International Telecommunication Union

ITU-T H.830.13

(08/2018)

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

SERIES H: AUDIOVISUAL AND MULTIMEDIA SYSTEMS

E-health multimedia services and applications – Interoperability compliance testing of personal health systems (HRN, PAN, LAN, TAN and WAN)

Conformance of ITU-T H.810 personal health system: Services interface Part 13: Capability Exchange: Health & Fitness Service sender

Recommendation ITU-T H.830.13

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
VEHICULAR GATEWAYS AND INTELLIGENT TRANSPORTATION SYSTEMS (ITS)	
Architecture for vehicular gateways	H.550–H.559
Vehicular gateway interfaces	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 SYSTEMS, 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
Safe listening	H.870–H.879

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

Recommendation ITU-T H.830.13

Conformance of ITU-T H.810 personal health system: Services interface Part 13: Capability Exchange: Health & Fitness Service sender

Summary

Recommendation ITU-T H.830.13 provides a test suite structure (TSS) and the test procedures (TP) for Capability Exchange through the Health & Fitness Service (HFS) sender in the Services interface, based on the requirements defined in the Recommendations of the ITU-T H.810 sub-series, of which Recommendation ITU-T H.810 (2017) is the base Recommendation. The objective of this test specification is to provide a high probability of interoperability at this interface.

This Recommendation includes an electronic attachment with the protocol implementation conformance statements (PICS) and the protocol implementation extra information for testing (PIXIT) required for the implementation of Annex A.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T H.830.13	2018-08-29	16	11.1002/1000/13674

Keywords

Capability exchange, conformance testing, continua design guidelines, e-health, health & fitness service receiver, personal connected health devices, services interface.

* 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

Electronic attachment: This Recommendation includes an electronic attachment with the protocol implementation conformance statements (PICS) and the protocol implementation extra information for testing (PIXIT) required for the implementation of Annex A.

Introduction

The table below shows the revision history of this test specification.

Version	Date	Revision history
1.0	2018-02-27	Initial release for the inclusion of Capability Exchange for Health & Fitness Service senders.

Recommendation ITU-T H.830.13

Conformance of ITU-T H.810 personal health system: Services interface Part 13: Capability Exchange: Health & Fitness Service sender

1 Scope

The scope of this Recommendation[1] is to provide test suite structure (TSS) and the test procedures (TP) for the Services interface based on the requirements defined in the Continua Design Guidelines (CDG) [ITU-T H.810 (2017)]. The objective of this test specification is to provide a high probability of interoperability at this interface.

The TSS and TP for the Services interface have been divided into the parts specified below. This Recommendation covers Part 13.

– Part 1: Web services interoperability: Health & Fitness Service sender
– Part 2: Web services interoperability: Health & Fitness Service receiver
– Part 3: SOAP/ATNA: Health & Fitness Service sender
– Part 4: SOAP/ATNA: Health & Fitness Service receiver
– Part 5: PCD-01 HL7 messages: Health & Fitness Service sender
– Part 6: PCD-01 HL7 messages: Health & Fitness Service receiver
– Part 7: Consent Management. Health & Fitness Service sender
– Part 8: Consent Management. Health & Fitness Service receiver
– Part 10: hData Observation Upload: Health & Fitness Service receiver
– Part 11: Questionnaires: Health & Fitness Service sender
– Part 12: Questionnaires: Health & Fitness Service receiver
– **Part 13: Capability Exchange: Health & Fitness Service sender**
– Part 14: Capability Exchange: Health & Fitness Service receiver
– Part 15: FHIR Observation Upload. Health & Fitness Service sender
– Part 16: FHIR Observation Upload. Health & Fitness Service receiver

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 (2017), *Interoperability design guidelines for personal connected health systems: Introduction.*

[ITU-T H.811] Recommendation ITU-T H.811 (2017), *Interoperability design guidelines for personal health systems: Personal Health Devices interface.*

---

[1] This Recommendation includes an electronic attachment with the protocol implementation conformance statements (PICS) and the protocol implementation extra information for testing (PIXIT) required for the implementation of Annex A.

