P11073-20702™/D4
Draft Standard for Medical Device Profile for Web Services

Sponsor

IEEE 11073 Standard Committee
of the
IEEE Engineering in Medicine and Biology Society

Approved <Date Approved>

IEEE-SA Standards Board

Abstract: <Select this text and type or paste Abstract—contents of the Scope may be used>

Keywords: <Select this text and type or paste keywords>

•

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

PDF: ISBN 978-0-XXXX-XXXX-X STDXXXXX
Print: ISBN 978-0-XXXX-XXXX-X STDPDXXXXX

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 Notice" or "Important Notices and Disclaimers Concerning IEEE Standards Documents."

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. Volunteers 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 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-SA Website at http://ieeexplore.ieee.org/xpl/standards.jsp 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 draft standard was completed, the Point of Care Devices Working Group had the following membership:

Jan Wittenber, *Chair*
Paul Schluter and Todd Cooper, *Vice Chair*

Participant1	Participant4	Participant7
Participant2	Participant5	Participant8
Participant3	Participant6	Participant9

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

[To be supplied by IEEE]

Balloter1	Balloter4	Balloter7
Balloter2	Balloter5	Balloter8
Balloter3	Balloter6	Balloter9

When the IEEE-SA Standards Board approved this standard on <Date Approved>, it had the following membership:

[To be supplied by IEEE]

<Name>, *Chair*
<Name>, *Vice Chair*
<Name>, *Past Chair*
Konstantinos Karachalios, *Secretary*

SBMember1	SBMember4	SBMember7
SBMember2	SBMember5	SBMember8
SBMember3	SBMember6	SBMember9

*Member Emeritus

Also included are the following nonvoting IEEE-SA Standards Board liaisons:

<Name>, *DOE Representative*
<Name>, *NIST Representative*

<Name>
IEEE-SA Content Production and Management
<Name>
IEEE-SA Technical Program Operations

Introduction

This introduction is not part of P11073-20702/D2, Draft Standard for Medical Device Profile for Web Services.

<Select this text and type or paste introduction text>

Contents

<After draft body is complete, select this text and click Insert Special->Add (Table of) Contents>

Draft Standard for Medical Device 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

This standard defines a discovery, messaging, and event propagation method for a distributed PoC medical device communication system. 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 defines implementation constraints and extensions on the Devices Profile for Web Services (DPWS) standard in order to allow the utilization of the DPWS specification in such an environment.

2. Normative references

The following referenced documents are indispensable for the application of this document (i.e., they must 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.

[BP20] WS-I Profile, Basic Profile Version 2.0, R. Chumbley, et al, Editors. Web Services Interoperability Organization (WS-I), 9 November 2010. Available at http://ws-i.org/profiles/BasicProfile-2.0-2010-11-09.html.

[DPWS] OASIS Standard, Devices Profile for Web Services Version 1.1, T. Nixon, et al, Editors. OASIS, 1 July 2009. Available at http://docs.oasis-open.org/ws-dd/dpws/1.1/os/wsdd-dpws-1.1-spec-os.html.

[HTTP11] RFC 2616, Hypertext Transfer Protocol – HTTP/1.1, R. Fielding, J. Gettys, J. C. Mogul, H. Frystyk Nielsen, P. Leach, L. Masinter and T. Berners-Lee, Editors. IETF, June 1999. Available at http://tools.ietf.org/html/rfc2616.

[SOAP12] W3C Recommendation, SOAP Version 1.2 Part 1: Messaging Framework, M. Gudgin, M. Hadley, N. Mendelsohn, J J. Moreau, H. Frystyk Nielson, Editors. World Wide Web Consortium (W3C), 27 April 2007. Available at http://www.w3.org/TR/soap12-part1/.

[SOAP-over-UDP] OASIS Standard, SOAP-over-UDP Version 1.1, T. Nixon, et al, Editors. OASIS, 1 July 2009. Available at http:/docs.oasis-open.org/ws-dd/soapoverudp/1.1/os/wsdd-soapoverudp-1.1-spec-os.html.

[WS-Addressing] W3C Recommendation, Web Services Addressing 1.0 (WS-Addressing), M. Gudgin, M. Hadley, T. Rogers, Editors. World Wide Web Consortium (W3C), 9 May 2006. Available at http:/www.w3.org/TR/ws-addr-core.

[WS-Discovery] OASIS Standard, Web Services Dynamic Discovery (WS-Discovery), V. Modi, and D. Kemp, Editors. OASIS, 1 July 2009. Available at http://docs.oasis-open.org/ws-dd/discovery/1.1/os/wsdd-discovery-1.1-spec-os.html.

