INTERNATIONAL STANDARD

ISO/IEEE 11073-20702

First edition
2018-09

Health informatics — Point-of-care medical device communication —

Part 20702: Medical devices communication profile for web services

Informatique de santé — Communication entre dispositifs médicaux sur le site des soins —

Reference number
ISO/IEEE 11073-20702:2018(E)

Institute of Electrical and Electronics Engineers, Inc
3 Park Avenue, New York
NY 10016-5997, USA

Email: stds.ipr@ieee.org
Website: www.ieee.org

Published in Switzerland

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted (see www.iso.org/directives).

IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE-SA) Standards Board. The IEEE develops its standards through a consensus development process, approved by the American National Standards Institute, which brings together volunteers representing varied viewpoints and interests to achieve the final product. Volunteers are not necessarily members of the Institute and serve without compensation. While the IEEE administers the process and establishes rules to promote fairness in the consensus development process, the IEEE does not independently evaluate, test, or verify the accuracy of any of the information contained in its standards.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

ISO/IEEE 11073-20702 was prepared by the IEEE 11073 Standards Committee of the IEEE Engineering in Medicine and Biology Society (as IEEE Std 11073-20702-2016) and drafted in accordance with its editorial rules. It was adopted, under the "fast-track procedure" defined in the Partner Standards Development Organization cooperation agreement between ISO and IEEE, by Technical Committee ISO/TC 215, *Health informatics*.

A list of all parts in the ISO/IEEE 11073 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Health informatics—Point-of-care medical device communication

Part 20702: Medical Devices Communication Profile for Web Services

Sponsor

IEEE 11073™ Standards Committee
of the
IEEE Engineering in Medicine and Biology Society

Approved 22 September 2016

IEEE-SA Standards Board

Abstract: Within the context of the ISO/IEEE 11073 family of standards for point-of-care (PoC) medical device communication, a communication protocol specification for a distributed system of PoC medical devices and medical IT systems that need to exchange data, or safely control networked PoC medical devices by profiling Web Service specifications, is defined by this standard. Additional Web Service specifications are part of this standard.

Keywords: Devices Profile for Web Services, DPWS, Efficient XML Interchange, EXI, IEEE 11073-20702™, ISO/IEEE 11073, MDC, medical device communication, PoC, point-of-care, safety, Simple Object Access Protocol, SOAP, Streaming Web Services, WS-Discovery

The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA

PDF: ISBN 978-1-5044-2324-3 STD21112
Print: ISBN 978-1-5044-2325-0 STDPD21112

Important Notices and Disclaimers Concerning IEEE Standards Documents

IEEE documents are made available for use subject to important notices and legal disclaimers. These notices and disclaimers, or a reference to this page, appear in all standards and may be found under the heading "Important Notices and Disclaimers Concerning IEEE Standards Documents." They can also be obtained on request from IEEE or viewed at http://standards.ieee.org/IPR/disclaimers.html.

Notice and Disclaimer of Liability Concerning the Use of IEEE Standards Documents

IEEE Standards documents (standards, recommended practices, and guides), both full-use and trial-use, are developed within IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association ("IEEE-SA") Standards Board. IEEE ("the Institute") develops its standards through a consensus development process, approved by the American National Standards Institute ("ANSI"), which brings together volunteers representing varied viewpoints and interests to achieve the final product. IEEE Standards are documents developed through scientific, academic, and industry-based technical working groups. Volunteers in IEEE working groups are not necessarily members of the Institute and participate without compensation from IEEE. While IEEE administers the process and establishes rules to promote fairness in the consensus development process, IEEE does not independently evaluate, test, or verify the accuracy of any of the information or the soundness of any judgments contained in its standards.

IEEE Standards do not guarantee or ensure safety, security, health, or environmental protection, or ensure against interference with or from other devices or networks. Implementers and users of IEEE Standards documents are responsible for determining and complying with all appropriate safety, security, environmental, health, and interference protection practices and all applicable laws and regulations.

IEEE does not warrant or represent the accuracy or content of the material contained in its standards, and expressly disclaims all warranties (express, implied and statutory) not included in this or any other document relating to the standard, including, but not limited to, the warranties of: merchantability; fitness for a particular purpose; non-infringement; and quality, accuracy, effectiveness, currency, or completeness of material. In addition, IEEE disclaims any and all conditions relating to: results; and workmanlike effort. IEEE standards documents are supplied "AS IS" and "WITH ALL FAULTS."

Use of an IEEE standard is wholly voluntary. The existence of an IEEE standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard.

In publishing and making its standards available, IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity nor is IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing any IEEE Standards document, should rely upon his or her own independent judgment in the exercise of reasonable care in any given circumstances or, as appropriate, seek the advice of a competent professional in determining the appropriateness of a given IEEE standard.

IN NO EVENT SHALL IEEE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE PUBLICATION, USE OF, OR RELIANCE UPON ANY STANDARD, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Translations

The IEEE consensus development process involves the review of documents in English only. In the event that an IEEE standard is translated, only the English version published by IEEE should be considered the approved IEEE standard.

Official statements

A statement, written or oral, that is not processed in accordance with the IEEE-SA Standards Board Operations Manual shall not be considered or inferred to be the official position of IEEE or any of its committees and shall not be considered to be, or be relied upon as, a formal position of IEEE. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that his or her views should be considered the personal views of that individual rather than the formal position of IEEE.

Comments on standards

Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of membership affiliation with IEEE. However, IEEE does not provide consulting information or advice pertaining to IEEE Standards documents. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Since IEEE standards represent a consensus of concerned interests, it is important that any responses to comments and questions also receive the concurrence of a balance of interests. For this reason, IEEE and the members of its societies and Standards Coordinating Committees are not able to provide an instant response to comments or questions except in those cases where the matter has previously been addressed. For the same reason, IEEE does not respond to interpretation requests. Any person who would like to participate in revisions to an IEEE standard is welcome to join the relevant IEEE working group.

Comments on standards should be submitted to the following address:

Secretary, IEEE-SA Standards Board
445 Hoes Lane
Piscataway, NJ 08854 USA

Laws and regulations

Users of IEEE Standards documents should consult all applicable laws and regulations. Compliance with the provisions of any IEEE Standards document does not imply compliance to any applicable regulatory requirements. Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

Copyrights

IEEE draft and approved standards are copyrighted by IEEE under U.S. and international copyright laws. They are made available by IEEE and are adopted for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making these documents available for use and adoption by public authorities and private users, IEEE does not waive any rights in copyright to the documents.

Photocopies

Subject to payment of the appropriate fee, IEEE will grant users a limited, non-exclusive license to photocopy portions of any individual standard for company or organizational internal use or individual, non-commercial use only. To arrange for payment of licensing fees, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Updating of IEEE Standards documents

Users of IEEE Standards documents should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect.

Every IEEE standard is subjected to review at least every ten years. When a document is more than ten years old and has not undergone a revision process, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE standard.

In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit the IEEE Xplore at http://ieeexplore.ieee.org/ or contact IEEE at the address listed previously. For more information about the IEEE-SA or IEEE's standards development process, visit the IEEE-SA Website at http://standards.ieee.org.

Errata

Errata, if any, for all IEEE standards can be accessed on the IEEE-SA Website at the following URL: http://standards.ieee.org/findstds/errata/index.html. Users are encouraged to check this URL for errata periodically.

Patents

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken by the IEEE with respect to the existence or validity of any patent rights in connection therewith. If a patent holder or patent applicant has filed a statement of assurance via an Accepted Letter of Assurance, then the statement is listed on the IEEE-SA Website at http://standards.ieee.org/about/sasb/patcom/patents.html. Letters of Assurance may indicate whether the Submitter is willing or unwilling to grant licenses under patent rights without compensation or under reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair discrimination to applicants desiring to obtain such licenses.

Essential Patent Claims may exist for which a Letter of Assurance has not been received. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims, or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

Participants

At the time this standard was submitted to the IEEE-SA Standards Board for approval, the Point-of-Care Devices Working Group had the following membership:

Jan Wittenber, *Chair*
Stefan Schlichting, *SubGroup Chair*

Bjoern Anderson
Malcolm Clarke
Todd Cooper
Chris Courville
Gion Durisch
Michael Faughn
Kenneth Fuchs
John Garguilo
David Gregorczyk
Kai Hassing
John Hatcliff
Stefan Karl
Martin Kasparick
Daniel Krahenbuhl
Koichiro Matsumoto
Joerg-Uwe Meyer
Ali Miller
Robert Mortonson
Stephan Poehlsen
Tracy Rausch
John Rhoads
Paul Schluter
Janek Schumann
Masato Tanaka
Eugene Vasserman
Stan Wiley

The following members of the individual balloting committee voted on this standard. Balloters may have voted for approval, disapproval, or abstention.

