

INTERNATIONAL STANDARD

NORME INTERNATIONALE



**Alarm and electronic security systems –
Part 11-33: Electronic access control systems – Access control configuration
based on Web services**

**Systèmes d'alarme et de sécurité électroniques –
Partie 11-33: Systèmes de contrôle d'accès électronique – Configuration du
contrôle d'accès en fonction des services Web**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 13.320

ISBN 978-2-8322-4690-0

Warning! Make sure that you obtained this publication from an authorized distributor. Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.
--

CONTENTS

FOREWORD.....	8
INTRODUCTION.....	10
1 Scope.....	11
2 Normative references	11
3 Terms and definitions	12
4 Overview	15
4.1 General.....	15
4.2 Namespaces	16
4.3 Error handling	17
5 Credential service.....	17
5.1 General.....	17
5.2 Service capabilities	18
5.2.1 General	18
5.2.2 ServiceCapabilities data structure.....	18
5.2.3 GetServiceCapabilities command	19
5.3 Credential information.....	20
5.3.1 General	20
5.3.2 Data structures	20
5.3.3 GetCredentialInfoList command.....	23
5.3.4 GetCredentials command	24
5.3.5 GetCredentialList command.....	25
5.3.6 CreateCredential command	26
5.3.7 SetCredential command.....	28
5.3.8 ModifyCredential command.....	30
5.3.9 DeleteCredential command.....	31
5.3.10 GetCredentialState command	32
5.3.11 EnableCredential command	32
5.3.12 DisableCredential command	33
5.3.13 ResetAntipassbackViolation command.....	33
5.3.14 GetSupportedFormatTypes command.....	34
5.3.15 GetCredentialIdentifiers command	34
5.3.16 SetCredentialIdentifier command	35
5.3.17 DeleteCredentialIdentifier command	36
5.3.18 GetCredentialAccessProfiles command	36
5.3.19 SetCredentialAccessProfiles command.....	37
5.3.20 DeleteCredentialAccessProfiles command.....	37
5.4 Notification topics	38
5.4.1 General	38
5.4.2 Event overview (informative).....	38
5.4.3 Status changes.....	38
5.4.4 Configuration changes	39
6 Access rules service.....	40
6.1 General.....	40
6.2 Service capabilities	41
6.2.1 General	41
6.2.2 ServiceCapabilities data structure.....	41

6.2.3	GetServiceCapabilities command	41
6.3	Access profile information	41
6.3.1	General	41
6.3.2	Data structures	42
6.3.3	GetAccessProfileInfo command	42
6.3.4	GetAccessProfileInfoList command	43
6.3.5	GetAccessProfiles command	44
6.3.6	GetAccessProfileList command	45
6.3.7	CreateAccessProfile command	46
6.3.8	SetAccessProfile command	47
6.3.9	ModifyAccessProfile command	48
6.3.10	DeleteAccessProfile command	49
6.4	Notification topics	50
6.4.1	General	50
6.4.2	Event overview (informative)	50
6.4.3	Configuration changes	50
7	Authentication behaviour service	51
7.1	General	51
7.2	Example	51
7.3	Service capabilities	52
7.3.1	General	52
7.3.2	ServiceCapabilities data structure	52
7.3.3	GetServiceCapabilities command	53
7.4	Authentication profile information	53
7.4.1	General	53
7.4.2	Data structures	54
7.4.3	GetAuthenticationProfileInfo command	55
7.4.4	GetAuthenticationProfileInfoList command	56
7.4.5	GetAuthenticationProfiles command	57
7.4.6	GetAuthenticationProfileList command	58
7.4.7	CreateAuthenticationProfile command	59
7.4.8	SetAuthenticationProfile command	60
7.4.9	ModifyAuthenticationProfile command	61
7.4.10	DeleteAuthenticationProfile command	62
7.5	Security level information	63
7.5.1	General	63
7.5.2	Data structures	64
7.5.3	GetSecurityLevelInfo command	66
7.5.4	GetSecurityLevelInfoList command	66
7.5.5	GetSecurityLevels command	67
7.5.6	GetSecurityLevelList command	68
7.5.7	CreateSecurityLevel command	69
7.5.8	SetSecurityLevel command	70
7.5.9	ModifySecurityLevel command	71
7.5.10	DeleteSecurityLevel command	72
7.6	Notification topics	73
7.6.1	General	73
7.6.2	Event overview (informative)	73
7.6.3	Configuration changes	73