[WS-MetadataExchange] W3C Member Submission , Web Services Metadata Exchange (WS-MetadataExchange) 1.1, D. Davis, et al., Editors. World Wide Web Consortium (W3C), 13 August 2008. Available at http://www.w3.org/Submission/2008/SUBM-WS-MetadataExchange-20080813.

[WS-Policy] W3C Recommendation, Web Services Policy (WS-Policy) 1.5 – Framework, A. Vedamuthu, et al., Editors. World Wide Web Consortium (W3C), 4 September 2007. Available at http://www.w3.org/TR/ws-policy/.

[WS-PolicyAttachment] W3C Recommendation, Web Services Policy (WS-Policy) 1.5 – Attachment, A. Vedamuthu, et al., Editors. World Wide Web Consortium (W3C), 4 September 2007. Available at http://www.w3.org/TR/ws-policy-attach.

[WSDL11] W3C Note, Web Services Description Language (WSDL) 1.1, E. Christensen, et al., Editors. World Wide Web Consortium (W3C), 15 March 2001 Available at http://www.w3.org/TR/2001/NOTE-wsdl-20010315.

[XSD11] W3C Recommendation, XML Schema 1.1, W3C, 28 October 2004. Available at http://www.w3.org/TR/xmlschema-1, http://www.w3.org/TR/xmlschema-2/

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

[EXI10] W3C Recommendation, Efficient XML Interchange (EXI) Format 1.0 (Second Edition), J. Schneider, and T. Kamiya, Editors. World Wide Web Consortium (W3C), 11 February 2014. Available at http://www.w3.org/TR/2014/REC-exi-20140211/

[RFC 3987] IETF RFC 3987, Internationalized Resource Identifiers, Duerst et al., January 2005, Available at https://tools.ietf.org/html/rfc3987.

[WS-Eventing] W3C Member Submission, Web Services Eventing (WS-Eventing), D. Box, et al, World Wide Web Consortium (W3C), 15 March 2006. Available at http://www.w3.org/Submission/2006/SUBM-WS-Eventing-20060315/.

[XPath] W3C Recommandation, XML Path Language (XPath) Version 1.0, J.Clark et al., World Wide Web Consortium (W3C), 7 September 2015, Available at http://www.w3.org/TR/1999/REC-xpath-19991116.

[XMLNS] W3C Recommendation, Namespaces in XML 1.0 (Third Edition), Bray T. et al., World Wide Web Consortium (W3C), 8 December 2009, Available at http://www.w3.org/TR/REC-xml-names/

3. 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. [1]

This document uses the terms and definitions defined in [DPWS].

3.1 XML namespaces

The following lists XML namespaces that are used in this specification. The choice of any namespace prefix is arbitrary and not semantically significant.

Prefix	XML Namespace	Specification(s)
S12	http://www.w3.org/2003/05/soap-envelope	[SOAP12]
wsdl	http://schemas.xmlsoap.org/wsdl/	[WSDL11]
wsa	http://www.w3.org/2005/08/addressing	[WS-Addressing]
wsp	http://www.w3.org/ns/ws-policy	[WS-Policy]
dpws	http://docs.oasis-open.org/ws-dd/ns/dpws/2009/01	[DPWS]
mex	http://schemas.xmlsoap.org/ws/2004/09/mex	[WS-MetadataExchange]
xs	http://www.w3.org/2001/XMLSchema	[XSD11]
mdpws	TBD by IEEE process	This specification
wsstm	TBD by IEEE process	This specification, sec. 8
si	TBD by IEEE process	This specification, sec. 9

4. General Messaging

The scope of this section 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:

[1] *IEEE Standards Dictionary Online* subscription is available at: http://www.ieee.org/portal/innovate/products/standard/standards_dictionary.html.

— [BP20] section 3 (Messaging)

— [DPWS] section 2 (Messaging)

— [SOAP-over-UDP]

— [HTTP11]

4.1 SOAP-over-UDP

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

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— dpws:R0029 defines a limit for SOAP ENVELOPEs send over UDP. In order to allow larger SOAP-over-UDP Streaming messages, this specification relaxes the utilization of MAX_UDP_ENVELOPE_SIZE. The same is true for dpws:R5018 and dpws:R5019.

4.2 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—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—dpws:R0026 restricts the size of a TEXT SOAP ENVELOPE that should be send by a SERVICE to MAX_ENVELOPE_SIZE octets. This limit will be 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—bp20:R1012 for example requires support for UTF-16 character encoding in contrast to dpws:5002. Thus we have to clarify the conflict.

5. Dynamic Discovery

The scope of this section 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:

— [DPWS] section 3 (Discovery)

— [SOAP-over-UDP]

— [WS-Discovery]

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

NOTE—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 a UDP WS-Discovery message if the WS-Discovery message size does not exceed the maximum size of an UDP message.

