehending the remainder of this document.

Clause 6: WAN-IF overview – This clause provides an overview of the WAN-IF CDCs.

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

Clause 8: Behavioural model – This clause is an overview of sequences of interactions under WAN common CDCs and summarizes typical interations, constraints and exceptions.

Clause 9: Implementation – This clause details the use of common payload content, and SOAP vs REST based transport methodology in the common WAN-IF certified device classes.

0.2 CDC 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: WAN interface: Common certified device class

1 Scope

This specification focuses on the following interface:

– **WAN-IF** The interface between application hosting devices (AHD) and the wide area network (WAN).

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

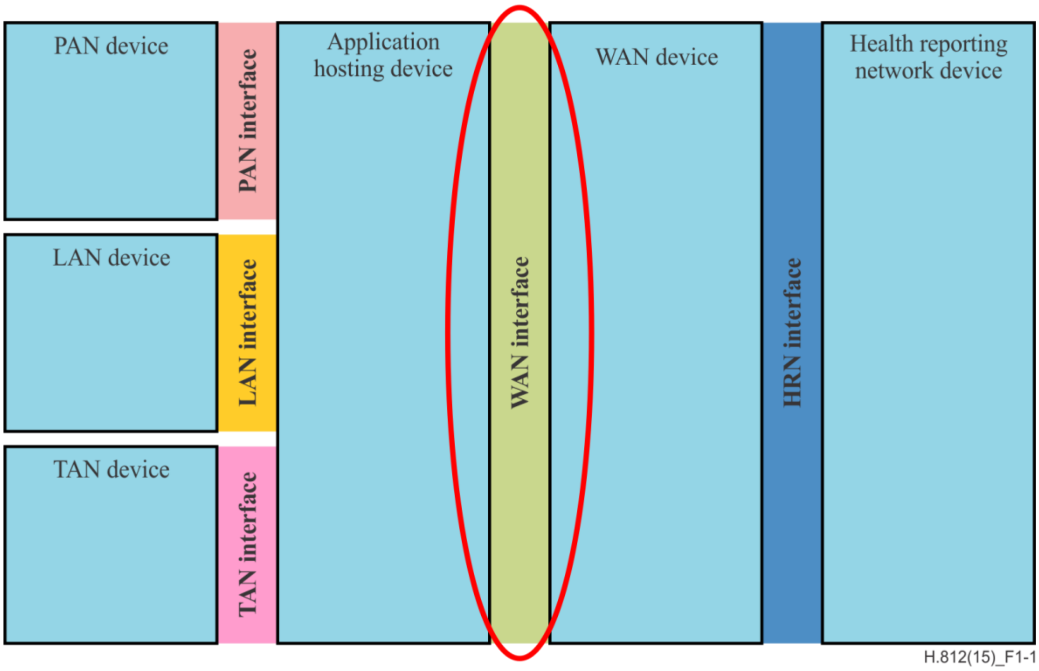

Figure 1-1 – WAN interface in the Continua architecture

There are a number of certified device classes (CDCs) related to the WAN-IF. This Recommendation contains interoperability design guidelines that are applicable to several CDCs. Security interoperability design guidelines is one such example. In addition, this document also contains the design guidelines for the Consent enabled AHD and WAN CDCs. These CDCs may be grouped with multiple other WAN-IF related CDCs, for example, WAN observation upload or Questionnaire enabled CDCs.

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 (2015), *Interoperability design guidelines for personal health systems*.

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

3 Definitions

These design guidelines use the terms defined in [ITU-T H810].

4 Abbreviations and acronyms

These design guidelines use the abbreviations and acronyms defined in [ITU-T H810].

5 Conventions

These design guidelines follow the conventions defined in [ITU-T H810].

6 Architecture

In this end-to-end reference architecture, the wide area network interface (WAN-IF) connects an application hosting device (AHD) to a WAN device (WD). See Figure 6-1 and Figure 6-2 below.

The WAN-IF design guidelines are focused on enabling the interoperable exchange of information across a wide area network. A set of WAN IF related certified device classes is defined for the AHD and WAN device to enable interoperability for a number of different use cases, including the uploading of measurement data, completing questionnaires and executing commands.

