

IEEE Adoption of Smart Energy Profile 2.0 Application Protocol Standard

IEEE Communications Society

Sponsored by the
Power Line Communications Committee

IEEE
3 Park Avenue
New York, NY 10016-5997
USA

IEEE Std 2030.5™-2013

IEEE Adoption of Smart Energy Profile 2.0 Application Protocol Standard

Sponsor

Power Line Communications Committee
of the
IEEE Communications Society

Approved 31 October 2013

IEEE-SA Standards Board

Abstract: The 'APPLICATION' layer with TCP/IP providing functions in the 'TRANSPORT' and 'INTERNET' layers is defined in this standard. Depending on the physical layer in use (e.g., IEEE 802.15.4™, IEEE 802.11™, IEEE 1901™), a variety of lower layer protocols may be involved in providing a complete solution. Generally, lower layer protocols are not discussed in this standard except where there is a direct interaction with the application protocol. This standard defines the mechanisms for exchanging application messages, the exact messages exchanged including error messages, and the security features used to protect the application messages. With respect to the OSI network model, this standard is built using the four-layer Internet stack model. The defined application protocol is an IEC 61968 common information model [61968] profile, mapping directly where possible, and using subsets and extensions where needed, and follows an IETF RESTful architecture [REST].

Keywords: adoption, application, application protocol, demand response, distributed energy resources, energy usage information, IEEE 2030.5, load control, metering, plugin electric vehicles, prepayment, pricing communication, RESTful, SEP 2, smart energy, smart energy profile, Smart Energy Profile 2

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

Copyright © 2013 by The Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 14 November 2013. Printed in the United States of America.

IEEE is a registered trademark in the U.S. Patent & Trademark Office, owned by The Institute of Electrical and Electronics Engineers, Incorporated.

PDF: ISBN 978-0-7381-8746-4 STD98454
Print: ISBN 978-0-7381-8747-1 STDPD98454

IEEE prohibits discrimination, harassment, and bullying.

For more information, visit <http://www.ieee.org/web/aboutus/whatis/policies/p9-26.html>.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher.

Notice and Disclaimer of Liability Concerning the Use of IEEE Documents: IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE-SA) Standards Board. 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 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.

Use of an IEEE Standard is wholly voluntary. IEEE disclaims liability for any personal injury, property or other damage, of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, or reliance upon any IEEE Standard document.

IEEE does not warrant or represent the accuracy or content of the material contained in its standards, and expressly disclaims any express or implied warranty, including any implied warranty of merchantability or fitness for a specific purpose, or that the use of the material contained in its standards is free from patent infringement. IEEE Standards documents are supplied "AS IS."

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. 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 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.

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 the official position of IEEE or any of its committees and shall not be considered to be, nor 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 to ensure 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. Any person who would like to participate in evaluating comments or revisions to an IEEE standard is welcome to join the relevant IEEE working group at <http://standards.ieee.org/develop/wg/>.

Comments on standards should be submitted to the following address:

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

Photocopies: Authorization to photocopy portions of any individual standard for internal or personal use is granted by The Institute of Electrical and Electronics Engineers, Inc., provided that the appropriate fee is paid to Copyright Clearance Center. To arrange for payment of licensing fee, 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.

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 IEEE standard was completed, the Smart Energy Profile 2.0 (COM/PLC/SEP2) Working Group had the following membership:

Robert Heile, *Chair (ZigBee Alliance)*
Don Sturek, *Vice Chair (Grid2Home)*

Michael Cowen (*Sensus*)
Robert Cragie (*Grid2Home*)
David Decker (*Toshiba Corporation*)
Yusuke Doi (*Toshiba Corporation*)
Ed Eckert (*Itron*)
Constantin Enascuta (*Freescale Semiconductor, Inc.*)
Gene Falendysz (*Itron*)
Mark Grazier (*Texas Instruments Incorporated*)
Thomas Herbst (*Silver Spring Networks Inc.*)
Jeffrey King (*Elster*)
Bill Lichtensteiger (*Toshiba Corporation*)

Daniel Popa (*Itron*)
Tobin Richardson (*ZigBee Alliance*)
Kazumasa Saito (*NEC Corporation*)
Ruben Salazar (*Toshiba Corporation*)
Noriyuki Sato (*Oki Electric Industry Co., Ltd.*)
Jeff Shudark (*Toshiba Corporation*)
Robby Simpson (*GE*)
Dongmin Son (*LG Electronics*)
Steve Urbanski (*Freescale Semiconductor, Inc.*)
Scott Willy (*MStar Semiconductor, Inc.*)

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

James Allen (*STMicroelectronics*)
Edward Eckert (*Itron Inc.*)
John Egan (*Marvell Semiconductor, Inc.*)
Omar Elloumi (*ALCATEL-LUCENT*)
Jean Philippe Faure (*Panasonic Corporation of North America*)
Tim Godfrey (*Electric Power Research Institute, Inc.*)
Mark Grazier (*Texas Instruments Incorporated*)
Robert Heile (*ZigBee Alliance*)
Thomas Herbst (*Silver Spring Networks Inc.*)
Jeffrey King (*Elster*)

Cees Links (*GreenPeak Technologies B.V.*)
Bill Lichtensteiger (*Toshiba Corporation*)
Stephen Palm (*Broadcom Corporation*)
Markus Rindchen (*Power Plus Communications AG*)
Kazumasa Saito (*NEC Corporation*)
Noriyuki Sato (*Oki Electric Industry Co., Ltd.*)
Dongmin Son (*LG Electronics*)
Gary Stuebing (*Cisco Systems, Inc.*)
Don Sturek (*Grid2Home*)
Steve Urbanski (*Freescale Semiconductor, Inc.*)
Scott Willy (*MStar Semiconductor, Inc.*)

When the IEEE-SA Standards Board approved this standard on 31 October 2013, it had the following membership:

John Kulick, *Chair*
David J. Law, *Vice Chair*
Richard H. Hulett, *Past Chair*
Konstantinos Karachalios, *Secretary*

Masayuki Ariyoshi
Peter Balma
Farooq Bari
Ted Burse
Wael William Diab
Stephen Dukes
Jean-Philippe Faure
Alexander Gelman

Mark Halpin
Gary Hoffman
Paul Houzé
Jim Hughes
Michael Janezic
Joseph L. Koepfinger*
Oleg Logvinov

Ron Petersen
Gary Robinson
Jon Walter Rosdahl
Adrian Stephens
Peter Sutherland
Yatin Trivedi
Phil Winston
Yu Yuan

*Member Emeritus

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

Richard DeBlasio, *DOE Representative*
Michael Janezic, *NIST Representative*

Catherine Berger
IEEE Standards Senior Program Manager, Document Development

Bill Ash
IEEE Strategic Technology Program Director

IEEE Adoption of Smart Energy Profile 2.0 Application Protocol Standard

IMPORTANT NOTICE: IEEE Standards documents are not intended to ensure safety, health, or environmental protection, or ensure against interference with or from other devices or networks. Implementers 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.

This IEEE document is made available for use subject to important notices and legal disclaimers. These notices and disclaimers appear in all publications containing this document and may be found under the heading “Important Notice” or “Important Notices and Disclaimers Concerning IEEE Documents.” They can also be obtained on request from IEEE or viewed at <http://standards.ieee.org/IPR/disclaimers.html>.



Smart Energy Profile 2 Application Protocol Standard

ZigBee Public Document 13-0200-00

April 2013

Sponsored by: ZigBee Alliance

Accepted by This document has been accepted for release by the ZigBee Alliance Board of Directors.

Abstract This document describes Smart Energy Profile 2, an IP-based standard for energy management and communications.

Keywords Smart Energy Profile 2, SEP 2, Demand Response and Load Control, Pricing Communication, Energy Usage Information, Metering, Prepayment, Plugin Electric Vehicles, Distributed Energy Resources, RESTful

April 2013

This page is intentionally blank.

Foreword

The empowerment of consumers to manage their usage and generation of energy is a critical feature of the Smart Grid and is a basis of innovation for new products and services in energy management. To enable this capability, information flow between devices such as meters, smart appliances, plug-in electric vehicles, energy management systems, and distributed energy resources (including renewable energy and storage elements) must occur in an open, standardized, secure, and interoperable fashion. The following specification is intended to fulfill those needs.

The development of this document has been driven by, and seeks to address the requirements of, many activities across the globe. Of note are the efforts within the United States by the National Institute of Standards and Technology (NIST) and the Smart Grid Interoperability Panel (SGIP) (in particular, Priority Action Plans 3, 9, 10, 11, and 18, with influence from many of the others) in fulfillment of the EISA 2007 legislation, the European Mandate on Smart Metering (M / 441) (in particular, efforts within CEN / CENELEC and ETSI, and the Smart Meter Working Group), as well as similar efforts in Australia, the United Kingdom, Japan, and China, and electric vehicle standardization efforts (in particular, ISO / IEC JWG automotive EV standards and SAE EV standards), to name only a few.

Readers should note that this document was readied for balloting under the policies set forth in the ZigBee Alliance. Previous revisions of this document have gone through review both within the ZigBee Alliance as well as made available for public comment. All previously received comments have been considered for this specification. This specification is intended to meet the requirements set forth in the previously published Technical Requirements Document (TRD).

This document is also intended to enable communications that are link-layer agnostic and run over the Internet Protocol. Careful consideration was given to premises networks with various architectures, numbers of devices, and constraints while maintaining flexibility, extensibility, and security.

