BS EN 60839-11-31:2017

BSI Standards Publication

Alarm and electronic security systems

Part 11-31: Electronic access control systems — Core interoperability protocol based on Web services

Documents
Document Sharing Hub

Full document details: BS EN 60839-11-31:2017

National foreword

This British Standard is the UK implementation of EN 60839-11-31:2017. It is identical to IEC 60839-11-31:2016.

The UK participation in its preparation was entrusted by Technical Committee GW/1, Electronic security systems, to Subcommittee GW/1/8, Access control.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2017.
Published by BSI Standards Limited 2017

ISBN 978 0 580 87352 2
ICS 13.320

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 March 2017.

Amendments/corrigenda issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: BS EN 60839-11-31:2017

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 60839-11-31

March 2017

ICS 13.320

English Version

Alarm and electronic security systems - Part 11-31: Electronic access control systems - Core interoperability protocol based on Web services (IEC 60839-11-31:2016)

Systèmes d'alarme et de sécurité électroniques - Partie 11-31: Systèmes de contrôle d'accès électronique - Protocole de base d'interopérabilité en fonction des services Web (IEC 60839-11-31:2016)

Alarmanlagen - Teil 11-31: Elektronische Zutrittskontrollanlagen - IP Interoperabilität auf Basis von Webservices - Kernspezifikation (IEC 60839-11-31:2016)

This European Standard was approved by CENELEC on 2016-12-29. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

© 2017 CENELEC All rights of exploitation in any form and by any means reserved worldwide for CENELEC Members.

Ref. No. EN 60839-11-31:2017 E

AVA Documents Document Sharing Hub

Full document details: BS EN 60839-11-31:2017

European foreword

The text of document 79/522/CDV, future edition 1 of IEC 60839-11-31, prepared by IEC/TC 79 "Alarm and electronic security systems" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN 60839-11-31:2017.

The following dates are fixed:

• latest date by which the document has to be implemented at national level by publication of an identical national standard or by endorsement	(dop)	2017-09-29
• latest date by which the national standards conflicting with the document have to be withdrawn	(dow)	2019-12-29

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC [and/or CEN] shall not be held responsible for identifying any or all such patent rights.

Endorsement notice

The text of the International Standard IEC 60839-11-31:2016 was approved by CENELEC as a European Standard without any modification.

Documents
Document Sharing Hub
Full document details: BS EN 60839-11-31:2017

Annex ZA
(normative)

Normative references to international publications with their corresponding European publications

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

NOTE 1 When an International Publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

NOTE 2 Up-to-date information on the latest versions of the European Standards listed in this annex is available here: www.cenelec.eu

Publication	Year	Title	EN/HD	Year
IEEE 1003.1	-	The Open Group Base Specifications Issue 6, IEEE Std 1003.1, 2004 Edition		
IEEE 802.11	2007	IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications	- -	-
IEEE 802.1X	2004	Port Based Network Access Control	-	-
IETF RFC 952	-	DoD Internet Host Table Specification	-	-
IETF RFC 1123	1989	Requirements for Internet Hosts - Application and Support	-	-
IETF RFC 2131	-	Dynamic Host Configuration Protocol	-	-
IETF RFC 2136	-	Dynamic Updates in the Domain Name System (DNS UPDATE)	-	-
IETF RFC 2246	-	The TLS Protocol Version 1.0	-	-
IETF RFC 2617	-	HTTP Authentication: Basic and Digest Access Authentication	-	-
IETF RFC 2986	-	PKCS #10: Certification Request Syntax Specification Version 1.7	-	-
IETF RFC 3268	-	Advanced Encryption Standard (AES) Cipher suites for Transport Layer Security (TLS)	-	-
IETF RFC 3315	-	Dynamic Host Configuration Protocol for IPv6 (DHCPv6)	-	-
IETF RFC 3927	-	Dynamic Configuration of IPv4 Link-Local Addresses	-	-
IETF RFC 4122	-	A Universally Unique IDentifier (UUID) URN Namespace	-	-

Documents
Document Sharing Hub
Full document details: BS EN 60839-11-31:2017

Publication	Year	Title	EN/HD	Year
IETF RFC 4514	-	Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names	-	-
IETF RFC 4702	-	The Dynamic Host Configuration Protocol (DHCP) Client Fully Qualified Domain Name (FQDN) Option	-	-
IETF RFC 4861	-	Neighbor Discovery for IP version 6 (IPv6)	-	-
IETF RFC 4862	-	IPv6 Stateless Address Auto configuration	-	-
ISO/IEC 8824-2	-	Information technology - Abstract Syntax Notation One (ASN.1): Information object specification	-	-
ISO/IEC 8824-3	-	Information technology - Abstract Syntax Notation One (ASN.1): Constraint specification	-	-
ISO/IEC 8824-4	-	Information technology - Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications	-	-
ISO/IEC 8825-1	-	Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)	-	-
OASIS WS-BaseNotification	-	Web Services Base Notification 1.3 (WS-BaseNotification)		
OASIS WS-Topics	-	Web Services Topics 1.3 (WS-Topics)		
W3C SOAP-MTOM	-	SOAP Message Transmission Optimization-Mechanism		-
W3C SOAP Part 1	-	SOAP Version 1.2 - Part 1: Messaging Framework	-	-
W3C WS-Addressing	-	Web Services Addressing 1.0 - Core	-	-
WS-I BP 2.0	-	Basic Profile Version 2.0		
XMLSOAP WS-Discovery	-	Web Services Dynamic Discovery (WS-Discovery)", J. Beatty et al., April 2005		

Documents
Document Sharing Hub
Full document details: BS EN 60839-11-31:2017

CONTENTS

FOREWORD 10
INTRODUCTION 12
1 Scope 13
2 Normative references 13
3 Terms, definitions and abbreviated terms 15
3.1 Terms and definitions 15
3.2 Abbreviated terms 16
4 Overview 17
4.1 General 17
4.2 Web services 17
4.3 IP configuration 18
4.4 Device discovery 18
4.5 Device management 19
4.5.1 General 19
4.5.2 Capabilities 19
4.5.3 Network 19
4.5.4 System 20
4.5.5 Retrieval of system information 20
4.5.6 Firmware upgrade 20
4.5.7 SystemRestore 20
4.5.8 Security 20
4.6 DeviceIO 21
4.7 Event handling 21
4.8 Security 21
5 Web services framework 21
5.1 General 21
5.2 Services overview 22
5.2.1 General 22
5.2.2 Services requirements 22
5.3 WSDL overview 22
5.4 Namespaces 23
5.5 Types 24
5.6 Messages 24
5.7 Operations 25
5.7.1 General 25
5.7.2 One-way operation type 26
5.7.3 Request-response operation type 26
5.8 Port types 27
5.9 Binding 27
5.10 Ports 27
5.11 Services 28
5.12 Error handling 28
5.12.1 General 28
5.12.2 Protocol errors 28
5.12.3 SOAP errors 28
5.13 Security 31

AVA Documents
Document Sharing Hub
Full document details: BS EN 60839-11-31:2017

5.13.1 Authentication ... 31
5.13.2 User-based access control ... 31
5.14 String representation ... 33
5.14.1 Character set ... 33
5.14.2 Allowed characters in strings ... 33
5.15 Proprietary extensions ... 33
6 IP configuration ... 33
7 Device discovery ... 34
7.1 General ... 34
7.2 Modes of operation ... 34
7.3 Discovery definitions ... 35
7.3.1 Endpoint reference ... 35
7.3.2 Hello ... 35
7.3.3 Probe and probe match ... 36
7.3.4 Resolve and resolve match ... 37
7.3.5 Bye ... 37
7.3.6 SOAP fault messages ... 37
8 Device management ... 37
8.1 General ... 37
8.2 Capabilities ... 38
8.2.1 Get WSDL URL ... 38
8.2.2 Capability exchange ... 38
8.3 Network ... 40
8.3.1 Get hostname ... 40
8.3.2 Set hostname ... 40
8.3.3 Set hostname from DHCP ... 41
8.3.4 Get DNS settings ... 41
8.3.5 Set DNS settings ... 42
8.3.6 Get NTP settings ... 42
8.3.7 Set NTP settings ... 43
8.3.8 Get dynamic DNS settings ... 43
8.3.9 Set dynamic DNS settings ... 44
8.3.10 Get network interface configuration ... 44
8.3.11 Set network interface configuration ... 45
8.3.12 Get network protocols ... 46
8.3.13 Set network protocols ... 47
8.3.14 Get default gateway ... 47
8.3.15 Set default gateway ... 48
8.3.16 Get zero configuration ... 48
8.3.17 Set zero configuration ... 48
8.3.18 Get IP address filter ... 49
8.3.19 Set IP address filter ... 49
8.3.20 Add an IP filter address ... 50
8.3.21 Remove an IP filter address ... 50
8.3.22 IEEE 802.11 configuration ... 51
8.4 System ... 55
8.4.1 Device information ... 55
8.4.2 Get system URIs ... 55
8.4.3 Backup ... 56

Documents
Document Sharing Hub
Full document details: BS EN 60839-11-31:2017

8.4.4 Restore ... 56
8.4.5 Start system restore ... 57
8.4.6 Get system date and time ... 57
8.4.7 Set system date and time ... 58
8.4.8 Factory default ... 59
8.4.9 Firmware upgrade ... 59
8.4.10 Start firmware upgrade ... 60
8.4.11 Get system logs ... 61
8.4.12 Get support information ... 61
8.4.13 Reboot ... 62
8.4.14 Get scope parameters ... 62
8.4.15 Set scope parameters ... 62
8.4.16 Add scope parameters ... 63
8.4.17 Remove scope parameters ... 63
8.4.18 Get discovery mode ... 64
8.4.19 Set discovery mode ... 64
8.5 Security ... 65
8.5.1 General ... 65
8.5.2 Get access policy ... 65
8.5.3 Set access policy ... 65
8.5.4 Get users ... 65
8.5.5 Create users ... 66
8.5.6 Delete users ... 67
8.5.7 Set users settings ... 67
8.5.8 IEEE 802.1X configuration ... 68
8.5.9 Create self-signed certificate ... 71
8.5.10 Get certificates ... 71
8.5.11 Get CA certificates ... 71
8.5.12 Get certificate status ... 72
8.5.13 Set certificate status ... 72
8.5.14 Get certificate request ... 72
8.5.15 Get client certificate status ... 73
8.5.16 Set client certificate status ... 73
8.5.17 Load device certificate ... 74
8.5.18 Load device certificates in conjunction with its private key ... 74
8.5.19 Get certificate information request ... 75
8.5.20 Load CA certificates ... 76
8.5.21 Delete certificate ... 76
8.5.22 Get remote user ... 76
8.5.23 Set remote user ... 77
8.5.24 Get endpoint reference ... 77
8.6 Auxiliary operation ... 78
8.7 Monitoring events ... 78
8.7.1 Processor usage ... 78
8.7.2 Link status ... 79
8.7.3 Upload status ... 79
8.7.4 Operating time ... 79
8.7.5 Environmental conditions ... 81
8.7.6 Battery capacity ... 81