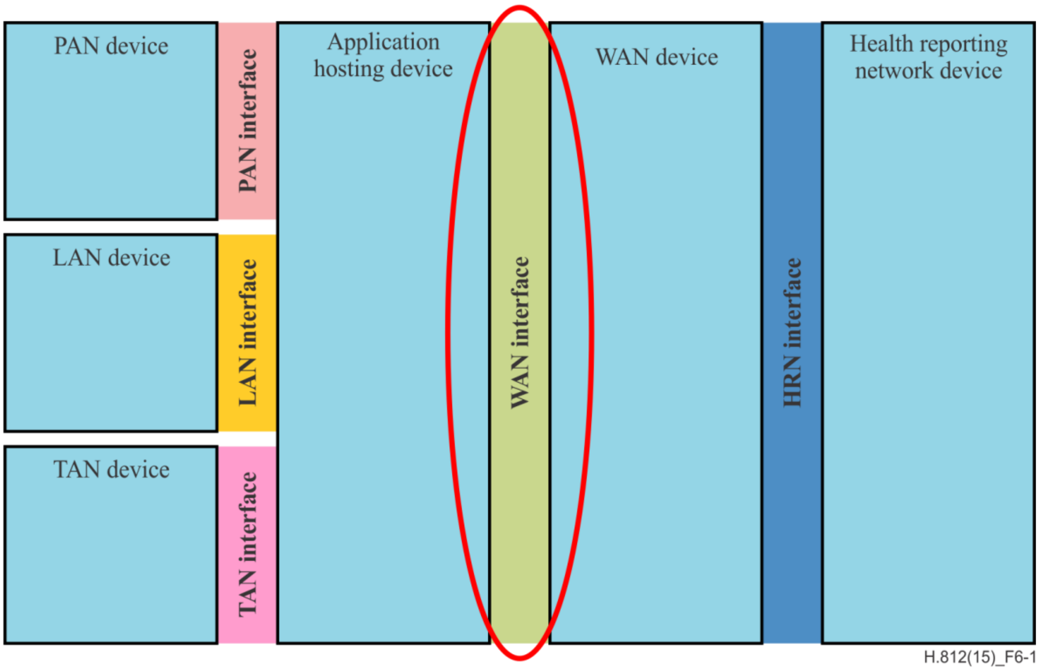

Figure 6-1 – WAN interface

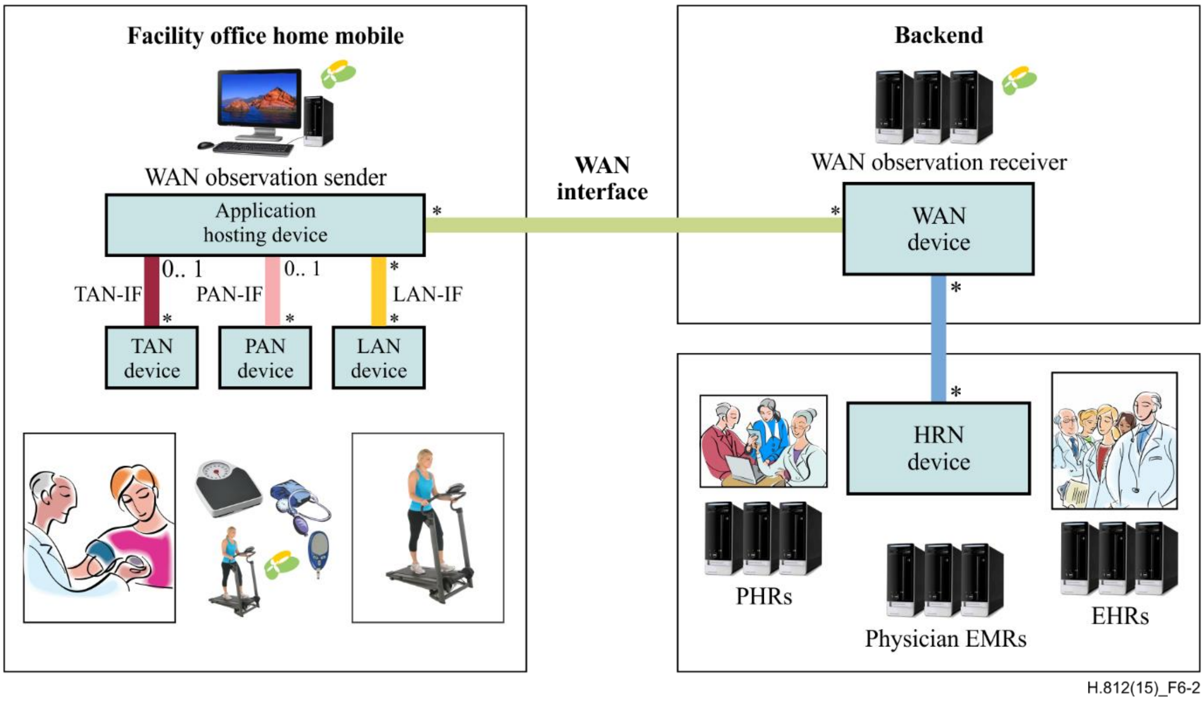

Figure 6-2 – WAN-IF examples

In addition to the WAN-IF, the end-to-end reference architecture also defines the health record network interface (HRN-IF). The WAN-IF is designed to enable granular information exchange between an application hosting device (typically a PC, laptop, tablet, mobile phone or other type of embedded device), which is a device close to the user/patient and a WAN device (typically a backend cloud based service) which collects the information from such users and makes it available for further usage. In contrast the HRN-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 HRN-IF is defined in [ITU-T H.813].

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

On the other hand, it is expected that a WAN device will be a more capable system such as a server or personal computer. Therefore, the design of the WAN-IF aims to push complexity and maintainability issues to the WAN device if this means that the issues can be avoided on the AHD.

The WAN-IF is an abstract channel composed of one or more CDC pairs that connect an AHD application with a WAN application. Each CDC pair has a component that resides in the WAN application and a component that resides in the AHD application. Continua defines certified device classes on both sides of the WAN-IF.

This version of the WAN-IF guidelines enables the following certified device classes:

[1] NOTE – Within the end-to-end architecture both the WAN and the HRN 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 device classes on specific hardware.

- the uploading of observations from the AHD to the WAN device in two different web services styles: (SOAP) and REST (hData) [ITU-T H.812.1];
- the uploading of consent information from the AHD to the WAN device in two different styles: web services (SOAP) and REST (hData) [ITU-T H.812];
- the downloading of to-be-completed questionnaires from the WAN device to the AHD and the uploading of completed questionnaires from the AHD to the WAN device [ITU-T H.812.2];
- the exchange of information (e.g., unsolicited commands) between the WAN device and the AHD over an authenticated persistent session [ITU-T H.812.4];
- the exchange of supported certified device class information (capability exchange) between the AHD and the WAN device as an enabler for the other use cases [ITU-T H.812.3].

An AHD can support one or more applications that each implements one or more Continua certified device classes. Figure 6-3 below depicts the Continua WAN-IF, showing an AHD application and a WAN application in which all of the possible WAN-IF certified device classes are implemented.