8	Schedule service	74
8.1	General.....	74
8.2	Recurrence	76
8.2.1	General	76
8.2.2	Weekly recurrence.....	76
8.2.3	Extended recurrence	77
8.2.4	Standard schedule recurrence	77
8.2.5	Special day recurrence	77
8.3	Service capabilities	78
8.3.1	General	78
8.3.2	ServiceCapabilities data structure.....	78
8.3.3	GetServiceCapabilities command	79
8.4	Schedule information	79
8.4.1	General	79
8.4.2	Data structures	79
8.4.3	GetScheduleInfo command	82
8.4.4	GetScheduleInfoList command	83
8.4.5	GetSchedules command	84
8.4.6	GetScheduleList command	85
8.4.7	CreateSchedule command.....	86
8.4.8	SetSchedule command	87
8.4.9	ModifySchedule command	88
8.4.10	DeleteSchedule command	89
8.5	Special day group information.....	90
8.5.1	General	90
8.5.2	Data structures	90
8.5.3	GetSpecialDayGroupInfo command	90
8.5.4	GetSpecialDayGroupInfoList command.....	91
8.5.5	GetSpecialDayGroups command	92
8.5.6	GetSpecialDayGroupList command.....	93
8.5.7	CreateSpecialDayGroup command	94
8.5.8	SetSpecialDayGroup command	95
8.5.9	ModifySpecialDayGroup command	96
8.5.10	DeleteSpecialDayGroup command.....	97
8.6	Schedule status	97
8.6.1	ScheduleState data structure.....	97
8.6.2	GetScheduleState command.....	98
8.7	Notification topics	99
8.7.1	General	99
8.7.2	Event overview (informative).....	99
8.7.3	Status changes.....	99
8.7.4	Configuration changes	100
8.8	Examples	101
8.8.1	General	101
8.8.2	Access 24 × 7 for admin staff.....	101
8.8.3	Access on Monday and Wednesday from 06:00 to 20:00 for cleaning staff	101
8.8.4	Access from Friday 18:00 to 07:00 for maintenance staff.....	101
8.8.5	Access on weekdays from 08:00 to 17:00 for employees	102

8.8.6	Access from January 15, 2014, to January 14, 2015, from 09:00 to 18:00	103
8.8.7	Special days example 1	103
8.8.8	Special days example 2	104
8.8.9	Special days example 3	106
Annex A (normative)	Access control interface XML schemata	107
A.1	Credential service WSDL	107
A.2	Access rules service WSDL	127
A.3	Authentication behaviour service WSDL	137
A.4	Schedule service WSDL	155
Annex B (informative)	Mapping of mandatory functions in IEC 60839-11-1	174
Bibliography		182
Figure 1	– Overview of service dependencies	16
Figure 2	– Main data structures in the credential service	18
Figure 3	– Main data structures in the access rules service	40
Figure 4	– Multiple schedules per access point	46
Figure 5	– Result of schedule union	47
Figure 6	– Authentication behaviour example	52
Figure 7	– Related objects of an authentication profile	54
Figure 8	– Related objects of a security level	63
Figure 9	– Security level examples	65
Figure 10	– Main data structures in the schedule service	74
Figure 11	– Recurrence support matrix	76
Figure 12	– Recurring events with an exception	77
Figure 13	– Recurring events with a special day	78
Figure 14	– SpecialDaysSchedule example	81
Figure 15	– Example of special day with time part	81
Figure 16	– Schedule states	98
Table 1	– Defined namespaces in this document	16
Table 2	– Referenced namespaces (with prefix)	16
Table 3	– GetServiceCapabilities command	19
Table 4	– GetCredentialInfo command	23
Table 5	– GetCredentialInfoList command	24
Table 6	– GetCredentials command	25
Table 7	– GetCredentialList command	26
Table 8	– CreateCredential command	27
Table 9	– SetCredential command	29
Table 10	– ModifyCredential command	31
Table 11	– DeleteCredential command	32
Table 12	– GetCredentialState command	32
Table 13	– EnableCredential command	33
Table 14	– DisableCredential command	33

