International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

H.830.4

(04/2017)

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 4: SOAP/ATNA: Health & Fitness Service receiver

Recommendation ITU-T H.830.4

International Telecommunication Union

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.830.4

Conformance of ITU-T H.810 personal health system: Services interface Part 4: SOAP/ATNA: Health & Fitness Service receiver

Summary

Recommendation ITU-T H.830.4 provides a test suite structure (TSS) and the test purposes (TP) for SOAP/ATNA messages through the Health & Fitness Service (HFS) receiver 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 (2016) is the base Recommendation. The objective of this test specification is to provide a high probability of interoperability at this interface.

Recommendation ITU-T H.830.4 is the transposition of Continua Test Tool DG2016, Test Suite Structure & Test Purposes, Services Interface; Part 4: SOAP/ATNA. HFS Receiver (Version 1.7, 2017-03-14), that was developed by the Personal Connected Health Alliance. A number of versions of this specification existed before transposition.

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.834	2015-01-13	16	11.1002/1000/12252
1.0	ITU-T H.830.4	2015-01-13	16	11.1002/1000/12590
2.0	ITU-T H.830.4	2016-07-14	16	11.1002/1000/12924
3.0	ITU-T H.830.4	2017-04-13	16	11.1002/1000/13211

Keywords

Conformance testing, Continua Design Guidelines, e-health, ITU-T H.810, personal connected health devices, Services interface, SOAP/ATNA, Health & Fitness Service receiver.

---

* 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

This Recommendation is a transposition of Continua Test Tool DG2016, Test Suite Structure & Test Purposes, Services Interface; Part 4: SOAP/ATNA. HFS Receiver (Version 1.7, 2017-03-14), that was developed by the Personal Connected Health Alliance. The table below shows the revision history of this test specification; it may contain versions that existed before transposition.

Version	Date	Revision history
1.2	2012-10-05	Initial release for Test Tool DG2011. This uses "TSS&TP_1.5_WAN_PART_4_(REC GEN)_v1.1.doc" as a baseline and adds new features included in [b-CDG 2011]: • Consent management
1.3	2013-05-24	Initial release for Test Tool DG2012. This uses "TSS&TP_DG2011_WAN_PART_4_(REC GEN)_v1.2.doc" as a baseline and fixes a typo error in ATNA reliable syslog test cases. It does not include technical changes in test procedures because new features included in [b-CDG 2012] do not affect the test procedures specified in this document.
1.3	2014-01-24	Initial release for Test Tool DG2013. This is the same version as "TSS&TP_DG2012_WAN_PART_4_(REC GEN)_v1.3.doc" because new features included in [b-ITU-T H.810 (2013)]/[b-CDG 2013] do not affect the test procedures specified in this document.
1.4	2014-04-24	TM Lite & Doc Enhancements (Test Tool v4.0 Maintenance Release 1). It uses "TSS&TP_DG2013_ WAN_PART_4_(REC GEN)_v1.3.doc" as a baseline and adds new features included in Documentation Enhancements: • "Other PICS" row has been added
1.5	2015-07-01	Initial release for Test Tool DG2015: • Test suite structure modified • Applicability modified due to the inclusion of hData OU
1.6	2016-09-20	Initial release for Test Tool DG2016. It implements changes according to [ITU-T H.810 (2016)]/[b-CDG 2016] (Iris + Errata) refreshments.
1.7	2017-03-14	Editorial: added insulin pump and continuous glucose monitor specializations to the TSS list in clause 6.

Recommendation ITU-T H.830.4

Conformance of ITU-T H.810 personal health system: Services interface Part 4: SOAP/ATNA: Health & Fitness Service receiver

1 Scope

The scope of this Recommendation[1] is to provide a test suite structure (TSS) and the test purposes (TP) for the Services interface based on the requirements defined in the Continua Design Guidelines (CDG) [ITU-T H.810 (2016)]. 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 4.

– 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 9: hData Observation Upload. Health & Fitness Service sender
– Part 10: hData Observation Upload. Health & Fitness Service receiver
– Part 11: Questionnaires. Health & Fitness Service sender
– Part 12: Questionnaires. 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 (2016)] Recommendation ITU-T H.810 (2016), *Interoperability design guidelines for personal health systems*.

[ITU-T H.812] Recommendation ITU-T H.812 (2016), *Interoperability design guidelines for personal health systems: Services interface: Common certified capability class.*

[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.812.1] Recommendation ITU-T H.812.1 (2016), *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 (2016), *Interoperability design guidelines for personal health systems: Services interface: Questionnaires certified capability class.*

[ITU-T H.812.3] Recommendation ITU-T H.812.3 (2016), *Interoperability design guidelines for personal health systems: Services interface: Capability exchange certified capability class.*

[ITU-T H.812.4] Recommendation ITU-T H.812.4 (2016), *Interoperability design guidelines for personal health systems: Services interface: Authenticated persistent session certified capability class.*

[IETF RFC 3195] IETF RFC 3195 (2001), *Reliable Delivery for syslog*.
https://datatracker.ietf.org/doc/rfc3195

[IETF RFC 3881] IETF RFC 3881 (2004), *Security Audit and Access Accountability Message XML Data Definitions for Healthcare Applications*.
https://datatracker.ietf.org/doc/rfc3881

[IHE ITI TF-2] IHE ITI TF 2 (2010), *IHE IT Infrastructure Technical Framework, Volume 2 (ITI TF-2)*, Revision 7.0. It comprises three sub-volumes: 2a (Transactions Part A), 2b (Transactions Part B) and 2x (Appendices).
http://www.ihe.net/Technical_Framework/upload/IHE_ITI_TF_Rev7-0_Vol2a_FT_2010-08-10.pdf
http://www.ihe.net/Technical_Framework/upload/IHE_ITI_TF_Rev7-0_Vol2b_FT_2010-08-10.pdf
http://www.ihe.net/Technical_Framework/upload/IHE_ITI_TF_Rev7-0_Vol2x_FT_2010-08-10.pdf

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

ATS Abstract Test Suite

CDG Continua Design Guidelines

CGM Continuous Glucose Monitor

DUT Device Under Test

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
PCT	Protocol Conformance Testing
PHD	Personal Health Device
PHDC	Personal Healthcare Device Class
PHG	Personal Health Gateway
PICS	Protocol Implementation Conformance Statement
PIXIT	Protocol Implementation extra Information for Testing
SABTE	Sleep Apnoea Breathing Therapy Equipment
SCR	Static Conformance Review
SDP	Service Discovery Protocol
SOAP	Simple Object Access Protocol
TCRL	Test Case Reference List
TCWG	Test and Certification Working Group
TP	Test Purpose
TSS	Test Suite Structure
URI	Uniform Resource Identifier
USB	Universal Serial Bus
WAN	Wide Area Network
WD	WAN Device
WDM	Windows Driver Model
WS	Web Service
WSDL	Web Service Description Language
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
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 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 H.810 is split into eight parts in the H.810-series.	–
2015	–	5.0	Release 2015 of the CDG including maintenance updates of the 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 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 CDG 2011 and additional guidelines that cover new functionalities.	Catalyst
2011 plus errata	–	2.1	CDG 2011 integrated with identified errata.	–
2011	–	2.0	Release 2011 of the CDG including maintenance updates of the CDG 2010 and additional guidelines that cover new functionalities [b-CDG 2011].	Adrenaline
2010 plus errata	–	1.6	CDG 2010 integrated with identified errata	–

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

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

6 Test suite structure (TSS)

The test purposes (TPs) for the Services interface have been divided into the main subgroups specified below. Annex A describes the TPs for subgroups 2.2 and 2.3 (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 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)

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.