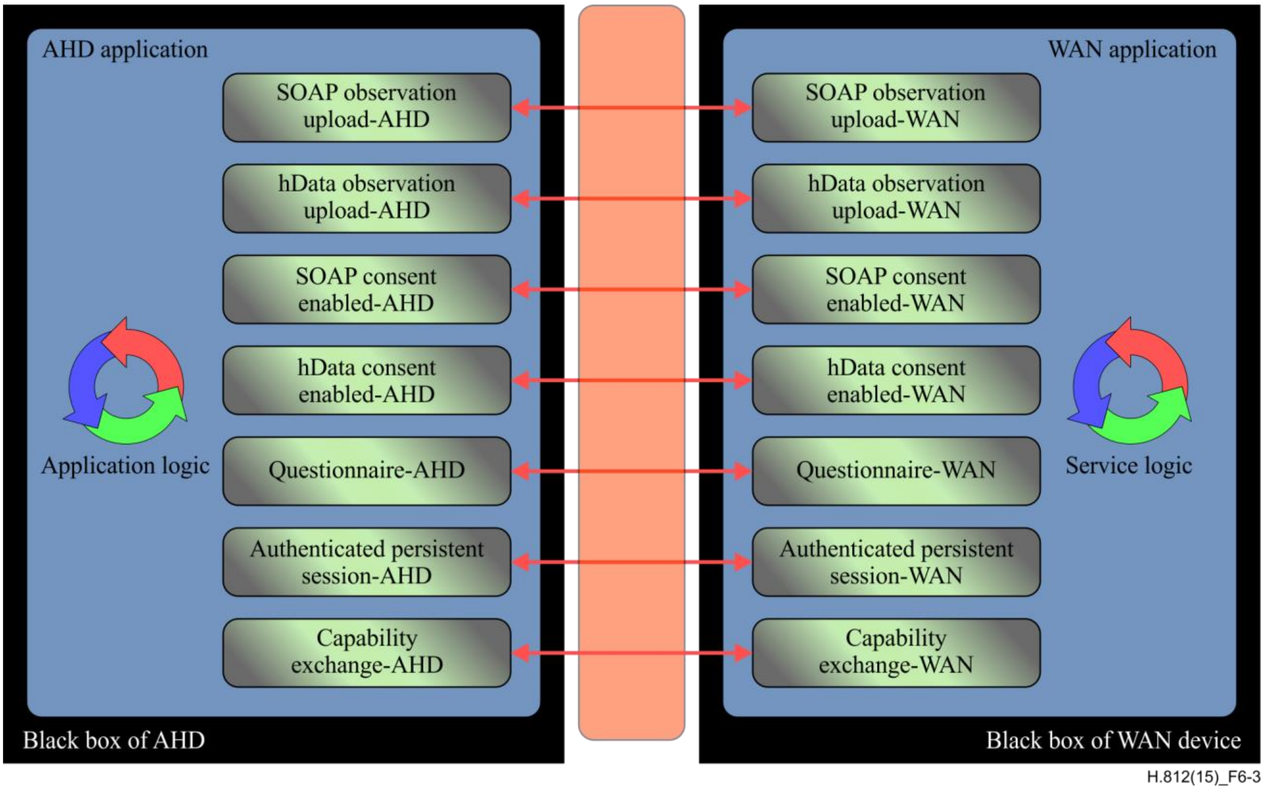

Figure 6-3 – Continua WAN-IF showing the WAN-IF certified device classes in this Release

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 device Class. The Guidelines make normative statements about how the network interface of the components of the CDC functions. For the WAN-IF these components exist in the context of applications or services that reside on an AHD or a WAN device.

Common platforms often limit the manner in which applications can communicate with each other to ensure stability of the overall platform. This limited interaction between applications is called sandboxing. In order to support sandboxed applications this version of the WAN-IF uses a reference model that defines an application as a container for one or more CDC 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 WAN-IF between the application's CDCs on the AHD and the corresponding CDCs on the WAN device are visible, and do have normative requirements in order to pass certification.