AVA Documents
Document Sharing Hub

8.7.7 Device management ... 82
8.8 Service specific fault codes ... 82
9 Device I/O ... 86
9.1 General ... 86
9.2 Relay outputs ... 86
9.2.1 Overview ... 86
9.2.2 Get relay outputs ... 86
9.2.3 Get relay output options ... 86
9.2.4 Set relay output settings ... 87
9.2.5 Trigger relay output ... 88
9.3 Digital inputs ... 88
9.3.1 Overview ... 88
9.3.2 GetDigitalInputs ... 88
9.4 SerialPorts ... 89
9.4.1 Overview ... 89
9.4.2 GetSerialPorts ... 89
9.4.3 GetSerialPortConfiguration ... 89
9.4.4 SetSerialPortConfiguration ... 89
9.4.5 GetSerialPortConfigurationOptions ... 90
9.4.6 Send and/or Receive serial command ... 90
9.5 Capabilities ... 92
9.6 Events ... 92
9.6.1 DigitalInput state change ... 92
9.6.2 Relay output trigger ... 92
9.7 Service specific fault codes ... 93
10 Event handling ... 93
10.1 General ... 93
10.2 Real-time Pull-Point notification interface ... 93
10.2.1 General ... 93
10.2.2 Create pull point subscription ... 95
10.2.3 Pull messages ... 95
10.2.4 Renew ... 96
10.2.5 Unsubscribe ... 96
10.2.6 Seek ... 97
10.2.7 Pull point lifecycle ... 98
10.2.8 Persistent notification storage ... 98
10.3 Basic notification interface ... 98
10.3.1 General ... 98
10.3.2 Summary ... 98
10.3.3 Requirements ... 99
10.4 Properties ... 100
10.5 Notification structure ... 100
10.5.1 General ... 100
10.5.2 Notification information ... 101
10.5.3 Message format ... 102
10.5.4 Message description language ... 103
10.5.5 Message content filter ... 104
10.6 Synchronization point ... 105
10.7 Topic structure ... 105

AVA Documents
Document Sharing Hub
Full document details: BS EN 60839-11-31:2017

10.7.1 General ... 105
10.7.2 ONVIF topic namespace ... 106
10.7.3 Topic type information ... 106
10.7.4 Topic filter ... 107
10.8 Get event properties ... 108
10.9 Capabilities ... 108
10.10 SOAP fault messages ... 109
10.11 Notification example ... 110
10.11.1 General ... 110
10.11.2 GetEventPropertiesRequest ... 110
10.11.3 GetEventPropertiesResponse ... 110
10.11.4 CreatePullPointSubscription ... 111
10.11.5 CreatePullPointSubscriptionResponse ... 111
10.11.6 PullMessagesRequest ... 112
10.11.7 PullMessagesResponse ... 112
10.11.8 UnsubscribeRequest ... 113
10.11.9 UnsubscribeResponse ... 113
10.12 Persistent storage event:BeginingOfBuffer ... 114
10.13 Service specific fault codes ... 114
11 Security ... 114
11.1 General ... 114
11.2 Transport level security ... 114
11.2.1 General ... 114
11.2.2 Supported cipher suites ... 115
11.2.3 Server authentication ... 115
11.2.4 Client authentication ... 115
11.3 IEEE 802.1X ... 116
Annex A (informative) Example for GetServices response with capabilities ... 117
Annex B (normative) Device IP network literface XML schemata ... 119
B.1 Device management service WSDL ... 119
B.2 Device IO service WSDL ... 161
B.3 Event service WSDL ... 168
B.4 Common schema ... 179
Bibliography ... 197

Figure 1 – Web services based development principles ... 18
Figure 2 – Sequence diagram for the Real-time Pull-Point notification interface ... 94
Figure 3 – Sequence diagram for the base notification interface ... 99

Table 1 – Defined namespaces in this document ... 23
Table 2 – Referenced namespaces (with prefix) ... 24
Table 3 – Referenced namespaces (without prefix) ... 24
Table 4 – Operation description outline used in this document ... 25
Table 5 – Generic faults ... 30
Table 6 – HTTP errors ... 31
Table 7 – Access class to user level mapping ... 32
Table 8 – Scope parameters ... 36

AVA Documents
Document Sharing Hub
Full document details: BS EN 60839-11-31:2017

Table 9 – GetWSDLUrl command 38
Table 10 – GetServices command 38
Table 11 – GetServiceCapabilities command 39
Table 12 – Capabilities in the GetServiceCapabilities command 39
Table 13 – GetHostname command 40
Table 14 – SetHostname command 41
Table 15 – SetHostnameFromDHCP command 41
Table 16 – GetDNS command 42
Table 17 – SetDNS command 42
Table 18 – GetNTP command 43
Table 19 – SetNTP command 43
Table 20 – GetDynamicDNS command 44
Table 21 – SetDynamicDNS command 44
Table 22 – GetNetworkInterfaces command 45
Table 23 – SetNetworkInterfaces command 46
Table 24 – GetNetworkProtocols command 47
Table 25 – SetNetworkProtocols command 47
Table 26 – GetNetworkDefaultGateway command 47
Table 27 – SetNetworkDefaultGateway command 48
Table 28 – GetZeroConfiguration command 48
Table 29 – SetZeroConfiguration command 49
Table 30 – GetIPAddressFilter command 49
Table 31 – SetIPAddressFilter command 50
Table 32 – AddIPAddressFilter command 50
Table 33 – RemoveIPAddressFilter command 51
Table 34 – GetDot11Capabilities 53
Table 35 – IEEE 802.11 capabilities 53
Table 36 – GetDot11Status 54
Table 37 – ScanAvailableDot11Networks 55
Table 38 – GetDeviceInformation command 55
Table 39 – GetSystemUris command 56
Table 40 – GetSystemBackup command 56
Table 41 – RestoreSystem command 57
Table 42 – StartSystemRestore command 57
Table 43 – GetSystemDateAndTime command 58
Table 44 – SetSystemDateAndTime command 59
Table 45 – SetSystemFactoryDefault command 59
Table 46 – UpgradeSystemFirmware command 60
Table 47 – StartFirmwareUpgrade command 60
Table 48 – GetSystemLog command 61
Table 49 – GetSystemSupportInformation command 61
Table 50 – SystemReboot command 62
Table 51 – GetScopes command 62

AVA Documents
Document Sharing Hub

Full document details: BS EN 60839-11-31:2017

Table 52 – SetScopes command 63
Table 53 – AddScopes command 63
Table 54 – RemoveScopes command 64
Table 55 – GetDiscoveryMode command 64
Table 56 – SetDiscoveryMode command 64
Table 57 – GetAccessPolicy command 65
Table 58 – SetAccessPolicy command 65
Table 59 – GetUsers command 66
Table 60 – CreateUsers command 66
Table 61 – DeleteUsers command 67
Table 62 – SetUser command 67
Table 63 – CreateDot1XConfiguration command 69
Table 64 – SetDot1XConfigurationRequest command 69
Table 65 – GetDot1XConfiguration command 70
Table 66 – GetDot1XConfigurations command 70
Table 67 – DeleteDot1XConfigurations command 70
Table 68 – CreateCertificate command 71
Table 69 – GetCertificates command 71
Table 70 – GetCACertificates command 72
Table 71 – GetCertificatesStatus command 72
Table 72 – SetCertificatesStatus command 72
Table 73 – GetPkcs10Request command 73
Table 74 – GetClientCertificateMode command 73
Table 75 – SetClientCertificateMode command 74
Table 76 – LoadCertificates command 74
Table 77 – LoadCertificateWithPrivateKey command 75
Table 78 – GetCertificateInformation command 75
Table 79 – LoadCACertificates command 76
Table 80 – DeleteCertificates command 76
Table 81 – GetRemoteUser command 77
Table 82 – SetRemoteUser command 77
Table 83 – GetEndpointReference command 78
Table 84 – SendAuxiliary command 78
Table 85 – Device service specific fault codes 82
Table 86 – GetRelayOutputs command 86
Table 87 – GetRelayOutputOptions command 87
Table 88 – SetRelayOutputSettings command. 88
Table 89 – SetRelayOutputState command 88
Table 90 – GetDigitalInputs command 89
Table 91 – GetSerialPorts command 89
Table 92 – GetSerialPortConfiguration command 89
Table 93 – SetSerialPortConfiguration command 90
Table 94 – GetSerialPortConfigurationOptions command 90

AVA Documents
Document Sharing Hub

Full document details: BS EN 60839-11-31:2017

Table 95 – Send and/or Receive serial command 91
Table 96 – GetServiceCapabilities command 92
Table 97 – DeviceIO service specific fault codes 93
Table 98 – CreatePullPointSubscription command 95
Table 99 – PullMessages command 96
Table 100 – Renew command 96
Table 101 – Unsubscribe command 97
Table 102 – Seek command 97
Table 103 – SetSynchronizationPoint command 105
Table 104 – GetEventProperties command 108
Table 105 – GetServiceCapabilities command 109

Documents
Document Sharing Hub
Full document details: BS EN 60839-11-31:2017

INTERNATIONAL ELECTROTECHNICAL COMMISSION

ALARM AND ELECTRONIC SECURITY SYSTEMS –

Part 11-31: Electronic access control systems – Core interoperability protocol based on Web services

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 60839-11-31 has been prepared by IEC technical committee 79: Alarm and electronic security systems.

The text of this standard is based on the following documents:

CDV	Report on voting
79/522/CDV	79/546/RVC

Full information on the voting for the approval of this standard can be found in the report on voting indicated in the above table.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

Documents
Document Sharing Hub
Full document details: BS EN 60839-11-31:2017

A list of all parts in the IEC 60839 series, published under the general title *Alarm and electronic security systems*, can be found on the IEC website.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC website under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

Documents
Document Sharing Hub

Full document details: BS EN 60839-11-31:2017

INTRODUCTION

The object of this document is to provide the common base for a fully interoperable network implementation comprised of products from different network vendors. This document describes the network model, interfaces, data types and data exchange patterns. This document reuses existing relevant standards where available, and introduces new specifications only where necessary.

This document is based upon work done by the ONVIF open industry forum. The ONVIF Core specification is compatible with this document.

This document is accompanied by a set of computer readable interface definitions:

- Device Service WSDL, see Clause B.1;
- Device IO Service WSDL, see Clause B.2;
- Event Service WSDL, see Clause B.3;
- Common schema, see Clause B.4.

This document is divided into the following clauses:

Document overview: Gives an overview of the different standard parts and how they are related to each other.

Web services frame work: Offers a brief introduction to Web services and the Web services basis for this document.