Table 15 – ResetAntipassbackViolation command	34
Table 16 – GetSupportedFormatTypes command.....	34
Table 17 – GetCredentialIdentifiers command.....	35
Table 18 – SetCredentialIdentifier command.....	35
Table 19 – DeleteCredentialIdentifier command	36
Table 20 – GetCredentialAccessProfiles command	36
Table 21 – SetCredentialAccessProfiles command	37
Table 22 – DeleteCredentialAccessProfiles command.....	38
Table 23 – GetServiceCapabilities command	41
Table 24 – GetAccessProfileInfo command.....	43
Table 25 – GetAccessProfileInfoList command	44
Table 26 – GetAccessProfiles command	45
Table 27 – GetAccessProfileList command	46
Table 28 – CreateAccessProfile command	47
Table 29 – SetAccessProfile command	48
Table 30 – ModifyAccessProfile command	49
Table 31 – DeleteAccessProfile command	50
Table 32 – Example of schedule state to security level mapping	51
Table 33 – GetServiceCapabilities command	53
Table 34 – GetAuthenticationProfileInfo command	56
Table 35 – GetAuthenticationProfileInfoList command	57
Table 36 – GetAuthenticationProfiles command	58
Table 37 – GetAuthenticationProfileList command	59
Table 38 – CreateAuthenticationProfile command	60
Table 39 – SetAuthenticationProfile command	61
Table 40 – ModifyAuthenticationProfile command	62
Table 41 – DeleteAuthenticationProfile command	63
Table 42 – GetSecurityLevelInfo command	66
Table 43 – GetSecurityLevelInfoList command.....	67
Table 44 – GetSecurityLevels command	68
Table 45 – GetSecurityLevelList command	69
Table 46 – CreateSecurityLevel command	70
Table 47 – SetSecurityLevel command	71
Table 48 – ModifySecurityLevel command	72
Table 49 – DeleteSecurityLevel command	72
Table 50 – GetServiceCapabilities command	79
Table 51 – GetScheduleInfo command.....	83
Table 52 – GetScheduleInfoList command	84
Table 53 – GetSchedules command.....	85
Table 54 – GetScheduleList command.....	86
Table 55 – CreateSchedule command.....	87
Table 56 – SetSchedule command.....	88
Table 57 – ModifySchedule command.....	89

Table 58 – DeleteSchedule command	89
Table 59 – GetSpecialDayGroupInfo command	91
Table 60 – GetSpecialDayGroupInfoList command	92
Table 61 – GetSpecialDayGroups command	93
Table 62 – GetSpecialDayGroupList command	94
Table 63 – CreateSpecialDayGroup command	95
Table 64 – SetSpecialDayGroup command	96
Table 65 – ModifySpecialDayGroup command	97
Table 66 – DeleteSpecialDayGroup command	97
Table 67 – GetScheduleState command	99
Table B.1 – Access point interface requirements.....	175
Table B.2 – Indication and annunciation requirements	176
Table B.3 – Recognition requirements	179
Table B.4 – Duress signalling requirements	180
Table B.5 – Overriding requirements.....	181
Table B.6 – System self protection requirements	181

INTERNATIONAL ELECTROTECHNICAL COMMISSION

ALARM AND ELECTRONIC SECURITY SYSTEMS –**Part 11-33: Electronic access control systems –
Access control configuration 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.

IEC 60839-11-33 has been prepared by IEC technical committee 79: Alarm and electronic security systems. It is an International Standard.

The text of this International Standard is based on the following documents:

FDIS	Report on voting
79/646/FDIS	79/648/RVD

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

The language used for the development of this International Standard is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/standardsdev/publications.

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 document will remain unchanged until the stability date indicated on the IEC website under webstore.iec.ch in the data related to the specific document. At this date, the document will be

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

IMPORTANT – The "colour inside" logo on the cover page of this document 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.

INTRODUCTION

This document makes it possible to build an alarm and electronic security system with clients, typically a monitoring console, and devices, typically an access control unit, from different manufacturers using common and well defined interfaces.