[ITU-T H.812] Recommendation ITU-T H.812 (2017), *Interoperability design guidelines for personal health systems: Services interface.*

[ITU-T H.812.1] Recommendation ITU-T H.812.1 (2017), *Interoperability design guidelines for personal health systems: Services interface: Observation Upload certified capability class.*

[ITU-T H.812.2] Recommendation ITU-T H.812.2 (2017), *Interoperability design guidelines for personal health systems: Services interface: Questionnaire capability.*

[ITU-T H.812.3] Recommendation ITU-T H.812.3 (2017), *Interoperability design guidelines for personal health systems: Services interface: Capability Exchange capability.*

[ITU-T H.812.4] Recommendation ITU-T H.812.4 (2017), *Interoperability design guidelines for personal connected health systems: Services interface: Authenticated Persistent Session capability.*

[ITU-T H.813] Recommendation ITU-T H.813 (2017), *Interoperability design guidelines for personal connected health systems: Healthcare Information System interface.*

3 Definitions

3.1 Terms defined elsewhere

None.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AHD Application Hosting Device

ATNA Audit Trail and Node Authentication

CDA Clinical Document Architecture

CDG Continua Design Guidelines

CGM Continuous Glucose Monitor

DUT Device Under Test

FHIR Fast Healthcare Interoperability Resources

GUI Graphical User Interface

HFS Health & Fitness Service

HFSS Health & Fitness Service Sender

HFSR Health & Fitness Service Receiver

HL7 Health Level 7

HTTP Hypertext Transfer Protocol

HTTPS Hypertext Transfer Protocol Secure

INR International Normalized Ratio

IP	Insulin Pump
IUT	Implementation Under Test
MDS	Medical Device System
NFC	Near Field Communication
PCD	Patient Care Device
PCO	Point of Control and Observation
PCT	Protocol Conformance Testing
PHD	Personal Health Device
PHDC	Personal Healthcare Device Class
PHG	Personal Health Gateway
PICS	Protocol Implementation Conformance Statement
SABTE	Sleep Apnoea Breathing Therapy Equipment
SCR	Static Conformance Review
SOAP	Simple Object Access Protocol
TCRL	Test Case Reference List
TCWG	Test and Certification Working Group
TLS	Transport Level Security
TP	Test Purpose
TSS	Test Suite Structure
URI	Uniform Resource Identifier
USB	Universal Serial Bus
WAN	Wide Area Network
WDM	Windows Driver Model
WS	Web Service
WSDL	Web Service Description Language
WSI	Web Services Interoperability
XDR	Cross-Enterprise Document Reliable Interchange
XML	extensible Markup Language

5 Conventions

The key words "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "MAY", "MAY NOT" in this Recommendation are to be interpreted as in [b-ETSI SR 001 262].

– SHALL is equivalent to 'must' or 'it is required to'.
– SHALL NOT is equivalent to 'must not' or 'it is not allowed'.
– SHOULD is equivalent to 'it is recommended to'.
– SHOULD NOT is equivalent to 'it is not recommended to'.
– MAY is equivalent to 'is permitted'.
– MAY NOT is equivalent to 'it is not required that'.

NOTE – The above-mentioned key words are capitalized for illustrative purposes only and they do not appear capitalized within this Recommendation.

Reference is made in the [ITU-T H.800-series] of Recommendations to different versions of the Continua Design Guidelines (CDG) by a specific designation. The list of terms that may be used in this Recommendation is provided in Table 1.

Table 1 – List of designations associated with the various versions of the CDG

CDG release	Transposed as	Version	Description	Designation
2017	–	7.0	Release 2017 of the CDG including maintenance updates of the [b-CDG 2016] and additional guidelines that cover new functionalities.	–
2016 plus errata	[ITU-T H.810 (2016)]	6.1	Release 2016 plus errata noting all ratified bugs [b-CDG 2016].	–
2016	–	6.0	Release 2016 of the CDG including maintenance updates of the [b-CDG 2015] and additional guidelines that cover new functionalities.	Iris
2015 plus errata	[b-ITU-T H.810 (2015)]	5.1	Release 2015 plus errata noting all ratified bugs [b-CDG 2015]. The 2013 edition of [ITU-T H.810] is split into eight parts in the [ITU-T H.810-series].	–
2015	–	5.0	Release 2015 of the CDG including maintenance updates of the [b-CDG 2013] and additional guidelines that cover new functionalities.	Genome
2013 plus errata	[b-ITU-T H.810 (2013)]	4.1	Release 2013 plus errata noting all ratified bugs [b-CDG 2013].	–
2013	–	4.0	Release 2013 of the CDG including maintenance updates of the [b-CDG 2012] and additional guidelines that cover new functionalities.	Endorphin
2012 plus errata	–	3.1	Release 2012 plus errata noting all ratified bugs [b-CDG 2012].	–
2012	–	3.0	Release 2012 of the CDG including maintenance updates of the [b-CDG 2011] and additional guidelines that cover new functionalities.	Catalyst
2011 plus errata	–	2.1	[b-CDG 2011] integrated with identified errata.	–
2011	–	2.0	Release 2011 of the CDG including maintenance updates of the [b-CDG 2010] and additional guidelines that cover new functionalities [b-CDG 2011].	Adrenaline
2010 plus errata	–	1.6	[b-CDG 2010] integrated with identified errata.	–
2010	–	1.5	Release 2010 of the CDG with maintenance updates of the CDG Version 1 and additional guidelines that cover new functionalities [b-CDG 2010].	1.5