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 purposes

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

A.1 TP definition conventions

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

- **TP Id**: This is a unique identifier (TP/<TT>/<DUT>/<GR>/<SGR>/<XX> – <NNN>). It is 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).
- **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 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 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 2.2.1: SOAP headers (HEAD)

TP Id		TP/HFS/REC/SOAP/HEAD/BV-000		
TP label		Requirements for Transactions which don't use HL7 V3 Messages		
Coverage	**Spec**	[IHE ITI TF-2], Volume 2x, Appendix V		
	Testable items	Namespaces; M	IHE-WSP201; M	IHE-WSP202; M
		IHE-WSP203; M	IHE-WSP205; M	IHE-WSP206; M
		IHE-WSP207; M	IHE-WSP208; M	IHE-WSP211; M
		IHE-WSP212; M	IHE-WSP300; M	IHE-WSA101; M
Test purpose		Check that: Table V.2.4-1 lists XML namespaces that are used in this appendix. [AND] IHE requires the profile writers and recommends the implementors to use the following naming convention for WSDL artifacts: - message request -> {Transaction Name}_Message - message response -> {Transaction Name}_Response_Message - portType -> {NAME}_PortType - Operation -> {NAME}_{Transaction Name}[_OperationID] - SOAP 1.2 binding -> {NAME}_Binding_Soap12 - SOAP 1.2 port -> {NAME}_Port_Soap12 [AND] The targetNamespace of the example WSDL shall be urn:ihe:{DOMAIN}:{PROFILE}:{YEAR} and may be extended to urn:ihe:{DOMAIN}:{PROFILE}:{YEAR}:{TYPE} [AND] The WSDL shall include XML Schema Definition references for the transactions payloads. [AND] Two WSDL messages shall be defined for a request-response transaction [AND] In the example WSDL provided by an IHE specification a single WSDL part named Body shall be defined for each WSDL message and the part type shall refer to an element defined in the Schema Definition required in IHE-WSP203 [AND] For each input and output message defined in the WSDL portType operation an attribute wsaw:Action shall be included [AND] WSDL operations shall use wsdl:operation/wsdl:input/@wasw:Action = "urn:ihe:{Domain}:{Year}:{Transaction name}" and wsdl:operation/wsdl:output/@wsaw:Action = "urn:ihe:{Domain}:{Year}:{Transaction name}Response" [AND] For each operation defined in the WSDL portType a wsoap:operation/@soapAction attribute shall be provided. The value of wsoap:operation/@soapAction shall be consistent with the name for the corresponding WSDL operation defined in the WSDL portType [AND] The WSDL provided with an IHE specification shall use the SOAP Binding described in WSDL 1.1 Chapter 3 and the binding extension for SOAP 1.2 [AND]		

	All <wsa:Action> elements shall have the mustUnderstand attribute set (mustUnderstand='1')
Applicability	C_REC_000 AND C_REC_GEN_003
Other PICS	
Initial condition	The HFS receiver under test has a WebService published and the simulated HFS sender is ready to send a SOAP message.
Test procedure	1. The simulated HFS sender takes the WSDL description of the WebService provided by the HFS receiver and checks: a. Namespaces: ❑ wsdl: "http://schemas.xmlsoap.org/wsdl/" ❑ soap12: "http://schemas.xmlsoap.org/wsdl/soap12" ❑ xsd: "http://www.w3.org/2001/XMLSchema" ❑ wsaw: "http://www.w3.org/2006/05/addressing/wsdl" b. WSDL artifacts: ❑ message request -> {Transaction Name}_Message ❑ message response -> {Transaction Name}_Response_Message ❑ portType -> {NAME}_PortType ❑ Operation -> {NAME}_{Transaction Name}[_OperationID] ❑ SOAP 1.2 binding -> {NAME}_Binding_Soap12 ❑ SOAP 1.2 port -> {NAME}_Port_Soap12 where NAME is the value of the /wsdl:definitions/@name attribute and Transaction Name represents the formal IHE transaction name for this particular web-service exchange with spaces omitted from the name. c. The targetNamespace is urn:ihe:{DOMAIN}:{PROFILE}:{YEAR} and can be extended to urn:ihe:{DOMAIN}:{PROFILE}:{YEAR}:{TYPE} d. Two WSDL messages are defined, one for the request transaction and another for the response transaction. e. A single WSDL part named Body is defined for each WSDL message and the part type refers to an element defined in the schema definition included in the xsd reference. f. For each input and output message defined in the WSDL portType operation an attribute wsaw:Action is included and: ❑ wsdl:operation/wsdl:input/@wsaw:Action = "urn:ihe:{Domain}:{Year}:{Transaction name}" ❑ wsdl:operation/wsdl:output/@wsaw:Action = "urn:ihe:{Domain}:{Year}:{Transaction name}Response" g. For each operation defined in the WSDL portType a wsoap:operation/@soapAction attribute is provided and its value is consistent with the name for the corresponding WSDL operation defined in the WSDL portType h. WSDL provided with an IHE specification uses the binding extension for SOAP 1.2 2. The simulated HFS sender sends a SOAP message to the HFS receiver using addressing header blocks. 3. The HFS receiver responds with another SOAP message. Check that all <wsa:Action> elements have the mustUnderstand attribute set (mustUnderstand='1' ir 'true)
Pass/Fail criteria	In step 1, all elements are in the WSDL description. In step 3, the response messages are as specified.
Notes	

TP Id		TP/HFS/REC/SOAP/HEAD/BV-001		
TP label		Security Guidelines		
Coverage	**Spec**	[ITU-T H.812]		
	Testable items	CommonReq 4; M	SecGuidelines 1; M	SecGuidelines 4; M
Test purpose		Check that: All Continua HFS connections shall be initiated from the HFS client component and shall not be initiated from the HFS service component. [AND] Continua HFS client and service components shall support the TLS protocol v1.0 (RFC 2246) from WS-I BSP v1.0 for secure communication [AND] Continua HFS client and service components shall support transfer of entity assertion information via SAML 2.0 token through WS-Security Header according to the Web Services Security: SAML Token Profile 1.1		
Applicability		C_REC_000 AND C_REC_GEN_003		
Other PICS				
Initial condition		The HFS receiver under test has a WebService published and the simulated HFS sender is ready to establish a connection using TLS [b-IETF RFC 2246] and SAML 2.0 as an authentication token [b-OASIS SAMLTP].		
Test procedure		1. The simulated HFS sender starts a connection with the HFS receiver using HTTP over TLS v1.0. 2. The HFS receiver under test allows the connection. 3. The HFS sender sends a message using an SAML 2.0 token as an authentication token. 4. The HFS receiver accepts the token and responds to the message without a security error.		
Pass/Fail criteria		All steps are as specified above. If the HFS receiver responds with an error in step 4, it shall not be provoked by security reasons.		
Notes				

TP Id		TP/HFS/REC/SOAP/HEAD/BV-002		
TP label		HFS Observation Receiver Requirements		
Coverage	**Spec**	[ITU-T H.812.1]		
	Testable items	ReceiverReq 2; M	ReceiverReq 3; M	
Test purpose		Check that: A Continua HFS service component shall support WS-ReliableMessaging as an RM Destination for CommunicatePCDDataResponse messages [AND] A Continua HFS service component shall support WS-ReliableMessaging as an RM Source for CommunicatePCDDataResponse messages		
Applicability		C_REC_000 AND C_REC_GEN_003		
Other PICS				
Initial condition		The simulated HFS sender is using WS-RM and the HFS receiver under test are in a none sequence state.		
Test procedure		1. The simulated HFS sender sends a CreateSequence message to the HFS receiver		

	with an offer element. 2. The HFS receiver under test responds with CreateSequenceResponse or with CreateSequenceRefused. 3. If the sequence created is not refused, the simulated HFS sender sends an HL7 message within the soap body of a sequence message indicating that it is the last one. 4. The HFS receiver responds with a SequenceAck header block message, a sequence header block and an HL7 message in the body. 5. The simulated HFS sender sends a SequenceAcknowledgement.
Pass/Fail criteria	All steps are as specified above.
Notes	The HFS receiver acts as an RM source in step 4 and as an RM destination in the other steps.