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

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

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

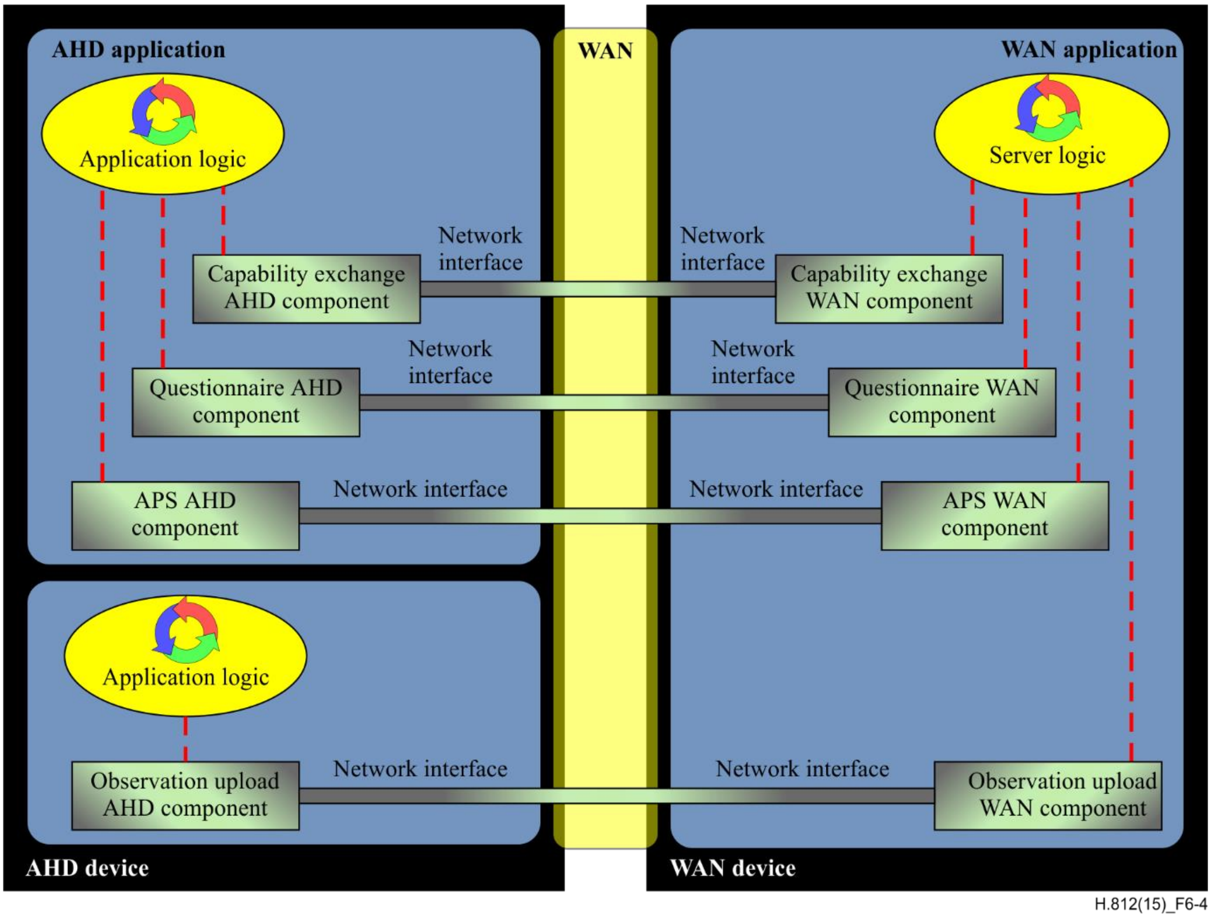

Figure 6-4 – WAN-IF Reference Model

Communications that use the WAN-IF start with the AHD's capability exchange component. This component sends a request to its peer component on the WAN device. The request asks the WAN service to specify the different certified device classes it supports. In common language the AHD application is asking "What things can you do?" The WAN application answers this in terms of the CDCs it supports. In Figure 6-4 above the WAN application would say "I support Capability Exchange, Questionnaires, SOAP observation upload and Authenticated Persistent Sessions". When the capability exchange component of the WAN application answers the AHD application, it will typically provide the AHD with additional information, such as a URL, which enables the AHD application to take the next step in communication with a particular CDC. An AHD that only supports observation uploading using SOAP does not need to implement capability exchange. Capability exchange does not need to be invoked if the AHD is already aware of the capabilities of the WAN device.

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 HIPAA (Health Information and Portability Accountability Act), 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 WAN-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 WAN 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 AHD 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 WAN 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., Disease Management Organization (DMO) which remotely monitors patients at home and collects health information from health measurement devices installed at Adam's home. During the time of registration, Adam fills in an eConsent form on the application hosting device (AHD). 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 AHD to DMO which provides remote patient monitoring service. Consent directive then governs access to patient data at the DMO and if Adam's data is sent to third parties (given that this is allowed, e.g., patient's PHR, EHRs, and EMRs), then Adam's privacy consent directive will 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

AHD provides a link to his latest version of the privacy consent directive document. Adam clicks on the link and AHD 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 AHD 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 WAN device 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 WAN device should enforce the consent preferences expressed in a consent document.

7.2.1 Encrypt to be uploaded content

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 AHD so 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 CDC use cases

See clause 6 in design guidelines

- H.812.1 Observation upload
- H.812.2 Questionnaire
- H.812.3 Capability exchange
- H.812.4 Authenticated persistent session

for their respective CDC use cases.

8 Behavioural Models

This clause includes

- WAN-IF message exchange behaviour
- Security behaviour of REST based CDCs
- The consent management and enforcement CDC behaviour

8.1 Common WAN-IF message exchange Behaviour

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

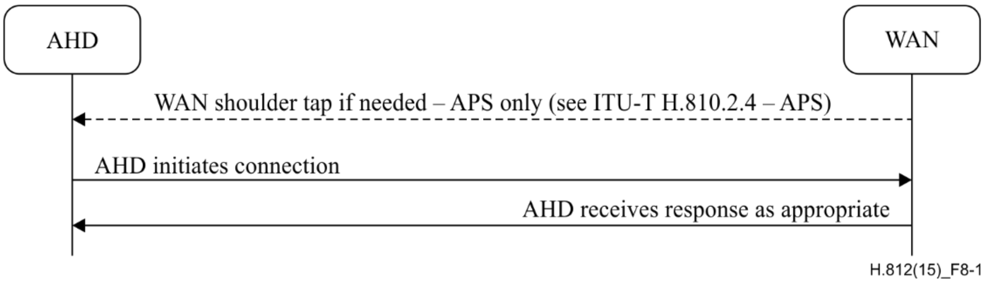
AHD
WAN
WAN shoulder tap if needed – APS only (see ITU-T H.810.2.4 – APS)
AHD initiates connection
AHD receives response as appropriate
H.812(15)_F8-1

Figure 8-1 – All connections are initiated from AHD

When TLS is required for point to point content security, the use of mutual certificate validation in the TLS handshake is up to policy.

When authentication is required,

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

– for hData, an OAuth 2.0 Bearer token.

How the AHD obtains these tokens is not specified by Continua. It depends upon the trust relationship established between the parties. The WAN 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 WAN device may support both services if it supports both hData and SOAP uploads. In either of these cases, an out-of-band operation must take place where the user of the AHD establishes some type of account on the WAN application allowing the client to obtain these tokens. The WAN device token service generates these tokens customized for the recipient which it can validate when it receives the content. On the other hand, the WAN device may require that these tokens be obtained from a third party authorization service (such as a CA) which the AHD has established a trust relationship with. In this case, the WAN device is letting the third party authorization service validate the client. The WAN device 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 policy.

8.2 Common security model for REST based CDC implementations

Figure 8-2 provides an interaction diagram for authorized RESTful transactions based on hData (REST) over HTTP. The authorization is realized using OAuth 2.0 authorization framework using resource owner password credentials as 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].