IP configuration: Defines the network IP configuration requirements.

Device discovery: Describes how devices are discovered in local and remote networks.

Device management: Defines the configuration of basics like network and security related settings.

Device IO: Defines the handling of input and output ports on a device.

Event handling: Defines how to subscribe to and receive notifications (events) from a device.

Security: Defines the transport and message level security requirements.

Documents
Document Sharing Hub
Full document details: BS EN 60839-11-31:2017

ALARM AND ELECTRONIC SECURITY SYSTEMS –

Part 11-31: Electronic access control systems – Core interoperability protocol based on Web services

1 Scope

This part of IEC 60839 defines procedures for communication between network clients and devices. This series of interoperability standards makes it possible to build an alarm and electronic security system with clients and devices from different manufacturers using common and well defined interfaces. The functions defined in this document covers discovery, device management and event framework. Supplementary dedicated services are defined in separate documents.

The management and control interfaces defined in this document are described as Web services. This document also contains full XML schema and Web Service Description Language (WSDL) definitions.

In order to offer full plug-and-play interoperability, this document defines procedures for device discovery. The device discovery mechanisms in this document are based on the WS-Discovery specification with extensions.

This document does not in any way limit a manufacturer to add other protocol or extend the protocol defined here and rules on how to accomplish this are also provided in this document.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEEE 1003.1, *The Open Group Base Specifications Issue 6, IEEE Std 1003.1, 2004 Edition* *<http://pubs.opengroup.org/onlinepubs/009695399/>*

IEEE 802.11, *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*
<http://standards.ieee.org/getieee802/download/802.11-2007.pdf>

IEEE 802.1X, *Port-Based Network Access Control*
<http://standards.ieee.org/getieee802/download/802.1X-2004.pdf>

IETF RFC 952, Internet Host Table Specification
<https://tools.ietf.org/html/rfc952

IETF RFC 1123:1989, Requirements for Internet Hosts – Application and Support
<https://tools.ietf.org/html/rfc1123>

IETF RFC 2131, *Dynamic Host Configuration Protocol*
<http://www.ietf.org/rfc/rfc2131.txt>

IETF RFC 2136, *Dynamic Updates in the Domain Name System (DNS UPDATE)*
<http://www.ietf.org/rfc/rfc2136.txt>

Documents
Document Sharing Hub
Full document details: BS EN 60839-11-31:2017

IETF RFC 2246, *The TLS Protocol Version 1.0*
<http://www.ietf.org/rfc/rfc2246.txt>

IETF RFC 2617, *HTTP Authentication: Basic and Digest Access Authentication*
<http://www.ietf.org/rfc/rfc2617.txt>

IETF RFC 2986, PKCS #10, *Certification Request Syntax Specification Version 1.7*
<http://www.ietf.org/rfc/rfc2986.txt>

IETF RFC 3268, *Advanced Encryption Standard (AES) Cipher suites for Transport Layer Security (TLS)*
<http://www.ietf.org/rfc/rfc3268.txt>

IETF RFC 3315, *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*
<http://www.ietf.org/rfc/rfc3315.txt>

IETF RFC 3927, *Dynamic Configuration of IPv4 Link-Local Addresses*
<http://www.ietf.org/rfc/rfc3927.txt>

IETF RFC 4122, *A Universally Unique IDentifier (UUID) URN Namespace*
<http://www.ietf.org/rfc/rfc4122.txt>

IETF RFC 4514, *Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names*
<http://www.ietf.org/rfc/rfc4514.txt>

IETF RFC 4702, *The Dynamic Host Configuration Protocol (DHCP) Client Fully Qualified Domain Name (FQDN) Option*
<http://www.ietf.org/rfc/rfc4702.txt>

IETF RFC 4861, *Neighbor Discovery for IP version 6 (IPv6)*
<http://www.ietf.org/rfc/rfc4861.txt>

IETF RFC 4862, *IPv6 Stateless Address Auto configuration*
<http://www.ietf.org/rfc/rfc4862.txt>

ISO/IEC 8824-2, *Information Technology – Abstract Syntax Notation One (ASN.1): Information object specification*

ISO/IEC 8824-3, *Information Technology – Abstract Syntax Notation One (ASN.1): Constraint specification*

ISO/IEC 8824-4, *Information Technology – Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications*

ISO/IEC 8825-1, *Information Technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER).*

OASIS WS-BaseNotification, *Web Services Base Notification 1.3 (WS-BaseNotification)*
<http://docs.oasis-open.org/wsn/wsn-ws_base_notification-1.3-spec-os.pdf>

OASIS WS-Topics, *Web Services Topics 1.3 (WS-Topics)*
<http://docs.oasis-open.org/wsn/wsn-ws_topics-1.3-spec-os.pdf>

Documents
Document Sharing Hub

Full document details: BS EN 60839-11-31:2017

W3C SOAP-MTOM, *SOAP Message Transmission Optimization Mechanism*
<http://www.w3.org/TR/soap12-mtom/>

W3C SOAP12-PART1, *SOAP 1.2 Part 1, Messaging Framework*
<http://www.w3.org/TR/soap12-part1/>

W3C WS-Addressing, *Web Services Addressing 1.0 – Core*
<http://www.w3.org/TR/ws-addr-core/>

WS-I BP 2.0, *Basic Profile Version 2.0*
<http://www.ws-i.org/Profiles/BasicProfile-2.0-2010-11-09.html>

XMLSOAP WS-Discovery, *Web Services Dynamic Discovery (WS-Discovery)", J. Beatty et al., April 2005*
<http://specs.xmlsoap.org/ws/2005/04/discovery/ws-discovery.pdf>

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

3.1.1
ad-hoc network
independent basic service set

Note 1 to entry: "Ad-hoc network" is a vernacular term.

3.1.2
basic service set
set of IEEE 802.11 stations that have successfully joined in a common network

3.1.3
capability
command which allows a client to ask for the services provided by a device

3.1.4
public key cryptography standards
PKCS
group of standards devised and published by RSA Security

Note 1 to entry: This note only applies to the French language.

3.1.5
pre shared key
static key that is distributed to the device

3.1.6
pull point
resource for pulling messages

Note 1 to entry: By pulling messages, notifications are not blocked by firewalls.

Documents
Document Sharing Hub

Full document details: BS EN 60839-11-31:2017

3.1.7
service set ID
identity of an IEEE 802.11 wireless network

[SOURCE: IEEE 802.11-2007]

3.1.8
Wi-Fi protected access
WPA
certification program created by the Wi-Fi Alliance to indicate compliance with the security protocol covered by the program

Note 1 to entry: This note only applies to the French language.

3.2 Abbreviated terms

API	Application Programming Interface
ASCII	American Standard Code for Information Interchange
ASN	Abstract Syntax Notation
BSSID	Basic Service Set Identification
CA	Certificate Authority
CBC	Cipher-Block Chaining
CCMP	Counter mode with Cipher-block chaining Message authentication code Protocol
DER	Distinguished Encoding Rules
DHCP	Dynamic Host Configuration Protocol
DM	Device Management
DNS	Domain Name Server
DP	Discovery Proxy
EAP	Extensible Authentication Protocol
GW	Gateway
HMAC	Hash-based Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer
IANA	Internet Assigned Numbers Authority
IO, I/O	Input/Output
IP	Internet Protocol
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
LAN	Local Area Network
MTOM	Message Transmission Optimization Mechanism
NAT	Network Address Translation
NFC	Near Field Communication
NTP	Network Time Protocol
OASIS	Organization for the Advancement of Structured Information Standards
POSIX	Portable Operating System Interface
PKCS	Public Key Cryptography Standards
PSK	Pre Shared Key
REL	Rights Expression Language

Documents
Document Sharing Hub
Full document details: BS EN 60839-11-31:2017

RSA	Rivest, Sharmir and Adleman
SAML	Security Assertion Markup Language
SOAP	Simple Object Access Protocol
SSID	Service Set ID
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TKIP	Temporal Key Integrity Protocol
TTL	Time To Live
UDDI	Universal Description, Discovery and Integration
UDP	User Datagram Protocol
URI	Uniform Resource Identifier
URN	Uniform Resource Name
USB	Universal Serial Bus
UTC	Coordinated Universal Time
UTF	Unicode Transformation Format
UUID	Universally Unique Identifier
WDR	Wide Dynamic Range
WS	Web services
WSDL	Web Services Description Language
WS-I	Web Services Interoperability
XML	eXtensible Markup Language
XPath	XML Path Language

4 Overview

4.1 General

This document defines a core set of interface functions for configuration and operation of network devices by defining their server side interfaces. This document covers device discovery, device configuration as well as an event framework.

All services share a common XML schema, see Clause B.4. The different services are defined in the respective sections and service WSDL documents.

4.2 Web services

The term Web services is the name of a standardized method of integrating applications using open, platform independent Web services standards such as XML, SOAP 1.2 [W3C SOAP12-PART1] and WSDL1.1 [W3C WSDL11] over an IP network. XML is used as the data description syntax, SOAP is used for message transfer and WSDL is used for describing the services.

This framework is built upon Web services standards. All configuration services defined in this document are expressed as Web services operations and defined in WSDL with HTTP [RFC 2616] as the underlying transport mechanism.

Documents
Document Sharing Hub
Full document details: BS EN 60839-11-31:2017

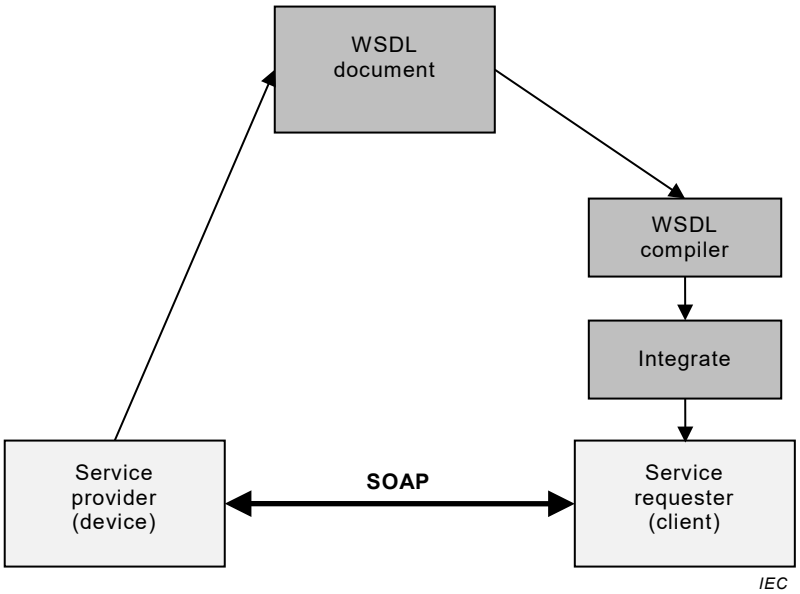

Figure 1 – Web services based development principles

Figure 1 gives an overview of the basic principles for development based on Web services. The service provider (device) implements the service or services. The service is described using the XML-based WSDL. Then, the WSDL is used as the basis for the service requester (client) implementation/integration. Client-side integration is simplified through the use of WSDL compiler tools that generate a platform specific code that can be used by the client side developer to integrate the Web Service into an application.