Table of Contents

Smart Energy Profile 2 Application Protocol Standard	1
1 Introduction	15
1.1 Purpose.....	15
1.2 Scope	15
1.3 Context Overview	15
1.4 Document Organization	15
1.5 Requirement Language	16
1.6 Typography Conventions Used	16
1.7 Design Principles	16
2 Acknowledgements	17
3 Document Revision History	18
4 References	19
4.1 Smart Energy 2.0 Documents	19
4.2 IEC Documents	19
4.3 IETF Documents.....	19
4.4 Other References.....	20
5 Definitions, Acronyms and Abbreviations	22
5.1 Acronyms and Abbreviations.....	22
5.2 Definitions	23
6 Design Pattern.....	26
6.1 Protocol Flexibility	26
6.2 General Rules / Best Practices	26
6.3 WADL.....	27
6.4 Schema.....	27
6.5 Uniform Resource Identifiers.....	27
6.6 List Resources	28
6.6.1 Query String Parameters	28
6.7 Resource Design Rules.....	31
7 Application Support	33
7.1 Overview	33
7.2 Use of TCP	33
7.3 URI Encoding	33
7.4 HTTP Headers	33
7.4.1 HTTP Header Field Recommended Usage	34
7.5 HTTP Response Codes.....	36
7.5.1 Common Responses	36
7.5.2 Minimal Understanding	38
7.6 Application Payload Syntax.....	39
7.6.1 XML Encoding	39
7.6.2 EXI Encoding.....	39
7.7 Content Negotiation.....	39
7.7.1 Schema Version Negotiation	39
8 Security	41
8.1 Introduction.....	41
8.2 Security Attributes.....	41
8.2.1 Local Registration Attributes	41
8.2.2 Access Control List (ACL) Attributes.....	42
8.3 Device Credentials	46

8.3.1	Certificate Fingerprint.....	47
8.3.2	Short-form Device Identifier (SFDI).....	47
8.3.3	Long-form Device Identifier (LFDI).....	47
8.3.4	6-digit PIN code.....	47
8.3.5	Registration Code	48
8.4	<i>Resource Access Authentication and Authorization context</i>	48
8.5	<i>Resource Access Authentication</i>	49
8.6	<i>Resource Access Authorization</i>	50
8.7	<i>Cipher Suites</i>	50
8.8	<i>Default Security Policy</i>	50
8.9	<i>Registration</i>	52
8.9.1	EndDeviceList.....	53
8.10	<i>Security LogEvents</i>	54
8.11	<i>Certificate Management</i>	54
8.11.1	Introduction.....	54
8.11.2	Certificate Usage – Authentication vs. Authorization	56
8.11.3	Manufacturing PKI.....	57
8.11.4	General Certificate Format	58
8.11.5	General Restrictions and Conditions	59
8.11.6	Extensions.....	59
8.11.7	Additional ASN1 Definitions	60
8.11.8	Certificate Profiles	61
8.11.9	Device Requirements	65
8.11.10	Certificate Verification.....	66
8.11.11	Certificate Related Labeling Requirements	66
9	Discovery	67
9.1	<i>Service Instance</i>	67
9.2	<i>Service Name</i>	68
9.3	<i>TXT Record</i>	68
9.4	<i>Subtype Queries</i>	69
9.5	<i>Discovery Procedure</i>	71
10	Support Resources	72
10.1	<i>Resource Section Outlines</i>	72
10.1.1	Overview	72
10.1.2	List Ordering	72
10.1.3	Application Guidelines / Behavior	72
10.1.4	LogEvents	73
10.2	<i>Device Capabilities Function Set</i>	73
10.2.1	Overview	73
10.2.2	List Ordering	73
10.2.3	Application Guidelines / Behavior	73
10.2.4	LogEvents	73
10.3	<i>Self Device Resource</i>	73
10.3.1	Overview	73
10.3.2	List Ordering	73
10.3.3	Application Guidelines / Behavior	73
10.3.4	LogEvents	74
10.4	<i>End Device Resource</i>	74
10.4.1	Overview	74

10.4.2	List Ordering	74
10.4.3	Application Guidelines / Behavior	74
10.4.4	LogEvents	75
10.5	<i>Function Set Assignments</i>	75
10.5.1	Overview	75
10.5.2	List Ordering	76
10.5.3	Application Guidelines / Behavior	76
10.5.4	LogEvents	76
10.6	<i>Subscription / Notification Mechanism</i>	76
10.6.1	Overview	76
10.6.2	List Ordering	77
10.6.3	Application Guidelines / Behavior	77
10.6.4	LogEvents	79
10.7	<i>Response</i>	79
10.7.1	Overview	79
10.7.2	List Ordering	79
10.7.3	Application Guidelines / Behavior	79
10.7.4	LogEvents	83
11	Common Resources	84
11.1	<i>Time Function Set</i>	84
11.1.1	Overview	84
11.1.2	List Ordering	84
11.1.3	Application Guidelines / Behavior	84
11.1.4	LogEvents	85
11.2	<i>DeviceInformation Function Set</i>	85
11.2.1	Overview	85
11.2.2	List Ordering	85
11.2.3	Application Guidelines / Behavior	85
11.2.4	LogEvents	85
11.3	<i>Power Status</i>	86
11.3.1	Overview	86
11.3.2	List Ordering	86
11.3.3	Application Guidelines / Behavior	86
11.3.4	LogEvents	86
11.4	<i>Network Status</i>	86
11.4.1	Overview	86
11.4.2	List Ordering	86
11.4.3	Application Guidelines / Behavior	87
11.4.4	LogEvents	87
11.5	<i>LogEvent List</i>	87
11.5.1	Overview	87
11.5.2	List Ordering	87
11.5.3	Application Guidelines / Behavior	88
11.6	<i>Configuration Resource</i>	88
11.6.1	Overview	88
11.6.2	List Ordering	88
11.6.3	Application Guidelines / Behavior	88
11.6.4	LogEvents	89
11.7	<i>File Download Function Set</i>	89

11.7.1	File List Resource	89
11.7.2	File Status Resource	92
12	Smart Energy Resources	94
12.1	<i>Common Functionality</i>	<i>94</i>
12.1.1	Overview	94
12.1.2	Active List Elements.....	94
12.1.3	Event Rules and Guidelines	94
12.1.4	Randomization	97
12.1.5	Multi-Server.....	99
12.2	<i>Demand Response and Load Control</i>	<i>100</i>
12.2.1	Overview	100
12.2.2	List Ordering	100
12.2.3	Application Guidelines / Behavior	101
12.2.4	LogEvents	103
12.3	<i>Metering Function Set</i>	<i>103</i>
12.3.1	Overview	103
12.3.2	List Ordering	103
12.3.3	Application Guidelines / Behavior	103
12.3.4	LogEvents	107
12.4	<i>Pricing Function Set.....</i>	<i>109</i>
12.4.1	Overview	109
12.4.2	List Ordering	109
12.4.3	Application Guidelines / Behavior	109
12.4.4	LogEvents	113
12.5	<i>Messaging Function Set</i>	<i>113</i>
12.5.1	Overview	113
12.5.2	List Ordering	113
12.5.3	Application Guidelines / Behavior	114
12.5.4	LogEvents	114
12.6	<i>Billing Function Set.....</i>	<i>114</i>
12.6.1	Overview	114
12.6.2	List Ordering	115
12.6.3	Application Guidelines / Behavior	115
12.6.4	LogEvents	117
12.7	<i>Prepayment Function Set</i>	<i>117</i>
12.7.1	Overview	117
12.7.2	List Ordering	117
12.7.3	Application Guidelines / Behavior	117
12.7.4	LogEvents	119
12.8	<i>Energy Flow Reservation Function Set</i>	<i>119</i>
12.8.1	Overview	119
12.8.2	List Ordering	119
12.8.3	Application Guidelines / Behavior	119
12.8.4	LogEvents	120
12.9	<i>Distributed Energy Resources Function Set</i>	<i>120</i>
12.9.1	Overview	120
12.9.2	Terminology and Conventions.....	121
12.9.3	List Ordering	122
12.9.4	Application Guidelines / Behavior	122

12.9.5	DER Client Device Requirements	125
12.9.6	LogEvents	127
12.10	<i>Metering Mirror</i>	127
12.10.1	Overview	127
12.10.2	List Ordering	127
12.10.3	Application Guidelines / Behavior	127
12.10.4	LogEvents	129
13	Manufacturer – Specific Proprietary Extensions	130
13.1	Overview	130
13.2	<i>xmDNS/DNS-SD</i>	130
13.3	URIs	130
13.4	Resources	130
13.5	<i>DeviceCapabilities Resource</i>	131
14	Appendix A - Web-Application Description Language (INFORMATIVE)	132
14.1	<i>Support Resources Section</i>	132
14.1.1	Device Capability Function Set	132
14.1.2	Self Device Resource Function Set	132
14.1.3	End Device Resource Function Set	132
14.1.4	Function Set Assignments Function Set	133
14.1.5	Subscription/Notification Mechanism Function Set	133
14.1.6	Response Function Set	134
14.2	<i>Common Resources Section</i>	135
14.2.1	Time Function Set	135
14.2.2	Device Information Function Set	135
14.2.3	Power Status Function Set	136
14.2.4	Network Status Function Set	136
14.2.5	Log/Event Log Function Set	138
14.3	<i>Smart Energy Resources Section</i>	138
14.3.1	Configuration Resource Function Set	138
14.3.2	Software Download Function Set	139
14.3.3	Demand Response and Load Control Function Set	139
14.3.4	Metering Function Set	140
14.3.5	Pricing Function Set	142
14.3.6	Messaging Function Set	143
14.3.7	Billing Function Set	144
14.3.8	Prepayment Function Set	147
14.3.9	Flow Reservation Function Set	149
14.3.10	Distributed Energy Resources Function Set	149
15	Appendix B – SEP 2 Model (INFORMATIVE)	153
15.1	<i>SEP 2 Package</i>	153
15.1.1	DeviceCapability Package	153
15.1.2	Common Package	154
15.1.3	EndDevice Package	173
15.1.4	FunctionSetAssignments Package	176
15.1.5	Pub-Sub Package	177
15.1.6	Response Package	179
15.1.7	Time Package	181
15.1.8	DeviceInformation Package	182
15.1.9	PowerStatus Package	185