NOTE—DPWS advices 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. Description

The scope of this section 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:

— [BP20] section 4 (Service Description) and 5 (WSDL Corrections)

— [DPWS] section 4 (Description) and appendix C (Declaring Discovery Types in WSDL)

6.1 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—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. In order to clarify that this should not be expressed in that way dpws:R2004 is relaxed and streams are explicitly excluded.

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

NOTE—As dpws:R2037 was ambiguous. This is now more clearly specified.

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

To indicate that a SERVICE is compliant with this profile, this profile defines the following WS-Policy [WS-Policy] assertion:

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

The following describes additional, normative constraints on the outline above:

`/mdpws:Profile`
Assertion indicating compliance with this profile is required. This assertion has Endpoint Policy Subject [WS-PolicyAttachment]: a policy expression containing this assertion MAY be attached to a wsdl:port, SHOULD be attached to a wsdl:binding, but MUST 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 [WS-Policy], 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 profile.

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—Statements R0012 and R0013 fix bp20:R2724 and bp20:R2725 [BP 2.0, Section 4] with respect to SOAP 1.2 nomenclature [SOAP12] similar to dpws:R2023 and dpws:R2024.

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

NOTE—In DPWS the inclusion of the dpws:DiscoveryType is non-normative.

7. Eventing

The scope of this section 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:

— [DPWS] section 5 (Eventing)

In this specification no additional normative statement are defined.

NOTE—The requirements of section 5 of [DPWS] are only applicable if a DEVICE or CLIENT needs an eventing mechanism in order to exchange information.

8. Streaming

The scope of this section is the definition of an announcement protocol by which a DEVICE can define the structure, content and transmission mechanism for streaming data from networked medical devices over

one physical, IP-based transmission medium to possible multiple CLIENTs. The message content is transmitted either in a SOAP message 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 …).

There is no reference to requirements of an external specification.

8.1 Advertising Stream Information

A Stream Source Provider MAY indicate its support of this part of this profile, or its features, by including the StreamSource Policy Assertion within its WSDL. This policy 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 specification is provided.

8.1.1 StreamSource Assertion

This specification defines a policy assertion (wsstm:StreamSource). The normative outline of this assertion is:

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

The following describes additional, normative constraints on the outline listed above:

`/wsstm:StreamSource`
This policy assertion has Endpoint Policy Subject. When present in a policy alternative, it indicates that the subject is a stream source provider.

`/wsstm:StreamSource/xs:any`
This extensibility point allows for additional specific metadata to be included within the policy assertion. Any metadata that appears is scoped to the operations and features of the WS-Streaming specification. If the Stream Source advertises StreamDescriptions data then it SHALL appear as a child of the StreamSource element.

8.2 Stream Types and Stream Descriptions

This section 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. StreamDescriptions element has the following form:

```
(01)        <wsstm:StreamDescriptions targetNamespace="xs:anyURI" ...>
(02)          <wsstm:types>
(03)            <xs:schema ...>
(04)              ...
(05)            </xs:schema>
```

```
(06)            xs:any*
(07)          </wsstm:types>?
(08)          <wsstm:streamType id="xs:ID"
(09)              streamType="xs:anyURI"
(10)              element="xs:QName"? actionURI="xs:anyURI"? ...>
(11)            <wsstm:StreamTransmission type="xs:anyURI"? ...>
(12)              xs:any*
(13)            </wsstm:StreamTransmission> ?
(14)            xs:any*
(15)          </wsstm:streamType> +
(16)          xs:any*
(17)        </wsstm:StreamDescriptions>
```

The following describes additional normative constraints on the outlined listed above:

`/wsstm:StreamDescriptions`
This element contains the declarations of all the Stream Types that apply to a given context.

`/wsstm:StreamDescriptions@targetNamespace`
This MANDATORY attribute defines the namespace affiliation of the Stream Types declared within the StreamDescriptions. Its value SHALL be an absolute IRI [RFC 3987]. It SHOULD be dereferenceable.

`/wsstm:StreamDescriptions/wsstm:types`
This OPTIONAL element encloses data type definitions that are relevant to the declared Stream Types.

`/wsstm:StreamDescriptions/wsstm:types/xs:schema`
As described earlier, a Stream Type may be defined by a Global Element Declaration (GED) in XML Schema. This element contains collections of imported and inlined schema components that describe the GEDs that are used to define Stream Types.

`/wsstm:StreamDescriptions/wsstm:streamType`
This element describes a specific Stream Type.