Bjoern Andersen
Charles Barest
Lyle Bullock
Todd Cooper
Sourav Dutta
Kenneth Fuchs
Joel Goergen
Frank Golatowski
Eric W. Gray
David Gregorczyk
Randall Groves
Kai Hassing
John Hatcliff
Werner Hoelzl
Noriyuki Ikeuchi
Atsushi Ito
Stefan Karl
Piotr Karocki
Martin Kasparick
William Lumpkins
Joerg-Uwe Meyer
Stephan Poehlsen
Beth Pumo
Bartien Sayogo
Stefan Schlichting
Paul Schluter
Eugene Stoudenmire
Walter Struppler
J. Wiley
Jan Wittenber
Oren Yuen
Daidi Zhong

When the IEEE-SA Standards Board approved this standard on 22 September 2016, it had the following membership:

Jean-Philippe Faure, *Chair*
Ted Burse, *Vice Chair*
John D. Kulick, *Past Chair*
Konstantinos Karachalios, *Secretary*

Chuck Adams
Masayuki Ariyoshi
Stephen Dukes
Jianbin Fan
J. Travis Griffith
Gary Hoffman
Ronald W. Hotchkiss
Michael Janezic
Joseph L. Koepfinger*
Hung Ling
Kevin Lu
Annette D. Reilly
Gary Robinson
Mehmet Ulema
Yingli Wen
Howard Wolfman
Don Wright
Yu Yuan
Daidi Zhong

*Member Emeritus

Introduction

This introduction is not part of IEEE Std 11073-20702-2016, Health informatics—Point-of-care medical device communication—Part 20702: Standard for Medical Devices Communication Profile for Web Services.

ISO/IEEE 11073 standards enable communication between medical devices and external computer systems. They provide automatic and detailed electronic data capture of patient vital signs information and device operational data. The primary goals are to:

— Provide real-time plug-and-play interoperability for patient-connected medical devices

— Facilitate the efficient exchange of vital signs and medical device data, acquired at the point-of-care (POC), in all healthcare environments

This standard defines a discovery, messaging, and event propagation method for a distributed POC medical device communication system. It serves as communication transport layer related to the existing ISO/IEEE 11073 standards series (ISO/IEEE 11073-10101:2004 [B6], ISO/IEEE 11073-10201:2004 [B7], and ISO/IEEE 11073-20101:2004 [B8]).[1] Moreover, a set of protocols is defined that allows transmission of real-time streams (e.g., waveforms) and remote control of a medical device in a safe way. For this purpose, it introduces implementation constraints and extensions on the Devices Profile for Web Services (DPWS) standard (OASIS DPWS V1.1) in order to allow the utilization of DPWS in such an environment.

Furthermore, this standard is intended to be compatible with the Integrating the Healthcare Enterprise (IHE) International's technical framework specifications for using Web Services for achieving interoperability in healthcare [e.g., Web Services Basic Profile 2.0 (WS-I Basic Profile V2.0)], which is used by Information Technology Infrastructure (ITI) Technical Framework Volume 2, Appendix V: Web Services for IHE Transactions, and further referenced for device information exchange in the Patient Care Device (PCD) Technical Framework Volume 2 [B5].

In the IHE Patient Care Device (PCD) domain, Web Services are used to wrap IHE PCD HL7 messages. Beyond that, this standard adds the capability of providing a plug-and-play and publish-subscribe supporting Web Services infrastructure to create a service-oriented architecture in distributed systems of medical devices.

The non-normative name of this standard is "Medical Devices Profile for Web Services" (MDPWS).

[1]The numbers in brackets correspond to those of the bibliography in Annex E.

Contents

Health informatics—Point-of-care medical device communication

Part 20702: Medical Devices Communication Profile for Web Services

1. Overview

1.1 Scope

The scope of this standard is a communication protocol specification for a distributed system of point-of-care (PoC) medical devices and medical IT systems that need to exchange data or safely control networked PoC medical devices by defining a profile for Web Service specifications and defining additional Web Service specifications as part of this standard.

1.2 Purpose

Currently, there is no part of the 11073 standard series that allows plug-and-play-enabled communication of medical devices in an Internet Protocol (IP)-based distributed PoC medical device communication system. Therefore, this standard defines a discovery, messaging, and event propagation method for a distributed PoC medical device communication system based on Web Services. Moreover, it proposes a set of protocols that allow advertisement of STREAMs (e.g., waveforms) as well as provision of remote control in a safe way. For this purpose, the Devices Profile for Web Services (DPWS) is used as a communication foundation and tailored to be utilized in a distributed PoC medical device communication system.

This standard can be used for any diagnostic, therapeutic, or monitoring communication needs where PoC medical devices shall be able to discover communication partners, exchange virtual device descriptions, provide and consume event-driven data, and enable safe remote control.

2. Normative references

The following referenced documents are indispensable for the application of this document (i.e., they shall be understood and used, so each referenced document is cited in text and its relationship to this document is explained). For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments or corrigenda) applies.

IETF RFC 2119, Key Words for Use in RFCs to Indicate Requirement Levels, March 1997. Available at http://www.ietf.org/rfc/rfc2119.txt.[2]

IETF RFC 2616, Hypertext Transfer Protocol—HTTP/1.1, June 1999. Available at https://tools.ietf.org/html/rfc2616.

IETF RFC 3987, Internationalized Resource Identifiers (IRIs), January 2005. Available at https://tools.ietf.org/html/rfc3987.

OASIS Devices Profile for Web Services (DPWS) Version 1.1, 1 July 2009. Available at http://docs.oasis-open.org/ws-dd/dpws/1.1/os/wsdd-dpws-1.1-spec-os.html.

OASIS SOAP-over-UDP Version 1.1, 1 July 2009. Available at http://docs.oasis-open.org/ws-dd/soapoverudp/1.1/os/wsdd-soapoverudp-1.1-spec-os.html.

OASIS Web Services Dynamic Discovery (WS-Discovery) Version 1.1, 1 July 2009. Available at http://docs.oasis-open.org/ws-dd/discovery/1.1/os/wsdd-discovery-1.1-spec-os.html.

OASIS Web Services Security, SOAP Message Security 1.0 (WS-Security 2004), March 2004. Available at https://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0.pdf.

W3C® Web Services Description Language (WSDL) 1.1, Note, 15 March 2001. Available at http://www.w3.org/TR/2001/NOTE-wsdl-20010315.[3]

W3C Web Services Eventing (WS-Eventing), Member Submission, 15 March 2006. Available at http://www.w3.org/Submission/2006/SUBM-WS-Eventing-20060315/.

W3C Web Services Metadata Exchange (WS-MetadataExchange) 1.1, Member Submission, 13 August 2008. Available at http://www.w3.org/Submission/2008/SUBM-WS-MetadataExchange-20080813.

W3C Efficient XML Interchange (EXI) Format 1.0 (Second Edition), Recommendation, 11 February 2014. Available at http://www.w3.org/TR/2014/REC-exi-20140211/.

W3C Exclusive XML Canonicalization Version 1.0, Recommendation, 18 July 2002. Available at http://www.w3.org/TR/2002/REC-xml-exc-c14n-20020718/.

W3C Extensible Markup Language (XML) 1.0 (Fifth Edition), Recommendation, 28 November 2008. Available at https://www.w3.org/TR/2008/REC-xml-20081126/.

W3C Namespaces in XML 1.0 (Third Edition), Recommendation, 8 December 2009. Available at http://www.w3.org/TR/REC-xml-names/.

W3C SOAP Version 1.2 Part 1: Messaging Framework, Recommendation, 27 April 2007. Available at http://www.w3.org/TR/soap12-part1/.

W3C Web Services Addressing 1.0 (WS-Addressing), Recommendation, 9 May 2006. Available at http://www.w3.org/TR/ws-addr-core.

W3C Web Services Policy 1.5—Attachment (WS-Policy Attachment), Recommendation, 4 September 2007. Available at http://www.w3.org/TR/ws-policy-attach.

[2]IETF documents (i.e., RFCs) are available for download at http://www.rfc-archive.org/.
[3]W3C is trademarks or registered trademarks of the W3C®, (registered in numerous countries) World Wide Web Consortium. Marks of W3C are registered and held by its host institutions: Massachusetts Institute of Technology (MIT), European Research Consortium for Information and Mathematics (ERCIM), and Keio University, Japan.

W3C Web Services Policy 1.5—Framework (WS-Policy), Recommendation, 4 September 2007. Available at http://www.w3.org/TR/ws-policy/.

W3C XML Information Set (Second Edition), Recommendation, 4 February 2004. Available at https://www.w3.org/TR/xml-infoset/.

W3C XML Path Language (XPath) Version 1.0, Recommendation, 7 September 2015. Available at http://www.w3.org/TR/1999/REC-xpath-19991116.

W3C XML Schema 1.1, Recommendation, 28 October 2004. Available at http://www.w3.org/TR/xmlschema-1, http://www.w3.org/TR/xmlschema-2/.

W3C Web Services Addressing 1.0—Metadata, Working Draft, 16 May 2007. Available at https://www.w3.org/TR/2007/WD-ws-addr-metadata-20070516/.

WS-I Basic Profile Version 2.0, 9 November 2010. Available at http://ws-i.org/profiles/BasicProfile-2.0-2010-11-09.html.