Table 1 – List of designations associated with the various versions of the CDG

CDG release	Transposed as	Version	Description	Designation
1.0	–	1.0	First released version of the CDG [b-CDG 1.0].	–

6 Test suite structure (TSS)

The test procedures (TPs) for the Services interface have been divided into the main subgroups specified below. Annex A describes the TPs for subgroups 1.8.1 and 1.8.2 (shown in bold):

– Group 1: HFS sender (HFSS)
  - Group 1.1: Web services interoperability (WSI)
    - Subgroup 1.1.1: Basic profile (BP)
    - Subgroup 1.1.2: Basic security profile (BSP)
    - Subgroup 1.1.3: Reliable messaging (RM)
  - Group 1.2: Simple object access protocol (SOAP)
    - Subgroup 1.2.1: SOAP headers (HEAD)
  - Group 1.3: Audit trail and node authentication (ATNA)
    - Subgroup 1.3.1: General (GEN)
    - Subgroup 1.3.2: PCD-01 (PCD-01)
    - Subgroup 1.3.3: Consent Management (CM)
  - Group 1.4: PCD-01 HL7 messages (PCD-01-DATA)
    - Subgroup 1.4.1: General (GEN)
    - Subgroup 1.4.2: Design guidelines (DG)
    - Subgroup 1.4.3: Pulse oximeter (PO)
    - Subgroup 1.4.4: Blood pressure monitor (BPM)
    - Subgroup 1.4.5: Thermometer (TH)
    - Subgroup 1.4.6: Weighing scales (WEG)
    - Subgroup 1.4.7: Glucose meter (GL)
    - Subgroup 1.4.8: Cardiovascular fitness and activity monitor (CV)
    - Subgroup 1.4.9: Strength fitness equipment (ST)
    - Subgroup 1.4.10: Independent living activity hub (HUB)
    - Subgroup 1.4.11: Adherence monitor (AM)
    - Subgroup 1.4.12: Peak expiratory flow monitor (PF)
    - Subgroup 1.4.13: Body composition analyser (BCA)
    - Subgroup 1.4.14: Basic electrocardiograph (ECG)
    - Subgroup 1.4.15: International normalized ratio (INR)
    - Subgroup 1.4.16: Sleep apnoea breathing therapy equipment (SABTE)
    - Subgroup 1.4.17: Insulin pump (IP)
    - Subgroup 1.4.18: Continuous glucose monitor (CGM)
  - Group 1.5: Consent Management (CM)
    - Subgroup 1.5.1: HFS XDR transaction (TRANS)