A.3 Subgroup 2.3.1: ATNA general (GEN)

TP Id		TP/HFS/REC/ATNA/GEN/BV-006		
TP label		Reliable Syslog ATNA Actor behaviour		
Coverage	**Spec**	[IHE ITI TF-2]		
	Testable items	Audit_MT-1; M		
Test purpose		Check that: If the Audit Record repository is not available, the HFS actor shall store the audit record in a local buffer until the audit record repository is available again.		
Applicability		C_REC_000 AND C_REC_GEN_001 AND C_REC_ATNA_001		
Other PICS		C_REC_GEN_003, C_REC_GEN_004		
Initial condition		The HFS receiver under test is shutdown. The simulated HFS sender has a SOAP message (a PCD-01 message or a consent document) ready to be sent and the Simulated Audit Repository with Reliable Syslog transport is intentionally disabled.		
Test procedure		1. The HFS receiver application under test is started and it sends the corresponding audit record message to the audit repository. As the simulated audit repository receiver is disabled, the message will not be delivered. 2. Wait for one minute. 3. The test tool starts the simulated audit repository. 4. If C_REC_GEN_002 = FALSE (the SUT does not support consent management) THEN the simulated HFS sender sends a PCD-01 message to the HFS receiver under test. IF C_REC_GEN_002 = TRUE (the SUT supports consent management) THEN the simulated HFS sender sends a consent document to the HFS receiver under test. 5. The test tool receives the SOAP message (a PCD-01 message or a consent document) acknowledge and the audit record messages sent by the HFS receiver under test.		
Pass/Fail criteria		• Two audit record messages must be received by the simulated audit repository: One for the HFS receiver start action (step 1) and the other for the SOAP message sent in step 4. • There is one audit record with the attribute "code" of the element EventID set to "110107" (PHI-import) and the EventDateTime attribute of the EventIdentification element is set to the expedition time of the SOAP message sent in step 4. • There is one audit record with the attribute "code" of the element EventID set to "110120" (start action) and the EventDateTime attribute of the EventIdentification element is set at least one minute before the expedition time of the SOAP message sent in step 4.		
Notes		In step 4, the way to force the HFS receiver to send the pending audit record not delivered in step 1 depends on the vendor implementation. A typical strategy could be to send		

	another HFS message and its corresponding ATNA record; in this way, when the HFS receiver under test sends the ATNA record PHI-import, then it would send the pending audit record along with the newer one.

A.4 Subgroup 2.3.2: ATNA PCD-01 (PCD-01)

TP Id		TP/HFS/REC/ATNA/PCD-01/BV-000		
TP label		PCD-01 - Reliable Syslog ATNA Actor Start		
Coverage	**Spec**	[IHE ITI TF-2]		
	Testable items	AuditMess-2; R	AuditMess-3; M	ActTrans-8; O
		ActTrans-6; O	ATNA_IP-2; O	ATNA_PF-1; M
		ChainTrust-2; M	DirectCert-1; M	DirectCert-2; M
		DirectCert-3; M	Trigg_Event-1; M	Audit_RF-1; M
		Rel_Syslog-1; M	Rel_Syslog-2; M	
	Spec	[ITU-T H.812]		
	Testable items	SecGuidelines 3; O		
	Spec	[IETF RFC 3881]		
	Testable items	SAAAM-DD-01; M	SAAAM-DD-02; O	SAAAM-DD-03; M
		SAAAM-DD-04; M	SAAAM-DD-05; O	SAAAM-DD-06; M
		SAAAM-DD-07; O	SAAAM-DD-08; O	SAAAM-DD-09; O
		SAAAM-DD-10; O	SAAAM-DD-11; O	SAAAM-DD-12; O
		SAAAM-DD-13; O	SAAAM-DD-14; M	SAAAM-DD-15; O
		SAAAM-DD-16; O	SAAAM-DD-17; O	SAAAM-DD-18; O
		SAAAM-DD-19; M	SAAAM-DD-20; O	SAAAM-DD-21; M
Test purpose		Check that: When SUT starts the application then audit log start message is received from the SUT and it is conformant to the ATNA specifications		
Applicability		C_REC_000 AND C_REC_GEN_001 AND C_REC_ATNA_001		
Other PICS		C_REC_GEN_003, C_REC_GEN_004		
Initial condition		The HFS receiver under test is shut down and a simulated audit repository with reliable syslog transport is running.		
Test procedure		1. The HFS receiver application under test is started and sends the corresponding audit record message to the audit repository. 2. The audit repository receives the audit record message and verifies that: a. TLS is used and the encryption suite is TLS_RSA_WITH_AES_128_CBC_SHA b. It conforms to the reliable syslog's cooked profile [IETF RFC 3195]		
Pass/Fail criteria		• The ATNA XML log file conforms to the [IETF RFC 3881] schema included in Annex B. • In the audit record, the attribute "code" of the element EventID is set to "110120" and the attribute "displayName" of the EventTypeCode element is set to "Communicate PCD Data". • The received audit message conforms to the reliable syslog's cooked profile [IETF RFC 3195].		
Notes				

TP Id		TP/HFS/REC/ATNA/PCD-01/BV-001		
TP label		PCD-01 - BSD Syslog ATNA Actor Start		
Coverage	**Spec**	[IHE ITI TF-2]		
	Testable items	AuditMess-2; R	AuditMess-3; M	ActTrans-8; O
		ActTrans-6; O	ATNA_IP-2; O	ATNA_PF-1; M
		ChainTrust-2; M	DirectCert-1; M	DirectCert-2; M
		DirectCert-3; M	Trigg_Event-1; M	Audit_RF-1; M
		BSD_Syslog-1; O	BSD_Syslog-2; M	BSD_Syslog-3; M
		BSD_Syslog-4; M	BSD_Syslog-5; R	BSD_Syslog-6; O
	Spec	[ITU-T H.812]		
	Testable items	SecGuidelines 3; O		
	Spec	[IETF RFC 3881]		
	Testable items	SAAAM-DD-01; M	SAAAM-DD-02; O	SAAAM-DD-03; M
		SAAAM-DD-04; M	SAAAM-DD-05; O	SAAAM-DD-06; M
		SAAAM-DD-07; O	SAAAM-DD-08; O	SAAAM-DD-09; O
		SAAAM-DD-10; O	SAAAM-DD-11; O	SAAAM-DD-12; O
		SAAAM-DD-13; O	SAAAM-DD-14; M	SAAAM-DD-15; O
		SAAAM-DD-16; O	SAAAM-DD-17; O	SAAAM-DD-18; O
		SAAAM-DD-19; M	SAAAM-DD-20; O	SAAAM-DD-21; M
Test purpose		Check that: When SUT starts the application then audit log start message is received from the SUT and it is conformant to the ATNA specifications		
Applicability		C_REC_000 AND C_REC_GEN_001 AND C_REC_ATNA_002		
Other PICS		C_REC_GEN_003, C_REC_GEN_004		
Initial condition		The HFS receiver under test is shut down and a simulated audit repository with BSD syslog transport is running.		
Test procedure		1. The HFS receiver application under test is started and sends the corresponding audit record message to the audit repository. 2. The audit repository receives the audit record message and verifies that it conforms to BSD Syslog [b-IETF RFC 3164].		
Pass/Fail criteria		• The ATNA XML log file conforms to the [IETF RFC 3881] schema included in Annex B. • In the audit record, the attribute "code" of the element EventID is set to "110120" and the attribute "displayName" of the EventTypeCode element is set to "Communicate PCD Data". • The received audit message conforms to the BSD Syslog [b-IETF RFC 3164].		
Notes				