15.1.10	NetworkStatus Package	187
15.1.11	LogEvents Package	192
15.1.12	Configuration Package	194
15.1.13	SoftwareDownload Package	196
15.1.14	DRLC Package	199
15.1.15	Metering Package	203
15.1.16	Pricing Package	210
15.1.17	Messaging Package	214
15.1.18	Billing Package	216
15.1.19	Prepayment Package	221
15.1.20	FlowReservation Package	226
15.1.21	DER Package	228
15.1.22	Links Package	244
16	Appendix C – Examples and Guidelines [INFORMATIVE]	250
16.1	Registration: Remote	250
16.2	Registration: Local	253
16.3	Discovery: Function Set Assignment	256
16.4	Discovery: Without Function Set Assignment	258
16.5	Discovery: Undirected Without Function Set Assignment	260
16.6	Subscription / Notification	261
16.7	Demand Response: General	264
16.8	Demand Response: Cancel	268
16.9	Distributed Energy Resource: General	270
16.10	Metering: Reading	274
16.11	Metering: Interval	279
16.12	Metering: Instantaneous	285
16.13	Metering: Mirroring	288
16.14	Pricing: Time of Use	301
16.15	Billing: Billing Period	307
16.16	Billing: Historical	310
16.17	Billing: Projection	313
16.18	File Loading	315
16.19	Flow Reservation: General	318
16.20	Flow Reservation: Cancel	322
16.21	Event Randomization	326
16.21.1	Simple Event	326
16.21.2	Event with Positive Randomized Duration	327
16.21.3	Event with Positive Randomized Start	327
16.21.4	Event with Negative Randomized Start	328
16.21.5	Event with Positive Randomization and Finishing in one Hour	329
16.21.6	Event with Negative Randomized Start and at Least One Hour Duration	329
16.21.7	Event with Randomized Start and Long Ramp Up	330
16.21.8	Event with Positive Randomized Start and Fixed End Time	331
17	Appendix D – Guidelines [INFORMATIVE]	332
17.1	Pricing Implementation Guidelines	332
17.1.1	Implementing Common Tariff Designs	332
17.1.2	Flat Rate Design	332
17.1.3	Time-of-Use Rate Design	333
17.1.4	Consumption-based Block Rate Design	334

17.1.5	Combined Time-of-Use and Consumption-based Block Rate Design	334
17.1.6	Coordinated and Uncoordinated Pricing and Metering Servers	336
17.2	<i>PEV Implementation Guidelines (subject to work with SAE and ISO / IEC)</i>	337



List of Tables

Table 7-1 HTTP Headers.	34
Table 8-1 Local Registration Attributes.	41
Table 8-2 Local Registration Descriptor Entry.	41
Table 8-3 ACL Attributes.	42
Table 8-4 AccessDescriptor Entry.	42
Table 8-5 SpecificIDDescriptor Entry.	43
Table 8-6 Example ACL for EndDeviceList.	45
Table 8-7 Example ACL entry for EndDevice at point of registration.	45
Table 8-8 Example local registration entry for registering device.	46
Table 8-9 Example ACL entry for EndDevice at point of client access.	46
Table 8-10 Example SpecificIDDescriptor for EndDevice at point of client access.	46
Table 8-11 Attribute values for Default Security Policy.	51
Table 8-12 Security LogEvents.	54
Table 8-13 TLS Authentication Matrix.	56
Table 8-14 SEP 2 Authorization Matrix.	56
Table 9-1 TXT record parameters.	68
Table 9-2 Service subtype strings and their corresponding SEP 2 function sets.	70
Table 10-1 Function Set List Ordering.	72
Table 10-2 Example LogEvents.	73
Table 10-3 Self Device LogEvents.	74
Table 10-4 End Device List Ordering.	74
Table 10-5 End Device LogEvents.	75
Table 10-6 Function Set Assignments List Ordering.	76
Table 10-7 Subscription / Notification List Ordering.	77
Table 10-8 Subscription / Notification LogEvents.	79
Table 10-9 Response List Ordering.	79
Table 10-10 Response Types by Function Set.	80
Table 10-11 Response LogEvents.	83
Table 11-1 Time LogEvents.	85
Table 11-2 Power Status LogEvents.	86
Table 11-3 Network Status List Ordering.	86
Table 11-4 Network Status LogEvents.	87
Table 11-5 LogEvent List Ordering.	87
Table 11-6 General LogEvents.	88
Table 11-7 Configuration LogEvents.	89
Table 11-8 File Download List Ordering.	89
Table 11-9 File Download LogEvents.	92
Table 12-1 Demand Response and Load Control List Ordering.	100
Table 12-2 Metering List Ordering.	103
Table 12-3 Reading Types.	106
Table 12-4 Metering LogEvents.	107
Table 12-5 Pricing List Ordering.	109
Table 12-6 Pricing LogEvents.	113
Table 12-7 Messaging List Ordering.	113
Table 12-8 Billing List Ordering.	115
Table 12-9 Prepayment List Ordering.	117
Table 12-10 Prepayment LogEvents.	119
Table 12-11 FlowReservation List Ordering.	119

Table 12-12 Flow Reservation LogEvents.	120
Table 12-13 Distributed Energy Resources List Ordering.	122
Table 12-14 Modes and Attributes for Generator Type DERs.	126
Table 12-15 Modes and Attributes for Storage Type DERs.	127
Table 12-16 Metering Mirror List Ordering.	127
Table 12-17 Metering Mirror LogEvents.....	129
Table 16-1 POX Example: Registration Remote.....	250
Table 16-2 EXI Example: Registration Remote.	252
Table 16-3 POX Example: Registration Local.	254
Table 16-4 POX Example: Discovery Function Set Assignment	256
Table 16-5 POX Example: Discovery Without Function Set Assignment.	258
Table 16-6 POX Example: Discovery Undirected Without Function Set Assignment.	260
Table 16-7 POX Example: Subscription / Notification.	262
Table 16-8 EXI Example: Subscription / Notification.	263
Table 16-9 POX Example: Demand Response – General.	264
Table 16-10 POX Example: Demand Response - Cancel.	268
Table 16-11 POX Example: Distributed Energy Resource - General.	271
Table 16-12 POX Example: Meter Reading.....	275
Table 16-13 POX Example: Metering Interval.....	280
Table 16-14 POX Example: Metering Instantaneous.	285
Table 16-15 POX Example: Meter Mirroring.	289
Table 16-16 POX Example: Pricing TOU.....	302
Table 16-17 POX Example: Billing Period.....	307
Table 16-18 POX Example: Billing Historical.	310
Table 16-19 POX Example: Billing Projection.....	313
Table 16-20 File Load: Flow Description.....	316
Table 16-21 POX Example: Flow Reservation - General.	319
Table 16-22 POX Example: Flow Reservation - Cancel	323
Table 16-23 Ramp Value.....	326
Table 16-24 Event Ramp Time.....	327
Table 16-25 Event Start Time.	328
Table 16-26 Event Start Time.	328
Table 16-27 Event Start Time.	329
Table 16-28 Event Start Time.	329
Table 16-29 Event Start Time.	330
Table 17-1 TOU Rate.....	333
Table 17-2 Consumption-based Rates.....	334
Table 17-3 Tariff Structure.....	334

List of Figures

Figure 8-1: Example Device Authentication Procedure Using HTTPS Port 443	49
Figure 8-2: Device authentication with registration procedure examples using HTTPS	53
Figure 8-3: SEP 2 including ZigBee IP deployment.....	55
Figure 12-1: Active and Reactive Power Flow Directions as Measured at the DER.....	122
Figure 12-2: Example Volt-VAr Curve and Hysteresis.....	124
Figure 12-3: Example Low and High - Voltage Ride Through Curves.....	124
Figure 13-1: Allowed and Disallowed Extension.....	130
Figure 15-1: Version Information	153
Figure 15-2: DeviceCapability	153
Figure 15-3: Identification	154
Figure 15-4: Events	157
Figure 15-5: Programs	157
Figure 15-6: Error.....	158
Figure 15-7: Types	160
Figure 15-8: Primitive Types	171
Figure 15-9: SelfDevice	173
Figure 15-10: EndDevice.....	174
Figure 15-11: FunctionSetAssignments	176
Figure 15-12: Pub-Sub	177
Figure 15-13: Response	179
Figure 15-14: Time.....	181
Figure 15-15: DeviceInformation.....	182
Figure 15-16: PowerStatus	185
Figure 15-17: NetworkStatus.....	187
Figure 15-18: LogEvents	192
Figure 15-19: Configuration.....	194
Figure 15-20: Files.....	196
Figure 15-21: DRLC Event	199
Figure 15-22: Load Shed Availability.....	200
Figure 15-23: Metering Data	203
Figure 15-24: Metering Data Types	204
Figure 15-25: Metering Mirror	207
Figure 15-26: Metering Mirror Inheritance	208
Figure 15-27: Pricing.....	210
Figure 15-28: TextMessage.....	214
Figure 15-29: Billing	216
Figure 15-30: Billing Readings.....	217
Figure 15-31: Prepayment	221
Figure 15-32: FlowReservation	226
Figure 15-33: DER Info	228
Figure 15-34: DER Info Types.....	229
Figure 15-35: DER Program.....	229
Figure 15-36: DER Curves	230
Figure 15-37: DER Control	231
Figure 15-38: DER Control Types	232
Figure 16-1: Remote Registration.....	250