        - Subgroup 1.5.2: HFS metadata validation (META)
        - Subgroup 1.5.3: HFS consent directive validation (CDV)
    - Group 1.6: hData Observation Upload (HDATA)
        - Subgroup 1.6.1: General (GEN)
    - Group 1.7: Questionnaires (QUE)
        - Subgroup 1.7.1: General (GEN)
        - Subgroup 1.7.2: CDA validation (CDA)
    - **Group 1.8: Capability Exchange (CE)**
        - **Subgroup 1.8.1: General (GEN)**
        - **Subgroup 1.8.2: hData record format (HRF)**
    - Group 1.9: FHIR Observation Upload (FHIR)
        - Subgroup 1.9.1: General (GEN)
        - Subgroup 1.9.2: Encoding Guidelines (ENC)
- Group 2: HFS receiver (HFSR)
    - Group 2.1: Web service interoperability (WSI)
        - Subgroup 2.1.1: Basic profile (BP)
        - Subgroup 2.1.2: Basic security profile (BSP)
        - Subgroup 2.1.3: Reliable messaging (RM)
    - Group 2.2: SOAP (SOAP)
        - Subgroup 2.2.1: SOAP headers (HEAD)
    - Group 2.3: Audit (ATNA)
        - Subgroup 2.3.1: General (GEN)
        - Subgroup 2.3.2: PCD-01 (PCD-01)
        - Subgroup 2.3.3: Consent Management (CM)
    - Group 2.4: PCD-01 HL7 messages (PCD-01-DATA)
        - Subgroup 2.4.1: General (GEN)
        - Subgroup 2.4.2: Design guidelines (DG)
        - Subgroup 2.4.3: Pulse oximeter (PO)
        - Subgroup 2.4.4: Blood pressure monitor (BPM)
        - Subgroup 2.4.5: Thermometer (TH)
        - Subgroup 2.4.6: Weighing scales (WEG)
        - Subgroup 2.4.7: Glucose meter (GL)
        - Subgroup 2.4.8: Cardiovascular fitness and activity monitor (CV)
        - Subgroup 2.4.9: Strength fitness equipment (ST)
        - Subgroup 2.4.10: Independent living activity hub (HUB)
        - Subgroup 2.4.11: Adherence monitor (AM)
        - Subgroup 2.4.12: Peak expiratory flow monitor (PF)
        - Subgroup 2.4.13: Body composition analyser (BCA)
        - Subgroup 2.4.14: Basic electrocardiograph (ECG)
        - Subgroup 2.4.15: International normalized ratio (INR)
        - Subgroup 2.4.16: Sleep apnoea breathing therapy equipment (SABTE)

    - Subgroup 2.4.17: Insulin pump (IP)
    - Subgroup 2.4.18: Continuous glucose monitor (CGM)
- Group 2.5: Consent Management (CM)
    - Subgroup 2.5.1: HFS XDR transaction (TRANS)
    - Subgroup 2.5.2: HFS service validation (SER)
- Group 2.6: hData Observation Upload (HDATA)
    - Subgroup 2.6.1: General (GEN)
    - Subgroup 2.6.2: hData record format (HRF)
- Group 2.7: Questionnaires (QUE)
    - Subgroup 2.7.1: General (GEN)
    - Subgroup 2.7.2: CDA validation (CDA)
    - Subgroup 2.7.3: hData record format (HRF)
- Group 2.8: Capability Exchange (CE)
    - Subgroup 2.8.1: General (GEN)
    - Subgroup 2.8.2: hData record format (HRF)
- Group 2.9: FHIR Observation Upload (FHIR)
    - Subgroup 2.9.1: General (GEN)

7 Electronic attachment

The protocol implementation conformance statements (PICS) and the protocol implementation extra information for testing (PIXIT) required for the implementation of Annex A can be downloaded from http://handle.itu.int/11.1002/2000/12067. See [b-HFSR PICS & PIXIT] and [b-HFSS PICS & PIXIT].

In the electronic attachment, letters "C" and "I" in the column labelled "Mandatory" are used to distinguish between "PICS" and "PIXIT" respectively during testing. If the cell is empty, the corresponding PICS is "independent". If the field contains a "C", the corresponding PICS is dependent on other PICS, and the logical expression is detailed in the "SCR_Expression" field. The static conformance review (SCR) is used in the test tool to assert whether the PICS selection is consistent.

Annex A

Test procedures

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

A.1 TP definition conventions

The test procedures (TPs) are defined according to the following rules:

- **TP Id**: This is a unique identifier (TP/<TT>/<DUT>/<GR>/<SGR>/<XX> – <NNN>). It i specified according to the naming convention defined below:
  - Each test purpose identifier is introduced by the prefix "TP".
  - <TT>: This is the test tool that will be used in the test case.
    - HFS: Health & Fitness Services interface
  - <DUT>: This is the device under test.
    - SEN: HFS sender
    - REC: HFS receiver
  - <GR>: This identifies a group of test cases.
  - <SGR>: This identifies a subgroup of test cases.
  - <XX>: This identifies the type of testing.
    - BV: Valid behaviour test
    - BI: Invalid behaviour test
  - <NNN>: This is a sequential number that identifies the test purpose.
- **TP label**: This is the title of the TP.
- **Coverage**: This contains the specification reference and clause to be checked by the TP.
  - Spec: This indicates the earliest version of the specification from which the testable items to be checked by the TP were included.
  - Testable item: This contains testable items to be checked by the TP.
- **Test purpose**: This is a description of the requirements to be tested.
- **Applicability**: This contains the protocol implementation conformance statement (PICS) items that define if the test case is applicable or not for a specific device. When a TP contains an "ALL" in this field it means that it applies to the device under test within that scope of the test (specialization, transport used, etc.).
- **Other PICS**: This contains additional PICS items (apart from the PICS specified in the Applicability row) which are used within the test case implementation and can modify the final verdict. When this row is empty, it means that only the PICS specified in the Applicability row are used within the test case implementation.
- **Initial condition**: This indicates the state to which the device under test (DUT) needs to be moved at the beginning of TC execution.
- **Test procedure**: This describes the steps to be followed in order to execute the test case.
- **Pass/Fail criteria**: This provides criteria to decide whether the DUT passes or fails the test case.