The document specifies only the data and control flow between a client and the services without reference to any physical device as the services required to implement a compliant electronic access control system (EACS) are not necessarily implemented on a single device, i.e. all services can be run on a control panel, event aggregator software on PC, etc.

This document does not define internal communication between an access control unit and its components if they are implemented on a single device.

This document is based upon work done by the ONVIF open industry forum. The ONVIF Credential specification, ONVIF Access Rules specification, ONVIF Authentication Behaviour specification and ONVIF Schedule specification are compatible with this document.

This document is accompanied by a set of computer readable interface definitions (see Annex A):

- credential service WSDL, see Clause A.1;
- access rules service WSDL, see Clause A.2;
- authentication behaviour service WSDL, see Clause A.3;
- schedule service WSDL, see Clause A.4.

Due to the differences in terminology used in IEC 60839-11-1:2013 and IEC 60839-11-2:2014 and the ONVIF specification that this part of IEC 60839 is based on, a reader should take special notice of the terms and definitions clause.

Additional services needed for monitoring of doors and access points (portal sides) are outside the scope of this document. These services are covered by IEC 60839-11-32.

ALARM AND ELECTRONIC SECURITY SYSTEMS –

Part 11-33: Electronic access control systems – Access control configuration based on Web services

1 Scope

This part of IEC 60839 defines the Web services interface for electronic access control systems. This includes listing electronic access control system components, their logical composition, monitoring their states and controlling them. It also includes a mapping of mandatory and optional requirements in accordance with IEC 60839-11-1:2013, as covered by Annex B.

This document applies to physical security only. Physical security prevents unauthorized personnel, attackers or accidental intruders from physically accessing a building, room, etc.

Web services usage and device management functionality are outside the scope of this document. Refer to IEC 60839-11-31:2016 for more information.

This document does not in any way limit a manufacturer to add other protocols or extend the protocol defined here. For rules on how to accomplish this, refer to IEC 60839-11-31:2016.

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.

IEC 60839-11-1:2013, *Alarm and electronic security systems – Part 11-1: Electronic access control systems – System and components requirements*

IEC 60839-11-2:2014, *Alarm and electronic security systems – Part 11-2: Electronic access control systems – Application guidelines*

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

IEC 60839-11-32:2016, *Alarm and electronic security systems – Part 11-32: Electronic access control systems – Access control monitoring based on Web services*

ISO 16484-5:2017, *Building automation and control systems (BACS) – Part 5: Data communication protocol*

RFC 5545, *Internet Calendaring and Scheduling Core Object Specification (iCalendar)*,
(available at <https://tools.ietf.org/html/rfc5545>)

RFC 5234, *Augmented BNF for Syntax Specifications: ABNF*,
(available at <https://tools.ietf.org/html/rfc5234>)

SOMMAIRE

AVANT-PROPOS	190
INTRODUCTION.....	192
1 Domaine d'application	193
2 Références normatives	193
3 Termes et définitions	194
4 Vue d'ensemble	197
4.1 Généralités	197
4.2 Espaces de nommage.....	198
4.3 Traitement des erreurs.....	199
5 Service de l'identifiant	199
5.1 Généralités	199
5.2 Fonctionnalités de service	200
5.2.1 Généralités	200
5.2.2 Structure de données ServiceCapabilities.....	200
5.2.3 Commande GetServiceCapabilities	201
5.3 Informations sur l'identifiant	202
5.3.1 Généralités	202
5.3.2 Structures de données.....	202
5.3.3 Commande GetCredentialInfoList	205
5.3.4 Commande GetCredentials	206
5.3.5 Commande GetCredentialList	207
5.3.6 Commande CreateCredential.....	208
5.3.7 Commande SetCredential	210
5.3.8 Commande ModifyCredential	212
5.3.9 Commande DeleteCredential	213
5.3.10 Commande GetCredentialState	214
5.3.11 Commande EnableCredential	214
5.3.12 Commande DisableCredential.....	215
5.3.13 Commande ResetAntipassbackViolation	215
5.3.14 Commande GetSupportedFormatTypes	216
5.3.15 Commande GetCredentialIdentifiers	216
5.3.16 Commande SetCredentialIdentifier	217
5.3.17 Commande DeleteCredentialIdentifier.....	218
5.3.18 Commande GetCredentialAccessProfiles	218
5.3.19 Commande SetCredentialAccessProfiles	219
5.3.20 Commande DeleteCredentialAccessProfiles	219
5.4 Rubriques de notification	220
5.4.1 Généralités	220
5.4.2 Présentation de l'événement (informative)	220
5.4.3 Changements d'état.....	220
5.4.4 Modifications de configuration	221
6 Service des règles d'accès	222
6.1 Généralités	222
6.2 Fonctionnalités de service	223
6.2.1 Généralités	223
6.2.2 Structure de données ServiceCapabilities.....	223