Figure 16-2: Registration Local	253
Figure 16-3: Discovery: Function Set Assignment	256
Figure 16-4: Discovery Without Function Set Assignment	258
Figure 16-5: Discovery Undirected Without Function Set Assignment	260
Figure 16-6: Subscription / Notification	261
Figure 16-7: Demand Response General	264
Figure 16-8: Demand Response - Cancel	268
Figure 16-9: Distributed Energy Resource: General	270
Figure 16-10: Meter Reading.....	275
Figure 16-11: Metering Interval.....	280
Figure 16-12: Metering Instantaneous	285
Figure 16-13: Meter Mirroring	289
Figure 16-14: Pricing Time of Use.....	302
Figure 16-15: Billing Period.....	307
Figure 16-16: Billing Historical	310
Figure 16-17: Billing Projection.....	313
Figure 16-18: File Load - FlowDiagram	315
Figure 16-19: Flow Reservation: General	318
Figure 16-20: Flow Reservation: Cancel	322
Figure 16-21: Simple Event - No Ramp Up - No Ramp Down	326
Figure 16-22: Event with Positive Randomization Duration	327
Figure 16-23: Event with Positive Randomization Start	328
Figure 16-24: Event with Negative Randomized Start	328
Figure 16-25: Positive Randomization in an Hour	329
Figure 16-26: Event with Negative Start in One Hour	329
Figure 16-27: Randomized Start and Long Ramp Up.....	330
Figure 16-28: Randomized Start and Fixed End Time	331

1 Introduction

1.1 Purpose

The purpose of this document is to define the application protocol used by the Smart Energy Profile release 2.0. The Smart Energy Profile Application Protocol 2.0 is designed to meet the requirements stated in the Smart Energy Profile 2.0 Marketing Requirements Document (SEP 2 MRD) [ZB 09-5162] and the Smart Energy Profile 2.0 Technical Requirements Document (SEP 2 TRD) [ZB 09-5449]. Per *Req[DataModel-1]*, this application protocol is an IEC 61968 common information model [61968] profile, mapping directly where possible, and using subsets and extensions where needed, and follows a RESTful architecture [REST].

1.2 Scope

With respect to the OSI network model, the Smart Energy Profile 2.0 Application Protocol is built using the four layer Internet stack model. This specification defines the 'APPLICATION' layer with TCP/IP providing functions in the 'TRANSPORT' and 'INTERNET' layers. Depending on the physical layer in use (e.g., 802.15.4, 802.11, 1901), a variety of lower layer protocols may be involved in providing a complete solution. Generally, lower layer protocols are not discussed in this document except where there is a direct interaction with the application protocol. The scope of this document is defining the mechanisms for exchanging application messages, the exact messages exchanged including error messages, and the security features used to protect the application messages.

1.3 Context Overview

The Smart Energy Profile 2.0 Application Protocol is proposed to the ZigBee Alliance and the HomePlug Powerline Alliance to meet the needs specified in the SEP 2 MRD and TRD. The Smart Energy Profile 2.0 has been identified as a "standard for implementation" in NIST's Framework and Roadmap for Smart Grid Interoperability Standards [NIST 1108]. As such, this document may be useful for anyone developing a Smart Grid solution.

All statements and descriptions made in this document on Smart Energy Profile, SEP, or SE are references to the Smart Energy Profile 2.0 Application Profile.

1.4 Document Organization

The following documents comprise the definition of SEP 2 and all SEP 2 devices will be required to maintain compliance to these documents:

- SEP 2 Application Protocol Specification (this document)
- SEP 2 XML Schema Definition (XSD) (sep.xsd in [ZB 13-0201])
- SEP 2 WADL (sep_wadl.xml in [ZB 13-0201])

The SEP 2 XSD contains the definitions of the SEP 2 resources, attributes, and elements as well as their textual descriptions. The SEP 2 WADL contains the recommended URI structures and use of HTTP methods associated with these objects. In addition a SEP 2 UML model (also contained in [ZB 13-0201]) has been utilized in the creation of the SEP 2 XSD. The SEP 2 UML model is an

informative document. Informative textual extracts of the SEP 2 XSD and the SEP 2 WADL are contained in this document for convenience.

1.5 Requirement Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document, when capitalized and in a normative section, constitute normative text and are to be interpreted as described in [RFC 2119].

1.6 Typography Conventions Used

Example URIs, protocol requests, protocol responses, and XML are presented in `fixed-width Courier New font, with a size of 8.`

1.7 Design Principles

As per the ZigBee Smart Energy Profile 2.0 Technical Requirements Document (TRD) [ZB 09-5449] Section 10.1, Smart Energy Profile 2.0 will follow a RESTful architecture [REST]. The TRD lists a large number of general design principles. Several specific ones are important for the application protocol:

- While devices MAY maintain state, interfaces SHOULD be stateless.
- URI structure SHOULD be clear but as efficient as possible.
- Minimize the number of transactions required to achieve a given function.

2 Acknowledgements

On behalf of the ZigBee Alliance, the HomePlug Powerline Alliance, and all of our liaison partners, we would like to extend our thanks to all who participated in the development of this specification.

Representatives from many organizations have participated in weekly calls, face-to-face meetings, email exchanges, and specialized editing sessions. Without the broad support from both member and external organizations that care about the development of smart energy solutions, this work would not have been possible. Select individuals stand out for their contributions to this document.

When this document was released, the Smart Energy Profile 2 Working Group leadership was composed of the following members:

Robby Simpson: Chair

Tim Gillman: Vice-chair

Jeff Shudark: Secretary

Don Sturek: Program Manager

Tobin Richardson: ZigBee Alliance Chairman and CEO

Steven Van Ausdall: Model, XSD, and WADL Editor

Al Petrick: Application Specification Editor

Our special thanks to the following members who contributed to the document:

Casey Anderson	Ed Eckert	Ricardo Montano
Skip Ashton	Gene Falendysz	Tim Moses
Dan Bailey	Matthew Gillmore	Leslie Mulder
Gary Birk	Tom Herbst	Don Olsen
Donald Bowen	Lance Hester	Ivan O'Neill
Doug Burman	Ken Holbrook	Barry Peirce
Paul Carreon	Shawn Hu	Joseph Reddy
Stephen Chasko	Rajagopal Iyengar	Emil Romascanu
Michael Cowan	Jeffrey King	David Smith
Robert Cragie	David Kravitz	Michael StJohns
Wayne Dennison	Chris Leclercq	Michael Stuber
Yusuke Doi	Kerry Lynn	Mark Ward
Jeff Drake	Zahra Makoui	
Paul Duffy	Tony Mauro	

3 Document Revision History

Revision	Version	Description
00	2.0	Smart Energy Profile 2

4 References

External references in this document are tagged with a document reference identifier placed inline within the text. The references section maps these identifiers to document titles and provides hyperlinks to where the source document may be obtained. Please note, not all referenced documents are freely available. Selected documents may require a membership, subscription, or fee to obtain.

4.1 Smart Energy 2.0 Documents

- [ZB 09-5162] ZigBee + HomePlug Joint Working Group Smart Energy Profile Market Requirements Document ([09-5162](#)).
<http://www.zigbee.org/Standards/ZigBeeSmartEnergy/HomePlugMarketingRequirementDocument.aspx>
- [ZB 09-5449] Smart Energy Profile Technical Requirements Document ([09-5449](#)).
<http://www.zigbee.org/Standards/ZigBeeSmartEnergy/20TechnicalRequirementsDoc.aspx>
- [ZB 13-0201] Smart Energy 2.0 UML Model ([13-0201](#)).

4.2 IEC Documents

- [61850] Communication networks and systems in substations - ALL PARTS (<http://webstore.iec.ch>).
- [61968] Application integration at electric utilities - System interfaces for distribution management – ALL PARTS (<http://webstore.iec.ch>).

4.3 IETF Documents

- [RFC 768] User Datagram Protocol (<http://tools.ietf.org/html/rfc768>).
- [RFC 793] Transmission Control Protocol (<http://tools.ietf.org/html/rfc793>).
- [RFC 1630] Universal Resource Identifiers in WWW (<http://tools.ietf.org/html/rfc1630>).
- [RFC 1738] Uniform Resource Locators (<http://tools.ietf.org/html/rfc1738>).
- [RFC 1808] Relative Uniform Resource Locators (<http://tools.ietf.org/html/rfc1808>).
- [RFC 2119] Key words for use in RFCs to Indicate Requirement Levels (<http://tools.ietf.org/html/rfc2119>).
- [RFC 2560] X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, IETF, M. Meyers et al, June 1999, (<http://tools.ietf.org/html/rfc2560>).
- [RFC 2616] Hypertext Transfer Protocol - HTTP/1.1 (<http://tools.ietf.org/html/rfc2616>).
- [RFC 2717] Registration Procedures for URL Scheme Names (<http://tools.ietf.org/html/rfc2717>).
- [RFC 2818] HTTP Over TLS (<http://tools.ietf.org/html/rfc2818>).
- [RFC 2863] The Interface MIB (<https://tools.ietf.org/html/rfc2863>).
- [RFC 3535] IAB Network Management Workshop (<http://tools.ietf.org/html/rfc3535>).