3. Definitions, terminology, notational conventions, and normative statements

3.1 Definitions

For the purposes of this document, the following terms and definitions apply. The *IEEE Standards Dictionary Online* should be consulted for terms not defined in this clause.[4]

ASSERTION: A WS-Policy assertion. A policy assertion identifies a behavior that is a requirement or capability of a policy subject. A policy subject is an entity (e.g., an endpoint, message, resource, operation) with which a policy can be associated. (adapted from W3C WS-Policy 1.5 Framework, Section 3.1)

ATTRIBUTE: References the attribute in a normative outline that is currently described.

NOTE—See normative outlines in 3.3.1.[5]

CLIENT: A network endpoint that sends MESSAGEs to and/or receives MESSAGEs from a SERVICE. (OASIS DPWS V1.1)

DEVICE: A distinguished type of SERVICE that hosts other SERVICEs and sends and/or receives one or more specific types of MESSAGEs. (OASIS DPWS V1.1)

ELEMENT: References the element in a normative outline that is currently described.

NOTE—See 3.3.1.

HOSTED SERVICE: A distinguished type of SERVICE that is hosted by another SERVICE. The lifetime of the HOSTED SERVICE is a subset of the lifetime of its host. The HOSTED SERVICE is visible (not encapsulated) and is addressed separately from its host. Each HOSTED SERVICE has exactly one host. The relationship is not transitive. (OASIS DPWS V1.1)

[4]The *IEEE Standards Dictionary Online* is available at: http://dictionary.ieee.org.
[5]Notes in text, tables, and figures of a standard are given for information only and do not contain requirements needed to implement this standard.

MESSAGE: Protocol elements that are exchanged, usually over a network, to affect a Web Service. Always includes a SOAP ENVELOPE. Typically also includes transport framing information such as HTTP headers, TCP headers, and IP headers. (OASIS DPWS V1.1)

RECEIVER: A CLIENT or SERVICE that receives a MESSAGE. (OASIS DPWS V1.1)

SECURE CHANNEL: A SECURE CHANNEL is a point-to-point transport-level TLS/SSL connection established between a CLIENT and a SERVICE.

SENDER: A CLIENT or SERVICE that sends a MESSAGE. (OASIS DPWS V1.1)

SERVICE: A software system that exposes its capabilities by receiving and/or sending MESSAGEs on one or several network endpoints. (OASIS DPWS V1.1)

SOAP ENVELOPE: An XML Infoset that consists of a document information item (W3C XML Information Set) with exactly one member in its [children] property, which MUST be the SOAP Envelope (W3C SOAP V1.2 Part 1) element information item. (OASIS DPWS V1.1)

STREAM: A STREAM designates MESSAGEs that are periodically delivered from a networked DEVICE over an IP-based transmission medium to one or more CLIENTs.

STREAMING: A mechanism to periodically deliver MESSAGEs from networked DEVICEs over an IP-based transmission medium to one or more CLIENTs.

TEXT SOAP ENVELOPE: A SOAP ENVELOPE serialized as application/soap+xml. (OASIS DPWS V1.1)

3.2 Terminology

The keywords “MUST NOT,” “REQUIRED,” “SHALL,” “SHALL NOT,” “SHOULD,” “SHOULD NOT,” “RECOMMENDED,” “MAY,” and “OPTIONAL” in this document are to be interpreted as described in IETF RFC 2119.[6]

3.3 Notational conventions

3.3.1 Normative outlines

According to OASIS DPWS V1.1, this standard uses the following syntax to define normative outlines:

— The syntax appears as an XML instance, but values in italics indicate data types instead of literal values.

— Characters are appended to elements and attributes to indicate cardinality:

- “?” (0 or 1)
- “*” (0 or more)
- “+” (1 or more)
- The character “|” is used to indicate a choice between alternatives.

— The characters “(“ and “)” are used to indicate that contained items are to be treated as a group with respect to cardinality or choice.

— The characters “[“ and “]” are used to call out references and property names.

[6]Information on references can be found in Clause 2.

— Ellipses (i.e., "...") indicate points of extensibility. Additional children and/or attributes MAY be added at the indicated extension points but SHALL NOT contradict the semantics of the parent and/or owner, respectively. By default, if a receiver does not recognize an extension, the receiver SHOULD ignore the extension; exceptions to this processing rule, if any, are clearly indicated below.

— XML namespace prefixes (see Table 1) are used to indicate the namespace of the element being defined.

Any normative outline is described in more detail by giving a set of XPath expressions followed by a description. The XPath expressions point to elements or attributes in the foregoing outline.

Example:

```
(01)   <SampleElement SampleAttribute="xs:string"? >
(02)     <NestedElement ...>
(03)       ...
(04)     </NestedElement> +
(05)   </SampleElement>
```

The remainder of this subclause describes additional, normative constraints on the previously listed outline.

`/SampleElement`
Detailed description of SampleElement. By definition, SampleElement is referenced here by using the keyword ELEMENT.

`/SampleElement/@SampleAttribute`
Detailed description of SampleElement's attribute SampleAttribute. By definition, SampleAttribute is referenced here by using the keyword ATTRIBUTE.

`/SampleElement/NestedElement`
Detailed description of NestedElement.

3.3.2 Normative statements

According to the notation given in OASIS DPWS V1.1, normative statements of requirements are presented in the following manner:

Rnnnn: Statement text here.

where "nnnn" is replaced by a number that is unique among the requirements in this standard, thereby forming a unique requirement identifier.

Requirements can be considered to possess a namespace qualifier, in such a way as to be compatible with QNames from Namespaces in XML (W3C Namespaces in XML 1.0). If there is no explicit namespace prefix on a requirement's identifier (e.g., "R9999" as opposed to "dpws:R9999"), it should be interpreted as being in the namespace identified for this standard. A prefixed requirement refers to the specification that defines that prefix. For example, dpws:R9999 refers to requirement R9999 defined in OASIS DPWS V1.1.

3.3.3 Extended Backus-Naur Form

This standard makes use of a simple Extended Backus-Naur Form (EBNF) notation to specify a grammar for XPath expressions. The simple EBNF notation is cited from W3C XML 1.0. Each rule in the grammar defines one symbol, in the form:

`symbol ::= expression`
Symbols are written with an initial capital letter if they are the start symbol of a regular language, otherwise with an initial lowercase letter. Literal strings are quoted. Within the expression on the right-hand side of a rule, the following expressions are used to match strings of one or more characters:

`#xN`
Where N is a hexadecimal integer, the expression matches the character whose number (code point) in ISO/IEC 10646 is N. The number of leading zeroes in the #xN form is insignificant.

`[a-zA-Z], [#xN-#xN]`
Matches any Char with a value in the range(s) indicated (inclusive).

`[abc], [#xN#xN#xN]`
Matches any Char with a value among the characters enumerated. Enumerations and ranges can be mixed in one set of brackets.

`[^a-z], [^#xN-#xN]`
Matches any Char with a value outside the range indicated.

`[^abc], [^#xN#xN#xN]`
Matches any Char with a value not among the characters given. Enumerations and ranges of forbidden values can be mixed in one set of brackets.

`"string"`
Matches a literal string matching that given inside the double quotes.

`'string'`
Matches a literal string matching that given inside the single quotes.

These symbols may be combined to match more complex patterns as follows, where A and B represent simple expressions:

`(expression)`
Expression is treated as a unit and may be combined as described in this list.

`A?`
Matches A or nothing; optional A.

`A B`
Matches A followed by B. This operator has higher precedence than alternation; thus A B | C D is identical to (A B) | (C D).

`A | B`
Matches A or B.

`A - B`
Matches any string that matches A but does not match B.

`A+`
Matches one or more occurrences of A. Concatenation has higher precedence than alternation; thus A+ | B+ is identical to (A+) | (B+).

`A*`
Matches zero or more occurrences of A. Concatenation has higher precedence than alternation; thus A* | B* is identical to (A*) | (B*).

3.3.4 Abbreviated notations

If not defined otherwise, this standard uses the following properties to designate SOAP parts:

[Action] The value to be used for the wsa:Action IRI.

[Body] A MESSAGE body.

These properties bind to a SOAP Envelope as follows:

```
<s12:Envelope>
  <s12:Header>
    <wsa:Action>[Action]</wsa:Action>
    ...
  </s12:Header>
  <s12:Body>[Body]</s:Body>
</s12:Envelope>
```

3.4 XML namespaces

Table 1 lists XML namespaces that are used in this standard. Although the choice of the namespace prefix is arbitrary and not semantically significant (W3C XML Information Set), it is RECOMMENDED by this standard that the prefixes shown in the left-most column are used.

Table 1—Namespace prefixes, their corresponding XML namespaces, and specifications

Prefix	XML namespace	Specification(s)
mdpws	http://standards.ieee.org/downloads/11073/11073-20702-2016 [a]	This standard
dpws	http://docs.oasis-open.org/ws-dd/ns/dpws/2009/01	OASIS DPWS V1.1
s12	http://www.w3.org/2003/05/soap-envelope	W3C SOAP V1.2 Part 1
wsa	http://www.w3.org/2005/08/addressing	W3C WS-Addressing 1.0
wsam	http://www.w3.org/2007/05/addressing/metadata	W3C Web Services Addressing 1.0—Metadata
wsdl	http://schemas.xmlsoap.org/wsdl/	W3C WSDL 1.1
wsp	http://www.w3.org/ns/ws-policy	W3C WS-Policy 1.5 Framework
wssu	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd	OASIS WS-Security 2004
wsx	http://schemas.xmlsoap.org/ws/2004/09/mex	W3C WS-Metadata Exchange 1.1
xs	http://www.w3.org/2001/XMLSchema	W3C XML Schema 1.1

[a]The xml schema files necessary to ease the understanding of this standard are available at the following URL: http://standards.ieee.org/downloads/11073/11073-20702-2016/MDPWS.xsd.