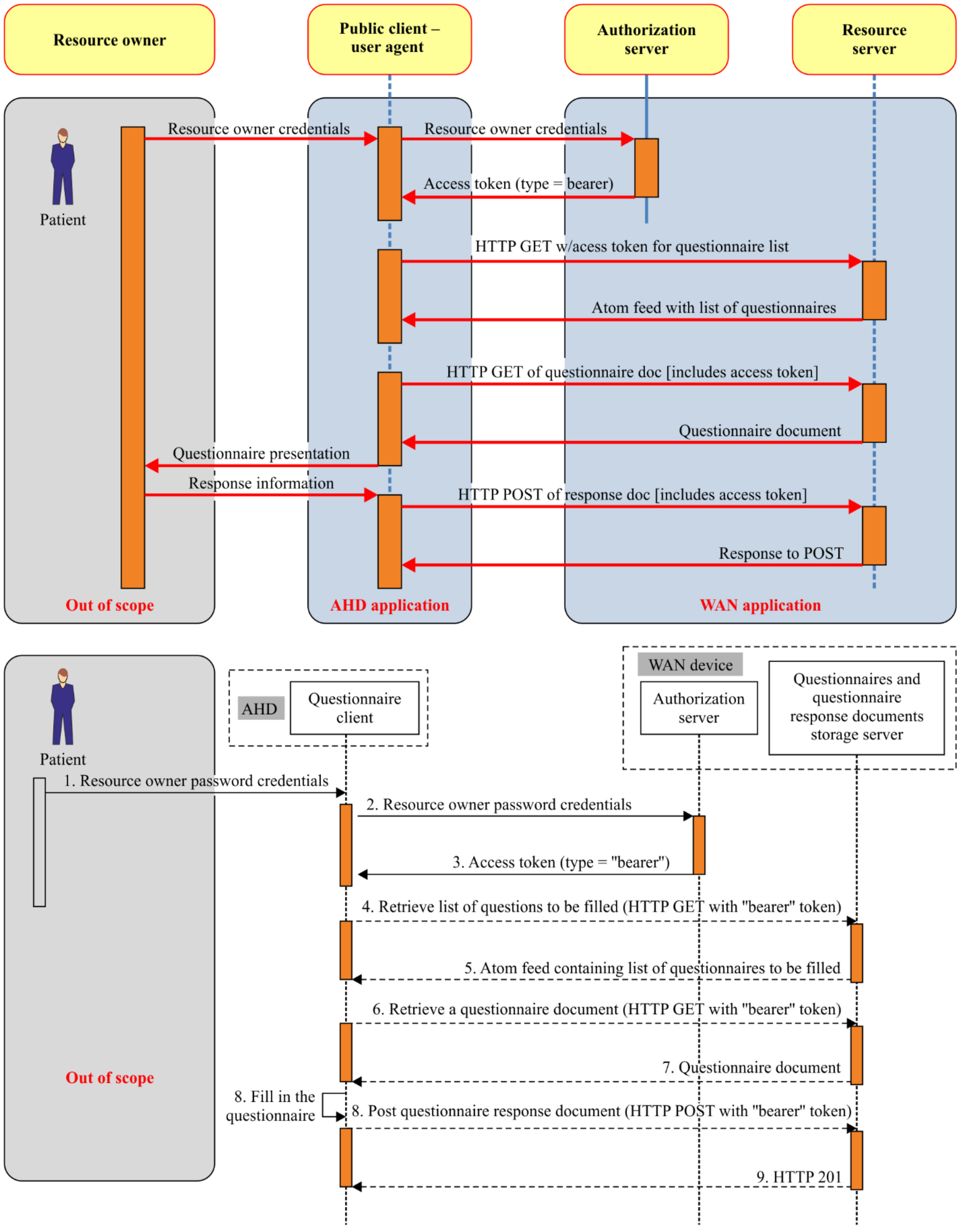
Resource owner
Public client – user agent
Authorization server
Resource server
Patient
Resource owner credentials
Resource owner credentials
Access token (type = bearer)
HTTP GET w/acess token for questionnaire list
Atom feed with list of questionnaires
HTTP GET of questionnaire doc [includes access token]
Questionnaire document
Questionnaire presentation
Response information
HTTP POST of response doc [includes access token]
Response to POST
Out of scope
AHD application
WAN application
Patient
AHD
Questionnaire client
WAN device
Authorization server
Questionnaires and questionnaire response documents storage server
1. Resource owner password credentials
2. Resource owner password credentials
3. Access token (type = "bearer")
4. Retrieve list of questions to be filled (HTTP GET with "bearer" token)
5. Atom feed containing list of questionnaires to be filled
6. Retrieve a questionnaire document (HTTP GET with "bearer" token)
7. Questionnaire document
8. Fill in the questionnaire
8. Post questionnaire response document (HTTP POST with "bearer" token)
9. HTTP 201
Out of scope
H.812(15)_F8-2

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

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

8.3 Consent management behavioural model

The following exchange mechanisms are specified for 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.

The following diagram illustrates transactions related to the consent management use cases described in this content profile.

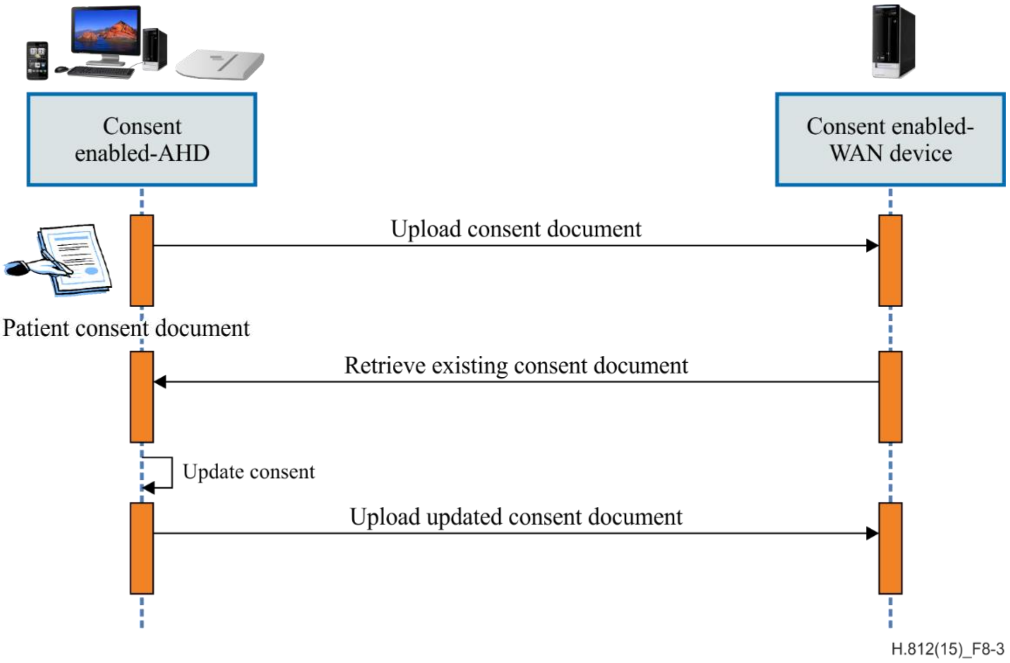

Figure 8-3 – Transactions between AHD and WAN device related to consent management

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.