A.2 Subgroup 1.8.1: General (GEN)

<table>
<tr><td colspan="2">TP Id</td><td colspan="3">TP/HFS/SEN/CAP/GEN/BV-000</td></tr>
<tr><td colspan="2">TP label</td><td colspan="3">Root file retrieval</td></tr>
<tr><td rowspan="5">Coverage</td><td>Spec</td><td colspan="3">[ITU-T H.812]</td></tr>
<tr><td rowspan="2">Testable items</td><td>RESTSec 3; M</td><td>RESTSec 4; M</td><td>RESTSec 5; M</td></tr>
<tr><td>CommonReq 5; M</td><td></td><td></td></tr>
<tr><td>Spec</td><td colspan="3">[ITU-T H.812.3]</td></tr>
<tr><td rowspan="2">Testable items</td><td>Capab 25; M</td><td>Capab 26; M</td><td>Capab 27; M</td></tr>
<tr><td>Capab 28; O</td><td></td><td></td></tr>
<tr><td colspan="2">Test purpose</td><td colspan="3">Check that:
The PHG retrieves the root file (in XML format) of the simulated Health & Fitness Service using HTTP GET, a TLS v1.1 secure channel and optionally an Oauth v2.0 authorization bearer token.
[AND]
If supported, the PHG retrieves the root file (in JSON format) of the simulated Health & Fitness Service using HTTP GET, a TLS v1.1 secure channel and, optionally, an Oauth v2.0 authorization bearer token.</td></tr>
<tr><td colspan="2">Applicability</td><td colspan="3">C_SEN_000 AND C_SEN_GEN_005</td></tr>
<tr><td colspan="2">Other PICS</td><td colspan="3">C_SEN_CAP_001</td></tr>
<tr><td colspan="2">Initial condition</td><td colspan="3">The simulated Health & Fitness Service is compliant with Capability Exchange and provides a URL ("baseURL") so that the PHG can obtain the H&FS root file in XML and JSON format. A simulated HFS receiver also provides an Oauth v2.0 token for authorization using resource owner password credentials grant type that requires TLS 1.1.</td></tr>
<tr><td colspan="2">Test procedure</td><td colspan="3">1. Ask the PHG to retrieve the root file of the simulated Health & Fitness Service in XML format.
2. The PHG optionally uses the provided client_id, client secret, username and password parameters to obtain an Oauth v2.0 bearer token from the test tool using resource owner password credentials grant type and TLS 1.1 security.
3. The PHG uses HTTP GET at the provided URL to request the root file of the H&FS in XML format using TLS 1.1 security. If an Oauth v2.0 token is used, the PHG uses the authorization request header field method as defined in Section 2.1 of RFC6750 [b-IETF RFC 6749] to send the obtained bearer token in the request.
4. The simulated H&FS accepts the request and sends the root.xml file to the PHG under test.
5. The user confirms that the PHG receives and processes the root.xml file of the simulated Health & Fitness Service correctly.
6. IF C_SEN_CAP_001=TRUE continue with step 7, ELSE the test case ends.
7. Ask the PHG to retrieve the root file of the simulated Health & Fitness Service in JSON format.
8. The PHG optionally uses the provided client_id, client secret, username and password parameters to obtain an Oauth v2.0 bearer token from the test tool using resource owner password credentials grant type and TLS 1.1 security.
9. The PHG uses HTTP GET at the provided URL to request the root file of the H&FS in JSON format using TLS 1.1 security. If an Oauth v2.0 token is used, the PHG uses the authorization request header field method as defined in Section 2.1 of RFC6750 [b-IETF RFC 6749] to send the obtained bearer token in the request.</td></tr>
</table>