The Web services provider and requester communicate using the SOAP message exchange protocol. SOAP is a lightweight, XML-based messaging protocol used to encode the information in a Web Service request and in a response message before sending them over a network. SOAP messages are independent of any operating system or protocol and may be transported using a variety of Internet protocols. This document defines conformant transport protocols for the SOAP messages for the described Web services.

The Web services subclause introduces the general service structure, the command definition syntax used in this document, error handling principles and the adopted Web Service security mechanisms.

To ensure interoperability, all services follow the Web services Interoperability Organization (WS-I) basic profile 2.0 recommendations and use the document/literal wrapped pattern.

4.3 IP configuration

The IP configuration subclause defines the IP configuration compliance requirements and recommendations. IP configuration includes:

- IP network communication capability,
- static IP configuration,
- dynamic IP configuration.

4.4 Device discovery

The configuration interfaces defined in this document are Web services interfaces that are based on the WS-Discovery standard. This use of this document makes it possible to reuse a suitable existing Web Service discovery framework, instead of requiring a completely new service or service addressing definition.

Documents
Document Sharing Hub
Full document details: BS EN 60839-11-31:2017

This document introduces a specific discovery behaviour suitable for alarm and electronic security systems. For example, a fully interoperable discovery requires a well defined service definition and a service searching criteria. This document covers device type and scopes definitions in order to achieve this.

A successful discovery provides the device service address. Once a client has the device service address it can receive detailed device information through the device service, see 4.5 below.

4.5 Device management

4.5.1 General

Device management functions are handled through the device service. The device service is the entry point to all other services provided by a device. WSDL for the device service is provided in the device management WSDL file. The device management interfaces consist of these subcategories:

- capabilities,
- network,
- system,
- security.

4.5.2 Capabilities

The capability commands allow a client to ask for the services provided by a device and to determine which general and vendor specific services are offered by the device. The capabilities are structured per service. This document defines the capability exchange for the device, device IO and the event service. For the other services refer to the respective service specification:

- device,
  - network,
  - system,
  - security,
- device IO,
- event.

The capabilities for the different categories indicate those commands and parameter settings that are available for the particular service or service subcategory.

4.5.3 Network

The following set of network commands allows standardized management of functions:

- Get and set hostname.
- Get and set DNS configurations.
- Get and set NTP configurations.
- Get and set dynamic DNS.
- Get and set network interface configurations.
- Enable/disable and list network protocols.
- Get and set default gateway.
- Get and set zero configuration.
- Get, set, add and delete IP address filter.

Documents
Document Sharing Hub
Full document details: BS EN 60839-11-31:2017

- Wireless network interface configuration.

4.5.4 System

The system commands are used to manage the following device system settings:

- Get device information.
- Make system backups.
- Get and set system date and time.
- Factory default reset.
- Upgrade firmware.
- Get system log.
- Get device diagnostics data (support information).
- Reboot.
- Get and set device discovery parameters.

4.5.5 Retrieval of system information

System information, such as system logs, vendor-specific support information and configuration backup images, may be retrieved using either MTOM or HTTP.

The MTOM method is supported by the GetSystemLog, GetSystemSupportInformation and GetSystemBackup commands. The HTTP method is supported by the GetSystemUris command; this retrieves URIs from which the files may be downloaded using an HTTP GET operation.

4.5.6 Firmware upgrade

Two mechanisms are provided for upgrading the firmware on a device. The first uses the UpgradeSystemFirmware command to send the new firmware image using MTOM.

The second is a two stage process; first the client sends the StartFirmwareUpgrade command to instruct the device to prepare for upgrade, then it sends the firmware image using HTTP POST.

The HTTP method is designed for resource-limited devices that may not be capable of receiving a new firmware image in its normal operating state.

4.5.7 SystemRestore

The SystemRestore capability allows a device's configuration to be restored from a backup image. Again two mechanisms are provided. The first uses the RestoreSystem command to send the backup image using MTOM. The second uses the StartSystemRestore command followed by an HTTP POST operation to send the backup image.

4.5.8 Security

The following security operations are used to manage the device security configurations:

- Get and set access security policy.
- Handle user credentials and settings.
- Handle HTTPS server certificates.
- Enable/disable HTTPS client authentication.
- Key generation and certificate download functions.

Documents
Document Sharing Hub
Full document details: BS EN 60839-11-31:2017

- Handle IEEE 802.1X supplicant certificate.
- Handle IEEE 802.1X CA certificate.
- IEEE 802.1X configuration.

4.6 DeviceIO

The DeviceIO service offers commands to retrieve and configure the settings of physical inputs and outputs of a device.

The DeviceIO service supports the configuration of the following device interfaces:

- RelayOutputs,
- DigitalInputs,
- Send and/or receive serial data communication.

4.7 Event handling

Event handling is based on the OASIS WS-BaseNotification and WS-Topics specifications. These specifications allow the reuse of a rich notification framework without the need to redefine event handling principles, basic formats and communication patterns.

Firewall traversal, according to WS-BaseNotification, is handled through a PullPoint notification pattern. This pattern, however, does not allow real-time notification. Hence, this standard defines an alternative PullPoint communication pattern and service interface. The PullPoint pattern allows a client residing behind a firewall to receive real-time notifications while utilizing the WS-BaseNotification framework.

A fully standardized event handling requires standardized notifications. However, the notification topics will, to a large extent, depend on the application needs. This document defines a set of basic notification topics.

WSDL for the event service including extensions is provided in the Event WSDL file.

4.8 Security

Subclause 4.8 describes network security requirements. This document defines security mechanism on two different communication levels:

- transport-level security,
- message-level security.

This document also defines port-based network security as follows.

- IEEE 802.1X

The general security requirements, definitions and transport security requirements are specified in 11.3. Message level security requirements are specified in 5.13. IEEE 802.1X requirements are specified in 8.4.8. Security management is handled through the device management service as listed above in 4.5.8.

5 Web services framework

5.1 General

All management and configuration commands are based on Web services.

For the purposes of this document:

Documents
Document Sharing Hub
Full document details: BS EN 60839-11-31:2017

- the device is a service provider;
- the client is a service requester.

A typical network system does have multiple clients that handle device configuration and device management operations for numerous devices. Additionally a device providing services may also act as a client.

Web services also require a common way to discover service providers. This discovery is achieved using the Universal Discovery, Description and Integration Registry (UDDI) specifications [UDDI API ver2], [UDDI Data Structure ver2]. The UDDI specifications utilize service brokers for service discovery. This document targets devices while the UDDI model is not device oriented. Consequently, UDDI and service brokers are outside the scope of this document.

According to this document, devices (service providers) are discovered using WS-Discovery [XMLSOAP WS-Discovery] based techniques. The service discovery principles are described in Clause 7.

Web services allow developers the freedom to define services and message exchanges, which may cause interoperability problems. The Web services interoperability organization (WS-I) develops standard profiles and guidelines to create interoperable Web services. The devices and the clients shall follow the guidelines in the WS-I Basic Profile 2.0 [WS-I BP 2.0]. The service descriptions in this document follow the WS-I Basic Profile 2.0 recommendations.

5.2 Services overview

5.2.1 General

A device shall support a number of Web services which are defined in this document and related specifications.

The device management service is the entry point for all other services of the device and therefore also the target service for the WS-Discovery behavior defined by this document, see Clause 7.

The entry point for the device management service is fixed to:

```
http://onvif_host/onvif/device_service
```

5.2.2 Services requirements

A device shall provide the device management and event service.

If a device supports a certain service, the device shall respond to all commands defined in the corresponding service WSDL. If the specific command is not required for that service and the device does not support the command, the device should respond to a request with the error codes:

env:Receiver,

ter:ActionNotSupported,

See 5.12.3 for the definitions of the error codes.

5.3 WSDL overview

“WSDL is an XML format for describing network services as a set of endpoints operating on messages containing either document-oriented or procedure-oriented information. The operations and messages are described abstractly, and then bound to a concrete network protocol and message format to define an endpoint. Related concrete endpoints are combined

AVA Documents
Document Sharing Hub

into abstract endpoints (services). WSDL is extensible to allow description of endpoints and their messages regardless of what message formats or network protocols are used to communicate" [SOURCE: W3C WSDL11].

This document follows the WSDL 1.1 specification, see [W3C WSDL11], and uses the document/literal wrapped pattern.

A WSDL document consists of the following sections:

- types – Definition of data types using XML schema definitions.
- message – Definition of the content of input and output messages.
- operation – Definition of how input and output messages are associated with a logical operation.
- portType – Groups a set of operations together.
- binding – Specification of which protocols that are used for message exchange for a particular portType.
- port – Specifies an address for a binding.
- service – Used to group a set of related ports.

5.4 Namespaces

Note that the Namespace URI, listed in Tables 1, 2 and 3, is primarily used to create a unique idenfier. It does not have to be useful for retrieving a corresponding document, for example an XML schema or WSDL file.

Prefix and namespaces used in this document are listed in Table 1. These prefixes are not part of this document and an implementation can use any prefix.

Table 1 – Defined namespaces in this document

Prefix	Namespace URI	Description
tt	http://www.onvif.org/ver10/schema	XML schema descriptions in this document.
tds	http://www.onvif.org/ver10/device/wsdl	The namespace for the WSDL device service.
tmd	http://www.onvif.org/ver10/deviceIO/wsdl	The namespace for the WSDL device IO service.
trt	http://www.onvif.org/ver10/media/wsdl	The namespace for the WSDL media service.
tev	http://www.onvif.org/ver10/events/wsdl	The namespace for the WSDL event service.
ter	http://www.onvif.org/ver10/error	The namespace used for faults defined by this document.
tns1	http://www.onvif.org/ver10/topics	The namespace used for topics defined by this document.

The namespaces listed in Table 2 are referenced by this document.