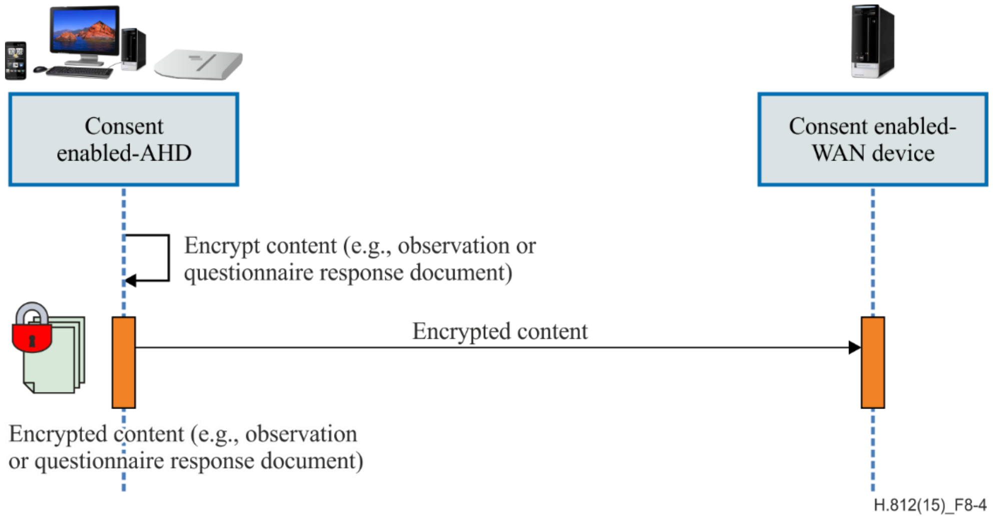
Consent enabled-AHD
Consent enabled-WAN device
Encrypt content (e.g., observation or questionnaire response document)
Encrypted content
Encrypted content (e.g., observation or questionnaire response document)
H.812(15)_F8-4

Figure 8-4 – Consent enforcement at the WAN-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 CD].

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 hData over HTTP

In this case, hData over HTTP is used as the transport protocol for the exchange of consent documents across WAN-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 hData over HTTP protocol between AHD and WAN devices 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 WAN-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 encrypiton

In the case of the transport protocol using [IHE ITI TFS XDR], XML encryption standard 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 WAN device.

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 hData over HTTP, consent enforcement is enabled through the use of the IHE DEN profile [IHE DEN].

Annex A

Normative guidelines

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

The WAN certified device classes are listed in Table A.1.

Table A.1 – Certified device classes

	Certified device classes	**Logo-ed device classes**
SOAP Observation Upload - AHD	Yes	Yes
SOAP Observation Upload - WAN	Yes	Yes
hData Observation Upload - AHD	Yes	Yes
hData Observation Upload - WAN	Yes	Yes
SOAP Consent Enabled - AHD	Yes	Yes
SOAP Consent Enabled - WAN	Yes	Yes
hData Consent Enabled - AHD	Yes	Yes
hData Consent Enabled - WAN	Yes	Yes
Questionnaire -AHD	Yes	Yes
Questionnaire - WAN	Yes	Yes
Capability Exchange - AHD	Yes	Yes
Capability Exchange - WAN	Yes	Yes
Authenticated Persistent Session - AHD	Yes	
Authenticated Persistent Session - WAN	Yes	

The guidelines that are applicable for each of the certified device classes are referenced in Table A.2 below.

Table A.2 – Guidelines for certified device classes

Certified device classes	**Relevant guidelines**
SOAP Observation Upload - AHD	See [ITU-T H.812.1] Tables A.0, A.1, C.0, C.1, D.1, and [ITU-T H.812] Table A.3, Table B.3
SOAP Observation Upload - WAN	See [ITU-T H.812.1] Tables A.0, A.2, C.0, C.2, D.1, and [ITU-T H.812] Table A.3, Table B.3
hData Observation Upload - AHD	See [ITU-T H.812.1] Tables A.0, A.1, B.1, D.1, and [ITU-T H.812] Table A.3, Table B.1
hData Observation Upload - WAN	See [ITU-T H.812.1] Tables A.0, A.2, B.2, D.1, and [ITU-T H.812] Table A.3, Table B.2
SOAP Consent Enabled - AHD	See [ITU-T H.812.1] Tables A.0, A.1, B.1, C.0, C.1, D.1, and [ITU-T H.812] Table A.3, Table B.3, Table C.5, Table C.7
SOAP Consent Enabled - WAN	See [ITU-T H.812.1] Tables A.0, A.2, B.2, C.0, C.2, D.1, and [ITU-T H.812] Table A.3, Table B.3, Table C.6, Table C.8
hData Consent Enabled - AHD	See [ITU-T H.812]Table A.3, Table C.1,Table C.3,

Table A.2 – Guidelines for certified device classes

Certified device classes	Relevant guidelines
	Table B.1
hData Consent Enabled - WAN	See [ITU-T H.812]Table A.3, Table C.2, Table C.4, Table B.2
Questionnaire - AHD	See [ITU-T H.812.2] Table A.1 and [ITU-T H.812] Table B.1
Questionnaire - WAN	See [ITU-T H.812.2] Table A.2 and [ITU-T H.812] Table A.3, Table B.2
Capability Exchange - AHD	See [ITU-T H.812.3] Table A.2 and [ITU-T H.812] Table A.3, Table B.1
Capability Exchange - WAN	See [ITU-T H.812.3] Table A.1, and [ITU-T H.812] Table A.3, Table B.2
Authenticated Persistent Session - AHD	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 - WAN	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 CDCs

Name	Description	Comments
CapX_WAN_Universality	All WAN devices **shall** support capability exchange	A WAN device that implements only SOAP based observation upload or consent enabled -WAN CDCs is not required to support the Capability Exchange-WAN CDC.
WAN_Transport_ Connection_Initiation	All Continua WAN connections **shall** be initiated from the WAN client component and **shall not** be initiated from the WAN application component	