TP Id		TP/HFS/REC/ATNA/PCD-01/BV-002		
TP label		PCD-01 - Reliable Syslog ATNA Actor PHI-import		
Coverage	**Spec**	[IHE ITI TF-2]		
	Testable items	AuditMess-2; R	AuditMess-3; M	ActTrans-8; O
		ActTrans-6; O	ATNA_IP-2; O	ATNA_PF-1; M
		ChainTrust-2; M	DirectCert-1; M	DirectCert-2; M
		DirectCert-3; M	Trigg_Event-16; M	Audit_RF-1; M

		Rel_Syslog-1; M	Rel_Syslog-2; M	
	Spec	[ITU-T H.812]		
	Testable items	SecGuidelines 3; O		
	Spec	[IETF RFC 3881]		
	Testable items	SAAAM-DD-01; M	SAAAM-DD-02; O	SAAAM-DD-03; M
		SAAAM-DD-04; M	SAAAM-DD-05; O	SAAAM-DD-06; M
		SAAAM-DD-07; O	SAAAM-DD-08; O	SAAAM-DD-09; O
		SAAAM-DD-10; O	SAAAM-DD-11; O	SAAAM-DD-12; O
		SAAAM-DD-13; O	SAAAM-DD-14; M	SAAAM-DD-15; O
		SAAAM-DD-16; O	SAAAM-DD-17; O	SAAAM-DD-18; O
		SAAAM-DD-19; M	SAAAM-DD-20; O	SAAAM-DD-21; M
Test purpose		Check that: When SUT receives a PCD-01 ORU message, then an audit log PHI-import message is received from the SUT and it is conformant to the ATNA specifications		
Applicability		C_REC_000 AND C_REC_GEN_001 AND C_REC_ATNA_001		
Other PICS		C_REC_GEN_003, C_REC_GEN_004		
Initial condition		The HFS receiver under test has a WebService enabled for PCD-01 message reception, the simulated HFS sender has a PCD-01 message ready to be sent and a simulated audit repository with reliable syslog transport is running.		
Test procedure		1. The simulated HFS sender sends a PCD-01 message to the HFS receiver under test. 2. The HFS receiver under test replies with PCD-01 ACK message and it sends the corresponding audit record message to the audit repository. 3. The audit repository receives the audit record message and verifies that: a. TLS is used and the encryption suite is TLS_RSA_WITH_AES_128_CBC_SHA b. It conforms to the reliable syslog's cooked profile [IETF RFC 3195].		
Pass/Fail criteria		• The ATNA XML log file conforms to the [IETF RFC 3881] schema included in Annex B. • In the audit record, the attribute "code" of the element EventID is set to "110107"and the attribute "displayName" of the EventTypeCode element is set to "Communicate PCD Data". • In the audit record, the value of the attribute EventDateTime of the element EventIdentification is inside a one minute interval of the Data and Time indicated in the MSH-7 field of the PCD-01 ACK message sent by the HFS receiver under test. • The received audit message conforms to the reliable syslog's cooked profile [IETF RFC 3195].		
Notes				

TP Id		TP/HFS/REC/ATNA/PCD-01/BV-003		
TP label		PCD-01 - BSD Syslog ATNA Actor PHI-import		
Coverage	**Spec**	[IHE ITI TF-2]		
	Testable items	AuditMess-2; R	AuditMess-3; M	ActTrans-8; O
		ActTrans-6; O	ATNA_IP-2; O	ATNA_PF-1; M
		ChainTrust-2; M	DirectCert-1; M	DirectCert-2; M
		DirectCert-3; M	Trigg_Event-16; M	Audit_RF-1; M
		BSD_Syslog-1; O	BSD_Syslog-2; M	BSD_Syslog-3; M
		BSD_Syslog-4; M	BSD_Syslog-5; R	BSD_Syslog-6; O
	Spec	[ITU-T H.812]		

	Testable items	SecGuidelines 3; O		
	Spec	[IETF RFC 3881]		
	Testable items	SAAAM-DD-01; M	SAAAM-DD-01; M	SAAAM-DD-01; M
		SAAAM-DD-04; M	SAAAM-DD-04; M	SAAAM-DD-04; M
		SAAAM-DD-07; O	SAAAM-DD-07; O	SAAAM-DD-07; O
		SAAAM-DD-10; O	SAAAM-DD-10; O	SAAAM-DD-10; O
		SAAAM-DD-13; O	SAAAM-DD-13; O	SAAAM-DD-13; O
		SAAAM-DD-16; O	SAAAM-DD-16; O	SAAAM-DD-16; O
		SAAAM-DD-19; M	SAAAM-DD-19; M	SAAAM-DD-19; M
Test purpose		Check that: When SUT receives a PCD-01 ORU message, then an audit log PHI-import message is received from the SUT and it is conformant to the ATNA specifications		
Applicability		C_REC_000 AND C_REC_GEN_001 AND C_REC_ATNA_002		
Other PICS		C_REC_GEN_003, C_REC_GEN_004		
Initial condition		The HFS receiver under test has a WebService enabled for PCD-01 message reception, the simulated HFS sender has a PCD-01 message ready to be sent and a simulated audit repository with BSD syslog transport is running.		
Test procedure		1. The simulated HFS sender sends a PCD-01 message to the HFS receiver under test. 2. The HFS receiver under test replies with a PCD-01 ACK message and sends the corresponding audit record message to the audit repository. 3. The audit repository receives the Audit Record Message and verifies that it conforms to the BSD Syslog [b-IETF RFC 3164].		
Pass/Fail criteria		• The ATNA XML log file conforms to the [IETF RFC 3881] schema included in Annex B. • The attribute "code" of the element EventID is set to "110107" and the attribute "displayName" of the EventTypeCode element is set to "Communicate PCD Data". • In the audit record, the value of the attribute EventDateTime of the element EventIdentification is inside a one-minute interval of the Data and Time indicated in the MSH-7 field of the PCD-01 ACK message sent by the HFS receiver under test. • The received audit message conforms to the BSD Syslog [b-IETF RFC 3164].		
Notes				

TP Id		TP/HFS/REC/ATNA/PCD-01/BV-004		
TP label		PCD-01 - Reliable Syslog ATNA Actor Stop		
Coverage	**Spec**	[IHE ITI TF-2]		
	Testable items	AuditMess-2; R	AuditMess-3; M	ActTrans-8; O
		ActTrans-6; O	ATNA_IP-2; O	ATNA_PF-1; M
		ChainTrust-2; M	DirectCert-1; M	DirectCert-2; M
		DirectCert-3; M	Trigg_Event-1; M	Audit_RF-1; M
		Rel_Syslog-1; M	Rel_Syslog-2; M	
	Spec	[ITU-T H.812]		
	Testable items	SecGuidelines 3; O		
	Spec	[IETF RFC 3881]		
	Testable items	SAAAM-DD-01; M	SAAAM-DD-02; O	SAAAM-DD-03; M
		SAAAM-DD-04; M	SAAAM-DD-05; O	SAAAM-DD-06; M
		SAAAM-DD-07; O	SAAAM-DD-08; O	SAAAM-DD-09; O