`/wsstm:StreamDescriptions/wsstm:streamType/@id`
This attribute provides an identifier for this Stream Type which SHALL be unique amongst all the Stream Types defined by the enclosing wsstm:StreamDescriptions element. In conjunction with a Prefix that is associated with the value of /wsstm:StreamDescriptions/@targetNamespace namespace IRI, the value of this attribute MAY be used as the LocalPart of a QName that identifies this Stream Type outside the context of the enclosing wsstm:StreamDescriptions element.

`/wsstm:StreamDescriptions/wsstm:streamType/@streamType`
This MANDATORY 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.

`/wsstm:StreamDescriptions/wsstm:streamType/@element`
This OPTIONAL attribute refers to a GED defined or imported in the /wsstm:StreamDescriptions/wsstm:types element. The referenced GED serves as the definition of this Stream Type payload.

`/wsstm:StreamDescriptions/wsstm:streamType/@actionURI`
This OPTIONAL attribute provides a value for the 'action' property used to transmit the Stream, serve as a potential aid to identifying the semantics implied by the message. When not present the implied value of this attribute is the concatenation of the /wsstm:StreamDescriptions/@targetNamespace attribute and the /wsstm:StreamDescriptions/wsstm:streamType/@id attribute separated by the '/' character.

`/wsstm:StreamDescriptions/wsstm:streamType/wsstm:StreamTransmission`

This OPTIONAL assertion 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 subscription process.

8.2.1 StreamTransmission Element

This element indicated the mechanisms that are utilized to transmit a stream.

```
(01)        <wsstm:StreamTransmission type="xs:anyURI"? ...>
(02)          <wsstm:streamAddress>xs:anyURI</wsstm:streamAddress> ?
(03)          <wsstm:streamPeriod>xs:duration</wsstm:streamPeriod> ?
(04)          xs:any*
(05)        </wsstm:StreamTransmission> ?
```

The following describes additional, normative constraints on the outline listed above:

`/wsstm:StreamTransmission`
This element describes a specific mechanism for the transmission of a Stream.

`/wsstm:StreamTransmission@type`
This OPTIONAL attribute references the mechanism for stream transmission. If omitted the value /wsstm:StreamDescriptions/wsstm:streamType@streamType is implied.

`/wsstm:StreamTransmission/wsstm:streamAddress`
This OPTIONAL 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.

`/wsstm:StreamTransmission/wsstm:streamPeriod`
This OPTIONAL element (XML schema duration type) 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 PT0.02S).

8.3 Retrieving Stream Descriptions

Although there are many ways in which an endpoint can make its StreamDescriptions available, this specification RECOMMENDS the use of the mechanisms described in section 9 of [WS-MetadataExchange]. In particular, this specification RECOMMENDS that the StreamDescriptions metadata be made available through the StreamSource Policy assertion. This MAY be done by either embedding the StreamDescriptions metadata directly within the assertion, or by including a MetadataExchange reference to the data.

R0025: A stream source MUST NOT have more than one StreamDescriptions document.

8.3.1 Embedded in Policy Assertion

The StreamDescriptions metadata might be embedded directly within the StreamSource Policy Assertion.

An informative example can be found in Annex C.

8.3.2 MetadataExchange Reference

A StreamDescriptions might appear within a WS-MetadataExchange MetadataSection. In this case the value of the @Identifier attribute, if present, SHALL be equal to the value of its wsstm:StreamDescriptions/@targetNamespace.

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 wsstm:StreamDescriptions/@targetNamespace.

An informative example can be found in Annex C.

8.4 SOAP-over-UDP Multicast Stream Binding

In this section a specific stream type is specified. The URI for this stream type is:

`wsstm:Mechanism/soap-over-udp`

8.4.1 Binding

The information about a Stream Type contained in the wsstm: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 wsstm: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 wsstm:streamType element corresponding to the type of the stream being transmitted. If the @element attribute is absent then the [Body] property has no children.

8.4.2 Addressing

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

8.4.3 Message sequencing

Messages within a multicast stream should have an application sequence number to allow a receiver to order messages and to notice packet loss.

This specification RECOMMENDS the AppSequence SOAP header from [WS-Discovery] (section 7).

R0027: The SequenceId should be set to the wsa:action URI and the MessageNumber SHALL be incremented by 1 (this is more restrictive).

Since the InstandeId has HOSTED SERVICE scope stream sinks cannot distinguish reliable between different stream sources. Thus it is RECOMMENDED to add the wsa:From header block with the services current transport address.

9. Safe Data Transmission

The scope of this section 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.

9.1 Advertising Safety Requirements

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 section defines a policy 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.

9.1.1 Assertion

This section normatively defines a safety requirement assertion that MAY be used during a 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.