4. General messaging

4.1 Introduction

All of the requirements in the following Web Services specifications are included by reference except where superseded by normative statements herein:

— WS-I Basic Profile V2.0, Section 3 (Messaging)

— OASIS DPWS V1.1 Section 2 (Messaging)

— OASIS SOAP-over-UDP V1.1

— IETF RFC 2616

4.2 SOAP-over-UDP

R0001: A SERVICE MAY send a SOAP ENVELOPE that has more octets than the MTU over UDP.

NOTE 1—dpws:R0029 defines a limit for SOAP ENVELOPEs sent over UDP. In order to allow larger SOAP-over-UDP STREAMING MESSAGEs, this standard relaxes this limitation.

R0002: A SERVICE MAY reject a SOAP ENVELOPE received over UDP that has more than MAX_UDP_ENVELOPE_SIZE octets if it is received via the discovery port. Otherwise, it SHOULD NOT be rejected.

R0003: A CLIENT MAY reject a SOAP ENVELOPE received over UDP that has more than MAX_UDP_ENVELOPE_SIZE octets if it is received via the discovery port. Otherwise, it SHOULD NOT be rejected.

NOTE 2—R0002 and R0003 reapply dpws:R5018 and dpws:R5019, but limit them to discovery related SOAP envelopes. This allows transmission of STREAMING MESSAGEs larger than MAX_UDP_ENVELOPE_SIZE.

4.3 SOAP-over-HTTP

R0004: A SERVICE SHALL at least implement the Responding SOAP Node of an HTTP one-way Message Exchange Pattern where the SOAP ENVELOPE is carried in the HTTP Request and the HTTP Response has a Status Code of 202 Accepted.

NOTE 1—dpws:R0030 requires an empty Entity Body (no SOAP ENVELOPE) in the response while bp20:R2714 allows a SOAP ENVELOPE for infrastructure-related faults and protocol extensions, thus R0004 relaxes the requirement to be more flexible.

R0005: A SERVICE MAY send a TEXT SOAP ENVELOPE with more than MAX_ENVELOPE_SIZE octets.

R0006: A SERVICE SHOULD NOT send a TEXT SOAP ENVELOPE with more than MAX_LARGE_ENVELOPE_SIZE octets.

NOTE 2—dpws:R0026 restricts the size of a TEXT SOAP ENVELOPE that should be sent by a SERVICE to MAX_ENVELOPE_SIZE octets. This limit is regularly violated by medical devices that provide a large number of metrics and therefore dpws:R0026 is relaxed and a new limit MAX_LARGE_ENVELOPE_SIZE is introduced.

R0007: A TEXT SOAP ENVELOPE SHALL be serialized using UTF-8 character encoding.

NOTE 3—In contrast to dpws:5002, bp20:R1012 requires support for UTF-16 character encoding. To reduce optionality in character encoding, R0007 excludes use of UTF-16 in any SOAP MESSAGE.

5. Dynamic discovery

All of the requirements in the following Web Services specifications are included by reference except where superseded by normative statements herein:

— OASIS DPWS V1.1 Section 3 (Discovery)

— OASIS SOAP-over-UDP V1.1

— OASIS WS-Discovery

R0008: If a DEVICE includes Types in a Hello, Probe Matches, or Resolve Matches SOAP ENVELOPE, it SHALL include the dpws:Device Type and mdpws:MedicalDevice Type.

NOTE 1—dpws:R1020 defines a default type for a DEVICE. For MDPWS an additional identifier is introduced.

R0024: DEVICEs SHALL NOT omit their Types and Scopes in an UDP WS-Discovery MESSAGE as long as the WS-Discovery MESSAGE size does not exceed the maximum size of an UDP MESSAGE. If the MESSAGE size exceeds the maximum size of an UDP MESSAGE, Types and Scopes MAY be omitted.

NOTE 2—DPWS advises a DEVICE to not omit Types and Scopes in a UDP WS-Discovery MESSAGE, R0024 transforms this note into a mandatory requirement as packet loss due to fragmentation is not a consideration.

6. Service description

6.1 General

All of the requirements in the following Web Services specifications are included by reference except where superseded by normative statements herein:

— WS-I Basic Profile V2.0, Section 4 (Service Description) and Section 5 (WSDL Corrections)

— OASIS DPWS V1.1 Section 4 (Description) and Appendix C (Declaring Discovery Types in WSDL)

6.2 Web Services Description Language (WSDL)

R0009: If a HOSTED SERVICE exposes Notifications that are not STREAMs, its portType SHALL include Notification and/or Solicit-Response Operations describing those Notifications.

NOTE 1—dpws:R2004 requires all services to describe notifications they provide in their portType as Notification and/or Solicit-Response Operation. This would also yield for STREAMs, which can be seen as notifications. R0009 relaxes dpws:R2004 such that STREAMs are explicitly excluded from being described as Notification and/or Solicit-Response Operation.

R0012: If a HOSTED SERVICE receives a MESSAGE that is inconsistent with its WSDL description, the HOSTED SERVICE SHOULD generate a SOAP Fault with a Code Value of "Sender," unless a "MustUnderstand" or "VersionMismatch" Fault is generated.

R0013: If a HOSTED SERVICE receives a MESSAGE that is inconsistent with its WSDL description, the HOSTED SERVICE SHALL check for "VersionMismatch," "MustUnderstand," and "Sender" fault conditions in that order.

NOTE 2—Statements R0012 and R0013 update bp20:R2724 and bp20:R2725 [BP 2.0, Section 4] with respect to SOAP 1.2 nomenclature (W3C SOAP V1.2 Part 1) similar to dpws:R2023 and dpws:R2024, where WS-Basic Profile 1.0 is referenced.

R0014: A SERVICE SHALL include the dpws:DiscoveryType attribute in its portType WSDL description.

NOTE 3—Even though the inclusion of the dpws:DiscoveryType is optional in DPWS, this standard makes it mandatory in order to allow optimized filtering of services based on their portType.

R0010: A SERVICE SHALL include the dpws:Profile ASSERTION in its policy even if it does not have any other policies. The wsp:Optional attribute SHALL be set to "true."

NOTE 4—As dpws:R2037 is ambiguous regarding the use of wsp:Optional, R0010 enforces usage of that attribute.

R0011: A SERVICE SHALL include the mdpws:Profile ASSERTION in its policy even if it does not have any other policies. The wsp:Optional attribute SHALL be set to "true."

To indicate that a SERVICE is compliant with the Web Services profile described by this standard, the following ASSERTION is defined:

```
(01)   <mdpws:Profile wsp:Optional="true" ... />
```

The remainder of this subclause describes additional, normative constraints on the outline listed above.

`/mdpws:Profile`
Indicates that compliance with this standard is required. This ASSERTION has [Endpoint Policy Subject] (W3C WS-Policy 1.5 Attachment). A WS-Policy expression containing the mdpws:Profile ASSERTION MAY be attached to a wsdl:port, SHOULD be attached to a wsdl:binding, but SHALL NOT be attached to a wsdl:portType; the latter is prohibited because the ASSERTION specifies a concrete behavior whereas the wsdl:portType is an abstract construct.

`/mdpws:Profile/@wsp:Optional="true"`
Per WS-Policy (W3C WS-Policy 1.5 Framework), this is compact notation for two policy alternatives, one with and one without the ASSERTION. The intuition is that the behavior indicated by the ASSERTION is optional, or in this case, that the SERVICE supports but does not require compliance with this standard.

7. Eventing

All of the requirements in the following Web Services specifications are included by reference except where superseded by normative statements herein:

— (OASIS DPWS V1.1) Section 5 (Eventing)

In this standard no additional normative statements are defined.

NOTE—Requirements of Section 5 of (OASIS DPWS V1.1) are only applicable if a DEVICE or CLIENT sends events in order to exchange information. A comprehensive set of exchanged MESSAGEs is given in W3C WS-Eventing.

8. Streaming

8.1 General

The scope of this clause is the definition of an announcement protocol to enable STREAMING. Data is transmitted either in SOAP MESSAGEs or in another format. The intent is to allow flexibility in terms of STREAM management and negotiation protocols (RTSP, SOAP-over-UDP STREAMING …) or transport bindings of the STREAM (RTP, SOAP-over-UDP Multicast …). A detailed scope definition of the streaming specification is given in Annex B.

There is no reference to requirements of an external specification.

8.2 Advertising stream information

8.2.1 General

A STREAM source provider MAY indicate its support of this part of this standard, or its features, by including the StreamSource ASSERTION within its WSDL. This ASSERTION has [Endpoint Policy Subject]. By doing so the STREAM source provider is indicating that information about at least one STREAM, according to policies defined in this standard, is provided.