Documents
Document Sharing Hub
Full document details: BS EN 60839-11-31:2017

Table 2 – Referenced namespaces (with prefix)

Prefix	Namespace URI	Description
wsdl	http://schemas.xmlsoap.org/wsdl/	WSDL namespace for WSDL framework.
wsoap12	http://schemas.xmlsoap.org/wsdl/soap12/	WSDL namespace for WSDL SOAP 1.2 binding.
http	http://schemas.xmlsoap.org/wsdl/http/	WSDL namespace for WSDL HTTP GET & POST binding.
soapenv	http://www.w3.org/2003/05/soap-envelope	Envelope namespace as defined by SOAP 1.2 [W3C SOAP12-PART11]
xs	http://www.w3.org/2001/XMLSchema	Instance namespace as defined by XS [W3C XML-Schema-1] and [W3C XML-Schema- 2]
xsi	http://www.w3.org/2001/XMLSchema-instance	XML schema instance namespace.
d	http://schemas.xmlsoap.org/ws/2005/04/discovery	Device discovery namespace as defined by [XMLSOAP WS-Discovery].
wsadis	http://schemas.xmlsoap.org/ws/2004/08/addressing	Device addressing namespace referred in WS-Discovery [XMLSOAP WS-Discovery].
wsa	http://www.w3.org/2005/08/addressing	Device addressing namespace as defined by [W3C WS-Addressing].
wstop	http://docs.oasis-open.org/wsn/t-1	Schema namespace of the [OASIS WS-Topics] specification.
wsnt	http://docs.oasis-open.org/wsn/b-2	Schema namespace of the [OASIS WS-BaseNotification] specification.
xop	http://www.w3.org/2004/08/xop/include	XML-binary Optimized Packaging namespace as defined by [W3C XOP]

In addition, this document refers without prefix to the namespaces listed in Table 3.

Table 3 – Referenced namespaces (without prefix)

Namespace URI	Description
http://docs.oasis-open.org/wsn/t-1/TopicExpression/Concrete	Topic expression dialect defined for topic expressions.
http://www.onvif.org/ver10/tev/topicExpression/ConcreteSet	Topic expressions dialect defined by this document.
http://www.onvif.org/ver10/tev/messageContentFilter/ItemFilter	Filter dialect, used for message content filtering, defined by this document.

5.5 Types

Data types are defined using XML schema descriptions Part 1 and Part 2. All data types defined in this document are included in the common schema, see Clause B.4.

5.6 Messages

According to WSDL 1.1 operations are described using input and output messages in XML. The message section contains the message content.

A message in this document contains two main elements:

- message name,
- message parts.

The message name specifies the name of the element and that name is used in the operation definition in the WSDL document. The message name defines the name of the message.

AVA Documents
Document Sharing Hub

The WSDL message part element is used to define the actual format of the message. Although there can be multiple parts in a WSDL message, this document follows the WS-I basic profile [WS-I BP 2.0] and does not allow more than one part element in a message. Hence the same name (“parameters”) is always used for the message part name.

The following WSDL notation is used for this document:

```
<message name="’Operation_Name’Request”>
      <part name="parameters" element="’prefix’:’Operation_Name’"/>
</message>
```

respectively,

```
<message name="’Operation_Name’Response”>
      <part name="parameters" element="’prefix’:’Operation_Name’Response”/>
</message>
```

where 'prefix' is the prefix for the namespace in which the message is defined.

This document uses message specific types that encapsulate multiple parts to allow multiple arguments (or data) in messages.

5.7 Operations

5.7.1 General

Operations are defined within the WSDL portType declaration. An operation can be one of these two types:

- One-way – The service provider receives a message.
- Request-response – The service provider receives a message and sends a corresponding message.

Depending on the operation, different port types can be used.

The operation name defines the name of the operation.

Operations in this document are defined using the following table format outlined in Table 4.

Table 4 – Operation description outline used in this document

Operation_Name	Access_Class_Name
Message name	**Description**
‘Operation_Name’Request	*Description of the request message.* *Type*$_{r1}$ **Name**$_{r1}$ [a_{r1}][b_{r1}] *Type*$_{r2}$ **Name**$_{r2}$ [a_{r2}][b_{r2}] : *Type*$_{rn}$ **Name**$_{rn}$ [a_{rn}][b_{rn}]
‘Operation_Name’Response	*Description of the response message.* *Type*$_{s1}$ **Name**$_{s1}$ [a_{s1}][b_{s2}] *Type*$_{s2}$ **Name**$_{s2}$ [a_{s2}][b_{s2}] : *Type*$_{sn}$ **Name**$_{sn}$ [a_{sn}][b_{sn}]
‘FaultMessage_Name’	*In the case that operation specific faults are defined, this field describes the structure of the defined fault message.*
Fault codes	**Description**
Code *Subcode* *Subcode*	*Description of the operation specific fault.*

AVA Documents
Document Sharing Hub
Full document details: BS EN 60839-11-31:2017

The description column includes a list of the elements (if applicable) included in the request and response messages respectively. The value between brackets defines the lower and upper limits of the number of occurrences that can be expected for the element of the specified type. For example, $Name_{s2}$ in the table above occurs at least a_{s2} times and at most b_{s2} times.

Most commands do not define any specific fault messages. If a message is defined, it follows in the table directly after the response message.

The fault codes listed in the tables are the specific fault codes that can be expected from the command, see 5.12.3.3. Any command can return a generic fault, see 5.12.3.3.

The Access_Class_Name defines the access class of the operation. The access class characterizes the impact of the operation, see 5.13.2.3.

5.7.2 One-way operation type

A one-way operation type is used when the service provider receives a control message and does not send any explicit acknowledgement message or confirmation. This document makes use of one-way operations for discovery and event purposes only.

This operation type is defined by a single input message.

Use the following table format to describe one-way operations:

Operation_Name	One-way
Message name	**Description**
'Operation_Name'Request	*Description of the request message.* *Type*$_1$ **Name**$_1$ [a_1][b_1] *Type*$_2$ **Name**$_2$ [a_2][b_2] : *Type*$_n$ **Name**$_n$ [a_n][b_n]

This table corresponds to the following WSDL notation in the service specifications:

```
<operation name="'Operation_Name'">
     <input message="'prefix':'Operation_Name'"/>
</operation>
```

5.7.3 Request-response operation type

A request-response operation type is used when a service provider receives a message and responds with a corresponding message.

This operation type is defined by one input, one output and multiple fault messages.

Use the following table format to describe request-response operations:

Documents
Document Sharing Hub
Full document details: BS EN 60839-11-31:2017

Operation_Name	Request-Response
Message name	**Description**
'Operation_Name'Request	*Description of the request message.* *Type*$_{r1}$ **Name**$_{r1}$ [a_{r1}][b_{r1}] *Type*$_{r2}$ **Name**$_{r2}$ [a_{r2}][b_{r2}] : *Type*$_{rn}$ **Name**$_{rn}$ [a_{rn}][b_{rn}]
'Operation_Name'Response	*Description of the response message.* *Type*$_{s1}$ **Name**$_{s1}$ [a_{s1}][b_{s2}] *Type*$_{s2}$ **Name**$_{s2}$ [a_{s2}][b_{s2}] : *Type*$_{sn}$ **Name**$_{sn}$ [a_{sn}][b_{sn}]
'"FaultMessage_Name'	*In the case that operation specific faults are defined, this field describes the structure of the defined fault message.*
Fault codes	**Description**
Code *Subcode* *Subcode*	*Description of the operation specific fault.*

This table corresponds to the following WSDL notation:

```
<operation name="'Operation_Name'">
     <input message="'prefix':'Operation_Name'"/>
      <output message="'prefix':'Operation_Name'Response"/>
      <fault name> = "Fault" message = "'prefix':'FaultMessage_Name'">
</operation>
```

5.8 Port types

A port type is a named set of abstract operations and the abstract messages involved. One single port type is a collection of several different operations.

All operation names in this document are sorted into categories. Each operation category contains one or more operations. Each category holds only one type of operation and is grouped into a single port type. A one-way operation and a request response operation can never exist for the same port type.

5.9 Binding

A binding defines a concrete protocol and transport data format specification for a particular port type. There may be any number of bindings for a given port type.

"Port_type" is a previously defined type and "Binding" is a character string starting with an upper case letter that defines the name of the binding.

Binding definitions for a compliant device shall follow the requirements in [WS-I BP 2.0]. This implies that the WSDL SOAP 1.2 bindings shall be used.

The SOAP binding can have different styles. A compliant device shall use the style 'document' specified at the operation level.

The bindings are defined in the WSDL specifications for respective services.

5.10 Ports

The individual endpoint is specified by a single address for a binding. Each port shall be given a unique name. A port definition contains a name and a binding attribute.

This document does not mandate any port naming principles.

AVA Documents
Document Sharing Hub

Full document details: BS EN 60839-11-31:2017

5.11 Services

A service is a collection of related ports. This document does not mandate any service naming principles.

5.12 Error handling

5.12.1 General

As with any other protocol, errors can occur during communications, protocol or message processing.

This document classifies error handling into the following categories:

- protocol errors,
- SOAP errors,
- application errors.

5.12.2 Protocol errors

Protocol errors are the result of an incorrectly formed protocol message, which could contain illegal header values, or be received when not expected or experience a socket timeout. To indicate and interpret protocol errors, HTTP and RTSP protocols have defined a set of standard status codes (e.g. 1xx, 2xx, 3xx, 4xx, 5xx). According to this document, devices and clients shall use appropriate RTSP and HTTP protocol defined status codes for error reporting and when received handle them accordingly.

5.12.3 SOAP errors

5.12.3.1 General

SOAP errors are generated as a result of Web services operation errors or during SOAP message processing. All such SOAP errors shall be reported and handled through SOAP fault messages. The SOAP specification provides a well defined common framework to handle errors through SOAP fault.

A SOAP fault message is a normal SOAP message with a single well-known element inside the body (soapenv:Fault). To understand the error in more detail, SOAP has defined a SOAP fault message structure with various components in it.

- Fault code
- Subcode
- Reason
- Node and Role
- Fault Details

Subcode and **Fault Detail** elements information items are intended for carrying application specific error information.

This document uses a separate name space for specific faults, see 5.12.3.3:

ter = “http://www.onvif.org/ver10/error”.

SOAP fault messages for different Web services are defined as part of the different Web services definitions. Server and client shall use SOAP 1.2 fault message handling [W3C SOAP12-PART1] as specified in this document and shall follow the WS-I Basic Profile 2.0 fault handling recommendations.

Documents
Document Sharing Hub
Full document details: BS EN 60839-11-31:2017

The following example is an error message (SOAP 1.2 fault message over HTTP). The values in italics are placeholders for actual values.

```
HTTP/1.1 500 Internal Server Error
CONTENT-LENGTH: bytes in body
CONTENT-TYPE: application/soap+xml; charset=”utf-8”
DATE: when response was generated
<?xml version=”1.0” ?>
<soapenv:Envelope        xmlns:soapenv="http://www.w3.org/2003/05/soap-
envelope"
   xmlns:ter="http://www.onvif.org/ver10/error"
   xmlns:xs="http://www.w3.org/2000/10/XMLSchema">
<soapenv:Body>
 <soapenv:Fault>
   <soapenv:Code>
     <soapenv:Value>fault code </soapenv:Value>
     <soapenv:Subcode>
       <soapenv:Value>ter:fault subcode</soapenv:Value>
         <soapenv:Subcode>
           <soapenv:Value>ter:fault subcode</soapenv:Value>
        </soapenv:Subcode>
     </soapenv:Subcode>
    </soapenv:Code>
    <soapenv:Reason>
      <soapenv:Text xml:lang="en">fault reason</soapenv:Text>
    </soapenv:Reason>
    <soapenv:Node>http://www.w3.org/2003/05/soap-
envelope/node/ultimateReceiver</soapenv:Node>
    <soapenv:Role>http://www.w3.org/2003/05/soap-
envelope/role/ultimateReceiver</soapenv:Role>
    <soapenv:Detail>
      <soapenv:Text>fault detail</soapenv:Text>
    </soapenv:Detail>
  </soapenv:Fault>
</soapenv:Body>
</soapenv:Envelope>
```

The following Table 5 summarizes the general SOAP fault codes (fault codes are defined in SOAP version 1.2 Part 1: Messaging Framework). Server and client may define additional fault subcodes for use by applications.