9.1.1.1 SafetyReqAssertion

To indicate that a MESSAGE SHALL include safety information while transmitted from a CLIENT to a SERVICE of a DEVICE, this profile defines the SafetyReqAssertion WS-Policy [WS-Policy] assertion.

```
(01)        <si:SafetyReqAssertion TransmitDualChannel='xs:boolean'
(02)          TransmitSafetyContext='xs:boolean' ...>
(03)          ...
(04)        </si:SafetyReqAssertion>
```

The following describes additional, normative constraints on the outline listed above:

`/si:SafetyReqAssertion`
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 additional safety information need to be transmitted for the specified message elements.

`/si:SafetyReqAssertion/@TransmitDualChannel`
Boolean attribute that indicates that dual channel transmission is required for the specified message elements.

`/si:SafetyReqAssertion/@TransmitSafetyContext`

Boolean attribute that indicates that specified safety context information is required to be transmitted for the subject.

`/si:SafetyReqAssertion/xs:any`
Extension point for elements.

`/si:SafetyReqAssertion/@anyAttribute`
Extension point for attributes.

9.1.2 Elements

9.1.2.1 SafetyReq

To specify a safety requirement for transmission, this profile defines the SafetyReq element.

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

The following describes additional, normative constraints on the outline listed above:

`/si:SafetyReq`
Defines one safety-related requirement block.

`/si:SafetyReq/si:DualChannelDef`
Defines a requirement for transmitting a second channel for at least one specified message element.

`/si:SafetyReq/si:SafetyContextDef`
Defines a requirement for transmitting a safety-relevant contextual information for at least one safety context information for the message transmission.

`/si:SafetyReq/xs:any`
Extension point for elements.

`/si:SafetyReq/@anyAttribute`
Extension point for attributes.

9.1.2.2 DualChannelDef

To specify a requirement for transmission of a second channel for a message element, this profile normatively defines the DualChannelDef element.

```
(01)        <si:DualChannelDef Algorithm='xs:boolean'
(02)          Transform='xs:boolean' ...>
(03)          <si:Selector ...>
(04)            ...
```

```
(05)          </si:Selector> +
(06)          ...
(07)        </si:DualChannelDef>
```

The following describes additional, normative constraints on the outline listed above:

`/si:DualChannelDef`
Defines a requirement for transmitting a second channel for at least one specified message element.

`/si:DualChannelDef/@Algorithm`
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 /si:Base64SHA1.

`/si:DualChannelDef/@Transform`
Qualified name of a transformation that should be applied on the data before an algorithm is applied. Default is /si:xml-exc-c14n.

`/si:DualChannelDef/si:Selector`
Specifies a selector to an attribute of an element or element text inside of a message for which a second channel SHOULD be transmitted using the provided transformation and algorithm. The root of this selector is the S12:Body element of the message that transports dual channel information.

9.1.2.3 SafetyContextDef

To specify a requirement for embedding safety-relevant contextual information for a transmitted message, this profile defines the SafetyContextDef element.

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

The following describes additional, normative constraints on the outline listed above:

`/si:SafetyContextDef`
Defines a requirement for transmitting at least one safety context.

`/si:SafetyContextDef/si:Selector`
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.

9.1.2.4 Selector

Specifies a means to select an attribute of an element or element text by defining a limited XPath expression.

```
(01)        <si:Selector Id='xs:string' ...>
(06)          ...
(07)        </si:Selector>
```

The following describes additional, normative constraints on the outline listed above:

`/si:Selector`

Specifies an XPath expression {Path} that points to an attribute of an element or element text.

The following rules SHALL apply:

a) {Path} must be a valid XPath expression, as defined in XPath [XPath].

b) {Path} must conform to the following Extended Backus Naur Form:

```
[1] Path     ::=  ( '/' Step )* '/' ( '@' Name | 'text()' )
[2] Step     ::=  Name | Name '[' Expr ']'
[3] Expr     ::=  '@' Name '=' ( Number | Literal ) | Number
[4] Name     ::=  QName | NCName
[5] Literal  ::=  '"' [^"]* '"' | "'" [^']* "'"
[6] Number   ::=  Digits ( '.' Digits? )?
[7] Digits   ::=  [0-9]+
```

where

— QName is defined in [XMLNS].

— NCName is defined in [XMLNS].

Examples:

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

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

`/si:Selector/@Id`
A unique identifier over all Selector elements. The uniqueness scope is determined by other means. The identifier can be used to address the XPath expression a selector defines.

9.2 Retrieving Safety Requirements

SafetyReq MAY be made available through the SafetyReqAssertion Policy 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.

R0029: A DEVICE SHOULD indicate its support of this part of this profile, or its features, by including the SafetyReqAssertion within its WSDL.

9.3 Transmitting Safety Information

To enable a CLIENT to transmit safety-related information for which a DEVICE has be stated a requirement, this section normatively defines the elements to be used for embedding the information into the transmitted message.