		SAAAM-DD-10; O	SAAAM-DD-11; O	SAAAM-DD-12; O
		SAAAM-DD-13; O	SAAAM-DD-14; M	SAAAM-DD-15; O
		SAAAM-DD-16; O	SAAAM-DD-17; O	SAAAM-DD-18; O
		SAAAM-DD-19; M	SAAAM-DD-20; O	SAAAM-DD-21; M
Test purpose		Check that: When SUT stops the application then audit log stop message is received from the SUT and it is conformant to the ATNA specifications		
Applicability		C_REC_000 AND C_REC_GEN_001 AND C_REC_ATNA_001		
Other PICS		C_REC_GEN_003, C_REC_GEN_004		
Initial condition		The HFS receiver under test has a WebService enabled and a simulated audit repository with reliable syslog transport is running.		
Test procedure		1. The HFS receiver application under test shuts down the application and sends the corresponding audit record message to the audit repository. 2. The audit repository receives the audit record message and verifies that: a. TLS is used and the encryption suite is TLS_RSA_WITH_AES_128_CBC_SHA b. It conforms to the reliable syslog's cooked profile [IETF RFC 3195].		
Pass/Fail criteria		• The ATNA XML log file conforms to the [IETF RFC 3881] schema included in Annex B. • In the audit record, the attribute "code" of the element EventID is set to "110121" and the attribute "displayName" of the EventTypeCode element is set to "Communicate PCD Data". • The received audit message conforms to the reliable syslog's cooked profile [IETF RFC 3195].		
Notes				

TP Id		TP/HFS/REC/ATNA/PCD-01/BV-005		
TP label		PCD-01 - BSD Syslog ATNA Actor Stop		
Coverage	**Spec**	[IHE ITI TF-2]		
	Testable items	AuditMess-2; R	AuditMess-3; M	ActTrans-8; O
		ActTrans-6; O	ATNA_IP-2; O	ATNA_PF-1; M
		ChainTrust-2; M	DirectCert-1; M	DirectCert-2; M
		DirectCert-3; M	Trigg_Event-1; M	Audit_RF-1; M
		BSD_Syslog-1; O	BSD_Syslog-2; M	BSD_Syslog-3; M
		BSD_Syslog-4; M	BSD_Syslog-5; R	BSD_Syslog-6; O
	Spec	[ITU-T H.812]		
	Testable items	SecGuidelines 3; O		
	Spec	[IETF RFC 3881]		
	Testable items	SAAAM-DD-01; M	SAAAM-DD-02; O	SAAAM-DD-03; M
		SAAAM-DD-04; M	SAAAM-DD-05; O	SAAAM-DD-06; M
		SAAAM-DD-07; O	SAAAM-DD-08; O	SAAAM-DD-09; O
		SAAAM-DD-10; O	SAAAM-DD-11; O	SAAAM-DD-12; O
		SAAAM-DD-13; O	SAAAM-DD-14; M	SAAAM-DD-15; O
		SAAAM-DD-16; O	SAAAM-DD-17; O	SAAAM-DD-18; O
		SAAAM-DD-19; M	SAAAM-DD-20; O	SAAAM-DD-21; M
Test purpose		Check that:		

	When SUT stops the application then audit log stop message is received from the SUT and it is conformant to the ATNA specifications
Applicability	C_REC_000 AND C_REC_GEN_001 AND C_REC_ATNA_002
Other PICS	C_REC_GEN_003, C_REC_GEN_004
Initial condition	The HFS receiver under test has a WebService enabled and a simulated audit repository with BSD syslog transport is running.
Test procedure	1. The HFS receiver application under test shuts down the application and sends the corresponding audit record message to the audit repository. 2. The audit repository receives the audit record message and verifies that it conforms to BSD Syslog [b-IETF RFC 3164].
Pass/Fail criteria	• The ATNA XML log file conforms to the [IETF RFC 3881] schema included in Annex B. • The attribute "code" of the element EventID is set to "110121" and the attribute "displayName" of the EventTypeCode element is set to "Communicate PCD Data". • The received audit message conforms to the BSD Syslog [b-IETF RFC 3164].
Notes	

A.5 Subgroup 2.3.3: ATNA consent management (CM)

TP Id		TP/HFS/REC/ATNA/CM/BV-000		
TP label		CM - Reliable Syslog ATNA Actor PHI-import		
Coverage	**Spec**	[IHE ITI TF-2], Volume 2a		
	Testable items	AuditMess-2; R	AuditMess-3; M	ActTrans-8; O
		ActTrans-6; O	ATNA_IP-2; O	ATNA_PF-1; M
		ChainTrust-2; M	DirectCert-1; M	DirectCert-2; M
		DirectCert-3; M	Trigg_Event-16; M	Audit_RF-1; M
		Rel_Syslog-1; M	Rel_Syslog-2; M	
	Spec	[IHE ITI TF-2], Volume 2b		
	Testable items	ProvideAudit1; O		
	Spec	[IETF RFC 3881]		
	Testable items	SAAAM-DD-01; M	SAAAM-DD-02; O	SAAAM-DD-03; M
		SAAAM-DD-04; M	SAAAM-DD-05; O	SAAAM-DD-06; M
		SAAAM-DD-07; O	SAAAM-DD-08; O	SAAAM-DD-09; O
		SAAAM-DD-10; O	SAAAM-DD-11; O	SAAAM-DD-12; O
		SAAAM-DD-13; O	SAAAM-DD-14; M	SAAAM-DD-15; O
		SAAAM-DD-16; O	SAAAM-DD-17; O	SAAAM-DD-18; O
		SAAAM-DD-19; M	SAAAM-DD-20; O	SAAAM-DD-21; M
Test purpose		Check that: When SUT receives a Consent Document, then an audit log PHI-import message is received from the SUT and it is conformant to the ATNA specifications		
Applicability		C_REC_000 AND C_REC_GEN_001 AND C_REC_ATNA_001 AND C_REC_GEN_002 AND C_REC_GEN_003		
Other PICS				
Initial condition		The HFS receiver under test has a WebService enabled for consent document reception. The simulated HFS sender has a consent message ready to be sent and a simulated audit repository with reliable syslog is running.		
Test procedure		1. The simulated HFS sender sends the consent document to the HFS receiver under		

	test. 2. When the HFS receiver under test receives the consent document it then sends the corresponding audit record message to the audit repository. 3. The audit repository receives the audit record message and verifies that: a. TLS is used and the encryption suite is TLS_RSA_WITH_AES_128_CBC_SHA b. It conforms to the reliable syslog's cooked profile [IETF RFC 3195]. 4. The audit record includes the following elements: a. An EventIdentification element that contains: ❑ "EventActionCode" attribute set to "C" ❑ EventID sub-element with attributes "code" set to "110107" and "displayName" set to "Import" ❑ EventTypeCode subelement with attributes "code" set to "ITI-41", "displayName" set to "Provide and Register Document Set-b" and "codeSystemName" set to "IHE Transactions" b. An ActiveParticipant element that contains: ❑ "UserIsRequestor" attribute set to "true" ❑ "NetworkAccessPointTypeCode" attribute set to "1" or "2" ❑ RoleIDCode sub-element with attributes "code" set to "110153" and "displayName" set to "Source" c. An ActiveParticipant element that contains: ❑ "UserIsRequestor" attribute set to "false" ❑ "NetworkAccessPointTypeCode" attribute set to "1" or "2" ❑ "AlternativeUserID" attribute is present ❑ RoleIDCode subelement with attributes "code" set to "110152" and "displayName" set to "Destination" d. A ParticipantObjectIdentification element that contains: ❑ "ParticipantObjectID" attribute is present and not empty ❑ "ParticipantObjectTypeCode" attribute set to "1" ❑ "ParticipantObjectTypeCodeRole" attribute set to "1" ❑ ParticipantObjectIDTypeCode sub-element with attributes "code" set to "2", "displayName" set to "Patient Number" and "codeSystemName" set to "RFC-3881" e. A ParticipantObjectIdentification element that contains: ❑ "ParticipantObjectID" attribute is present and not empty ❑ "ParticipantObjectTypeCode" attribute set to "2" ❑ "ParticipantObjectTypeCodeRole" attribute set to "20" ❑ ParticipantObjectIDTypeCode sub-element with attributes "code" set to "urn:uuid:a54d6aa5-d40d-43f9-88c5-b4633d873bdd", "displayName" set to "submission set classificationNode" and "codeSystemName" set to "IHE XDS Metadata"
Pass/Fail criteria	• The ATNA XML log file conforms to the [IETF RFC 3881] schema included in Annex B. • The audit record content conforms to the values described in step 4. • The received audit message conforms to the reliable syslog's cooked profile [IETF RFC 3195].
Notes	