Annex B

General security guidelines for WAN-IF CDCs

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

Table B.1 – AHD security guidelines using REST

Name	Description	Comments
AHD_Grant_Type	AHD may use Resource Owner Password Credential as Authorization Grant Type as defined in Section 1.3.3 of OAuth v2.0 [IETF RFC 6749].	AHD may use other means to get authorization token from the authorization server.
AHD_authorization_request	AHD may obtain authorization token from the authorization server according to Section 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 WAN_authorization_request_ response for the response
AHD_bearer_token	AHD **shall** use "bearer" token according to [IETF RFC 6750] when requesting access to a protected resource on the WAN device [IETF RFC 6750].	See the related guideline WAN_authorization_ request_response.
AHD_Token_Transmit	AHD **shall** use the Authorization Request Header Field Method when sending the bearer token as defined in Section 2.1 of [IETF RFC 6750].	
AHD_Confidentiality	AHD **shall** use TLS protocol v1.1 for secure point-to-point communication with the authorization server and WAN device [IETF RFC 4346].	
AHD_Cipher	AHD **should** use an encryption cipher suite of TLS_RSA_WITH_AES_128_ CBC_SHA	

Table B.2 – WAN Security Guidelines using REST

Name	Description	Comments
WAN_authorization_ request_response	WAN device 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 AHD_authorization_request for the request format. Authorization could be a separate entity and does not need to be the part of the WAN device.
WAN_refresh_token	WAN device implementing the authorization server **shall** return refresh token.	
WAN_Token_Evaluation	WAN device **shall** evaluate the authorization token and its scope before granting access to a record on the WAN device.	

Table B.3 – WAN IF transport security guidelines

Name	Description	Comments
WAN_Security_Transport	Continua WAN application and client components **shall** 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
WAN_Security_ Transport_Cipher	Continua WAN application and client components **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 HRN 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 AHD and WAN device
WAN_Confidentiality	WAN device **shall** use TLS protocol v1.1 for secure point-to-point communication with the authorization server and Questionnaire enabled WAN device [IETF RFC 4346].	
WAN_Cipher	WAN device **should** support TLS_RSA_WITH_AES_128_CBC_SHA encryption cipher suite.	

Annex C

Normative guidelines for consent management using REST

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

Table C.1 – Consent management guidelines using REST for the consent enabled AHD

Name	Description	Comments
AHD_Consent_Enabled	Consent enabled AHD shall comply with HL7 CDA R2 Consent Directive standard for the representation of patient consent preference [HL7 CDA CD].	
AHD_Consent_Enabled_ Transport_Standards	Consent enabled AHD shall comply to the following transport standards: HL7 Version 3 Specification: hData Record Format, Release 1 [HL7 hRF] OMG hData REST Binding for RLUS [OMG/hData BIND] OMG Retrieve, Locate, and Update Service (RLUS) Specification 1.0.1 [OMG/hData RLUS]	
AHD_Post_Consent	Consent enabled AHD shall use HTTP POST with the following URL for posting consent to the WAN device: *baseURL/continua/consent*	See the use case in Clause 7.1 For RLUS hData 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_AHD_ Observation_Association	The consent document transmitted by the Consent enabled AHD shall contain the same patient identifier as the WAN observation measurement message(s).	This is to associate the consent document to the WAN observation measurement messages.
Consent_Enabled_AHD_ 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_AHD_ Questionnaire Response_Confidentilality	Consent enabled AHD shall set the confidentiality code value to "R" in the header of the Questionnaire response document.	
Consent_Enabled_AHD_ Questionnaire Response_Association_Value	To associate Questionnaire response documents(s) with a patient consent document, Consent enabled AHD shall use the translation element of the confidentiality code system as defined in Table IV.3	See Table IV.1, Table IV.2, and Table IV.4

Table C.1 – Consent management guidelines using REST for the consent enabled AHD

Name	Description	Comments
Retrieving_Consent	Consent enabled AHD shall use HTTP GET with the following URL for retrieving consent from the WAN device: *baseURL/continua/consent* Consent enabled AHD shall use HTTP GET with the value of the link element from the ATOM feed entry for retrieving actual consent document from the WAN device and shall validate that it is a valid HL7 CDA R2 Consent Directive document [HL7 CDA CD].	See the use case in clause 7.1 For RLUS hData over REST transport, this is performed by performing an HTTP GET request without query parameters at the URL representing patient's consent hData section path which returns the ATOM feed entry. For further info Atom feed entry element consult Table I.1

Table C.2 – Consent management guidelines using REST for consent enabled WAN device

Name	Description	Comments
Consent_Enabled_WAN_Device	Consent enabled WAN device shall be able to receive, HL7 CDA R2 Consent Directive consent document(s) [HL7 CDA CD].	
WAN_Consent_Enabled_Transport_Standards	Consent enabled AHD shall comply to the following transport standards: HL7 Version 3 Specification: hData Record Format, Release 1 [HL7 hRF] OMG hData REST Binding for RLUS [OMG/hData BIND] OMG Retrieve, Locate, and Update Service (RLUS) Specification 1.0.1 [OMG/hData RLUS]	
WAN_Consent_Root	Consent enabled WAN device 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/2015/01/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/xml”	

Table C.2 – Consent management guidelines using REST for consent enabled WAN device

Name	Description	Comments
WAN_Consent_Validate	Consent enabled WAN device 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.	
WAN_Post_Consent-Response	Consent enabled WAN device shall create a consent document record after receiving POST message from the consent enabled AHD and send the HTTP 201 as a response.	See the AHD_Post_Consent above
AHD_Delete_Consent_Response	Consent enabled WAN device 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 hData for the consent enabled AHD

Name	Description	Comments
Consent_Enabled_AHD_ Content_Encryption_Actor	Consent enabled AHD shall encrypt the content in compliance with IHE Document Encryption (DEN) Profile [IHE DEN].	The content here could be the payload of the PCD-01 transaction or questionnaire response document.
Consent_Enabled_AHD_ Questionnaire_Response_MIMEtype_	Consent enabled AHD 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_AHD_Observation _Upload_MIMEtype_	Consent enabled AHD 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.
Consent_Enabled_AHD_ Content_Encryption_Algorithm	Consent enabled AHD 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_AHD_ Encryption_Recipient_Binding_PKI	Consent enabled AHD shall use PKI based key management method from IHE DEN Profile [IHE 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 hData for consent enabled WAN device