- [RFC 3635] Definitions of Management Objects for the Internet-Like Interface Types (<http://tools.ietf.org/html/rfc3625>).
- [RFC 4108] Using Cryptographic Message Syntax (CMS) to Protect Firmware, IETF, R. Housley, April 2005, (<http://tools.ietf.org/html/rfc4108>).
- [RFC 4193] Unique IPv6 Unicast Addresses (<http://tools.ietf.org/html/rfc4193>).
- [RFC 4291] IP Version 6 Addressing Architecture (<http://tools.ietf.org/html/rfc4291>).
- [RFC 4293] Management Information Base for the Internet Protocol (IP) (<http://tools.ietf.org/html/rfc4293>).
- [RFC 5246] Transport Layer Security (TLS) Protocol V1.2 (<http://tools.ietf.org/html/rfc5246>).
- [RFC 5280] Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, IETF, D Cooper et al, May 2008, (<http://tools.ietf.org/html/rfc5280>).
- [RFC 5480] Elliptic Curve Cryptography Subject Public Key Information, IETF, S. Turner et al., March 2009, (<http://tools.ietf.org/html/rfc5480>).
- [RFC 6550] RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks (<http://tools.ietf.org/html/rfc6550>).
- [RFC 6554] An IPv6 Routing Header for Source Routes with the Routing Protocol for Low-Power and Lossy Networks (RPL) (<http://tools.ietf.org/html/rfc6554>).
- [RFC 6762] Multicast DNS (<http://tools.ietf.org/html/rfc6762>).
- [RFC 6763] DNS Based Service Discovery (<http://tools.ietf.org/html/rfc6763>).
- [I-D AESCCM] AES-CCM ECC Cipher Suites for TLS (<https://docs.zigbee.org/zigbee-docs/dcn/12/docs-12-0462-00-SEP 2-aes-ccm.pdf>).
- [I-D XMDNS] Extended Multicast DNS (<https://docs.zigbee.org/zigbee-docs/dcn/12/docs-12-0461-00-SEP 2-xmdns.pdf>).

4.4 Other References

- [ASN.1] ITU-T Recommendation X.680 – Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation, ITU, July 2002.
- [CSEP] Consortium for SEP 2 Interoperability (<http://www.csep.org>).
- [DOCSIS] DOCSIS (<http://cablelabs.com/cablemodem/specifications/index.html>).
- [EPRI] Common Functions for Smart Inverters. EPRI, Palo Alto, CA: 2011. Product ID Number 1023059 (<http://my.epri.com/portal/server.pt?space=CommunityPage&cached=true&parentname=ObjMgr&parentid=2&control=SetCommunity&CommunityID=221&PageIDqueryComId=0>).
- [EXI] Efficient XML Interchange (EXI) Format 1.0 (<http://www.w3.org/TR/2008/WD-exi-20080919/>).

- [EXIBP] Efficient XML Interchange (EXI) best practices (<http://www.w3.org/TR/exi-best-practices/>).
- [Fielding] Fielding, Roy Thomas (2000), "Architectural Styles and the Design of Network-based Software Architectures", Doctoral Dissertation, University of California, Irvine (<http://www.ics.uci.edu/~fielding/pubs/dissertation/top.html>).
- [IEEE 802.1AR].....Standard for Local and Metropolitan Area Networks: Secure Device Identity, IEEE, 2009 (<http://www.ieee802.org/1/pages/802.1ar.html>).
- [ISO 4217] Codes for the representation of currencies and funds (http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=46121).
- [Linux] Linux (<https://www.linux.com/>).
- [NIST-1108] NIST framework and roadmap for Smart Grid Interoperability Standards, Release 1.0. (http://collaborate.nist.gov/twikisggrid/pub/SmartGrid/IKBFramework/NISTFrameworkAndRoadmapForSmartGridInteroperability_Release1final.pdf).
- [NIST SP800-131A] Transition: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths (<http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf>).
- [NIST SP800-131B].....Transition: Validation of Transitioning Cryptographic Algorithm and Key Lengths (http://csrc.nist.gov/publications/drafts/800-131B/draft-SP800-131B_February2011.pdf).
- [NIST SP800-131C].....Transitions: Validating the Transition from FIPS 1862 to FIPS 1863 (http://csrc.nist.gov/publications/drafts/800-131C/draft-SP800-131C_February2011.pdf).
- [PEN] Internet Authority Assignment numbers (IANA) PEN (<http://pen.iana.org/pen/PenApplication.page>).
- [REST] Representational State Transfer (http://www.ics.uci.edu/~fielding/pubs/dissertation/rest_arch_style.htm).
- [SunSpec].....SunSpec Alliance Inverter Control Model, work in progress. (<http://www.sunspec.org/specifications/>).
- [WADL] Web Application Description Language (<http://www.w3.org/Submission/wadl/>).
- [XML] Extensible Markup Language (<http://www.w3.org/TR/REC-xml/>).

5 Definitions, Acronyms and Abbreviations

5.1 Acronyms and Abbreviations

This subsection provides a list of acronyms and abbreviations introduced in this document. For a comprehensive treatment of acronyms and abbreviations used, please refer to Section 4 of the Smart Energy Profile Technical Requirements Document [ZB 09-5449].

ACL	Access Control List
CA.....	Certificate Authority
CRL.....	Certificate Revocation List
CSEP.....	Consortium for SEP 2 Interoperability
DER	Distributed Energy Resource
DNS	Domain Name System
DNS-SD	DNS-based Service Discovery
DRLC.....	Demand Response and Load Control
ECDSA	Elliptic Curve Digital Signature Algorithm
EMS	Energy Management System
ESI	Energy Services Interface
EVSE	Electric Vehicle Supply Equipment
EXI.....	Efficient XML Interchange
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
IP	Internet Protocol
LFDI	Long Form Device Identifier
MCA	Manufacturer's CA
MICA	Manufacturing Issuing CA
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKI.....	Public Key Infrastructure
REST.....	Representational State Transfer
SERCA.....	Smart Energy Root CA
SFDI.....	Short Form Device Identifier
TCP.....	Transmission Control Protocol
UOM.....	Units of Measure
URI	Uniform Resource Identifier
XML	Extensible Markup Language



WADL Web Application Description Language

5.2 Definitions

A limited set of terms specific to this application specification are introduced below. For a comprehensive treatment of the terms used, please refer to Section 4 of the Smart Energy Profile Technical Requirements Document [ZB 09-5449].

ACCESS CONTROL LIST

A security mechanism in which entities and authorizations (e.g., read, write, create, delete) are related to resources to determine the entities' allowed operations on the resources.

CERTIFICATE AUTHORITY

An entity that issues digital certificates for use by other entities.

CERTIFICATE CHAIN

A chain of certificates, with each certificate's signature verified using the key from the next certificate in the chain. The single exception is the certificate at the end of the chain (the trust anchor), known as the root CA certificate, which is self signed.

CLIENT

The device or host that interacts with a server to obtain information related to a resource hosted by the server.

DEVICE CERTIFICATE

A digital certificate installed within a device that binds the device identity to the device. Device Certificates are exchanged by network access control and application protocols to authenticate devices as genuine SEP 2 and further to prove specific device identity.

ENERGY SERVICES INTERFACE (ESI)

A device, with multiple network interfaces, which is a member of both the home smart energy network and a service provider's private network. This is the primary mechanism for the service provider to contribute data and directives into the smart energy network and to receive responses from smart energy devices.

FINGERPRINT

This is the result of summarizing a certificate with a secure hash function. The fingerprint is generally expressed as a hex string. It is used to confirm the integrity of a certificate obtained over an untrusted channel.

FUNCTION SET

A logical grouping of resources that cooperate to implement SEP 2 features (e.g., Metering, Demand Response and Load Control).

FUNCTION SET ASSIGNMENTS

A logical addressing mechanism in SEP 2 that allows devices to be directed to use specific resources (e.g., to facilitate a device's participation in a program). Please see Section 10.5 for details.

HOST

This is the representation of a device in its application context. Typically represented by an IP address or domain name.

INTERMEDIATE CA

A CA below the root CA that issues certificates to subordinate CA's.

ISSUING CA

A CA that issues certificates to devices or code-signers.

MANUFACTURER'S CA (MCA)

An Intermediate CA operated by a specific manufacturer for the purpose of issuing MICA's for that manufacturer.

MANUFACTURING ISSUING CA (MICA)

An Issuing CA that issues certificates to devices during the manufacturing process.

MANUFACTURING PKI

The set of CAs that issue certificates to devices during the manufacturing process. The set includes the Smart Energy Root CA, Manufacturer's CA's and Manufacturing Issuing CA's.

NODE

This is the representation of a device in its network context, typically represented as an IP address.

OID

Object identifier. An OID consists of a node in a hierarchically-assigned namespace, formally defined using the ITU-T's ASN.1 standard [ASN.1].

PEM FORMAT CERTIFICATE

An X.509 certificate that has been Base64 encoded and wrapped in "-----BEGIN CERTIFICATE-----", "-----END CERTIFICATE-----" sentinels for transport as a text file or block.

PKI

Public Key Infrastructure. A set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates.

REGISTERED

The state of a device with regards to a particular server wherein an EndDevice record for the device has been populated on the server and that record contains a valid registration record. These records are typically populated with device information transmitted out-of-band to the server's owner.

RESOURCE

URI addressable object that is manipulated via the RESTful uniform interface.

RESOURCE DISCOVERY

The process whereby Clients identify Resources being served on the network. Clients issue a request to all devices on the network requesting resource(s) of interest. Servers hosting the requested resource(s) respond with information necessary to access the Server and its resource(s).

ROOT CA

A CA whose certificate or public key is a trust anchor for any other certificates in a chain of trust.

ROOT CERTIFICATE

The Root CA's self-signed certificate. Generally also a Trust Anchor.

SELF-SIGNED CERTIFICATE

A certificate whose issuer and subject are identical, and whose public key verifies its signature.

SERVER

The device or host that holds a resource and exposes representations of that resource.

SMART ENERGY ROOT CA (SERCA)

The top-level CA for the SEP 2 Manufacturing PKI.

TRUST ANCHOR

The root of trust for a certificate chain. This is an authoritative entity represented by a public key and associated data and is generally provided in the SEP 2 hierarchy in the form of a self-signed certificate.

TRUSTED ROOT STORE

An integrity-protected location for storing root certificates.