TP Id	TP/HFS/REC/ATNA/CM/BV-001
TP label	CM - BSD Syslog ATNA Actor PHI-import

<table>
<tr><td rowspan="15">Coverage</td><td>Spec</td><td colspan="3">[IHE ITI TF-2], Volume 2a</td></tr>
<tr><td rowspan="6">Testable items</td><td>AuditMess-2; R</td><td>AuditMess-3; M</td><td>ActTrans-8; O</td></tr>
<tr><td>ActTrans-6; O</td><td>ATNA_IP-2; O</td><td>ATNA_PF-1; M</td></tr>
<tr><td>ChainTrust-2; M</td><td>DirectCert-1; M</td><td>DirectCert-2; M</td></tr>
<tr><td>DirectCert-3; M</td><td>Trigg_Event-16; M</td><td>Audit_RF-1; M</td></tr>
<tr><td>BSD_Syslog-1; O</td><td>BSD_Syslog-2; M</td><td>BSD_Syslog-3; M</td></tr>
<tr><td>BSD_Syslog-4; M</td><td>BSD_Syslog-5; R</td><td>BSD_Syslog-6; O</td></tr>
<tr><td>Spec</td><td colspan="3">[IHE ITI TF-2], Volume 2b</td></tr>
<tr><td>Testable items</td><td>ProvideAudit1; O</td><td></td><td></td></tr>
<tr><td>Spec</td><td colspan="3">[IETF RFC 3881]</td></tr>
<tr><td rowspan="6">Testable items</td><td>SAAAM-DD-01; M</td><td>SAAAM-DD-01; M</td><td>SAAAM-DD-01; M</td></tr>
<tr><td>SAAAM-DD-04; M</td><td>SAAAM-DD-04; M</td><td>SAAAM-DD-04; M</td></tr>
<tr><td>SAAAM-DD-07; O</td><td>SAAAM-DD-07; O</td><td>SAAAM-DD-07; O</td></tr>
<tr><td>SAAAM-DD-10; O</td><td>SAAAM-DD-10; O</td><td>SAAAM-DD-10; O</td></tr>
<tr><td>SAAAM-DD-13; O</td><td>SAAAM-DD-13; O</td><td>SAAAM-DD-13; O</td></tr>
<tr><td>SAAAM-DD-16; O</td><td>SAAAM-DD-16; O</td><td>SAAAM-DD-16; O</td></tr>
<tr><td>SAAAM-DD-19; M</td><td>SAAAM-DD-19; M</td><td>SAAAM-DD-19; M</td></tr>
<tr><td colspan="2">Test purpose</td><td colspan="3">Check that:
Audit log message is received from the SUT and it is conformant to the ATNA specifications</td></tr>
<tr><td colspan="2">Applicability</td><td colspan="3">C_REC_000 AND C_REC_GEN_001 AND C_REC_ATNA_002 AND C_REC_GEN_002 AND C_REC_GEN_003</td></tr>
<tr><td colspan="2">Other PICS</td><td colspan="3"></td></tr>
<tr><td colspan="2">Initial condition</td><td colspan="3">The HFS receiver under test has a WebService enabled and the simulated HFS sender has a consent message and an audit repository with BSD syslog transport is running.</td></tr>
<tr><td colspan="2">Test procedure</td><td colspan="3">1. The HFS sender application under test sends an audit record message to the audit repository.
2. The audit repository receives the audit record message and verifies that it conforms to BSD syslog [b-IETF RFC 3164].
3. The audit record includes the following elements:
a. An EventIdentification element that contains:
❑ "EventActionCode" attribute set to "C"
❑ EventID subelement with attributes "code" set to "110107" and "displayName" set to "Import"
❑ EventTypeCode subelement with attributes "code" set to "ITI-41", "displayName" set to "Provide and Register Document Set-b" and "codeSystemName" set to "IHE Transactions"
b. An ActiveParticipant element that contains:
❑ "UserIsRequestor" attribute set to "true"
❑ "NetworkAccessPointTypeCode" attribute set to "1" or "2"
❑ RoleIDCode subelement with attributes "code" set to "110153" and "displayName" set to "Source"
c. An ActiveParticipant element that contains:
❑ "UserIsRequestor" attribute set to "false"
❑ "NetworkAccessPointTypeCode" attribute set to "1" or "2"
❑ "AlternativeUserID" attribute is present</td></tr>
</table>

	❑ RoleIDCode subelement with attributes "code" set to "110152" and "displayName" set to "Destination" d. A ParticipantObjectIdentification element that contains: ❑ "ParticipantObjectID" attribute is present and not empty ❑ "ParticipantObjectTypeCode" attribute set to "1" ❑ "ParticipantObjectTypeCodeRole" attribute set to "1" ❑ ParticipantObjectIDTypeCode subelement with attributes "code" set to "2", "displayName" set to "Patient Number" and "codeSystemName" set to "RFC-3881" e. A ParticipantObjectIdentification element that contains: ❑ "ParticipantObjectID" attribute is present and not empty ❑ "ParticipantObjectTypeCode" attribute set to "2" ❑ "ParticipantObjectTypeCodeRole" attribute set to "20" ❑ ParticipantObjectIDTypeCode subelement with attributes "code" set to "urn:uuid:a54d6aa5-d40d-43f9-88c5-b4633d873bdd", "displayName" set to "submission set classificationNode" and "codeSystemName" set to "IHE XDS Metadata"
Pass/Fail criteria	• The ATNA XML log file conforms to the [IETF RFC 3881] schema included in Annex B. • The audit record content conforms to values described in step 4. • The received audit message conforms to the BSD Syslog [b-IETF RFC 3164].
Notes	