8.2.2 StreamSource Assertion

This standard defines an ASSERTION (mdpws:StreamSource) to indicate a source for STREAMING. The normative outline of this ASSERTION is:

```
(01)   <mdpws:StreamSource ...>
(02)     xs:any*
(03)   </mdpws:StreamSource>
```

The remainder of this subclause describes additional, normative constraints on the outline listed above.

`/mdpws:StreamSource`
ELEMENT describes an ASSERTION that has [Endpoint Policy Subject]. When present in a policy alternative, it indicates that the subject is a STREAM source provider.

`/mdpws:StreamSource/xs:any`
ELEMENT is an extensibility point that allows for additional specific metadata to be included within the ASSERTION. Any metadata that appears is scoped to the operations and features of the WS-Streaming specification. If the StreamSource provides StreamDescriptions, then a StreamDescriptions element SHALL appear as a child of the StreamSource element.

8.3 Stream types and stream descriptions

8.3.1 General

This subclause describes the “Stream Type” concept for the description and advertisement of STREAM information. A Stream Type MAY contain a description of the syntactic structure and value space of the set of STREAMs that share that type.

Stream Types are described within a StreamDescriptions element where they may contain a complete description of a STREAM. A key aspect of this description is the associated XML Schema Global Element Declaration (GED) for a STREAM. The StreamDescriptions element has the following form:

```
(01)   <mdpws:StreamDescriptions TargetNamespace="xs:anyURI" ...>
(02)     <mdpws:Types>
(03)       <xs:Schema ...>
(04)         ...
(05)       </xs:Schema>
(06)       xs:any*
(07)     </mdpws:Types> ?
(08)     <mdpws:StreamType Id="xs:ID"
(09)         StreamType="xs:anyURI"
(10)         Element="xs:QName"? ActionUri="xs:anyURI"? ...>
(11)       <mdpws:StreamTransmission ...>
(12)         xs:any*
(13)       </mdpws:StreamTransmission> ?
(14)       xs:any*
(15)     </mdpws:StreamType> +
(16)     xs:any*
(17)   </mdpws:StreamDescriptions>
```

The remainder of this subclause describes additional, normative constraints on the outline listed above.

`/mdpws:StreamDescriptions`
ELEMENT contains the declarations of all the Stream Types that apply to a given context.

`/mdpws:StreamDescriptions@TargetNamespace`
ATTRIBUTE defines the namespace affiliation of the Stream Types declared within the StreamDescriptions. Its value SHALL be an absolute IRI (IETF RFC 3987). It SHOULD be dereferenceable.[7]

`/mdpws:StreamDescriptions/mdpws:Types`
ELEMENT encloses data type definitions that are relevant to the declared Stream Types.

`/mdpws:StreamDescriptions/mdpws:Types/xs:schema`
ELEMENT contains collections of imported and inlined schema components that describe the GEDs that are used to define Stream Types (as mentioned earlier).

`/mdpws:StreamDescriptions/mdpws:StreamType`
ELEMENT describes a specific Stream Type.

`/mdpws:StreamDescriptions/mdpws:StreamType/@Id`
ATTRIBUTE provides an identifier for this Stream Type, which SHALL be unique among all the Stream Types defined by the enclosing mdpws:StreamDescriptions element. In conjunction with a prefix that is associated with the value of /mdpws:StreamDescriptions/@TargetNamespace namespace IRI, the value of ATTRIBUTE MAY be used as the LocalPart of a QName that identifies this Stream Type outside the context of the enclosing mdpws:StreamDescriptions element.

`/mdpws:StreamDescriptions/mdpws:StreamType/@StreamType`
ATTRIBUTE indicates that the STREAM follows the specifications of the provided type. This value should be compared directly, as a case-sensitive string, with no attempt to unescape or to otherwise canonicalize it.

`/mdpws:StreamDescriptions/mdpws:StreamType/@Element`
ATTRIBUTE refers to a GED defined or imported in the /mdpws:StreamDescriptions/mdpws:Types element. The referenced GED serves as the definition of the payload that is transmitted using the underlying Stream Type.

[7]Dereferencing is a process of looking up an IRI in order to get information about the referenced resource, e.g., requesting a resource using HTTP with an URI identifying the resource.

/mdpws:StreamDescriptions/mdpws:StreamType/@ActionUri
ATTRIBUTE provides a value for the "action'" property used to transmit the STREAM and serves as a potential aid to identify the semantics implied by the MESSAGE. When not present the implied value of ATTRIBUTE is the concatenation of the /mdpws:StreamDescriptions/@TargetNamespace attribute and the /mdpws:StreamDescriptions/mdpws:StreamType/@Id attribute separated by the "/" character.

/mdpws:StreamDescriptions/mdpws:StreamType/mdpws:StreamTransmission
ELEMENT describes a specific mechanism for the transmission of the STREAM. If omitted it is implied that necessary information for receiving a STREAM is handled by other means, e.g., during a subscription process.

8.3.2 StreamTransmission element

This element indicates the mechanisms that are utilized to transmit a STREAM.

```
(18)   <mdpws:StreamTransmission Type="xs:anyURI"? ...>
(19)     <mdpws:StreamAddress>xs:anyURI</mdpws:StreamAddress> ?
(20)     <mdpws:StreamPeriod>xs:duration</mdpws:StreamPeriod> ?
(21)     xs:any*
(22)   </mdpws:StreamTransmission> ?
```

The remainder of this subclause describes additional, normative constraints on the outline listed above.

/mdpws:StreamTransmission
ELEMENT describes a specific mechanism for the transmission of a STREAM.

/mdpws:StreamTransmission@Type
ATTRIBUTE references the mechanism for STREAM transmission. If omitted the value /mdpws: StreamDescriptions/mdpws:StreamType@StreamType is implied.

/mdpws:StreamTransmission/mdpws:StreamAddress
ELEMENT specifies the address for STREAM transmission. In case it contains a multicast address this address needs to be joined for receiving the multicast STREAM.

/mdpws:StreamTransmission/mdpws:StreamPeriod
ELEMENT contains the duration with a fractional second between two MESSAGEs of the STREAM (e.g., if the STREAM source provider publishes data with 50 Hz, it is designated as PT0.02S, conforming to XML schema duration type).

8.4 Retrieving stream descriptions

8.4.1 General

Although there are many ways in which an endpoint can make its StreamDescriptions available, this standard RECOMMENDS the use of the mechanisms described in Section 9 of W3C WS-Metadata Exchange 1.1. In particular, this standard RECOMMENDS that the StreamDescriptions metadata is made available through the StreamSource ASSERTION. This SHOULD be done by either inserting the StreamDescriptions metadata directly within the ASSERTION, or by including a MetadataExchange reference to the data.

If StreamDescriptions is inserted as a MetadataExchange reference, the MetadataSection element's Dialect attribute SHALL be set to the following URI:

http://standards.ieee.org/downloads/11073/11073-20702-2016

R0025: A STREAM source SHALL NOT have more than one StreamDescriptions document.

8.4.2 Embedded in Policy Assertion

The StreamDescriptions metadata MAY be inserted directly into the StreamSource ASSERTION.

An informative example can be found in C.2.

8.4.3 MetadataExchange Reference

A StreamDescriptions MAY be inserted within a WS-MetadataExchange (W3C WS Metadata Exchange 1.1) MetadataSection.

R0026: If a StreamDescriptions is transmitted in a WS-MetadataExchange MetadataSection, the value of the @Identifier attribute, if present, SHALL be equal to the value of its mdpws:StreamDescriptions/@TargetNamespace.

An informative example can be found in C.3.

8.5 SOAP-over-UDP Multicast Stream Binding

8.5.1 General

In this subclause a concrete STREAM type is specified. The URI for this STREAM type is:

```
mdpws:Mechanism/soap-over-udp
```

8.5.2 Binding

The information about a Stream Type contained in the mdpws:StreamType element binds to STREAM MESSAGE for that type as follows:

— The [Action] property of the MESSAGE has the value of the @ActionUri attribute of the mdpws:StreamType element corresponding to the type of the STREAM being transmitted.

— The [Body] property of the MESSAGE has a single child element. This child element is an instance of the Global Element Declaration referenced by the @Element attribute of the mdpws:StreamType element corresponding to the type of the STREAM being transmitted. If the @Element attribute is absent then the [Body] property has no children.

8.5.3 Addressing

The URI scheme of the address SHALL be soap.udp (e.g., soap.udp://239.12.23.23:12345).

8.5.4 Message sequencing

MESSAGEs within a multicast STREAM should have an application sequence number to allow a receiver to order MESSAGEs and detect packet loss.

This standard RECOMMENDS using the AppSequence SOAP Header from OASIS WS-Discovery (Section 7) to establish MESSAGE sequence numbering.

R0027: If the AppSequence header from OASIS WS-Discovery is used to establish MESSAGE sequence numbering, the SequenceId attribute SHOULD be set to the wsa:action URI of the transmitted MESSAGE and the MessageNumber attribute SHALL be incremented by 1.

Since the InstanceId attribute of the AppSequence element has HOSTED SERVICE scope, STREAM sinks cannot distinguish between different STREAM sources reliably. Thus it is RECOMMENDED to add the wsa:From header block with the service's current transport address.