6 Design Pattern

6.1 Protocol Flexibility

The Smart Energy Profile is designed to implement a REST architecture. It is built around the core actions of GET, HEAD, PUT, POST, and DELETE (as used in [REST]), with the addition of a lightweight subscription mechanism as discussed in Section 10.6. Any application protocol that can implement a RESTful command set could likely be used with SEP 2, but HTTP is a required baseline for interoperable SEP 2 implementations. HTTP utilizes TCP as its transport protocol. As a result, TCP manages the session providing delivery assurance and windowing.

Smart Energy Profile 2.0 servers and clients SHALL be compliant with [RFC 2616].

6.2 General Rules / Best Practices

This specification shall not make distinctions between servers, clients, or devices, when defining interfaces and URIs. The goal is to avoid having a resource that has one behavior on a server and a different behavior on a client or different type of server. The distinction between the server and client role depends on whether a device exposes a resource (server) or interacts with the resource (client).

The default mechanism for obtaining a resource representation is a pull mechanism, implemented with GET. A client requests and retrieves data from a server or creates, modifies, or deletes data on a server.

The use of a subscription mechanism for retrieving a resource representation is also optionally supported, where convenient and appropriate. Resources that support subscription are denoted by their subscribable attribute.

Objects have a defined granularity and whole objects (not partial objects) are to be updated with the granularity defined in the schema.

Clients that expect to have intermittent connections to the network (e.g., battery-powered sleepy devices, mobile devices, etc.) use a pull mechanism as their default behavior for resource retrieval, as a subscription / notification mechanism may not be reliable. It should be noted that clients that expect to have intermittent connections to the network may still POST, PUT, and DELETE resources, provided they have the appropriate security permissions.

The TCP ports used for HTTP or HTTPS SHALL be specified in the xmDNS service advertisement for the service.

Content SHALL be transferred with either one of the content types: "application/sep+xml" or "application/sep-exi".

Devices do not assume the use of the URIs and their structures given throughout this specification. All resources are self-describing as it is acknowledged that URIs, schemas, and resources might change in the future. All resources SHALL contain links to their subordinate resources to support flexibility in URIs and future extensibility. Thus, to allow for extensibility and granularity, all objects are described in schemas and referenced via URIs. The URIs presented throughout this specification are recommendations. Thus, clients do not assume that URIs for resources are fixed on all servers or even on a given server (over time), but rather retrieve the appropriate URIs through resource discovery and links within resources. For network efficiency, devices MAY assume URIs are fixed on a particular server over time. If a URI returns an unexpected result, the client SHOULD execute resource discovery to determine the new URI value.



Version information should not be presented in the URI unless that version information is inherent to the name of that resource. If necessary and for reasons of extensibility, version information is provided within the associated resources and / or schemas.

All values in XML and EXI SHOULD be represented as compactly as possible. Decimal values SHOULD be represented without leading zeros. Hexadecimal values SHALL be represented with one leading zero, if needed, to ensure an even number of digits.

6.3 WADL

The SEP 2 RESTful interface is defined using the Web Application Description Language (WADL) [ZB 13-0201].

Smart Energy Profile 2.0 devices SHALL conform to the interface specifications contained in the WADL as follows.

- Devices SHALL conform to the WADL specification as per [WADL].
- Devices SHALL conform to the WADL definition in [ZB 13-0201]. By implication, all resource representations SHALL validate per the schema [ZB 13-0201] within the standardized SEP XML namespace (<http://zigbee.org/sep>).
- Compliance (MODE) designations are interpreted as follows.
 - Mandatory ("M") - Devices MUST implement and conform.
 - Optional ("O") - Devices MAY implement, and if implemented, MUST conform.
 - Discouraged ("D") - Devices SHOULD NOT implement, but if implemented, MUST conform.
 - Error ("E") - Devices MUST return one of the specified response status codes (e.g. 400 – Bad Request or 405 – Method Not Allowed).

6.4 Schema

- Resources located at URIs returned in the href attribute of "Link" specializations (e.g., EndDeviceListLink, SelfDeviceLink) SHALL conform to the schema definition for that object, which is the tag name with the "Link" suffix removed. For example, the resource at SelfDeviceLink href follows the definition for the SelfDevice resource.
- If a client PUTs or POSTs a resource to a server containing attributes or elements that instead are to be populated by the server (e.g., href), the server SHALL return an HTTP 400 error.
- If a function set is not implemented, Link elements to resources in that function set SHALL NOT be included.

6.5 Uniform Resource Identifiers

HTTP uses ASCII text for transferring URIs between clients and servers, as well as for including options and details regarding the message content. These transfers occur with every transaction. If the naming scheme used for URIs is overly verbose, these transactions become needlessly inefficient on constrained networks. Of course, if the naming scheme used is overly cryptic, the advantages of a text-based protocol are lost, and it becomes difficult for someone troubleshooting to decipher a transaction.

The following conventions are used for URI naming:

- 1) URI elements are at most 4 characters, but recognizable to a knowledgeable engineer. Element names as short as 1 character are acceptable provided their meaning is clear.
- 2) URI elements are constructed of consonants only, unless inclusion of a vowel adds clarity, such as a leading vowel or well-known abbreviation.

- 3) URI elements are in all lower case.
- 4) URIs SHALL NOT be greater than 255-bytes in length. In practice, URIs SHOULD be much smaller than 80-bytes.

6.6 List Resources

Many resources within this specification are derived from the <List> object. Throughout this specification, these resources will collectively be referred to as list resources.

The following attributes are defined for list resources:

- `all` – used to indicate the total number of items (subordinate resources) that exist in the list resource. This number may vary according to the client's access privileges.
- `results` – used to indicate the number of items (subordinate resources) included in a specific subset of the list (result from a paged GET query to the list, etc.). This value will always be less than or equal to 'all'.

Clients and servers use these attributes, combined with the query string parameters described below, to implement paged access to lists. Client control of list paging is important for resource-constrained devices.

List items (subordinate resources) are read using one of the two idioms described below:

- 1) Ordinal access to the first, second, nth, etc. item in the list is supported via query string parameters included with a GET to the list resource URI.
- 2) Random access to specific list items is supported via a GET directly to the URI of the list item.

Some list items may be written by POSTing a list item representation to the URI of the list. (e.g., notifications), while others may be created using private interfaces over the provider network. Ordinal placement of the new resource within the list is determined by the list sort order (defined by each list).

Each function set defined in this specification that contains list resources includes a List Ordering table. Each list resource has an entry in the corresponding table that describes the details of one or more unique sort keys and the precedence of those keys. A list resource's elements SHALL be ordered according to this specified List Ordering.

6.6.1 Query String Parameters

Query string parameters are parameters added to a URI to provide filtering / paging of list items returned in query results.

The list paging mechanism allows GET requests to specify the range of list items to be returned in a query result set. The general syntax of a paged query is as follows:

{URI}?s={x}&a={y}&l={z}

Where {URI} represents a URI used to address a list resource, (s | a | l) represent query string parameters (further defined below), and {x}, {y}, and {z} represent the respective query string parameter values.

The query string parameters are defined as:

- `s` – ("start") is used to indicate the first ordinal position in the list to be returned in the query result list as determined by the list's ordering. The value is specified in decimal. The first ordinal position of the list SHALL be designated with a value of '0' and the maximum possible value is '65535'. If this query string parameter is not specified, the default start value SHALL be '0'.

- `a` – ("after") is used to indicate that only items whose primary key occurs after the given date / time parameter should be included in the query result list. This query string parameter is only applied to list resources that are ordered using a time-based primary key. The parameter SHALL be ignored if the primary key is not time-based. The format of the parameter SHALL be a 64-bit decimal number with identical semantics as that of the TimeType (see Section 12.2 and the XML XSD in [ZB 13-0201]).
- `1` – ("limit") is used to set the maximum number of list items (up to 255) to be included in the query result list. The value is specified in decimal. If this query string parameter is not specified, the default limit SHALL be '1'. Servers MAY return a result list smaller than that specified by the client provided limit.

If both a "start" and "after" query string parameter are used simultaneously, the "after" query string parameter SHALL have precedence. The "start" position 0 SHALL be relative to the position specified by the "after" parameter.

If a query string requests a list element that does not exist (e.g., `s=3` when there are two items in the list), servers SHALL return an empty list representation.

Readers should note that the "after" query string parameter SHOULD NOT be used alone for paging through a list. As some list resources MAY contain multiple subordinate resources with the same time-based primary key, it is RECOMMENDED that clients wishing to paginate a list resource while using the "after" query string parameter should keep the value for the "after" query string parameter constant while changing the "start" query string parameter.

If a particular query string parameter appears more than once, then the first occurrence of the query string parameter SHALL be used (in left-to-right order) and subsequent occurrences MUST be ignored.

Server receipt of a query parameter unknown to the server MUST be ignored by the server and MUST NOT generate an HTTP error. Servers MUST NOT generate resource representations containing `href` attributes that contain query parameters. Clients MUST ignore query parameters contained in resource `hrefs`, but SHOULD NOT remove them if the URI is used for subsequent RESTful exchanges.

Should an empty list representation be requested (either through the use of query string parameters such as `1=0` or when the list itself is empty), the server SHALL return no subordinate representations, but SHALL return any other elements that may be defined for the list.

Clients MUST NOT assume any index semantics for list URIs. For example, a client desiring to read the 3rd item from the list at `http://some-host/somelist` MUST NOT assume a GET to `http://some-host/somelist/2` will return the third item. The correct access is supported by the client issuing a GET to `http://some-host/somelist?s=2&l=1`.