6.2.3	Commande GetServiceCapabilities	223
6.3	Informations sur les profils d'accès	224
6.3.1	Généralités	224
6.3.2	Structures de données	224
6.3.3	Commande GetAccessProfileInfo	225
6.3.4	Commande GetAccessProfileInfoList	225
6.3.5	Commande GetAccessProfiles	226
6.3.6	Commande GetAccessProfileList	227
6.3.7	Commande CreateAccessProfile	228
6.3.8	Commande SetAccessProfile	230
6.3.9	Commande ModifyAccessProfile	230
6.3.10	Commande DeleteAccessProfile	231
6.4	Rubriques de notification	232
6.4.1	Généralités	232
6.4.2	Présentation de l'événement (informative)	232
6.4.3	Modifications de configuration	232
7	Service de comportement d'authentification	233
7.1	Généralités	233
7.2	Exemple	233
7.3	Fonctionnalités de service	234
7.3.1	Généralités	234
7.3.2	Structure de données ServiceCapabilities	234
7.3.3	Commande GetServiceCapabilities	235
7.4	Informations sur le profil d'authentification	235
7.4.1	Généralités	235
7.4.2	Structures de données	236
7.4.3	Commande GetAuthenticationProfileInfo	238
7.4.4	Commande GetAuthenticationProfileInfoList	238
7.4.5	Commande GetAuthenticationProfiles	239
7.4.6	Commande GetAuthenticationProfileList	240
7.4.7	Commande CreateAuthenticationProfile	241
7.4.8	Commande SetAuthenticationProfile	242
7.4.9	Commande ModifyAuthenticationProfile	243
7.4.10	Commande DeleteAuthenticationProfile	244
7.5	Informations sur le niveau de sécurité	245
7.5.1	Généralités	245
7.5.2	Structures de données	246
7.5.3	Commande GetSecurityLevelInfo	248
7.5.4	Commande GetSecurityLevelInfoList	248
7.5.5	Commande GetSecurityLevels	249
7.5.6	Commande GetSecurityLevelList	250
7.5.7	Commande CreateSecurityLevel	251
7.5.8	Commande SetSecurityLevel,	252
7.5.9	Commande ModifySecurityLevel	253
7.5.10	Commande DeleteSecurityLevel	254
7.6	Rubriques de notification	255
7.6.1	Généralités	255
7.6.2	Présentation de l'événement (informative)	255
7.6.3	Modifications de configuration	255