9. Safe data transmission

9.1 General

The scope of this clause is the definition of a protocol for safe, single-fault safe remote control of networked medical devices based on the exchange of SOAP MESSAGEs over one physical, IP-based transmission medium, where possible concurrent conflicting remote control commands are issued to one medical device.

There is no reference to requirements of an external specification.

9.2 Advertising safety requirements

9.2.1 General

To enable a CLIENT to communicate with a DEVICE that has requirements regarding remote control-related MESSAGE exchange, the CLIENT has to be able to retrieve the DEVICE's requirements. This subclause defines an ASSERTION that allows a DEVICE to announce its safety-related requirements for a remote control–related MESSAGE exchange during binding of the discovery of the DEVICE. Safety requirements comprise transmission of dual channel and safety context information.

NOTE 1—A typical challenge that arises during remote control of medical devices is to establish single-fault safety, which is a requirement from the IEC 60601-1. IEC 60601-1 defines single-fault safe as a "characteristic of medical equipment or its parts whereby it remains free of unacceptable risk during its expected service life under single fault condition." To ensure single-fault safety, a medical device might utilize a dual-channel architecture, i.e., data is somehow processed by means of a redundant information channel. Detailed information regarding dual channel establishment in distributed systems of medical devices is presented by Pöhlsen, Schöch, and Schlichting [B10].[8]

NOTE 2—It is impossible for two networked devices to synchronize their shared data such that they will never work on outdated information. Therefore, in a remote control scenario, a device might request information on the assumptions a client made to invoke a remote control command on that device. In the following, such information is called safety context information. For example, a client application likes to adjust the drug dose of an infusion pump to a certain value. For that purpose the infusion pump provides the current configured dose to let the client decide the level of adjustment. Since that data could be outdated when the client submits a set request MESSAGE to the device, the device requires the client to also deliver the "old" drug dose value on which it decides the adjustment. Besides the new value the old value is inserted as a safety context within the MESSAGE.

9.2.2 Assertion

9.2.2.1 General

This subclause defines a safety requirement ASSERTION that MAY be used to specify that transmission of safety information is expected during MESSAGE transmission.

In addition to the element outlines below the following normative statement applies.

R0028: A SERVICE SHALL embed a SafetyReqAssertion either at a [Message Policy Subject] or [Operation Policy Subject] or [Endpoint Policy Subject] policy attachment point, if it requires safety information to be transmitted from a CLIENT for a MESSAGE exchange.

An informative example can be found in C.6.

[8]The numbers in brackets correspond to those of the bibliography in Annex E.

9.2.2.2 SafetyReqAssertion

To indicate that safety information is REQUIRED when a MESSAGE is transmitted from a CLIENT to a SERVICE of a DEVICE, this subclause defines the SafetyReqAssertion ASSERTION.

```
(01)   <mdpws:SafetyReqAssertion
(02)     TransmitDualChannel="xs:boolean"
(03)     TransmitSafetyContext="xs:boolean" ...>
(04)     ...
(05)   </mdpws:SafetyReqAssertion>
```

The remainder of this subclause describes additional, normative constraints on the outline listed above.

`/mdpws:SafetyReqAssertion`
ELEMENT is an ASSERTION that has [Message Policy Subject] or [Operation Policy Subject] or [Endpoint Policy Subject]. When present in a policy alternative, it indicates that for the subject additional safety information needs to be transmitted for the specified MESSAGE elements.

`/mdpws:SafetyReqAssertion/@TransmitDualChannel`
ATTRIBUTE that indicates that dual-channel transmission is required for the specified MESSAGE elements. Default value is “true.”

`/mdpws:SafetyReqAssertion/@TransmitSafetyContext`
ATTRIBUTE that indicates that specified safety context information is required to be transmitted for the subject. Default value is “true.”

9.2.3 XML elements

9.2.3.1 General

To designate which safety information is required by a transmitted MESSAGE, this subclause defines corresponding building blocks.

An informative example can be found in C.4.

9.2.3.2 SafetyReq

To announce a safety requirement for transmission, the SafetyReq element SHALL be used.

```
(01)   <mdpws:SafetyReq ...>
(02)     <mdpws:DualChannelDef ...>
(03)       ...
(04)     </mdpws:DualChannelDef> ?
(05)     <mdpws:SafetyContextDef ...>
(06)       ...
(07)     </mdpws:SafetyContextDef> ?
(08)     ...
(09)   </mdpws:SafetyReq>
```

The remainder of this subclause describes additional, normative constraints on the outline listed above.

`/mdpws:SafetyReq`
ELEMENT is an XML container to include safety requirement information.

`/mdpws:SafetyReq/mdpws:DualChannelDef`
ELEMENT defines a requirement for transmitting a second channel for at least one specified MESSAGE element.

`/mdpws:SafetyReq/mdpws:SafetyContextDef`
ELEMENT defines a requirement for transmitting a safety-relevant contextual information for at least one safety context information for the MESSAGE transmission.

9.2.3.3 DualChannelDef

This standard introduces the DualChannelDef element to define a requirement for establishment of second channel within a MESSAGE.

```
(01)   <mdpws:DualChannelDef
(02)     Transform="xs:QName"
(03)     Algorithm="xs:QName"
(04)     ...>
(05)     <mdpws:Selector ...>
(06)       ...
(07)     </mdpws:Selector> +
(08)     ...
(09)   </mdpws:DualChannelDef>
```

The remainder of this subclause describes additional, normative constraints on the outline listed above.

`/mdpws:DualChannelDef`
ELEMENT defines a requirement for transmitting a second channel for at least one specified MESSAGE element.

`/mdpws:DualChannelDef/@Transform`
A transformation mechanism transforms raw input data to a canonical representation that is compliant with XML and unambiguous w.r.t. to hash generation. ATTRIBUTE is a qualified name that designates a transformation mechanism that SHALL be applied on the data before a second channel representation algorithm is applied. Default is /mdpws:xml-exc-c14n.

`/mdpws:DualChannelDef/@Algorithm`
ATTRIBUTE defines a qualified name of an algorithm that SHALL be applied on the transformed data in order to compute the value of the second channel representation. Default is /mdpws:HexSHA1.

`/mdpws:DualChannelDef/mdpws:Selector`
ELEMENT specifies an expression (in the following called selector) to select an attribute of an element or element text inside of a MESSAGE for which a second channel SHALL be established using the provided transformation and algorithm. The XML root that is specified by the selector is the s12:Body element of the MESSAGE that transports dual-channel information.

NOTE—Since dual-channel information is considered as a safety value and not as a security-related signature, it is sufficient to use the more collision-prone SHA-1 hash algorithm instead of the SHA-2 or SHA-3 hash algorithm. This offers a reasonable trade-off between computational complexity/hash length and collision probability.

9.2.3.4 SafetyContextDef

This standard introduces the SafetyContextDef element to define a requirement for transmission of safety context information within a MESSAGE.

```
(01)   <mdpws:SafetyContextDef ...>
(02)     <mdpws:Selector ...>
(03)       ...
(04)     </mdpws:Selector> +
(05)     ...
(06)   </mdpws:SafetyContextDef>
```

The remainder of this subclause describes additional, normative constraints on the outline listed above.

`/mdpws:SafetyContextDef`
ELEMENT defines a requirement for transmitting at least one safety context.

`/mdpws:SafetyContextDef/mdpws:Selector`
ELEMENT specifies a selector to an attribute of an element or element text of an underlying XML structure that has to be embedded into the transmitted MESSAGE. The underlying XML structure is designated by other means not defined in this standard.

9.2.3.5 Selector

A selector is an element used to select an attribute of an element or element text by defining a limited XPath expression.

```
(01)   <mdpws:Selector Id='xs:string' ...>
(02)     ...
(03)   </mdpws:Selector>
```

The remainder of this subclause describes additional, normative constraints on the outline listed above.

`/mdpws:Selector`
ELEMENT specifies an XPath expression {Path} that points to an attribute of an element or element text.

The following rules SHALL be applied on {Path}:

— {Path} is a valid XPath expression, as defined in XPath (W3C XPath V1.0).

— {Path} conforms to the following Extended Backus-Naur Form:

```
Path        ::=  ( '/' Step )* '/' ( '@' Name | 'text()' )
Step        ::=  Name ('[' Expr ']')*
Expr        ::=  '@' Name '=' ( Number | Literal | ConcatCall) | Digits
Name        ::=  QName | NCName
Literal     ::=  '"' [^"]* '"' | "'" [^']* "'"
ConcatCall  ::=  concat '(' ( Literal ( ',' Literal )+ ')'
Number      ::=  Digits ( '.' Digits? )?
Digits      ::=  [0-9]+
```

where

— QName is defined in W3C Namespaces in XML 1.0.

— NCName is defined in W3C Namespaces in XML 1.0.

NOTE—XPath expressions that can be built by the aforementioned rules are any absolute paths to xml element texts and attributes. Simple predicates, i.e., attribute or element index matches, can be assigned to the nodes within the paths.