Annex B

Schema for IETF RFC 3881 verification

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

```
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
     elementFormDefault="qualified" attributeFormDefault="unqualified">
     <xs:element name="AuditMessage">
          <xs:complexType>
               <xs:sequence>
                    <xs:element name="EventIdentification"
                         type="EventIdentificationType" />
                    <xs:element name="ActiveParticipant"
                         maxOccurs="unbounded">
                         <xs:complexType>
                              <xs:complexContent>
                                   <xs:extension base="ActiveParticipantType" />
                              </xs:complexContent>
                         </xs:complexType>
                    </xs:element>
                    <xs:element name="AuditSourceIdentification"
                         type="AuditSourceIdentificationType"
                         maxOccurs="unbounded" />
                    <xs:element name="ParticipantObjectIdentification"
                         type="ParticipantObjectIdentificationType" minOccurs="0"
                         maxOccurs="unbounded" />
               </xs:sequence>
          </xs:complexType>
     </xs:element>
     <xs:complexType name="EventIdentificationType">
          <xs:sequence>
               <xs:element name="EventID" type="CodedValueType" />
               <xs:element name="EventTypeCode" type="CodedValueType"
                    minOccurs="0" maxOccurs="unbounded" />
          </xs:sequence>
          <xs:attribute name="EventActionCode" use="optional">
               <xs:simpleType>
                    <xs:restriction base="xs:string">
                         <xs:enumeration value="C">
                              <xs:annotation>
                                   <xs:appinfo>Create</xs:appinfo>
                              </xs:annotation>
                         </xs:enumeration>
                         <xs:enumeration value="R">
                              <xs:annotation>
                                   <xs:appinfo>Read</xs:appinfo>
                              </xs:annotation>
                         </xs:enumeration>
                         <xs:enumeration value="U">
                              <xs:annotation>
                                   <xs:appinfo>Update</xs:appinfo>
                              </xs:annotation>
                         </xs:enumeration>
                         <xs:enumeration value="D">
                              <xs:annotation>
                                   <xs:appinfo>Delete</xs:appinfo>
                              </xs:annotation>
                         </xs:enumeration>
                         <xs:enumeration value="E">
                              <xs:annotation>
                                   <xs:documentation>Execute</xs:documentation>
```

```
                              </xs:annotation>
                         </xs:enumeration>
                    </xs:restriction>
               </xs:simpleType>
          </xs:attribute>
          <xs:attribute  name="EventDateTime"  type="xs:dateTime"  use="required"
/>
          <xs:attribute name="EventOutcomeIndicator" use="required">
               <xs:simpleType>
                    <xs:restriction base="xs:integer">
                         <xs:enumeration value="0">
                              <xs:annotation>
                                   <xs:appinfo>Success</xs:appinfo>
                              </xs:annotation>
                         </xs:enumeration>
                         <xs:enumeration value="4">
                              <xs:annotation>
                                   <xs:appinfo>Minor failure</xs:appinfo>
                              </xs:annotation>
                         </xs:enumeration>
                         <xs:enumeration value="8">
                              <xs:annotation>
                                   <xs:appinfo>Serious failure</xs:appinfo>
                              </xs:annotation>
                         </xs:enumeration>
                         <xs:enumeration value="12">
                              <xs:annotation>
                                   <xs:appinfo>
                                        Major failure; action made unavailable
                                   </xs:appinfo>
                              </xs:annotation>
                         </xs:enumeration>
                    </xs:restriction>
               </xs:simpleType>
          </xs:attribute>
     </xs:complexType>
     <xs:complexType name="AuditSourceIdentificationType">
          <xs:sequence>
<xs:element name="AuditSourceTypeCode" type="CodedValueType"      minOccurs="0"
maxOccurs="unbounded" />
          </xs:sequence>
          <xs:attribute name="AuditEnterpriseSiteID"
                         type="xs:string" use="optional" />
          <xs:attribute name="AuditSourceID" type="xs:string" use="required" />
     </xs:complexType>
     <xs:complexType name="ActiveParticipantType">
          <xs:sequence minOccurs="0">
<xs:element name="RoleIDCode" type="CodedValueType" minOccurs="0"
     maxOccurs="unbounded" />
          </xs:sequence>
          <xs:attribute name="UserID" type="xs:string" use="required" />
          <xs:attribute name="AlternativeUserID"
                         type="xs:string" use="optional" />
          <xs:attribute name="UserName" type="xs:string" use="optional" />
          <xs:attribute name="UserIsRequestor"
                         type="xs:boolean" use="optional"
default="true" />
          <xs:attribute name="NetworkAccessPointID"
                         type="xs:string" use="optional" />
          <xs:attribute name="NetworkAccessPointTypeCode"
               use="optional">
               <xs:simpleType>
                    <xs:restriction base="xs:unsignedByte">
                         <xs:enumeration value="1">
```

```
                    <xs:annotation>
                         <xs:appinfo>
                              Machine Name, including DNS name
                         </xs:appinfo>
                    </xs:annotation>
               </xs:enumeration>
               <xs:enumeration value="2">
                    <xs:annotation>
                         <xs:appinfo>IP Address</xs:appinfo>
                    </xs:annotation>
               </xs:enumeration>
               <xs:enumeration value="3">
                    <xs:annotation>
                         <xs:appinfo>Telephone Number</xs:appinfo>
                    </xs:annotation>
               </xs:enumeration>
          </xs:restriction>
     </xs:simpleType>
</xs:attribute>
</xs:complexType>
<xs:complexType name="ParticipantObjectIdentificationType">
     <xs:sequence>
          <xs:element name="ParticipantObjectIDTypeCode"
                    type="CodedValueType" />
          <xs:choice minOccurs="0">
               <xs:element name="ParticipantObjectName"
                    type="xs:string" minOccurs="0" />
               <xs:element name="ParticipantObjectQuery"
                    type="xs:base64Binary" minOccurs="0" />
          </xs:choice>
          <xs:element name="ParticipantObjectDetail"
                    type="TypeValuePairType"
                    minOccurs="0" maxOccurs="unbounded" />
     </xs:sequence>
     <xs:attribute name="ParticipantObjectID"
                    type="xs:string" use="required" />
     <xs:attribute name="ParticipantObjectTypeCode" use="optional">
          <xs:simpleType>
               <xs:restriction base="xs:unsignedByte">
                    <xs:enumeration value="1">
                         <xs:annotation>
                              <xs:appinfo>Person</xs:appinfo>
                         </xs:annotation>
                    </xs:enumeration>
                    <xs:enumeration value="2">
                         <xs:annotation>
                              <xs:appinfo>System object</xs:appinfo>
                         </xs:annotation>
                    </xs:enumeration>
                    <xs:enumeration value="3">
                         <xs:annotation>
                              <xs:appinfo>Organization</xs:appinfo>
                         </xs:annotation>
                    </xs:enumeration>
                    <xs:enumeration value="4">
                         <xs:annotation>
                              <xs:appinfo>Other</xs:appinfo>
                         </xs:annotation>
                    </xs:enumeration>
               </xs:restriction>
          </xs:simpleType>
     </xs:attribute>
     <xs:attribute name="ParticipantObjectTypeCodeRole"
          use="optional">
```

```
<xs:simpleType>
     <xs:restriction base="xs:unsignedByte">
          <xs:enumeration value="1">
               <xs:annotation>
                    <xs:appinfo>Patient</xs:appinfo>
               </xs:annotation>
          </xs:enumeration>
          <xs:enumeration value="2">
               <xs:annotation>
                    <xs:appinfo>Location</xs:appinfo>
               </xs:annotation>
          </xs:enumeration>
          <xs:enumeration value="3">
               <xs:annotation>
                    <xs:appinfo>Report</xs:appinfo>
               </xs:annotation>
          </xs:enumeration>
          <xs:enumeration value="4">
               <xs:annotation>
                    <xs:appinfo>Resource</xs:appinfo>
               </xs:annotation>
          </xs:enumeration>
          <xs:enumeration value="5">
               <xs:annotation>
                    <xs:appinfo>Master file</xs:appinfo>
               </xs:annotation>
          </xs:enumeration>
          <xs:enumeration value="6">
               <xs:annotation>
                    <xs:appinfo>User</xs:appinfo>
               </xs:annotation>
          </xs:enumeration>
          <xs:enumeration value="7">
               <xs:annotation>
                    <xs:appinfo>List</xs:appinfo>
               </xs:annotation>
          </xs:enumeration>
          <xs:enumeration value="8">
               <xs:annotation>