Name	Description	Comments
WAN_Device_HTTP_Ack	Consent enabled WAN device shall send the HTTP 202 as a response after successful reception of the encrypted content.	
Consent_Enabled_WAN_Device_Content_Decryption_Actor_XDR	Consent enabled WAN device shall comply with IHE DEN Profile to decrypt the encrypted content [IHE DEN].	
Consent_Enabled_WAN_Device_Key_Management	Consent enabled WAN device shall use PKI based key management method as specified by the IHE DEN Profile [IHE DEN].	
Consent_Enabled_WAN_Device_Decryption_Algorithm	Consent enabled WAN device 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_WAN_Device_Consent_Enforcement_	Consent enabled WAN device shall enforce consent preferences expressed in consent document.	E.g., prevents further disclosure of the content to the unauthorized entities

Table C.5 – Consent management guidelines using SOAP for the consent enabled AHD

Name	Description	Comments
WAN_Observation_AHD_Consent	Consent enabled WAN observation AHD **shall** comply with [HL7 CDA IG] Consent Directive to represent patient consent in a consent document	
WAN_Observation_AHD_Consent_Transport	Consent enabled WAN observation AHD **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	

Table C.5 – Consent management guidelines using SOAP for the consent enabled AHD

Name	Description	Comments
WAN_Observation_AHD_ Consent_Frequency	Consent enabled WAN observation AHD **shall** send the consent document at least once to the Observation WAN device	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 WAN device. 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 WAN device
WAN_Observation_ Measurement_ Consent_Document_ Association	The consent document transmitted by the consent enabled WAN observation AHD **shall** contain the same patient identifier as the WAN observation measurement message(s)	This is to associate the consent document to the WAN observation measurement messages
WAN_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 WAN device

Name	Description	Comments
Observation_WAN_ Device_Consent	Consent enabled observation WAN device **shall** be able to receive, [HL7 CDA IG] Consent Directive consent document(s)	
Observation_WAN_ Device_Consent_Transport	Consent enabled observation WAN device **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 WAN device 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 AHD

Name	Description	Comments
WAN_AHD_Content_Encryption_Actor	Consent enabled WAN observation AHD **shall** encrypt the payload (6.5.3 Data Guidelines) of the PCD-01 transaction in compliance with the encryption processing rules defined in clause 4.1 of the XML Encryption Specification [W3C XMLENC]	
WAN_AHD_Content_Encryption_MIMEtype	Consent enabled WAN observation AHD **shall** set the MIME type to "application/hl7-v2+xml"	The purpose is to indicate the type of payload that is encrypted
WAN_AHD_Content_Encryption_Algorithm	Consent enabled WAN observation AHD **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]
WAN_AHD_Encryption_ Recipient_Binding_PKI	For the content key transport, consent enabled WAN observation AHD **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 HRN-IF. To find out more, consult [b-RFC 3370] and the consent enforcement guidelines for the HRN-IF
WAN_AHD_Encryption_ Recipient_Binding_Symmetric	For the content key transport, the consent enabled WAN observation AHD **may** use AES-128 symmetric key wrap algorithm from the XML Encryption Specification. In case of password based encryption, the consent enabled WAN observation AHD **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
WAN_AHD_Integrity_Payload_PCD-01_Create	Consent enabled WAN observation AHD **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].

Table C.7 – Consent enforcement guidelines using SOAP for the consent enabled AHD

Name	Description	Comments
WAN_Encrypted_ Payload_PCD-01_ transaction	Consent enabled WAN observation AHD **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.
WAN_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 WAN device

Name	Description	Comments
WAN_Device_HTTP_Ack	Consent enabled observation WAN device **shall** send the SOAP HTTP response with the status code equal to 202 after the successful reception of the encrypted message. Consent enabled observation WAN device **should not** send the PCD-01 application level acknowledgement	The reason is that the observation WAN device may not be in possession of the decryption key as the content may be encrypted for a specific recipient on the WAN device
WAN_Device_Payload_ PCD-01_Verify_Integrity	Consent enabled observation WAN device **shall** verify the message digest of the encrypted payload	
WAN_Device_Payload_ PCD-01_Verify_Integrity_ Algorithm	Consent enabled observation WAN device **shall** support the SHA256 algorithm	
WAN_ Device_Content_ Decryption_Actor	Consent enabled observation WAN device **shall** comply with decryption rules specified in clause 4.2 of the XML Encryption Specification [W3C XMLENC].	
WAN_Device_Key_ Transport_RSA	Consent enabled observation WAN device **shall** support RSA Version 1.5 from the XML Encryption Specification [W3C XMLENC].	

Table C.8 – Consent enforcement guidelines using SOAP for consent enabled WAN device

Name	Description	Comments
WAN_Device_Key_ Transport_Symmetric	Consent enabled observation WAN device **shall** support AES-128 symmetric key wrap algorithm from the XML Encryption Specification [W3C XMLENC]. The consent enabled observation WAN device **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.
WAN_ Device _Content_ Decryption_Algorithm	Consent enabled observation WAN device **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 hData record.
Published	The published element shall be set to the data 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/2015/01/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

Consent using SOAP examples

(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_AHD^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_AHD^1234567890ABCDEF^EUI-64|POTest^AT4_AHD*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+
            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>
```

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/DeviceObservationCon
sumer_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/DeviceObservationCon
sumer_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 AHD 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 AHD.

– Authorization: Basic MTIwMDk0NTc0NjczNzY3OmI1NGRjODI0NzZhZjI4MTRlNjIwYjg2Nzc2YzQyYzBl

– This is a basic HTTP authorization header that is generated by Questionnaire enabled AHD 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":"789f3daf81a3
02e0636325114113e4b4","token_type":"bearer","expires_in":899}
```

Where

- "f779da766bfd1b9164b0fd6d280d52f1"is access token that would be used by AHD 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 AHD 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 AHD 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 III.7 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 WAN-IF	
2.16.840.1.113883.3.1817.1.7	Root OID for the HRN-IF	
2.16.840.1.113883.3.1817.1.2.1	E2E Security and Privacy: OID for the Continua Consent Directive code system	

Bibliography

See ITU-T H.810 (2015)] for a list of non-normative references and publications that contain further background information.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
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	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
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 and next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2016