In addition to the element definitions below 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 state a safety requirement.

9.3.1 Elements

This section normatively defines the safety information elements that are used during a message transmission.

9.3.1.1 SafetyInfo

To embed safety information in a message header, this profile defines the SafetyInfo container element.

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

The following describes additional, normative constraints on the outline listed above:

`/si:SafetyInfo`
Container element for embedding safety information in a SOAP message header.

`/si:SafetyInfo/si:DualChannel`
Dual channel element that can be used to embed dual channel information in a SOAP message header.

`/si:SafetyInfo/si:SafetyContext`
Safety context information element related to a required safety context definition.

`/si:SafetyInfo/xs:any`
Extension point for elements.

`/si:SafetyInfo/@anyAttribute`
Extension point for attributes.

9.3.1.2 DualChannel

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

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

The following describes additional, normative constraints on the outline listed above:

`/si:DualChannel`
Dual Channel element that can be used to embed dual channel information in a message header.

`/i:DualChannel/si:DcValue`
Dual Channel value element that contains the actual value of the second channel as well as information about how the value has been determined.

`/si:DualChannel/xs:any`
Extension point for elements.

`/si:DualChannel/@anyAttribute`
Extension point for attributes.

9.3.1.3 DcValue

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

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

The following describes additional, normative constraints on the outline listed above:

`/si:DcValue`
Dual channel value that contains the representation of the second channel. What algorithm and transformation is used to encode the second channel, is designated by the DualChannellDef element.

`/si:DcValue/@ReferencedSelector`
The referenced selector identifier of the element inside of the message that this second channel information is related to.

`/si:DcValue/@anyAttribute`
Extension point for attributes.

9.3.1.4 SafetyContext

To embed contextual information for a message into a message header, this profile defines the SafetyContext element.

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

The following describes additional, normative constraints on the outline listed above:

`/si:SafetyContext`
Safety context information element for a required safety context definition.

`/si:SafetyContext/si:CtxtValue`
List of safety context values.

9.3.1.5 CtxtValue

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

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

The following describes additional, normative constraints on the outline listed above:

`/si:CtxtValue`
The representation of the contextual information.

`/si:CtxtValue/@ReferencedSelector`
Specifies the referenced selector of the targeted element.

`/si:CtxtValue/xs:anyAttribute`
Extension point for attributes.

9.3.2 Binding Safety Information to SOAP 1.2 Message

When 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.

9.4 Qualified Names

9.4.1 Representation Generation Algorithms

R0034: A DEVICE MAY use other QNames for referencing representation generation algorithms that are not defined in this profile.

Table 1 defines QNames for referencing algorithms that are used in the generation of the second channel representation.

Table 1— Qualified Name of Representation Generation Algorithms

QName	Definition
si:Base64SHA1	QName for an algorithm that is used to determine the Base64-encoded SHA-1 digest of the XML Infoset representation of an attribute or element.

R0035: A CLIENT SHALL support the si:Base64SHA1

R0036: A DEVICE SHOULD support si:Base64SHA1 if safety-related transmission with a second channel is required.

9.4.2 Transformation Algorithms

R0037: A DEVICE MAY use other QNames for referencing transformation algorithms that are not defined in this profile.

Table 2 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 2— Qualified Names of Transformation Algorithms

QName	Definition
si:xml-exc-c14n	QName of a transformation on an XML Infoset representation of an attribute or element where exclusive XML canonicalization [XMLEXC] on the canonical lexical representation [XSD11] is applied.
si:noTransformation	QName of a transformation on an XML Infoset representation of an attribute or element where 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 [XSD11].

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

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

10. Security Considerations

The scope of this section 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:

- [BP20] section 7 (Security)
- [DPWS] section 6 (Security)
- [WS-Discovery] section 8 (Security)

NOTE—The requirements of section 6.5, section 6.7, and section 6.8 of [DPWS] and section 8 of [WS-Discovery] are only applicable if a DEVICE or CLIENT need these mechanism 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—dpws:R4072 is replaced by this requirement in order to allow devices to not support a Secure Channel.

NOTE—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 MUST NOT use HTTP Authentication to request CLIENT credentials.

NOTE—DPWS section 6.6.3.2 (CLIENT Authentication with HTTP Authentication) is withdrawn in favor of section 6.6.3.1

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

11. Message Serialization

The scope of this section 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:

- [EXI10]
- [BP20] section 3.1 (Message Serialization)
- [BP20] section 4.6 (Bindings)

R0019: If a SERVICE needs to use compact representation for the Extensible Markup Language (XML) Information Set the Efficient XML Interchange Format [EXI10] SHALL be used.