                    <xs:appinfo>Doctor</xs:appinfo>
               </xs:annotation>
          </xs:enumeration>
          <xs:enumeration value="9">
               <xs:annotation>
                    <xs:appinfo>Subscriber</xs:appinfo>
               </xs:annotation>
          </xs:enumeration>
          <xs:enumeration value="10">
               <xs:annotation>
                    <xs:appinfo>Guarantor</xs:appinfo>
               </xs:annotation>
          </xs:enumeration>
          <xs:enumeration value="11">
               <xs:annotation>
                    <xs:appinfo>
                         Security User Entity
                    </xs:appinfo>
               </xs:annotation>
          </xs:enumeration>
          <xs:enumeration value="12">
               <xs:annotation>
                    <xs:appinfo>Security User Group</xs:appinfo>
               </xs:annotation>
          </xs:enumeration>
```

```
                <xs:enumeration value="13">
                     <xs:annotation>
                          <xs:appinfo>Security Resource</xs:appinfo>
                     </xs:annotation>
                </xs:enumeration>
                <xs:enumeration value="14">
                     <xs:annotation>
                          <xs:appinfo>
                               Security Granualarity Definition
                          </xs:appinfo>
                     </xs:annotation>
                </xs:enumeration>
                <xs:enumeration value="15">
                     <xs:annotation>
                          <xs:appinfo>Provider</xs:appinfo>
                     </xs:annotation>
                </xs:enumeration>
                <xs:enumeration value="16">
                     <xs:annotation>
                          <xs:appinfo>Report Destination</xs:appinfo>
                     </xs:annotation>
                </xs:enumeration>
                <xs:enumeration value="17">
                     <xs:annotation>
                          <xs:appinfo>Report Library</xs:appinfo>
                     </xs:annotation>
                </xs:enumeration>
                <xs:enumeration value="18">
                     <xs:annotation>
                          <xs:appinfo>Schedule</xs:appinfo>
                     </xs:annotation>
                </xs:enumeration>
                <xs:enumeration value="19">
                     <xs:annotation>
                          <xs:appinfo>Customer</xs:appinfo>
                     </xs:annotation>
                </xs:enumeration>
                <xs:enumeration value="20">
                     <xs:annotation>
                          <xs:appinfo>Job</xs:appinfo>
                     </xs:annotation>
                </xs:enumeration>
                <xs:enumeration value="21">
                     <xs:annotation>
                          <xs:appinfo>Job Stream</xs:appinfo>
                     </xs:annotation>
                </xs:enumeration>
                <xs:enumeration value="22">
                     <xs:annotation>
                          <xs:appinfo>Table</xs:appinfo>
                     </xs:annotation>
                </xs:enumeration>
                <xs:enumeration value="23">
                     <xs:annotation>
                          <xs:appinfo>Routing Criteria</xs:appinfo>
                     </xs:annotation>
                </xs:enumeration>
                <xs:enumeration value="24">
                     <xs:annotation>
                          <xs:appinfo>Query</xs:appinfo>
                     </xs:annotation>
                </xs:enumeration>
           </xs:restriction>
      </xs:simpleType>
```

```
</xs:attribute>
<xs:attribute name="ParticipantObjectDataLifeCycle"
     use="optional">
     <xs:simpleType>
          <xs:restriction base="xs:unsignedByte">
               <xs:enumeration value="1">
                    <xs:annotation>
                         <xs:appinfo>
                              Origination / Creation
                         </xs:appinfo>
                    </xs:annotation>
               </xs:enumeration>
               <xs:enumeration value="2">
                    <xs:annotation>
                         <xs:appinfo>
                              Import / Copy from original
                         </xs:appinfo>
                    </xs:annotation>
               </xs:enumeration>
               <xs:enumeration value="3">
                    <xs:annotation>
                         <xs:appinfo>Amendment</xs:appinfo>
                    </xs:annotation>
               </xs:enumeration>
               <xs:enumeration value="4">
                    <xs:annotation>
                         <xs:appinfo>Verification</xs:appinfo>
                    </xs:annotation>
               </xs:enumeration>
               <xs:enumeration value="5">
                    <xs:annotation>
                         <xs:appinfo>Translation</xs:appinfo>
                    </xs:annotation>
               </xs:enumeration>
               <xs:enumeration value="6">
                    <xs:annotation>
                         <xs:appinfo>Access / Use</xs:appinfo>
                    </xs:annotation>
               </xs:enumeration>
               <xs:enumeration value="7">
                    <xs:annotation>
                         <xs:appinfo>De-identification</xs:appinfo>
                    </xs:annotation>
               </xs:enumeration>
               <xs:enumeration value="8">
                    <xs:annotation>
                         <xs:appinfo>
                              Aggregation, summarization, derivation
                         </xs:appinfo>
                    </xs:annotation>
               </xs:enumeration>
               <xs:enumeration value="9">
                    <xs:annotation>
                         <xs:appinfo>Report</xs:appinfo>
                    </xs:annotation>
               </xs:enumeration>
               <xs:enumeration value="10">
                    <xs:annotation>
                         <xs:appinfo>
                              Export / Copy to target
                         </xs:appinfo>
                    </xs:annotation>
               </xs:enumeration>
               <xs:enumeration value="11">
```

```
                              <xs:annotation>
                                   <xs:appinfo>Disclosure</xs:appinfo>
                              </xs:annotation>
                         </xs:enumeration>
                         <xs:enumeration value="12">
                              <xs:annotation>
                                   <xs:appinfo>
                                        Receipt of disclosure
                                   </xs:appinfo>
                              </xs:annotation>
                         </xs:enumeration>
                         <xs:enumeration value="13">
                              <xs:annotation>
                                   <xs:appinfo>Archiving</xs:appinfo>
                              </xs:annotation>
                         </xs:enumeration>
                         <xs:enumeration value="14">
                              <xs:annotation>
                                   <xs:appinfo>Logical deletion</xs:appinfo>
                              </xs:annotation>
                         </xs:enumeration>
                         <xs:enumeration value="15">
                              <xs:annotation>
                                   <xs:appinfo>
                                        Permanent erasure / Physical destruction
                                   </xs:appinfo>
                              </xs:annotation>
                         </xs:enumeration>
                    </xs:restriction>
               </xs:simpleType>
          </xs:attribute>
          <xs:attribute name="ParticipantObjectSensitivity"
                         type="xs:string"
                         use="optional" />
     </xs:complexType>
     <xs:complexType name="CodedValueType">
          <xs:attribute name="code" type="xs:string" use="required" />
          <xs:attributeGroup ref="CodeSystem" />
          <xs:attribute name="displayName" type="xs:string" use="optional" />
          <xs:attribute name="originalText" type="xs:string" use="optional" />
     </xs:complexType>
     <xs:complexType name="TypeValuePairType">
          <xs:attribute name="type" type="xs:string" use="required" />
          <xs:attribute name="value" type="xs:base64Binary" use="required" />
     </xs:complexType>
     <xs:attributeGroup name="CodeSystem">
          <xs:attribute name="codeSystem" type="OID" use="optional" />
          <xs:attribute name="codeSystemName" type="xs:string" use="optional" />
     </xs:attributeGroup>
     <xs:simpleType name="OID">
          <xs:restriction base="xs:string">
               <xs:whiteSpace value="collapse" />
          </xs:restriction>
     </xs:simpleType>
</xs:schema>
```

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

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

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

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

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

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

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

[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] Services HFS Receiver DG2016 PICS and PIXIT excel sheet v1.7. http://handle.itu.int/11.1002/2000/12067

[b-HFSS PICS & PIXIT] Services HFS Sender DG2016 PICS and PIXIT excel sheet v1.7. http://handle.itu.int/11.1002/2000/12067

[b-IETF RFC 2246] IETF RFC 2246 (1999), *The TLS Protocol version 1.0*. https://datatracker.ietf.org/doc/rfc2246

[b-IETF RFC 3164] IETF RFC 3164 (2001), *The BSD Syslog Protocol*.

[b-OASIS SAMLTP] OASIS (2006), *Web Services Security: SAML Token Profile 1.1*. http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-SAMLTokenProfile.pdf

[b-OASIS SAML 2.0] OASIS SAML 2.0 (2005), *Security Assertion Markup Language 2.0*. http://docs.oasis-open.org/security/saml/v2.0/

SERIES OF ITU-T RECOMMENDATIONS

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

Printed in Switzerland
Geneva, 2017