The following examples demonstrate the use of query string parameters with a list resource. Consider the MyTypeList resource, depicted below:

```
<MyTypeList href="http://host1/the/list" all="7" results="7">
  <MyType href="http://host1/instance/of/type/red">
    <timeStamp>100</timeStamp>
  </MyType>
  <MyType href="http://host2/instance/of/type/green">
    <timeStamp>200</timeStamp>
  </MyType>
  <MyType href="http://host3/instance/of/type/blue">
    <timeStamp>300</timeStamp>
  </MyType>
  <MyType href="http://host4/instance/of/type/yellow">
    <timeStamp>400</timeStamp>
  </MyType>
  <MyType href="http://host5/instance/of/type/black">
    <timeStamp>500</timeStamp>
  </MyType>
</MyTypeList>
```

```

    <MyType href="http://host6/instance/of/type/white">
      <timeStamp>600</timeStamp>
    </MyType>
    <MyType href="http://host7/instance/of/type/orange">
      <timeStamp>700</timeStamp>
    </MyType>
  </MyTypeList>

```

This list is sorted in ascending order per the `<timeStamp/>` element of `MyType`.

A GET to `http://host1/the/list?s=0&l=1` will return:

```

<MyTypeList href="http://host1/the/list" all="7" results="1">
  <MyType href="http://host1/instance/of/type/red">
    <timeStamp>100</timeStamp>
  </MyType>
</MyTypeList>

```

A GET to `http://host1/the/list?s=0&l=5` will return:

```

<MyTypeList href="http://host1/the/list" all="7" results="5">
  <MyType href="http://host1/instance/of/type/red">
    <timeStamp>100</timeStamp>
  </MyType>
  <MyType href="http://host2/instance/of/type/green">
    <timeStamp>200</timeStamp>
  </MyType>
  <MyType href="http://host3/instance/of/type/blue">
    <timeStamp>300</timeStamp>
  </MyType>
  <MyType href="http://host4/instance/of/type/yellow">
    <timeStamp>400</timeStamp>
  </MyType>
  <MyType href="http://host5/instance/of/type/black">
    <timeStamp>500</timeStamp>
  </MyType>
</MyTypeList>

```

A GET to `http://host1/the/list?s=5&l=1` will return:

```

<MyTypeList href="http://host1/the/list" all="7" results="1">
  <MyType href="http://host6/instance/of/type/white">
    <timeStamp>600</timeStamp>
  </MyType>
</MyTypeList>

```

A GET to `http://host1/the/list?s=5&l=5` will return:

```

<MyTypeList href="http://host1/the/list" all="7" results="2">
  <MyType href="http://host6/instance/of/type/white">
    <timeStamp>600</timeStamp>
  </MyType>
  <MyType href="http://host7/instance/of/type/orange">
    <timeStamp>700</timeStamp>
  </MyType>
</MyTypeList>

```

A GET to `http://host1/the/list?s=12&l=2` will return a list representation containing 0 items:

```

<MyTypeList href="http://host1/the/list" all="7" results="0">
</MyTypeList>

```

OR `<MyTypeList href="http://host1/the/list" all="7" results="0" />`



A GET to `http://host6/instance/of/type/white` will return:

```
<MyType href="http://host6/instance/of/type/white">
  <timestamp>600</timestamp>
</MyType>
```

A GET to `http://host1/the/list?a=400&l=4` will return:

```
<MyTypeList href="http://host1/the/list" all="7" results="3">
  <MyType href="http://host5/instance/of/type/black">
    <timestamp>500</timestamp>
  </MyType>
  <MyType href="http://host6/instance/of/type/white">
    <timestamp>600</timestamp>
  </MyType>
  <MyType href="http://host7/instance/of/type/orange">
    <timestamp>700</timestamp>
  </MyType>
</MyTypeList>
```

A GET to `http://host1/the/list?a=400&s=0&l=2` will return:

```
<MyTypeList href="http://host1/the/list" all="7" results="2">
  <MyType href="http://host5/instance/of/type/black">
    <timestamp>500</timestamp>
  </MyType>
  <MyType href="http://host6/instance/of/type/white">
    <timestamp>600</timestamp>
  </MyType>
</MyTypeList>
```

A GET to `http://host1/the/list?a=400&s=2&l=2` will return:

```
<MyTypeList href="http://host1/the/list" all="7" results="1">
  <MyType href="http://host7/instance/of/type/orange">
    <timestamp>700</timestamp>
  </MyType>
</MyTypeList>
```

6.7 Resource Design Rules

The following rules apply to the design and use of list resources:

- List resources SHALL support "start" and "limit" query string parameters, thus always supporting paging.
- List resources that have a time-based primary key SHALL support the "after" query string parameters.
- All subordinate resources of list resources SHALL include an `href` attribute containing the URI of the subordinate resource.
- Each list resource described in this specification includes a List Ordering that defines how the list is ordered, including the details of one or more keys used to order the list and the precedence of these keys.
- When queried, list resources SHALL return subordinate resources in the order defined by the List Ordering.
- All subordinate resources of list resources that support multiple types, e.g., NotificationList, SHALL include an `xsi:type` attribute. In this case, the XML Schema Instance Namespace must also be declared. See Section 16 for examples.

The following rules apply to the design and use of non-list resources:

- Non-list resources SHALL NOT support the defined query string parameters. Query string parameters applied to non-list resource URIs SHOULD be ignored.



7 Application Support

7.1 Overview

This section details the standards-based application transport protocol and other lower-layer requirements required for interoperability of SEP 2 devices.

The application support layer provides the following services:

- RESTful HTTP/1.1 as the application data exchange semantics, as described in [RFC 2616] and [Fielding].
- XML [XML] and / or EXI [EXI] encoding as the data payload of the RESTful operations.
- Transport authentication and encryption using TLS over HTTP [RFC 2818] and [RFC 5246].

7.2 Use of TCP

The choice of HTTP/1.1 as the application data exchange protocol leads directly to the use of TCP as the transport protocol. [RFC 2616] states that:

"HTTP communication usually takes place over TCP / IP connections. The default port is TCP 80 [19], but other ports can be used. This does not preclude HTTP from being implemented on top of any other protocol on the Internet, or on other networks. HTTP only presumes a reliable transport; any protocol that provides such guarantees can be used; the mapping of the HTTP/1.1 request and response structures onto the transport data units of the protocol in question are outside the scope of this specification."

Hence, albeit that other transport protocols may be used to carry HTTP, they are required to provide reliable transport. Clearly, the de facto choice is TCP [RFC 793].

7.3 URI Encoding

The address of the resources presented by an SEP 2 host will use the standard URI syntax specific to HTTP/1.1 (i.e., `http://`) as per [RFC 1630], [RFC 1738], and [RFC 1808].

It is recommended that SEP 2 use the formally defined and registered (IANA) URN namespace definitions to address its application level resources as referenced in [RFC 2717] and [RFC 1808].

Given the constrained nature of many SEP 2 hosts, it is critical to devise the URL namespace scheme (hierarchy) that is both descriptive and compact. For more information, see Section 6.5.

7.4 HTTP Headers

HTTP/1.1 defines a variety of header types that have the potential to be verbose. As an example, the Accept header is illustrated below showing lengths varying from 35 octets to 106 octets:

- Accept: audio/*; q=0.2, audio/basic (35 octets)
- Accept: text/*; q=0.3, text/html; q=0.7, text/html; level=1, text/html; level=2; q=0.4, */*; q=0.5 (92 octets)
- Accept: text/xml, application/xml, application/xhtml+xml, text/html; q=0.9, text/plain; q=0.8, image/png, */*; q=0.5 (106 octets)

Given the packet size constraints for many SEP 2 networks, the set of HTTP headers supported must be curtailed through best practices recommendations realizing that a host cannot prevent a verbose message from being sent to it.

SEP 2 provides a set of Mandatory, Optional, and Discouraged recommendations for each HTTP header. SEP 2 implementations SHOULD employ only Mandatory HTTP headers, minimize the use of Optional HTTP headers, and avoid the use of Discouraged headers.

7.4.1 HTTP Header Field Recommended Usage

In the following table, the HTTP/1.1 header fields have been annotated with the following labels:

- **MANDATORY:** support for the field is REQUIRED.
- **OPTIONAL:** support for this field is left to the implementer's discretion.
- **DISCOURAGED:** to conserve code space and / or bandwidth, support for this field, while not explicitly forbidden, is not recommended.

The following table summarizes the recommended use of HTTP/1.1 headers in SEP 2:

Table 7-1 HTTP Headers.

Header	Used in Message Type		RFC Required / Optional	SEP 2 Use
Accept	Request		Optional	Mandatory
Accept-Charset	Request		Optional	Discouraged
Accept-Encoding	Request		Optional	Discouraged
Accept-Language	Request		Optional	Discouraged
Accept-Ranges	Request	Response	Optional	Discouraged
Age		Response	Optional (Required for a cache)	Discouraged
Allow		Response	Required	Mandatory
Authorization	Request	Response	Optional	Discouraged
Cache-Control	Request	Response	Optional	Discouraged
Connection	Request		Optional (Required in some situations (e.g., HTTP/1.1 applications that do not support persistent connections))	Optional (Mandatory in some situations)
Content-Encoding		Response	Optional (Required when an encoding is applied)	Discouraged
Content-Language		Response	Optional	Discouraged
Content-Length	Request	Response	Optional (Required in many situations, see section 4.4 of [RFC 2616])	Optional (Mandatory in many situations, see section 4.4 of [RFC 2616])
Content-Location		Response	Optional	Discouraged
Content-MD5		Response	Optional	Discouraged