	10. The simulated H&FS accepts the request and sends the root.json file to the PHG under test. 11. The user confirms that the PHG receives and processes the root.json file of the simulated Health & Fitness Service correctly.
Pass/Fail criteria	• The PHG application uses HTTP GET with the provided URL for requesting the H&FS root file (XML or JSON format) using a TLS v1.1 secure channel. • If the PHG provides an Oauth 2.0 bearer token, it uses the authorization request header field method as defined in Section 2.1 of RFC6750 [b-IETF RFC 6749] to send the obtained bearer token when requesting the root file (XML or JSON format). • The PHG specifies "application/xml" in the HTTP accept header when requesting the root file of the H&FS in XML format. • The user confirms the correct retrieval and processing of the root.xml file by the PHG. • The PHG specifies "application/jsonl" in the HTTP accept header if it requests the root file of the H&FS in JSON format. • If requested, the user confirms the correct retrieval and processing of the root.json file by the PHG.
Notes	

TP Id		TP/HFS/SEN/CAP/GEN/BV-001		
TP label		Root file posting		
Coverage	**Spec**	[ITU-T H.812]		
	Testable items	RESTSec 3; M	RESTSec 4; M	RESTSec 5; M
		CommonReq 5; M		
	Spec	[ITU-T H.812.3]		
	Testable items	Capab 29; O		
Test purpose		Check that: The PHG sends its root file (in XML of JSON format) to the simulated Health & Fitness Service using HTTP POST, a TLS v1.1 secure channel and an Oauth v2.0 authorization bearer token.		
Applicability		C_SEN_000 AND C_SEN_GEN_005 AND (C_SEN_CAP_002 OR C_SEN_CAP_003)		
Other PICS				
Initial condition		Simulated Health & Fitness Service is compliant with Capability Exchange and provides a URL so that the PHG can send its root file (baseURL/roots). Simulated HFS receiver also provides an Oauth v2.0 token for authorization using resource owner password credentials grant type that requires TLS 1.1.		
Test procedure		1. IF C_SEN_CAP_002=TRUE, proceed to step 2, ELSE go to step 6. 2. Ask the PHG under test to send its root.xml file to the simulated H&FS. 3. The PHG uses the provided client_id, client_secret, username and password parameters to obtain an Oauth v2.0 bearer token from the test tool using resource owner password credentials grant type and TLS 1.1 security. 4. The PHG uses the authorization request header field method as defined in Section 2.1 of RFC6750 [b-IETF RFC 6749] to send the obtained bearer token with the root file to the test tool according to RFC6750 and using TLS 1.1 security. 5. The simulated H&FS receives the root.xml file at the expected URL.		

	6. IF C_SEN_CAP_003=TRUE, ask the PHG under test to send its root.json file to the simulated H&FS. 7. The PHG uses the provided client_id, client_secret, username and password parameters to obtain an Oauth v2.0 bearer token from the test tool using resource owner password credentials grant type and TLS 1.1 security. 8. The PHG uses the authorization request header field method as defined in Section 2.1 of RFC6750 [b-IETF RFC 6749] to send the obtained bearer token with the root file to the test tool according to RFC6750 and using TLS 1.1 security. 9. The simulated H&FS receives the root.json file at the expected URL.
Pass/Fail criteria	• The PHG under test uses HTTP POST with the provided URL, TLS 1.1 and an Oauth v2.0 bearer token using authorization request header field method for uploading the root.xml (and/or the root.json) file to the simulated H&FS. • The root file is uploaded to the correct URL.
Notes	

TP Id		TP/HFS/SEN/CAP/GEN/BV-002		
TP label		Root file content		
	Spec	[ITU-T H.812.3]		
	Testable items	Capab 31; M		
Test purpose		Check that: The root file of the PHG contains a profile element for each CCC it supports.		
Applicability		C_SEN_000 AND C_SEN_GEN_005 AND (C_SEN_CAP_002 OR C_SEN_CAP_003)		
Other PICS		C_SEN_GEN_003, C_SEN_GEN_004, C_SEN_GEN_006, C_SEN_GEN_007, C_SEN_GEN_008		
Initial condition		The simulated Health & Fitness Service is compliant with Capability Exchange and provides a URL so that the PHG can send its root file (baseURL/roots). A Simulated HFS receiver also provides an Oauth v2.0 token for authorization using resource owner password credentials grant type that requires TLS 1.1.		
Test procedure		1. IF C_SEN_CAP_002=TRUE, proceed to step 2, ELSE go to step 4. 2. Ask the PHG under test to send its root.xml file to the simulated H&FS using TLS 1.1 security and an OAuth v2.0 bearer token. 3. The simulated H&FS receives the root.xml file and checks that: a) The root file contains a <profile> element with an <id> element with the value "CapabilityExchange". b) If C_SEN_GEN_003=TRUE the root file contains a <profile> element with an <id> element with the appropriate value for SOAP Observation Upload – PHG Continua Certified Capability Class. c) If C_SEN_GEN_004=TRUE the root file contains a <profile> element with an <id> element with the appropriate value for hData Observation Upload – PHG Continua Certified Capability Class. d) If C_SEN_GEN_006=TRUE the root file contains a <profile> element with an <id> element with the appropriate value for the Questionnaire Continua Certified Capability Class. e) If C_SEN_GEN_007=TRUE the root file contains a <profile> element with an <id> element with the appropriate value for the FHIR Observation Client Continua Certified Capability Class.		