Examples:

— /ns:Foo[@FooAttr='sample']/Bar[21]/text()

— /Foo[@FooAttr="sample"]/ns:Bar/@BarAttr

`/mdpws:Selector/@Id`
ATTRIBUTE designates a unique identifier over all mdpws:Selector elements. The uniqueness scope is determined by other means not defined in this standard. The identifier can be used to address the XPath expression a selector defines.

9.3 Retrieving safety requirements

SafetyReq MAY be made available through the SafetyReqAssertion ASSERTION by either embedding SafetyReq directly within the ASSERTION, or by including a MetadataExchange reference to it. The provision of SafetyReq MAY be also facilitated by other means not defined in this standard.

R0029: A DEVICE SHOULD indicate its feature support of Clause 9 of this standard by including the SafetyReqAssertion within its WSDL.

9.4 Transmitting safety information

9.4.1 General

To enable a CLIENT to transmit safety-related information for which a DEVICE has provided a requirement, this subclause defines the elements to be used for embedding the information into the transmitted MESSAGE.

In addition to the element definitions in 9.4.2 the following normative statements apply.

R0030: A DEVICE SHALL reply with a SOAP Fault, if required SafetyInformation is missing in a MESSAGE or has been corrupted during transport of the MESSAGE.

R0031: A CLIENT SHALL embed safety information into a MESSAGE, if a DEVICE has provided a safety requirement.

An informative example can be found in C.5.

9.4.2 XML elements

9.4.2.1 General

This subclause defines the safety information XML elements that are inserted into a MESSAGE.

9.4.2.2 SafetyInfo

To insert safety information in a MESSAGE header, this standard defines the SafetyInfo container element.

```
(01)   <mdpws:SafetyInfo ...>
(02)     <mdpws:DualChannel ...>
(03)       ...
(04)     </mdpws:DualChannel> ?
(05)     <mdpws:SafetyContext ...>
(06)       ...
(07)     </mdpws:SafetyContext> ?
(08)     ...
(09)   </mdpws:SafetyInfo>
```

The remainder of this subclause describes additional, normative constraints on the outline listed above.

`/mdpws:SafetyInfo`
ELEMENT is an XML container for embedding safety information in a SOAP MESSAGE header.

`/mdpws:SafetyInfo/mdpws:DualChannel`
ELEMENT is used to embed dual-channel information in a SOAP MESSAGE header.

`/mdpws:SafetyInfo/mdpws:SafetyContext`
ELEMENT that provides safety context information related to a required safety context definition.

9.4.2.3 DualChannel

To embed information of a second channel into a MESSAGE header, this standard defines the DualChannel element.

```
(01)   <mdpws:DualChannel ...>
(02)     <mdpws:DcValue ...>
(03)       ...
(04)     </mdpws:DcValue> +
(05)     ...
(06)   </mdpws:DualChannel>
```

The remainder of this subclause describes additional, normative constraints on the outline listed above.

`/mdpws:DualChannel`
ELEMENT that is used to embed dual-channel information in a MESSAGE header.

`/mdpws:DualChannel/mdpws:DcValue`
ELEMENT that contains the actual value of the second channel as well as information about how the value has been determined.

9.4.2.4 DcValue

To represent the actual value of a second channel as well as how the value has been determined by the CLIENT, this standard defines the DcValue element.

```
(01)   <mdpws:DcValue ReferencedSelector='xs:string' ...>
(02)     xs:string
(03)   </mdpws:DcValue>
```

The remainder of this subclause describes additional, normative constraints on the outline listed above.

`/mdpws:DcValue`
ELEMENT is a dual-channel value that contains the representation of the second channel. The particular algorithm and transformation to encode the second channel is designated by the DualChannelDef element.

`/mdpws:DcValue/@ReferencedSelector`
ATTRIBUTE references a selector identifier to designate the target that the underlying second channel value refers to.

9.4.2.5 SafetyContext

To embed contextual information for a MESSAGE into a MESSAGE header, this standard defines the SafetyContext element.

```
(01)   <mdpws:SafetyContext ...>
(02)     <mdpws:CtxtValue ...>
(03)       ...
(04)     </mdpws:CtxtValue> +
(05)     ...
(06)   </mdpws:SafetyContext>
```

The remainder of this subclause describes additional, normative constraints on the outline listed above.

`/mdpws:SafetyContext`
ELEMENT that is used to embed Safety context information in a MESSAGE header.

`/mdpws:SafetyContext/mdpws:CtxtValue`
ELEMENT that contains safety context values.

9.4.2.6 CtxtValue

To represent a safety-relevant contextual information item, this standard defines the CtxtValue element.

```
(01)   <mdpws:CtxtValue ReferencedSelector='xs:string' ...>
(02)     xs:anySimpleType
(03)   </mdpws:CtxtValue>
```

The remainder of this subclause describes additional, normative constraints on the outline listed above.

`/mdpws:CtxtValue`
ELEMENT provides the contextual information.

`/mdpws:CtxtValue/@ReferencedSelector`
ATTRIBUTE references a selector identifier to designate the target that the underlying contextual information refers to.

9.4.3 Binding safety information to SOAP 1.2 Message

In the event that a MESSAGE needs to transport a safety information representation, the XML Infoset representation of each safety information representation is inserted into the MESSAGE as a SOAP Header block subject to the following additional constraint:

— Each optional element or attribute that has a value equal to the defined default value for that element or attribute MAY be omitted.

R0032: Elements with safety information representation SHALL be added to the SOAP Header.

9.5 Qualified Names

9.5.1 Representation generation algorithms

R0034: A DEVICE MAY use other QNames than the QName defined in Table 2 for referencing representation generation algorithms that are not defined in this standard.

Table 2 defines QNames for referencing algorithms that are used in the generation of the second channel representation.

Table 2—Qualified Name of representation generation algorithms

QName	Definition
mdpws:HexSHA1	QName for an algorithm that is used to determine the hex-encoded SHA-1 digest of the XML Infoset representation of an attribute or element. The hex string SHALL be treated as case-insensitive, i.e., “bd3e01” equals “BD3E01”.

R0035: A CLIENT SHALL support the mdpws:HexSHA1.

R0036: A DEVICE SHOULD support mdpws:HexSHA1 if safety-related transmission with a second channel is required.

NOTE—If mdpws:HexSHA1 is not supported by a DEVICE, there is no guarantee that a client is able to constitute dual-channel information that is appropriate for that DEVICE.

Example

— mdpws:HexSHA1(“any-value”) = bd3e01717d5ac1448288a6ace82b1e3c509f00a9

9.5.2 Transformation algorithms

R0037: A DEVICE MAY use QNames other than the QNames defined in Table 3 for referencing transformation algorithms that are not defined in this standard.

Table 3 defines QNames for referencing algorithms that are used for transforming the content of selected element or attribute before the representation generation algorithm is applied.

Table 3—Qualified Names of transformation algorithms

QName	Definition
mdpws:xml-exc-c14n	QName of a transformation on an XML Infoset representation of an attribute or element in which exclusive XML canonicalization (W3C Exclusive XML Canonicalization V1.0) on the canonical lexical representation (W3C XML Schema 1.1) is applied.
mdpws:noTransformation	QName of a transformation on an XML Infoset representation of an attribute or element in which the transformation that is applied does not change the representation.

CAUTION

The content of the attribute or element SHALL every time be transformed to “Canonical Lexical Representation” of the XML schema data types (W3C XML Schema 1.1).

R0038: A CLIENT SHALL support the mdpws:xml-exc-c14n and the mdpws:noTransformation algorithm.

R0039: A DEVICE SHOULD support mdpws:xml-exc-c14n if safety-related transmission with a second channel is required.

NOTE—If mdpws:xml-exc-c14n and mdpws:noTransformation are not supported by a DEVICE, there is no guarantee that a client is able to constitute dual-channel information that is appropriate for that DEVICE.

10. Security considerations

The scope of this clause is the following set of Web Services specifications. All of the requirements in these specifications are included by reference except where superseded by normative statements herein:

— WS-I Basic Profile V2.0, Section 7 (Security)

— OASIS DPWS V1.1, Section 6 (Security)

— OASIS WS-Discovery, Section 8 (Security)

NOTE 1—The requirements of Sections 6.5, 6.7, and 6.8 of OASIS DPWS V1.1 and Section 8 of OASIS WS-Discovery are applicable only if a DEVICE or CLIENT need these mechanisms in order to exchange information securely.

R0015: A DEVICE SHOULD support receiving and responding to a Probe SOAP ENVELOPE over HTTP using a SECURE CHANNEL.

NOTE 2—Because there might be devices that do not require secure communication, dpws:R4072 is replaced by this requirement in order to allow devices to not support a SECURE CHANNEL.

NOTE 3—dpws:R4039 requires a CLIENT to initiate authentication by setting up a TLS/SSL session, but it does not define the authorization.

R0016: A DEVICE SHALL NOT use HTTP Authentication to request CLIENT credentials.

NOTE 4—The reason to not allow HTTP Authentication is that DPWS allows two methods of authentication. Section 6.6.3.2 allows for CLIENT authentication with HTTP Authentication whereas section 6.6.3.1 allows for CLIENT authentication with x.509.v3 certificates. The latter one is more appropriate for medical device communication since it is able to establish a trust chain and provide authorization information.