NOTE—[BP20] section 3.1 and [BP20] section 4.6 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 it SHALL support schema-less EXI streams with the default Options [EXI10].

R0021: If a CLIENT supports EXI it SHALL support schema-less EXI streams with the default Options [EXI10].

R0022: If a DEVICE supports EXI it SHOULD support schema-informed EXI streams with compressed option set to true and default values for the other Options [EXI10].

R0023: If a CLIENT supports EXI it SHOULD support schema-informed EXI streams with compressed option set to true and default values for the other Options [EXI10].

11.1 Advertising Compact Transmission

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

NOTE—It should be noted that as defined in R0007 an UTF-8 XML Infoset representation for a message SHALL always been 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—x-exi is proposed as the name for the content encoding in HTTP in [EXIBP].

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 [WS-Eventing] Subscription request, the Event Source MAY transmit events related to that subscription in the compact XML Infoset representation.

11.1.1 Compression Assertion

Services indicate requirements for a compact transmission as defined in this specification through the use of the Web Services Policy – Framework ([WS-Policy]) and Web Services Policy – Attachment ([WS-Policy Attachment]) specifications.

This specification defines a policy assertion (mdpws:Compression). The normative outline of this assertion is:

```
(1)         <mdpws:Compression method="xs:Qname"?
(2)                            compression="xs:Qname"?>
(3)                            xs:any*
(4)         </mdpws:Compression>
```

The following describes the attributes and elements listed in the schema overview above:

`/mdpws:Compression`

This policy 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 encode/decode message to/from the compact transmission representation. This specification defines the following set of values for method:

- mdpws:EXI-sl: The [EXI10] schema-less algorithm SHALL be applied. The default value.
- mdpws:EXI-si: The [EXI10] schema-informed algorithm SHALL be applied.

`/mdpws:Compression/@compression`
Specifies if a compression is applied to output according to chapter 9 in [EXI10].This specification defines the following set of values for method:

- mdpws:EXI-nocmpr: No [EXI10] compression SHALL be applied. The default value.
- mdpws:EXI-cmpr: [EXI10] compression SHALL be applied.

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

12. Conformance

A conformant implementation MUST satisfy all the SHALL or REQUIRED level requirements defined herein.

Annex A

(normative)

Constants

C0002: The MAX_LARGE_ENVELOPE_SIZE is 4096K bytes.

C0003: The MAX_URI_SIZE is 1024 Octets

Annex B

(informative)

Streaming Requirements

This specification intends to meet the following requirements:

c) It should be independent of the actual streaming mechanism.

d) Define a mechanism to describe the structure and contents of streams.

   1) Streams could be 1-to-1 or 1-to-many streams.
   2) The description might contain information about the streams size (data rate, file size in data transfers, …)

e) Define a mechanism how to establish streams (e.g., subscriptions, multicast listening). There are two conceivable types of streams

   1) Without handshake: Streaming protocols that do not require a subscription. This is the case for connection less streams (UDP broadcast/multicast) or protocols that have their own subscription methods. A stream description with information is sufficient.

   2) With handshake: The mechanism is currently out of scope of this specification and might be specified in future versions.

f) Support alternative streaming technologies without requiring a new streaming specification.

g) Leverage WS-MetadataExchange [WS-MetadataExchange] to allow an endpoint to advertise streams that might be generated.

Annex C

(informative)

Example StreamSource Policy Assertion

The following examples show how StreamDescriptions metadata might appear within a StreamSource Policy assertion.:

```
(01)        <wsstm:StreamSource ...>
(02)          <wsstm:StreamDescriptions ...>
(03)            ...
(04)          </wsstm:StreamDescriptions>
(05)        </wsstm:StreamSource>
```

Instead of embedding the StreamDescriptions directly it is replaced with a reference to an HTTP resource whose representation is the StreamDescriptions metadata. The data can be retrieved via an HTTP GET to the specified URL:

```
(01)        <wsstm:StreamSource ...>
(02)          <mex:Location
(03)              Type="wsstm:StreamDescriptions"
(04)              URI="http:/example.com/Stream_Metadata" />
(05)        </wsstm:StreamSource>
```

Example GetMetadataResponse with StreamDescriptions

The GetMetadataResponse message in this case might look like:

```
(01)        <mex:GetMetadataResponse>
(02)          <mex:Metadata>
(03)            <mex:MetadataSection Dialect='wsstm:StreamDescriptions'
(04)                Identifier='...'>
(05)              <wsstm:StreamDescriptions ...>
(06)                ...
(07)              </wsstm:StreamDescriptions>
(08)            </mex:MetadataSection>
(09)          </mex:Metadata>
(10)        </mex:GetMetadataResponse>
```