8	Service de programmation	256
8.1	Généralités	256
8.2	Périodicité.....	258
8.2.1	Généralités	258
8.2.2	Périodicité hebdomadaire	258
8.2.3	Périodicité étendue.....	259
8.2.4	Périodicité de programme normalisé.....	259
8.2.5	Périodicité de jours particuliers.....	259
8.3	Fonctionnalités de service	260
8.3.1	Généralités	260
8.3.2	Structure de données ServiceCapabilities.....	260
8.3.3	Commande GetServiceCapabilities	261
8.4	Informations sur le programme.....	261
8.4.1	Généralités	261
8.4.2	Structures de données.....	262
8.4.3	Commande GetScheduleInfo	264
8.4.4	Commande GetScheduleInfoList.....	265
8.4.5	Commande GetSchedules	266
8.4.6	Commande GetScheduleList.....	267
8.4.7	Commande CreateSchedule	268
8.4.8	Commande SetSchedule	269
8.4.9	Commande ModifySchedule	270
8.4.10	Commande DeleteSchedule.....	271
8.5	Informations sur les groupes de jours particuliers	272
8.5.1	Généralités	272
8.5.2	Structures de données.....	272
8.5.3	Commande GetSpecialDayGroupInfo.....	272
8.5.4	Commande GetSpecialDayGroupInfoList	273
8.5.5	Commande GetSpecialDayGroups	274
8.5.6	Commande GetSpecialDayGroupList.....	275
8.5.7	Commande CreateSpecialDayGroup.....	276
8.5.8	Commande SetSpecialDayGroup	277
8.5.9	Commande ModifySpecialDayGroup.....	278
8.5.10	Commande DeleteSpecialDayGroup	279
8.6	Etat du programme	280
8.6.1	Structure de données ScheduleState	280
8.6.2	Commande GetScheduleState	280
8.7	Rubriques de notification	281
8.7.1	Généralités	281
8.7.2	Présentation de l'événement (informative)	281
8.7.3	Changements d'état.....	281
8.7.4	Modifications de configuration	282
8.8	Exemples	283
8.8.1	Généralités	283
8.8.2	Accès 24h/24, 7j/7 pour le personnel administratif	283
8.8.3	Accès le lundi et le mercredi de 06:00 à 20:00 pour l'équipe de nettoyage	283
8.8.4	Accès le vendredi de 18:00 à 07:00 pour le personnel d'entretien.....	283
8.8.5	Accès en semaine de 08:00 à 17:00 pour les employés	284

8.8.6	Accès du 15 janvier 2014 au 14 janvier 2015 de 09:00 à 18:00	285
8.8.7	Exemple de jours particuliers 1	285
8.8.8	Exemple de jours particuliers 2	286
8.8.9	Exemple de jours particuliers 3	288
Annexe A (normative) Schéma XML d'interface de contrôle d'accès		289
A.1	Service de l'identifiant WSDL	289
A.2	Service des règles d'accès WSDL	309
A.3	Service de comportement d'authentification WSDL	319
A.4	Service de programmation WSDL	337
Annexe B (informative) Mapping des fonctions obligatoires spécifiées dans l'IEC 60839-11-1		355
Bibliographie		364
Figure 1 – Présentation des dépendances de services		198
Figure 2 – Structures de données principales dans le service de l'identifiant		200
Figure 3 – Structures de données principales dans le service des règles d'accès		222
Figure 4 – Plusieurs programmes par point d'accès		229
Figure 5 – Résultat de l'union des programmes		229
Figure 6 – Exemple de comportement d'authentification		234
Figure 7 – Objets connexes d'un profil d'authentification		236
Figure 8 – Objets connexes d'un niveau de sécurité		245
Figure 9 – Exemples de niveaux de sécurité		247
Figure 10 – Structures de données principales dans le service de programmation		256
Figure 11 – Matrice de prise en charge de la périodicité		258
Figure 12 – Événements récurrents avec une exception		259
Figure 13 – Événements récurrents avec un jour particulier		260
Figure 14 – Exemple de SpecialDaysSchedule		263
Figure 15 – Exemple de jour particulier avec plage horaire		263
Figure 16 – Etats du programme		280
Tableau 1 – Espaces de nommage définis dans le présent document		198
Tableau 2 – Espaces de nommage référencés (avec préfixe)		199
Tableau 3 – Commande GetServiceCapabilities		201
Tableau 4 – Commande GetCredentialInfo		205
Tableau 5 – Commande GetCredentialInfoList		206
Tableau 6 – Commande GetCredentials		207
Tableau 7 – Commande GetCredentialList		208
Tableau 8 – Commande CreateCredential		209
Tableau 9 – Commande SetCredential		211
Tableau 10 – Commande ModifyCredential		213
Tableau 11 – Commande DeleteCredential		214
Tableau 12 – Commande GetCredentialState		214
Tableau 13 – Commande EnableCredential		215
Tableau 14 – Commande DisableCredential		215