We distinguish between generic faults and specific faults. Any command can generate a generic fault. Specific faults are related to a specific command or set of commands. Specific faults that apply to a particular command are defined in the command definition tables.

In Table 5, the Fault Code, Subcode and Fault Reason are normative values. The description column is added for information.

5.12.3.2 Generic faults

Table 5 lists the generic fault codes and, if applicable, subcodes. All server and client implementations shall handle all the faults listed below. Any Web service command may return one or several of the generic faults.

The faults listed without subcode do not have any subcode value.

Documents
Document Sharing Hub
Full document details: BS EN 60839-11-31:2017

Table 5 – Generic faults

Fault code	Subcode	Fault reason	Description
env:VersionMismatch		SOAP version mismatch	The device found an invalid element information item instead of the expected Envelope element information item.
env:MustUnderstand		SOAP header blocks not understood	One or more mandatory SOAP header blocks were not understood.
env:DataEncodingUnknown		Unsupported SOAP data encoding	SOAP header block or SOAP body child element information item is scoped with data encoding that is not supported by the device.
env:Sender	ter:WellFormed	Well-formed error	XML well-formed violation occurred.
env:Sender	ter:TagMismatch	Tag mismatch	There was a tag name or namespace mismatch.
env:Sender	ter:Tag	No tag	XML element tag was missing.
env:Sender	ter:Namespace	Namespace error	SOAP namespace error occurred.
env:Sender	ter:MissingAttr	Required attribute not present	There was a missing required attribute.
env:Sender	ter:ProhibAttr	Prohibited attribute	A prohibited attribute was present.
env:Sender	ter:InvalidArgs	Invalid arguments	An error due to any of the following: – missing argument – too many arguments – arguments are of the wrong data type.
env:Sender	ter:InvalidArgVal	Argument value invalid	The argument value is invalid.
env:Sender	ter:UnknownAction	Unknown action	An unknown action is specified.
env:Sender	ter:OperationProhibited	Operation not permitted	The requested operation is not permitted by the device.
env:Sender	ter:NotAuthorized	Sender not authorized	The action requested requires authorization and the sender is not authorized.
env:Receiver	ter:ActionNotSupported	Optional action not implemented	The requested action is optional and is not implemented by the device.
env:Receiver	ter:Action	Action failed	The requested SOAP action failed.
env:Receiver	ter:OutofMemory	Out of memory	The device does not have sufficient memory to complete the action.
env:Receiver	ter:CriticalError	Critical error	The device has encountered an error condition which it cannot recover by itself and needs reset or power cycle.

5.12.3.3 Specific faults

Specific faults apply only to a specific command or set of commands. The specific faults are declared as part of the service definitions.

5.12.3.4 HTTP errors

If the server waits for the start of the inbound message and no SOAP message is received, the server shall not generate a SOAP fault and instead sends an HTTP error response (see Table 6.

Documents
Document Sharing Hub
Full document details: BS EN 60839-11-31:2017

Table 6 – HTTP errors

HTTP error	HTTP error code	HTTP reason
Malformed request	400	Bad request
Requires authorization	401	Unauthorized
HTTP method is neither POST or GET	405	Method not allowed
Unsupported message encapsulation method	415	Unsupported media

A server should avoid reporting internal errors as this can expose security weaknesses that can be misused.

5.13 Security

5.13.1 Authentication

A device shall support digest authentication according to [RFC 2617] for authentication of web service requests.

Digest authentication gives only a rudimentary level of security. In a system where security is important, it is recommended to always configure the device for TLS-based access (see 11.2). Digest authentication combined with TLS, with client and server authentication, protected transport level security give an acceptable level of security in many systems.

A device should authenticate an RTSP request at the RTSP level. If HTTP is used to tunnel the RTSP request the device shall not authenticate on the HTTP level.

A device shall, when authenticating RTSP and HTTP methods, use user/credentials from the same set of users/credentials that are used for the WS part and digest authentication [RFC 2617] shall be used for RTSP and HTTP.

5.13.2 User-based access control

5.13.2.1 General

The authorization framework described in 5.13 allows for authentication of service requests. Once a service request is authenticated, the device shall decide based on its access policy whether the requestor is authorized to receive the service.

This document defines a set of command for managing the user credentials, see 8.4. These commands allow associating users with the different user levels defined in 5.13.2.2.

A device may support the definition of a custom access policy by the device user through the get and set access policy operations defined in 8.4.

5.13.2.2 User levels

Each user is associated with exactly one of the following user levels:

1) Administrator
2) Operator
3) User
4) Anonymous

Unauthenticated users are placed into the anonymous category and a device shall not allow users to be added to the anonymous user level category.

Documents
Document Sharing Hub
Full document details: BS EN 60839-11-31:2017

5.13.2.3 Access classes for service requests

The service requests are classified into access classes based to their impact. The following access classes are defined:

- PRE_AUTH

  The service shall not require user authentication.

  Example: GetEndpointReference
- READ_SYSTEM

  The service reads system configuration information from the device.

  Example: GetNetworkInterfaces
- READ_SYSTEM_SENSITIVE

  The service reads sensitive (but not really confidential) system configuration information from the device.
- READ_SYSTEM_SECRET

  The service reads confidential system configuration information from the device.

  Example: GetSystemLog
- WRITE_SYSTEM

  The service causes changes to the system configuration of the device.

  Example: SetNetworkDefaultGateway
- UNRECOVERABLE

  The service causes unrecoverable changes to the system configuration of the device.

  Example: SetSystemFactoryDefault
- READ_MEDIA

  The service reads data related to recorded media.

  Example: GetRecordings
- ACTUATE

  The service affects the runtime behaviour of the system.

  Example: CreateRecordingJob

Table 7 defines for each access class which user levels are allowed access. A user of level c shall be granted access to a service request associated to access class r if and only if an "X" is present in the cell at column c and row r.

Table 7 – Access class to user level mapping

	Administrator	Operator	User	Anonymous
PRE_AUTH	X	X	X	X
READ_SYSTEM	X	X	X	
READ_SYSTEM_SENSITIVE	X	X		
READ_SYSTEM_SECRET	X			
WRITE_SYSTEM	X			
UNRECOVERABLE	X			
READ_MEDIA	X	X	X	
ACTUATE	X	X		

Documents
Document Sharing Hub
Full document details: BS EN 60839-11-31:2017

5.13.2.4 Default access policy

By default the device should enforce the default access policy defined by this document, and other specifications based on this document, which gives an acceptable level of security in many systems.

The default access policy is defined for each service request. It is done by identifying which access class that should be associated with that service request. See 5.7.1 for details on how this is done.

5.14 String representation

5.14.1 Character set

A device shall support the UTF-8 character set and it may support other character sets. If a client sends a request using UTF-8, the device shall always reply using the UTF-8 character set.

5.14.2 Allowed characters in strings

A device shall not have any restriction regarding legal characters in string that are not explicitly stated in this document or other specification based on this document.

5.15 Proprietary extensions

Proprietary extensions to this document shall be handled as follows:

1) It is strongly recommended to add proprietary extensions through defining new web services commands, in a namespace different from the target namespace, and not through extensions of the existing schema elements. This option allows full backward and forward interoperability with extensions from different vendors.
2) If new commands are not the best way to add proprietary extensions, it is recommeneded, whenever possible, to declare proprietary element extensions as attribute declarations instead of adding new schema elements in existing types. New proprietary attributes shall be declared in a namespace different from the target namespace. This option allows full backward and forward interoperability.
3) If it is not possible to declare the proprietary extensions using new commands or attributes, the proprietary extensions shall be declared adding a unique mandatory type of extension element before the extension point and then add all new proprietary elements in this extension element. The new elements shall be declared in a namespace different from the target namespace. Each proprietary extension element shall have minOccurs="0" and the proprietary extension element declarations in the schema shall be followed by an xs:any element declaration in the target namespace with minOccurs="0" and maxOccurs="unbounded".

6 IP configuration

The device and client communicate over an open or closed IP network. This document does not place any general restrictions or requirements on the network type. It shall be possible, however, to establish communication links between the entities according to the architectural framework specified in Clause 4. Device IP configuration includes parameters such as IP addresses and a default gateway.

A device shall have at least one network interface that gives it IP network connectivity. Similarly, the client shall have at least one network interface that gives IP connectivity and allows data communication between the device and the client.

Both device and client shall support IPv4 based network communication. The device and client should support IPv6 based network communication.

AVA Documents
Document Sharing Hub

Full document details: BS EN 60839-11-31:2017

It shall be possible to make static IP configuration on the device using a network or local configuration interface.

A device should support dynamic IP configuration of link-local addresses according to [RFC 3927]. A device that supports IPv6 shall support stateless IP configuration according to [RFC 4862] and neighbour discovery according to [RFC 4861].

The device shall support dynamic IP configuration according to [RFC 2131]. A device that supports IPv6 shall support stateful IP configuration via DHCPv6 according to [RFC 3315] if signaled via the corresponding capability.

The device may support any additional IP configuration mechanism.

Network configuration of a device shall be provided via the device management service as specified in 8.3 and may additionally be provided through local interfaces. The latter is outside the scope of this document.

The default device configuration shall have both DHCP and dynamic link-local (stateless) address configuration enabled. Even if the device is configured through a static address configuration it should have the link-local address default enabled.

When a device is connected to an IPv4 network, address assignment priorities (link local versus routable address) should be done as recommended in [RFC 3927].

Further details regarding how the IP connectivity is achieved are outside the scope of this document.

7 Device discovery

7.1 General

A client searches for available devices using the dynamic Web services discovery protocol [XMLSOAP WS-Discovery].

A device compliant with this document shall implement the Target Service role as specified in [XMLSOAP WS-Discovery].

If necessary a client compliant with this document shall implement the Client role as specified in [XMLSOAP WS-Discovery].

[XMLSOAP WS-Discovery] describes the Universally Unique Identifier (UUID): URI format recommendation for endpoint references, but this document overrides this recommendation. Instead, the Uniform Resource Name: Universally Unique Identifier (URN:UUID) format is used [RFC 4122] (see 7.3.1).