Example Binding of Safety Information to SOAP 1.2 Message

This section shows a non-normative example of a message that contains a second channel representation as well as safety context information items. For the sake of brevity, some contents are abbreviated with dots.

```
(01)        <s12:Envelope ...>
(02)          <s12:Header>
(03)            <wsa:Action>...</wsa:Action>
(04)            <wsa:MessageID>...</wsa:MessageID>
(05)            <wsa:To>...</wsa:To>
```

```
(06)            <si:SafetyInfo>
(07)              <si:DualChannel>
(08)                <si:DcValue ReferencedSelector="sel1">
(09)                  VeJp6LdVGlc1Vvh7XGDz3kz+Xgs
(10)                </si:DcValue>
(11)                <si:DcValue ReferencedSelector="sel2">
(12)                  fYNvS+/KK9o+irsfe9kzRaWxCuk
(13)                </si:DcValue>
(14)              </si:DualChannel>
(15)              <si:SafetyContext>
(16)                <si:CtxtValue ReferencedSelector="sel3">
(17)                  262656
(18)                </si:CtxtValue>
(19)                <si:CtxtValue ReferencedSelector="sel4">
(20)                  Safety context information
(21)                </si:CtxtValue>
(22)              </si:SafetyContext>
(23)            </si:SafetyInfo>
(24)          </s12:Header>
(25)          <s12:Body>
(26)            <msg:SetString>
(27)              <msg:OperationHandleRef>
(28)                op1
(29)              </msg:OperationHandleRef>
(30)              <msg:RequestedStringValue>
(31)                Value
(32)              </msg:RequestedStringValue>
(33)            </msg:SetString>
(34)          </s12:Body>
(35)        </s12:Envelope>
```

Depending on the safety requirement definition, dual channel values may point to msg:OperationHandleRef and msg:RequestedStringValue.

Example Stream Description Embedded in GetMetadataResponse

```
(01)        <s12:Envelope ...>
(02)         <s12:Header>
(03)          ...
(04)         </s12:Header>
(05)        <s12:Body>
(06)        <wsx:Metadata>
(07)         <wsx:MetadataSection
(08)             Dialect="http://schemas.xmlsoap.org/wsdl/">
(09)          ...
(10)         </wsx:MetadataSection>
(11)         <wsx:MetadataSection
(12)             Dialect="http://docs.oasis-open.org/ws-
(13)                             dd/ns/dpws/2009/01/Relationship">
(14)          ...
(15)        </wsx:MetadataSection>
(16)        <wsx:MetadataSection
(17)             Dialect="http://standardized.namespace.org/ws-
(18)                             streaming/StreamDescriptions"
```

```
(19)             Identifier="http://message-model-
uri/15/04/Waveform">
(20)              <n1:StreamDescriptions
(21)                 targetNamespace="http://message-model-
(22)                                          uri/15/04/Waveform"
(23)                 xmlns:n1="http://standardized.namespace.org/
(24)                           ws-streaming">
(25)                 <n1:types>
(26)                  ...
(27)                 </n1:types>
(28)                 <n1:streamType id="WaveformStream"
(29)                     streamType="http://docs.oasis-open.org/ws-
(30)                          dd/soapoverudp/1.1/os/wsdd-soapoverudp-
(31)                          1.1-spec-os.html"
(32)                     element="n4:WaveformStream"
(33)                     actionURI="http://message-model-
(34)                               uri/15/04/Waveform/WaveformStream"
(35)                     xmlns:n4="http://message-model-uri/15/04">
(36)                   <n1:StreamTransmission>
(37)                     <n1:streamAddress>
(38)                       soap.udp://239.239.239.235:5555
(39)                     </n1:streamAddress>
(40)                     <n1:streamPeriod>
(41)                      60
(42)                    </n1:streamPeriod>
(43)                 </n1:StreamTransmission>
(44)               </n1:streamType>
(45)         </n1:StreamDescriptions>
(46)         </wsx:MetadataSection>
(47)         </wsx:Metadata>
(48)         </s12:Body>
(49)         </s12:Envelope>
```

Annex D

(informative)

Bibliography

Bibliographical references are resources that provide additional or helpful material but do not need to be understood or used to implement this standard. Reference to these resources is made for informational use only.

[EXIBP] W3C Working Draft, Efficient XML Interchange (EXI) Best Practices, M. Cokus, Editors. World Wide Web Consortium (W3C), 19 December 2007. Available at http://www.w3.org/TR/exi-best-practices/

[SOAP11] W3C Note, "Simple Object Access Protocol (SOAP) 1.1, D. Box, et al, Editors. World Wide Web Consortium (W3C), 8 May 2000. Available at http://www.w3.org/TR/2000/NOTE-SOAP-20000508/.