	f) If C_SEN_GEN_008=TRUE the root file contains a <profile> element with an <id> element with the appropriate value for the FHIR Observation Reporting Client Continua Certified Capability Class. 4. IF C_SEN_CAP_003=TRUE, ask PHG under test to send its root.json file to the simulated H&FS. 5. The simulated H&FS receives the root.json file and checks that its content is as described in step 3 for the XML version.
Pass/Fail criteria	• The root file (XML, JSON or both) contains all the CCCs declared by the PHG.
Notes	Contents of the JSON version of the root file can be checked by applying the XML-to-JSON conversion rules in [b-HL7 V3 HRF]

A.3 Subgroup 1.8.2: hData record format (HRF)

TP Id		TP/HFS/SEN/CAP/HRF/BV-000		
TP label		Root file format		
Coverage	**Spec**	[ITU-T H.812]		
	Testable items	CommonReq 5;M		
	Spec	[ITU-T H.812.3]		
	Testable items	Capab 30; M		
	Spec	[b-HL7 V3 HRF]		
	Testable items	Root 1; M	Root 2; M	Root 3; M
		Root 4; M	Root 5; M	Root 6; M
		Root 7; M	Root 8; M	Root 9; M
		Root 10; M	Root 11; M	Root 12; M
		Root 13; M	Root 14; M	Root 15; M
		Root 16; M	Root 17; M	Root 18; M
		Root 19; M	Root 20; M	Root 21; M
		Root 22; M	Root 23; M	Root 24; M
Test purpose		Check that: The root file of the PHG complies to the HL7 Version 3 Specification: hData Record Format, Release 1		
Applicability		C_SEN_000 AND C_SEN_GEN_005 AND C_SEN_CAP_002		
Other PICS		C_SEN_CAP_003		
Initial condition		The simulated Health & Fitness Service is compliant with Capability Exchange and provides a URL so that the PHG can send its root file (baseURL/roots). The simulated HFS receiver also provides an Oauth v2.0 token for authorization using resource owner password credentials grant type that requires TLS 1.1.		

Test procedure	1. Ask the PHG under test to send its root file in XML format to the simulated H&FS (using the provided URL, TLS 1.1 and an Oauth v2.0 bearer token). 2. In the received root file check that: a) The id element of the root is present (1..1) and its type is xs:string. b) The version element of the root is present (1..1), its type is xs:integer, and its value is "1". c) The created element of the root is present (1..1) and its type is xs:dateTime. The value of this element should be significant to at least the second. d) The lastModified element of the root is present (1..1) and its type is xs:dateTime. The value of this element should be significant to at least the second. e) The author element of the root may be present (0..*). • The name element of the author is present (1..1) and its type is xs:string. • The uri element of the author may be present (0..1) and its type is xs:anyURI. • Te email element of the author may be present (0..1) and its type is xs:string. f) The profile element of the root may be present (0..*). • The id element of the profile is present (1..1) and its type is xs:string. The id must be unique within the root file. • The reference element of the profile is present (1..1) and its type is xs:string. It is recommended to use a URL. g) The resourceType element of the root is present (1..*). Each type of resource must have a resourceType element. • The id element of resourceType is present (1..1) and its type is xs:string. The id must be unique within the root file. It is recommended to use a human-readable class or type name for this id. • The reference element of resourceType is present (1..1) and its type is xs:string. It is recommended to use a URL. • The representation element of resourceType MAY be present (0..*). It is recommended to provide an explicit representation. ▪ The mediaType element of representation is present (1..1) and its type is xs:string. ▪ The validator element of representation may be present (0..*) and its type is xs:string. It is recommended to use a URL. h) The section element of the root is present (1..*). Each section except the top level section of the hierarchy must have a corresponding section element. • The path element of a section is present (1..1) and its type is xs:string. The path is used to construct the full path to the section. A section path must not begin with the "@" symbol. • The profileID element of a section may be present (0..*) and its type is xs:string. The value of this element must be equal to the id attribute of a profile element. • The resourcePrefix element of a section may be present (0..*) and its type is xs:boolean. If resourcePrefix is false, path templates must not be used. • The resourceTypeID element of a section may be present (0..*) and its type is xs:string. The value of this element must be equal to the id attribute of a resourceType element. • The metadataSupport element of a section may be present (0..*) and its type is xs:boolean. • The section element of a section may be present (0..*), as subsections of the current section. 3. IF C_SEN_CAP_003=TRUE, ask the PHG under test to send its root file in JSON format to the simulated H&FS (using the provided URL, TLS 1.1 and an Oauth v2.0 bearer token).