7.2 Modes of operation

The device shall be able to operate in two modes:

- discoverable,
- non-discoverable.

A device in discoverable mode sends multicast Hello messages once connected to the network or sends its Status changes according to [XMLSOAP WS-Discovery]. In addition it always listens for Probe and Resolve messages and sends responses accordingly. A device in non-discoverable shall not listen to [XMLSOAP WS-Discovery] messages or send such messages.

AVA Documents
Document Sharing Hub
Full document details: BS EN 60839-11-31:2017

The devices default behaviour shall be the discoverable mode. In order to thwart denial-of-service attacks, it shall be possible to set a device into non-discoverable mode through the operation defined in 8.4.19.

7.3 Discovery definitions

7.3.1 Endpoint reference

A device or an endpoint that takes the client role shall use a URN:UUID [RFC 4122] as the address property of its endpoint reference.

The device or an endpoint that takes the client role shall use a stable, globally unique identifier that is constant across network interfaces as part of its endpoint reference property. The combination of an wsadis:Address and wsadis:ReferenceProperties provide a stable and globally-unique identifier.

7.3.2 Hello

7.3.2.1 Types

A device shall include the device management service port type, i.e. tds:Device, in the `<d:Types>` declaration.

The following example shows how the type is encoded in the SOAP Hello body:

```
<d:Types>tds:Device</d:Types>.
```

The Hello message may include additional types.

7.3.2.2 Scopes

7.3.2.2.1 General

A device shall include the scope `<d:Scopes>` attribute with the scopes of the device in the Hello message.

The device scope is set by using [RFC 3986] URIs. This document defines scope attributes as follows:

The scheme attribute:onvif

The authority attribute:www.onvif.org

This implies that all scope URIs defined by this document have the following format:

```
onvif://www.onvif.org/<path>
```

A device may have other scope URIs. These URIs are not restricted by the scope attributes defined in this document.

Table 8 defines a set of scope parameters. Apart from these standardized parameters, it shall be possible to set any scope parameter as defined by the device owner. Scope parameters can be listed and set through the commands defined in 8.4.

Documents
Document Sharing Hub
Full document details: BS EN 60839-11-31:2017

Table 8 – Scope parameters

Category	Defined values	Description
Location	Any character string or path value.	The location defines the physical location of the device. The location value might be any string describing the physical location of the device.
Hardware	Any character string or path value.	A string or path value describing the hardware of the device. A device shall include at least one hardware entry into its scope list.
Name	Any character string or path value.	The searchable name of the device. A device shall include at least one name entry into its scope list.

A device shall include at least one fixed entry (defined by the device vendor) of the hardware and name categories respectively in the scopes list. A device may include any other additional scope attributes in the scopes list.

A device might include an arbitrary number of scopes in its scope list. This implies that one unit might for example define several different location scopes. A probe is matched against all scopes in the list.

7.3.2.2.2 Example

The following example illustrates the usage of the scope value. This is just an example, and not at all an indication of what type of scope parameter to be part of a device configuration. In this example we assume that the device is configured with the following scopes:

```
onvif://www.onvif.org/hardware/D1-566
onvif://www.onvif.org/location/country/china
onvif://www.onvif.org/location/city/bejing
onvif://www.onvif.org/location/building/headquarter
onvif://www.onvif.org/location/floor/R5
onvif://www.onvif.org/name/ARV-453
```

A client that probes for the device with scope onvif://www.onvif.org will get a match. Similarly, a probe for the device with scope:

onvif://www.onvif.org/location/country/china

will give a match. A probe with:

`onvif://www.onvif.org/hardware/D1`

will not give a match.

7.3.2.3 Addresses

A device shall include the <d:XAddrs> element with the address(es) for the device service in the Hello message. A URI shall be provided for each protocol (http, https) and externally available IP address.

The device should provide a port 80 device service entry in order to allow firewall traversal.

The IP addressing configuration principles for a device are defined in Clause 6.

7.3.3 Probe and probe match

For the device probe match types, scopes and addresses definitions, see 7.3.2 Hello.

Documents
Document Sharing Hub
Full document details: BS EN 60839-11-31:2017

A device shall at least support the following scope matching rule:

```
http://schemas.xmlsoap.org/ws/2005/04/discovery/
```

This scope matching definitions differs slightly from the definition in [XMLSOAP WS-Discovery] as [RFC 2396] is replaced by [RFC 3986].

A device shall include the `<d:XAddrs>` element with the addresses for the device service in a matching probe match message. The `<d:XAddrs>` element will in most cases only contain one address to the device management service as defined in 5.2.

7.3.4 Resolve and resolve match

This document requires end point address information to be included into Hello and Probe Match messages. In most cases, there is no need for the resolve and resolve match exchange. To be compatible with the [XMLSOAP WS-Discovery] specification, however, a device should implement the resolve match response.

7.3.5 Bye

A device should send a one-way Bye message when it prepares to leave a network as described in [XMLSOAP WS-Discovery].

7.3.6 SOAP fault messages

If an error exists with the multicast packet, the device and client should silently discard and ignore the request. Sending an error response is not recommended due to the possibility of packet storms if many devices send an error response to the same request. For completeness, unicast packet error handling is described below.

If a device receives a unicast Probe message and it does not support the matching rule, then the device may choose not to send a Probe Match, and instead generate a SOAP fault bound to SOAP 1.2 as follows:

[action] `http://schemas.xmlsoap.org/ws/2005/04/discovery/fault`

[Code] `s12:Sender`

[Subcode] `d:MatchingRuleNotSupported`

[Reason] `E.g., the matching rule specified is not supported`

[Detail]
```
<d: SupportedMatchingRules>

    List of xs:anyURI

</d: SupportedMatchingRules>
```

8 Device management

8.1 General

The device service is divided into five different categories: capabilities, network, system, I/O and security commands. This set of commands can be used to obtain information about the device capabilities and configurations or to set device configurations. A device shall support the device management service as specified in Clause B.1. A basic set of operations are

AVA Documents
Document Sharing Hub

required for the device management service, other operations are recommended or optional to support. The detailed requirements are listed under the command descriptions.

8.2 Capabilities

8.2.1 Get WSDL URL

It is possible for an endpoint to request a URL that can be used to retrieve the complete schema and WSDL definitions of a device. The command gives in return a URL entry point where all the necessary product specific WSDL and schema definitions can be retrieved. The device shall provide a URL for WSDL and schema download through the GetWsdlUrl command.

Table 9 – GetWSDLUrl command

GetWsdlUrl	Access class: PRE_AUTH
Message name	**Description**
GetWsdlUrlRequest	*This is an empty message*
GetWsdlUrlResponse	*The requested URL.* xs:anyURI **WsdlUrl** [1][1]
Fault codes	**Description**
	No command specific faults!

8.2.2 Capability exchange

8.2.2.1 General

Any endpoint can ask for the capabilities of a device using the capability exchange request response operation. A device shall indicate its capabilities through the GetServices/GetServiceCapabilities commands.

The capability list includes references to the addresses (XAddr) of the service implementing the interface operations in the category.

8.2.2.2 GetServices

Returns a collection of the devices services and possibly their available capabilities. The returned capability response message is untyped to allow future addition of services, service revisions and service capabilities. All returned service capabilities shall be structured by different namespaces which are supported by a device.

A device shall support this method. For complementary information on the structure of GetServices response with capabilities, refer to Annex A.

Table 10 – GetServices command

GetServices	Access class: PRE_AUTH
Message name	**Description**
GetServicesRequest	*The message contains a request for all services in the device and possibly the capabilities for each service. If the Boolean IncludeCapability is set, then the response shall include the services capabilities.* boolean **IncludeCapability**[1][1]
GetServicesResponse	*The capability response message contains the requested information about the services.* tt:ServiceList [1][unbounded]
Fault codes	**Description**
	No command specific faults!

Documents
Document Sharing Hub

8.2.2.3 GetServiceCapabilities

This command returns the capabilities of the device service. A device shall support this command.

Table 11 and Table 12 describe how to interpret the indicated capabilities.

Table 11 – GetServiceCapabilities command

GetServiceCapabilities	Access class: PRE_AUTH
Message name	**Description**
GetServiceCapabilitiesRequest	*This is an empty message.*
GetServiceCapabilitiesResponse	*The capability response message contains the requested device capabilities using a hierarchical XML capability structure.* tds:DeviceServiceCapabilities **Capabilities** [1][1]
Fault codes	**Description**
	No command specific faults!

Table 12 – Capabilities in the GetServiceCapabilities command

Category	Capability	Description
Network	IPFilter	Indication if the device supports IP filtering control using the commands in 8.3.18, 8.3.19, 8.3.20 and 8.3.21.
	ZeroConfiguration	Indication if the device supports zero configuration according to the commands in 8.3.16 and 8.3.17.
	IPVersion6	Indication if the device supports IP version 6.
	DynDNS	Indication if the device supports Dynamic DNS configuration according to 8.3.8 and 8.3.9 .
	Dot11Configuration	Indication if the device supports IEEE802.11 configuration as specified in 8.3.22
	HostnameFromDHCP	Indicates whether retrieval of hostname from DHCP is supported by the device.
	NTP	Indicates the maximum number of supported NTP servers by the devices SetNTP command.
	Dot1XConfigurations	Indicates the maximum number of Dot1X configurations supported by the device, see 8.5.8
	DHCPv6	Indicates support for Stateful IPv6 DHCP.
System	DiscoveryResolve	Indication if the device responses to resolve requests as described in 7.3.4.
	DiscoveryBye	Indication if the device sends Bye messages as described in 7.3.5
	SystemBackup	Indication if the device supports system backup and restore as specified in 8.4.3 and 8.4.5
	FirmwareUpgrade	Indication if the device supports firmware upgrade as specified in 8.4.10.
	SystemLogging	Indication if the device supports system log retrieval as specified in 8.4.11.
	HttpSystemBackup	Indication if the device supports system backup and restore using HTTP GET and POST.
	HttpFirmwareUpgrade	Indication if the device supports firmware upgrade using HTTP POST.
	HTTPSystemLogging	Indication if the device supports retrieval of system log using HTTP Get, see 8.4.2.
	HTTPSupportInformation	Indication if the device supports retrieval of support information using HTTP Get, see 8.4.2.
Security	TLS1.0	Support of TLS 1.0.