R0017: A SENDER SHALL authenticate itself to a RECEIVER using credentials acceptable to the RECEIVER. Acceptable credentials are those credentials that have been requested by the RECEIVER.

NOTE 5—R0017 replaces dpws:R4004 for clarification purposes.

R0018: A SERVICE SHALL not send a SOAP ENVELOPE without protecting the integrity of any Message Information Header blocks matching the following XPath expressions:

(a) /soap:Envelope/soap:Header/wsa:Action,

(b) /soap:Envelope/soap:Header/wsa:MessageID,

(c) /soap:Envelope/soap:Header/wsa:To,

(d) /soap:Envelope/soap:Header/wsa:ReplyTo,

(e) /soap:Envelope/soap:Header/wsa:RelatesTo, /soap:Envelope/soap:Header/wsa:faultTo and

(f) /soap:Envelope/soap:Header/*[@isReferenceParameter='true'].

NOTE 6—R0018 replaces dpws:R4000 due to the fact that /soap:Envelope/soap:Header/wsa:FaultTo was missing.

11. Message serialization

11.1 General

All of the requirements in the following Web Services specifications are included by reference except where superseded by normative statements herein:

— W3C EXI Format 1.0

— WS-I Basic Profile V2.0, Section 3.1 (Message Serialization)

— WS-I Basic Profile V2.0, Section 4.6 (Bindings)

R0019: If a SERVICE needs to use compact representation for the Extensible Markup Language (XML) Information Set, then the Efficient XML Interchange Format (W3C EXI Format 1.0) SHALL be used.

NOTE—Sections 3.1 and 4.6 of WS-I Basic Profile V2.0 explicitly allow the usage of alternative MESSAGE serializations, which have to announced in the wsdl:binding element by a WSDL extensibility element.

R0020: If a DEVICE supports EXI, then it SHALL support schema-less EXI streams with the default Options (W3C EXI Format 1.0).

R0021: If a CLIENT supports EXI, then it SHALL support schema-less EXI streams with the default Options (W3C EXI Format 1.0).

R0022: If a DEVICE supports EXI, then it SHOULD support schema-informed EXI streams with compressed option set to true and default values for the other Options (W3C EXI Format 1.0).

R0023: If a CLIENT supports EXI, then it SHOULD support schema-informed EXI streams with compressed option set to true and default values for the other Options (W3C EXI Format 1.0).

11.2 Advertising compact transmission

11.2.1 General

R0040: A DEVICE SHALL advertise the utilization of a compact XML Infoset representation for a MESSAGE exchange by using the mdpws:Compression ASSERTION.

NOTE 1—As defined in R0007, an UTF-8 XML Infoset representation for a MESSAGE is always provided.

R0041: A CLIENT MAY indicate acceptance of a compact XML Infoset representation by including the Accept-Encoding header field into the HTTP-Header of a request MESSAGE where the list of encodings contains the value "x-exi".

NOTE 2—x-exi is proposed as the name for the content encoding in HTTP in W3C EXI Best Practices [B12].

R0042: A DEVICE SHALL include the Content-Encoding HTTP-field in a SOAP-over-HTTP MESSAGE with a value of "x-exi", if the XML Infoset is encoded using EXI.

R0043: If a CLIENT includes an Accept-Encoding header field in an HTTP-Header that contains the value "x-exi" in a WS-Eventing (W3C WS-Eventing) Subscription request, then the Event Source MAY transmit events related to that subscription in the compact XML Infoset representation.

11.2.2 Compression assertion

Services indicate requirements for a compact transmission as defined in this standard through the use of the Web Services Policy—Framework (W3C WS-Policy 1.5 Framework) and Web Services Policy—Attachment (W3C WS-Policy 1.5 Attachment) specifications.

This standard defines an ASSERTION (mdpws:Compression) to indicate compression requirements. The normative outline of this ASSERTION is:

```
(01)   <mdpws:Compression method="xs:Qname"?
(02)     compression="xs:Qname"?>
(03)     xs:any*
(04)   </mdpws:Compression>
```

The remainder of this subclause describes additional, normative constraints on the outline listed above.

`/mdpws:Compression`
This ASSERTION has [Message Policy Subject] or [Operation Policy Subject] or [Endpoint Policy Subject]. When present in a policy alternative, it indicates that for the subject compact transmission representation is required for the specified MESSAGEs.

`/mdpws:Compression/@method`
Specifies the method used to encode/decode MESSAGEs to/from the compact transmission representation. This standard defines the following set of values for method:

- mdpws:EXI-sl: The W3C EXI Format 1.0 schema-less algorithm SHALL be applied. This is the default value.
- mdpws:EXI-mdpws: The W3C EXI Format 1.0 schema-informed algorithm SHALL be applied.

`/mdpws:Compression/@compression`
Specifies if a compression is applied to output according to Chapter 9 in W3C EXI Format 1.0. This standard defines the following set of values for method:

- mdpws:EXI-nocmpr: No W3C EXI Format 1.0 compression SHALL be applied. This is the default value.
- mdpws:EXI-cmpr: W3C EXI Format 1.0 compression SHALL be applied.

`/mdpws:Compression/xs:any`
This is an extensibility mechanism that further describes the compact representation requirement.

12. Conformance

12.1 General

A conformant implementation SHALL satisfy all the SHALL and REQUIRED-level requirements defined in this standard.

To support interoperability of applications and systems, an implementation based on this standard SHALL provide specific details about the way that the definitions of this standard are applied. These details have to be provided in the form of a set of implementation conformance statements (ICSs). An ICS is a form of data sheet that discloses details of a specific implementation and specifies which features are provided.

NOTE—The ICSs defined in 12.3 provide understanding of the details of an implementation. However, they are not sufficient to guarantee interoperability of applications or systems. For such interoperability, additional specifications have to be taken into account. These specifications are out of scope of this standard.

12.2 General format

The ICSs have to be supplied in the form of tables. Templates for these ICS tables are given in Table 4 through Table 8. The tables have to be filled out and provided as an overall conformance statement document.

Generally the column headers of an ICS table contain the following information:

— Index, which is an identifier of a specific feature.

— Feature, which briefly describes the characteristic for which a conformance statement SHALL be made.

— Reference, which is a reference to the requirement of the feature (may be empty).

— Status, which specifies the conformance requirement (i.e., the requirements for a conforming implementation regarding the feature). In some cases, this standard does not specify conformance requirements, but still wants a definition of the status of a particular feature.

— Support, which is filled out by the implementer and specifies the characteristics of the feature in the implementation.

— Comment, which contains additional information provided by the implementer.

The value of the Status and Support columns are permitted to range from simple to complex entries. Examples of simple values are as follows:

— **m** mandatory

— **o** optional

— **x** prohibited

— **c** conditional

— **n/a** not applicable

12.3 ICS tables

Table 4—General ICSs

Index	Feature	Reference	Status	Support	Comment
GEN-1	SOAP-over-UDP messaging	R0002		o	Pertains to streaming conformance statements only.
GEN-2	SOAP-over-UDP messaging	R0003		o	Pertains to streaming conformance statements only.
GEN-3	SOAP-over-HTTP messaging	R0006		c	If not implemented, communication partners might not be able to accept MESSAGES.
GEN-4	Service Description	R0012		m	Making this requirement mandatory increases interoperability and allows clients to process fault rationales.

Table 5—Streaming ICSs

Index	Feature	Reference	Status	Support	Comment
STRM-1	SOAP-over-UDP messaging	R0002		m	If not implemented, STREAMING MESSAGEs might not be transmitted.
STRM-2	SOAP-over-UDP messaging	R0003		m	If not implemented, STREAMING MESSAGEs might not be received.
STRM-3	Message sequencing	R0027		o	It is sufficient to follow the requirements led by WS-Discovery. Using another SequenceId value than wsa:action URI does not affect interoperability.
STRM-4	Ability of dereferencing target namespace	8.3		o	

Table 6—Safe data transmission ICSs

Index	Feature	Reference	Status	Support	Comment
SAFE-1	Safety Requirements Advertising	R0029		m	Required to express support of dual channels or safety contexts.
SAFE-2	Representation Generation Algorithms	R0036	Are all clients required to be interoperable with the dual-channel implementation a device provides?	c	Implement Hex-SHA-1 encoding on device side to let all clients be able to conceive appropriate dual-channel information.
SAFE-3	Transformation Algorithms	R0039	Are all clients required to be interoperable with the dual-channel implementation a device provides?	c	Implement exclusive XML canonicalization encoding on device side to let all clients be able to conceive appropriate dual-channel information.

Table 7—Compact Representation ICSs

CP-1	EXI	R0022		m	Mandatory if compact representation of MESSAGEs is used.
CP-2	EXI	R0023		m	Mandatory if compact representation of MESSAGEs is used.

Table 8—Security ICSs

Index	Feature	Reference	Status	Support	Comment
SEC-1	Security of Probe MESSAGEs	R0015		m	If security profile is implemented, all requirements have to be fulfilled.

Annex A

(normative)

Constants

C0002: The MAX_LARGE_ENVELOPE_SIZE is 4096K bytes.