	4. In the received root file check compliance to the format described in 2, applying the following rules to create the JSON representation: • Simple XML elements are represented by JSON name-value pairs. • Complex XML elements are represented by JSON objects, whose names are the same as the corresponding XML element names. • XML attributes appear as JSON properties, using the name of the attribute as the property name. • Namespace references are not present. • Repeating XML elements are represented as JSON arrays. This rule applies even to XML elements that appear only once in a particular instance, if the upper cardinality of that element is greater than one. • xs:integer values are represented using a native JSON int. • xs:boolean values are represented using JSON's "true" and "false" values. • xs:dateTime is represented as plain text. • Other primitive types are represented as JSON strings, using the same serialization as the XML form.
Pass/Fail criteria	• Uploaded root.xml file is compliant with the format described in 2. • Uploaded root.json file is compliant with the format described in 4.
Notes	xs prefix refers to the XML Schema namespace (http://www.w3.org/2001/XMLSchema)

Bibliography

[b-ITU-T H.810 (2013)] Recommendation ITU-T H.810 (2013), *Interoperability design guidelines for personal health systems*.

[b-ITU-T H.810 (2015)] Recommendation ITU-T H.810 (2015), *Interoperability design guidelines for personal health systems.*

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

[b-HSTP-H812-FHIR] ITU-T Technical Paper HSTP-H812-FHIR (2017), *Interoperability design guidelines for personal health systems: Services interface: FHIR Observation Upload for trial implementation*. https://www.itu.int/pub/publications.aspx?lang=en&parent=T-TUT-EHT-2017-H812FHIR

[b-CDG 1.0] Continua Health Alliance (2008) *Continua Design Guidelines v1.0.*

[b-CDG 2010] Continua Health Alliance (2010), *Continua Design Guidelines v1.5.*

[b-CDG 2011] Continua Health Alliance (2011), *Continua Design Guidelines, Adrenaline*.

[b-CDG 2012] Continua Health Alliance (2012), *Continua Design Guidelines, Catalyst.*

[b-CDG 2013] Continua Health Alliance (2013), *Continua Design Guidelines, Endorphin.*

[b-CDG 2015] Continua Health Alliance (2015), *Continua Design Guidelines, Genome.*

[b-CDG 2016] Personal Connected Health Alliance (2016), *Continua Design Guidelines, Iris.*

[b-ETSI SR 001 262] ETSI SR 001 262 v1.8.1 (2003), *ETSI drafting rules*. <https://docbox.etsi.org/MTS/MTS/10-PromotionalMaterial/MBS-20111118/Referenced%20Documents/Drafting%20Rules.pdf>

[b-HFSR PICS & PIXIT] HFS Receiver PICS and PIXIT Test Tool v7.0.0.0 – Excel sheet v1.8. <https://handle.itu.int/11.1002/2000/12067>

[b-HFSS PICS & PIXIT] HFS Sender PICS and PIXIT Test Tool v7.0.0.0 – Excel sheet v1.8. <https://handle.itu.int/11.1002/2000/12067>

[b-IETF RFC 6749] IETF RFC 6749 (2012), *The OAuth 2.0 Authorization Framework.* <http://tools.ietf.org/html/rfc6749>

[b-IETF RFC 6750] IETF RFC 6750 (2012), *The OAuth 2.0 Authorization Framework: Bearer Token Usage.* <http://tools.ietf.org/html/rfc6750>

[b-HL7 V3 HRF] Health Level Seven (2014), *HL7 Version 3 Specification: hData Record Format, Release 1*. <http://www.hl7.org/documentcenter/private/standards/v3/V3_ITS_HDATA_RF_R1_2014JUN.pdf>

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, 2018