Documents
Document Sharing Hub
Full document details: BS EN 60839-11-31:2017

Category	Capability	Description
	TLS1.1	Support of TLS 1.1.
	TLS1.2	Support of TLS 1.2.
	OnboardKeyGeneration	Indication if the device supports onboard key generation and creation of self-signed certificates as specified in 8.5.9.
	AccessPolicyConfig	Indication if the device supports retrieving and loading device access control policy according to 8.5.2 and 8.5.3.
	DefaultAccessPolicy	Indicates if the device supports the default access policies as defined in 5.13.2.4.
	HttpDigest	Indication if the device supports the HTTP digest authentication.
	Dot1X	Indication if the device supports IEEE 802.1X port-based network authentication
	SupportedEAPMethod	List of supported EAP method types. The numbers correspond to the IANA [EAP-Registry].
	RemoteUserHandling	Indication if the device supports remote user handling and the corresponding methods defined in 8.5.22 and 8.5.23.
	MaxUsers	The maximum number of users that the device supports

8.3 Network

8.3.1 Get hostname

This operation is used by an endpoint to get the hostname from a device. The device shall return its hostname configurations through the GetHostname command as described in Table 13.

Table 13 – GetHostname command

GetHostname	Access Class: PRE_AUTH
Message name	**Description**
GetHostnameRequest	*This is an empty message.*
GetHostnameResponse	*This message contains:* • *"FromDHCP": True if the hostname is obtained via DHCP* • *"Name": The hostname. In case of DHCP the hostname has been obtained from the DHCP server.* xs:boolean **FromDHCP** [1][1] xs:token **Name** [0][1]
Fault codes	**Description**
	No command specific faults!

8.3.2 Set hostname

This operation sets the hostname on a device. It shall be possible to set the device hostname configurations through the SetHostname command as described in Table 14. Attention: a call to SetDNS may result in overriding a previously set hostname.

A device shall accept strings formated according to RFC 1123:1989, Section 2.1 or alternatively to RFC 952; other string shall be considered as invalid strings.

A device shall try to retrieve the name via DHCP when the HostnameFromDHCP capability is set and an empty name string is provided.

Documents
Document Sharing Hub
Full document details: BS EN 60839-11-31:2017

Table 14 – SetHostname command

SetHostname	Access class: WRITE_SYSTEM
Message name	**Description**
SetHostnameRequest	*This message contains:* • *"Name": The hostname. If Name is an empty string hostname should be retrieved from DHCP, otherwise the specified Name shall be used.* xs:token **Name** [1][1]
SetHostnameResponse	*This is an empty message*
Fault codes	**Description**
env:Sender ter:InvalidArgVal ter:InvalidHostname	*The requested hostname cannot be accepted by the device.*

8.3.3 Set hostname from DHCP

This operation, as described in Table 15, controls whether the hostname shall be retrieved from DHCP.

A device shall support this command if support is signalled via the HostnameFromDHCP capability. Depending on the device implementation the change may only become effective after a device reboot.

Table 15 – SetHostnameFromDHCP command

SetHostnameFromDHCP	Access class: WRITE_SYSTEM
Message name	**Description**
SetHostnameFromDHCPRequest	*This message contains:* • *"FromDHCP": True if the hostname shall be obtained via DHCP.* xs:boolean **FromDHCP**[1][1]
SetHostnameFromDHCPResponse	*An indication if a reboot is needed in case of changes in the hostname settings.* xs:boolean **RebootNeeded** [1][1]
Fault codes	**Description**
	No command specific faults!

8.3.4 Get DNS settings

This operation gets the DNS settings from a device as described in Table 16. The device shall return its DNS configurations through the GetDNS command.

Documents
Document Sharing Hub
Full document details: BS EN 60839-11-31:2017

Table 16 – GetDNS command

GetDNS	Access class: READ_SYSTEM
Message name	**Description**
GetDNSRequest	*This is an empty message.*
GetDNSResponse	*This message contains:* • *"FromDHCP": True if the DNS servers are obtained via DHCP.* • *"SearchDomain": The domain(s) to search if the hostname is not fully qualified.* • *"DNSFromDHCP": A list of DNS servers obtained via DHCP in case FromDHCP is equal to true. This means that the resolved addresses in the field DNSFromDHCP are coming from DHCP and describe the configuration status.* • *"DNSManual": A list of manually given DNS servers* xs:boolean **FromDHCP** [1][1] xs:token **SearchDomain** [0][unbounded] tt:IPAddress **DNSFromDHCP** [0][unbounded] tt:IPAddress **DNSManual** [0][unbounded]
Fault codes	**Description**
	No command specific faults!

8.3.5 Set DNS settings

This operation sets the DNS settings on a device as described in Table 17. It shall be possible to set the device DNS configurations through the SetDNS command.

Table 17 – SetDNS command

SetDNS	Access class: WRITE_SYSTEM
Message name	**Description**
SetDNSRequest	*This message contains:* • *"FromDHCP": True if the DNS servers are obtained via DHCP* • *"SearchDomain": The domain(s) to search if the hostname is not fully qualified.* • *"DNSManual": A list of manually given DNS servers* xs:boolean **FromDHCP** [1][1] xs:token **SearchDomain** [0][unbounded] tt:IPAddress **DNSManual** [0][unbounded]
SetDNSResponse	*This is an empty message.*
Fault codes	**Description**
env:Sender ter:InvalidArgVal ter:InvalidIPv6Address	*The suggested IPv6 address is invalid.*
env:Sender ter:InvalidArgVal ter:InvalidIPv4Address	*The suggested IPv4 address is invalid.*

8.3.6 Get NTP settings

This operation gets the NTP settings from a device as described in Table 18. If the device supports NTP, it shall be possible to get the NTP server settings through the GetNTP command.

Documents
Document Sharing Hub
Full document details: BS EN 60839-11-31:2017

Table 18 – GetNTP command

GetNTP	Access class: READ_SYSTEM
Message name	**Description**
GetNTPRequest	*This is an empty message.*
GetNTPResponse	*This message contains:* • *"FromDHCP": True if the NTP servers are obtained via DHCP.* • *"NTPFromDHCP": A list of NTP servers obtained via DHCP in case FromDHCP is equal to true. This means that the NTP server addresses in the field NTPFromDHCP are coming from DHCP and describe the current configuration status.* • *"NTPManual": A list of manually given NTP servers* xs:boolean **FromDHCP** [1][1] tt:NetworkHost **NTPFromDHCP** [0][unbounded] tt:NetworkHost **NTPManual** [0][unbounded]
Fault codes	**Description**
	No command specific faults!

8.3.7 Set NTP settings

This operation sets the NTP settings on a device as described in Table 19. If support for NTP is signalled via the NTP capability, it shall be possible to set the NTP server settings through the SetNTP command.

A device shall accept string formated according to RFC 1123 section 2.1; other strings shall be considered as invalid strings.

Changes to the NTP server list shall not affect the clock mode DateTimeType. Use SetSystemDateAndTime to activate NTP operation.

Table 19 – SetNTP command

SetNTP	Access class: WRITE_SYSTEM
Message name	**Description**
SetNTPRequest	*This message contains:* • *"FromDHCP": True if the NTP servers are obtained via DHCP.* • *"NTPManual": A list of manually given NTP servers when they are not obtained via DHCP.* xs:boolean **FromDHCP** [1][1] tt:NetworkHost **NTPManual** [0][unbounded]
SetNTPResponse	*This is an empty message.*
Fault codes	**Description**
env:Sender ter:InvalidArgVal ter:InvalidIPv4Address	*The suggested IPv4 address is invalid.*
env:Sender ter:InvalidArgVal ter:InvalidIPv6Address	*The suggested IPv6 address is invalid.*
env:Sender ter:InvalidArgVal ter:InvalidDnsName	*The suggested NTP server name is invalid.*
env:Sender ter:InvalidArgVal ter:TimeSyncedToNtp	*Current DateTimeType requires an NTP server.*

8.3.8 Get dynamic DNS settings

This operation gets the dynamic DNS settings from a device as described in Table 20. If the device supports dynamic DNS as specified in [RFC 2136] and [RFC 4702], it shall be possible to get the type, name and TTL through the GetDynamicDNS command.

Documents
Document Sharing Hub
Full document details: BS EN 60839-11-31:2017

Table 20 – GetDynamicDNS command

GetDynamicDNS	Access class: READ_SYSTEM
Message name	**Description**
GetDynamicDNSRequest	*This is an empty message.*
GetDynamicDNSResponse	*This message contains:* • *"Type": The type of update. There are three possible types: the device desires no update (NoUpdate), the device wants the DHCP server to update (ServerUpdates) and the device does the update itself (ClientUpdates).* • *"Name": The DNS name in case the device does the update.* • *"TTL": Time to live.* *tt:DynamicDNSType **Type** [1][1]* *tt:DNSName **Name** [0][1]* *xs:duration **TTL** [0][1]*
Fault codes	**Description**
	No command specific faults!

8.3.9 Set dynamic DNS settings

This operation sets the dynamic DNS settings on a device as described in Table 21. If the device supports dynamic DNS as specified in [RFC 2136] and [RFC 4702], it shall be possible to set the type, name and TTL through the SetDynamicDNS command.

Table 21 – SetDynamicDNS command

SetDynamicDNS	Access class: WRITE_SYSTEM
Message name	**Description**
SetDynamicDNSRequest	*This message contains:* • *"Type": The type of update. There are three possible types: the device desires no update (NoUpdate), the device wants the DHCP server to update (ServerUpdates) and the device does the update itself (ClientUpdates).* • *"Name": The DNS name in case the device does the update.* • *"TTL": Time to live.* *tt:DynamicDNSType **Type** [1][1]* *tt:DNSName **Name** [0][1]* *xs:duration **TTL** [0][1]*
SetDynamicDNSResponse	*This is an empty message.*
Fault codes	**Description**
	No command specific faults!

8.3.10 Get network interface configuration

This operation gets the network interface configuration from a device as described in Table 22. The device shall support return of network interface configuration settings as defined by the NetworkInterface type through the GetNetworkInterfaces command.

Documents
Document Sharing Hub
Full document details: BS EN 60839-11-31:2017

Table 22 – GetNetworkInterfaces command

GetNetworkInterfaces	Access class: READ_SYSTEM
Message name	**Description**
GetNetworkInterfacesRequest	*This is an empty message.*
GetNetworkInterfacesResponse	*This message contains an array of device network interfaces.* tt:NetworkInterface **NetworkInterfaces** [0][unbounded]
Fault codes	**Description**
	No command specific faults!

8.3.11 Set network interface configuration

This operation sets the network interface configuration on a device as described in Table 23. The device shall support network configuration of supported network interfaces through the SetNetworkInterfaces command.

If a device responds with RebootNeeded set to false, the device can be reached via the new IP address without further action. A client should be aware that a device may not be responsive for a short period of time until it signals availability at the new address via the discovery Hello messages as defined in 7.3.2.

If a device responds with RebootNeeded set to true, it will be further available under its previous IP address. The settings will only be activated when the device is rebooted via the SystemReboot command.

For interoperability with a client unaware of the IEEE 802.11 extension a device shall retain its IEEE 802.11 configuration if the IEEE 802.11 configuration element is not present in the request.

Documents
Document Sharing Hub
Full document details: BS EN 60839-11-31:2017