Tableau 15 – Commande ResetAntipassbackViolation	216
Tableau 16 – Commande GetSupportedFormatTypes	216
Tableau 17 – Commande GetCredentialIdentifiers	217
Tableau 18 – Commande SetCredentialIdentifier	217
Tableau 19 – Commande DeleteCredentialIdentifier	218
Tableau 20 – Commande GetCredentialAccessProfiles	218
Tableau 21 – Commande SetCredentialAccessProfiles	219
Tableau 22 – Commande DeleteCredentialAccessProfiles	220
Tableau 23 – Commande GetServiceCapabilities	223
Tableau 24 – Commande GetAccessProfileInfo	225
Tableau 25 – Commande GetAccessProfileInfoList	226
Tableau 26 – Commande GetAccessProfiles	227
Tableau 27 – Commande GetAccessProfileList	228
Tableau 28 – Commande CreateAccessProfile	229
Tableau 29 – Commande SetAccessProfile	230
Tableau 30 – Commande ModifyAccessProfile	231
Tableau 31 – Commande DeleteAccessProfile	232
Tableau 32 – Exemple de mapping de l'état du programme et du niveau de sécurité	233
Tableau 33 – Commande GetServiceCapabilities	235
Tableau 34 – Commande GetAuthenticationProfileInfo	238
Tableau 35 – Commande GetAuthenticationProfileInfoList	239
Tableau 36 – Commande GetAuthenticationProfiles	240
Tableau 37 – Commande GetAuthenticationProfileList	241
Tableau 38 – Commande CreateAuthenticationProfile	242
Tableau 39 – Commande SetAuthenticationProfile	243
Tableau 40 – Commande ModifyAuthenticationProfile	244
Tableau 41 – Commande DeleteAuthenticationProfile	245
Tableau 42 – Commande GetSecurityLevelInfo	248
Tableau 43 – Commande GetSecurityLevelInfoList	249
Tableau 44 – Commande GetSecurityLevels	250
Tableau 45 – Commande GetSecurityLevelList	251
Tableau 46 – Commande CreateSecurityLevel	252
Tableau 47 – Commande SetSecurityLevel	253
Tableau 48 – Commande ModifySecurityLevel	254
Tableau 49 – Commande DeleteSecurityLevel	254
Tableau 50 – Commande GetServiceCapabilities	261
Tableau 51 – Commande GetScheduleInfo	265
Tableau 52 – Commande GetScheduleInfoList	266
Tableau 53 – Commande GetSchedules	267
Tableau 54 – Commande GetScheduleList	268
Tableau 55 – Commande CreateSchedule	269
Tableau 56 – Commande SetSchedule	270
Tableau 57 – Commande ModifySchedule	271

Tableau 58 – Commande DeleteSchedule.....	271
Tableau 59 – Commande GetSpecialDayGroupInfo	273
Tableau 60 – Commande GetSpecialDayGroupInfoList	274
Tableau 61 – Commande GetSpecialDayGroups.....	275
Tableau 62 – Commande GetSpecialDayGroupList.....	276
Tableau 63 – Commande CreateSpecialDayGroup.....	277
Tableau 64 – Commande SetSpecialDayGroup.....	278
Tableau 65 – Commande ModifySpecialDayGroup.....	279
Tableau 66 – Commande DeleteSpecialDayGroup	279
Tableau 67 – Commande GetScheduleState	281
Tableau B.1 – Exigences concernant les interfaces de points d'accès.....	356
Tableau B.2 – Exigences concernant les indications et les annonces.....	357
Tableau B.3 – Exigences concernant la reconnaissance	361
Tableau B.4 – Exigences concernant les signalements d'agression	363
Tableau B.5 – Exigences concernant la neutralisation	363
Tableau B.6 – Exigences concernant l'autoprotection du système.....	363

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

SYSTÈMES D'ALARME ET DE SÉCURITÉ ÉLECTRONIQUES –

Partie 11-33: Systèmes de contrôle d'accès électronique –
Configuration du contrôle d'accès en fonction des services Web

AVANT-PROPOS

- 1) La Commission Electrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
- 2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
- 3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
- 4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
- 5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
- 6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
- 7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
- 8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
- 9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets.

L'IEC 60839-11-33 a été établie par le comité d'études 79 de l'IEC: Systèmes d'alarme et de sécurité électroniques. Il s'agit d'une Norme internationale.