Header	Used in Message Type		RFC Required / Optional	SEP 2 Use
Content-Range		Response	Optional	Optional (see Section 11.7.1.4)
Content-Type	Request	Response	Required	Mandatory
Cookies			Optional	Discouraged
Date	Request	Response	Mandatory	Mandatory
ETag		Response	Optional	Optional (see Section 11.7.1.4)
Expect	Request		Optional	Discouraged
Expires		Response	Optional	Discouraged
From	Request		Optional	Discouraged
Host	Request		Required	Mandatory
If-Match	Request		Optional	Discouraged
If-Modified-Since	Request		Optional	Discouraged
If-None-Match	Request		Optional	Discouraged
If-Range	Request		Optional	Discouraged
If-Unmodified-Since	Request		Optional	Discouraged
Last-Modified		Response	Optional	Discouraged
Location		Response	Optional	Mandatory in many situations (e.g., POST responses)
Max-Forwards	Request		Optional	Discouraged
Pragma	Request	Response	Optional	Discouraged
Proxy-Authenticate		Response	Optional	Discouraged
Proxy-Authorization	Request		Optional	Discouraged
Range	Request		Optional	Optional (see Section 11.7.1.4)
Referrer	Request		Optional	Discouraged
Retry-After		Response	Optional	Optional (see Section 11.7.1.4)
Server		Response	Optional	Discouraged
TE	Request		Discouraged	Discouraged
Trailer		Response	Discouraged	Discouraged

Header	Used in Message Type		RFC Required / Optional	SEP 2 Use
Transfer-Encoding		Response	Optional	Discouraged
Upgrade	Request		Optional	Discouraged
User-Agent	Request		Optional	Discouraged
Vary		Response	Discouraged	Discouraged
Via	Request	Response	Optional	Discouraged
Warning	Request	Response	Discouraged	Discouraged
WWW-Authenticate		Response	Optional	Discouraged

7.5 HTTP Response Codes

Response codes are expected to be generalized across RESTful platforms. The specific uses detailed below are likely to be generalized. In the interest of clarity and completeness, they are included here. Please note that these response codes follow general best practices for RESTful interfaces, though they are tuned to address some of the limitations of the embedded space.

This sub-section attempts to highlight HTTP response codes that are felt to be more important or that need special attention from developers. However, SEP 2 clients may encounter any HTTP response code defined by [RFC 2616] and, all use of, and response to HTTP response codes SHALL be specification and RFC compliant.

7.5.1 Common Responses

The following HTTP response codes are those considered to be of utmost importance for this specification.

7.5.1.1 1xx (Informational)

These response codes are informational in purpose and are used to indicate that the server is continuing to process in some fashion.

[RFC 2616] states, "A client MUST be prepared to accept one or more 1xx status responses prior to a regular response, even if the client does not expect a 100 (Continue) status message. Unexpected 1xx status responses MAY be ignored by a user agent."

7.5.1.2 200 ("OK")

This response code is sent to indicate a successful transaction.

This response code is often used in response to a successful GET request, with the entity-body containing a representation of the requested resource. Use of this response code in response to PUT, POST, or DELETE requests is discouraged, to avoid the potentially unnecessary traffic generated by returning the resource representation in the entity-body (see 201 ("Created") and 204 ("No Content")).

7.5.1.3 201 ("Created")

This response code is sent to indicate a new resource has been created, at the client's request with a PUT or POST.

The Location header SHALL be used in conjunction with this response code to indicate the URI of the newly created resource. The inclusion of a representation of the newly created resource in the entity-body of the response is discouraged, to conserve bandwidth.

[RFC 2616] states, "If a new resource is created, the origin server MUST inform the user agent via the 201 (Created) response."

7.5.1.4 **204 ("No Content")**

This response code is sent to indicate a successful transaction, but one where the response does not include an entity-body.

This response code is often used in response to a successful PUT or POST request, where the resource is modified, not created. This response code is also sent in response to a successful DELETE request. This response code is also sent in response to a successful GET request, where the resource exists but has an empty representation.

Further, when there are URIs that point to a resource that does not yet have content (an "empty representation"), this response code SHOULD be returned. For instance, if a client created a new resource with a POST and that new resource contains URIs pointing to resources that were not yet created and then a client were to request those linked resources, this response code would be the best response. When those resources are created (via a PUT, for instance), this response code (204) SHOULD be returned (in response to the PUT, for instance).

7.5.1.5 **206 ("Partial Content")**

This response code is sent to indicate the server has fulfilled the partial GET request (as specified by the Range header) for a resource. Note that [RFC 2616] requires the Content-Range and Date headers MUST be present in the response.

7.5.1.6 **301 ("Moved Permanently")**

This response code is sent to indicate that the requested resource has a new URI. The Location header SHOULD be used in conjunction with this response code to indicate the new URI of the requested resource. The entity-body of the response SHOULD be empty. Upon unexpected receipt of this response code, clients SHOULD perform resource discovery to determine which resources have changed location.

7.5.1.7 **302 ("Redirect")**

The Location header SHALL be used in conjunction with this response code to indicate the new URI of the requested resource. The entity-body of the response SHOULD be empty.

This response code is often used to redirect URI's requested as HTTP to HTTPS.

7.5.1.8 **400 ("Bad Request")**

This response code is used to indicate a client-side error and is used when no other 4xx response code is appropriate. Often, this response code indicates that the representation sent by a client with a PUT or POST is not appropriate or is malformed.

[RFC 2616] states, "All Internet-based HTTP/1.1 servers MUST respond with a 400 (Bad Request) status code to any HTTP/1.1 request message which lacks a Host header field."

7.5.1.9 **401 ("Unauthorized")**

This response code is used when a client does not have proper authorization to perform the requested action on a resource.

Note, if a server did not wish a client to know of the existence of the resource, it should instead send a 404 ("Not Found") response code.

[RFC 2616] states, "The response MUST include a WWW-Authenticated header field containing a challenge applicable to the requested resource."

7.5.1.10 **404 ("Not Found")**

This response code is used to indicate that no resource can be found at the specified URI.

This response code MAY also be used in lieu of a 401 response code.

7.5.1.11 **405 ("Method Not Allowed")**

This response code is used to indicate that the resource does not allow the HTTP method used by the client.

[RFC 2616] states, "The response MUST include an Allow header containing a list of valid methods for the requested resource."

7.5.1.12 **406 ("Not Acceptable")**

This response code is used to indicate that a server is unable to generate a response that is acceptable according to the Accept headers sent in the request.

7.5.1.13 **413 ("Request Entity Too Large")**

This response code is used to indicate that a server is refusing to process a request, as the request is larger than the server is willing or able to process.

7.5.1.14 **416 ("Requested Range Not Satisfiable")**

This response code is used to indicate that a server has received a Range request that does not overlap any of the resource content.

[RFC 2616] states "A server sending a response with status code 416 (Requested range not satisfiable) SHOULD include a Content-Range field with a byte-range-resp-spec of "*". The instance-length specifies the current length of the selected resource. A response with status code 206 (Partial Content) MUST NOT include a Content-Range field with a byte-range-resp-spec of "*".

7.5.1.15 **417 ("Expectation Failed")**

This response code is used to indicate that an expectation given in an Expect request-header field cannot be met by the server or that the server does not support the given expectation.

[RFC 2616] states, "If a server receives a request containing an Expect field that includes an expectation-extension that it does not support, it MUST respond with a 417 (Expectation Failed) status."

7.5.1.16 **500 ("Internal Server Error")**

This response code is used to indicate that the server has an internal problem and is a generic server error response.

7.5.1.17 **501 ("Not Implemented")**

This response code is used when a client attempts to use a feature of HTTP (such as a method) that the server does not support.

[RFC 2616] states, "The recipient of the entity MUST NOT ignore any Content - (e.g., Content-Range) headers that it does not understand or implement and MUST return a 501 (Not Implemented) response in such cases."

7.5.1.18 **503 ("Service Unavailable")**

This response code is used when a server, due to a temporary overload condition, is unable to service a request.

7.5.2 **Minimal Understanding**

Should a client wish to operate with minimal understanding of HTTP response codes, it need only examine the first digit of the response code to understand the general category of the response and "treat any unrecognized response as being equivalent to the x00 status code of that class, with the exception that an unrecognized response MUST NOT be cached." [RFC 2616].

7.6 Application Payload Syntax

Application payload message encoding using both XML [XML] and EXI [EXI] SHALL be supported by all servers. Application payload message encoding using either XML [XML] or EXI [EXI] SHALL be supported by all clients.

7.6.1 XML Encoding

The XML declaration is optional as per [XML] and SHOULD NOT be included in SEP 2 transactions, to reduce packet sizes. The XML version used SHALL be 1.0. For XML payloads, the encoding SHALL be UTF-8.

7.6.2 EXI Encoding

The options for encoding EXI documents SHALL be as follows, and transactions will likely fail if different options are declared in the EXI option header. Options marked as (default) are EXI specification [EXI] defaults and SHOULD NOT be specified explicitly.

- Non-strict schema-informed grammar with the schema [ZB 13-0201]
- Alignment is bit-packed (default)
- Compression is false (default)
- Strict is false (default)
- Fragment is false (default)
- Preserve options are all false (default)
- selfContained is false (default)
- schemaId is "S0" (two bytes: 0x53, 0x30, without quotes). This schemaId corresponds to the normative schema of SEP 2.0 [ZB 13-0201].
- datatypeRepresentationMap is not used (default)
- valueMaxLength is unbounded (default)
- valuePartitionCapacity is unbounded (default)
- No user defined meta-data

The following XML document describes the EXI option header that SHALL be used to encode the messages.

```
<header xmlns="http://www.w3.org/2009/exi">
  <common><schemaId>S0</schemaId></common>
</header>
```

7.7 Content Negotiation

A client SHALL declare acceptable media types using the HTTP Accept header.

7.7.1 Schema Version Negotiation

When specifying an "application/sep-exi" media type, an extensibility level ("level") SHALL be specified in the HTTP Accept header for schema version negotiation. "level" is an Accept-extension defined in [RFC 2616]. The extensibility level specified using an HTTP Accept header supersedes an extensibility declaration discovered during resource discovery (see Section 9.3).

The Extensibility Level defines the base schema and its capability for arbitrary extension. The Extensibility Level is one of "-S0" or "+S0". The S0 indicates the base schema version: SEP 2. "-S0"