Le texte de cette Norme internationale est issu des documents suivants:

FDIS	Rapport de vote
79/646/FDIS	79/648/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à son approbation.

La langue employée pour l'élaboration de cette Norme internationale est l'anglais.

Le présent document a été rédigé selon les Directives ISO/IEC, Partie 2, il a été développé selon les Directives ISO/IEC, Partie 1 et les Directives ISO/IEC, Supplément IEC, disponibles sous www.iec.ch/members_experts/refdocs. Les principaux types de documents développés par l'IEC sont décrits plus en détail sous www.iec.ch/standardsdev/publications.

Une liste de toutes les parties de la série IEC 60839, publiées sous le titre général *Systèmes d'alarme et de sécurité électroniques*, se trouve sur le site web de l'IEC.

Le comité a décidé que le contenu du présent document ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous webstore.iec.ch dans les données relatives au document recherché. A cette date, le document sera

- reconduit,
- supprimé,
- remplacé par une édition révisée, ou
- amendé.

IMPORTANT – Le logo "colour inside" qui se trouve sur la page de couverture du présent document indique qu'il contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

INTRODUCTION

Le présent document permet d'établir un système d'alarme et de sécurité électroniques avec les clients (généralement une console de commande) ainsi que les dispositifs (généralement une unité de contrôle d'accès) de différents fabricants qui utilisent des interfaces courantes et bien définies.

Le présent document spécifie uniquement les flux de données et de commande entre un client et les services sans aucune référence aux dispositifs physiques, car les services exigés pour la mise en œuvre d'un système de contrôle d'accès électronique (EACS, *Electronic Access Control System*) conforme peuvent ne pas être nécessairement mis en œuvre sur un dispositif unique, c'est-à-dire que l'ensemble des services peuvent être exécutés sur un panneau de commande, un logiciel agrégateur d'événements sur PC, etc.

Le présent document ne définit pas la communication interne entre une unité de contrôle d'accès et ses composants s'ils sont mis en œuvre sur un dispositif unique.

Le présent document a été élaboré sur la base des travaux réalisés par le forum de l'industrie ONVIF (Open Network Video Interface Forum). La spécification Credential de l'ONVIF, la spécification Access Rules de l'ONVIF, la spécification Authentication Behavior de l'ONVIF et la spécification Schedule de l'ONVIF sont compatibles avec le présent document.

Le présent document s'accompagne d'un ensemble de définitions d'interfaces informatiques (voir Annexe A):

- WSDL du service de l'identifiant, voir Article A.1;
- WSDL du service des règles d'accès, voir Article A.2;
- WSDL du service de comportement d'authentification, voir Article A.3;
- WSDL du service de programmation, voir Article A.4.

En raison des différences terminologiques qui existent entre l'IEC 60839-11-1:2013, l'IEC 60839-11-2:2014 et les spécifications de l'ONVIF sur lesquelles repose la présente partie de l'IEC 60839, il convient que les lecteurs lisent l'article Termes et définitions avec attention.

Les services supplémentaires nécessaires à la commande des portes et des points d'accès (côtés accès contrôlé) ne relèvent pas du domaine d'application du présent document. Ces services sont couverts par l'IEC 60839-11-32.

SYSTÈMES D'ALARME ET DE SÉCURITÉ ÉLECTRONIQUES –

Partie 11-33: Systèmes de contrôle d'accès électronique – Configuration du contrôle d'accès en fonction des services Web

1 Domaine d'application

La présente partie de l'IEC 60839 définit l'interface de services Web pour les systèmes de contrôle d'accès électronique. Elle répertorie notamment les composants des systèmes de contrôle d'accès électronique et spécifie leur composition logique, leur contrôle et celui de leurs états. Elle définit également le mapping des exigences obligatoires et facultatives conformément à l'IEC 60839-11-1:2013 à l'Annexe B.

Le présent document s'applique uniquement à la sécurité physique. La sécurité physique empêche l'accès physique à un bâtiment, un local, etc., à tout personnel non autorisé, à des agresseurs ou à des intrus occasionnels.

L'utilisation des services Web et la fonctionnalité de gestion de dispositif ne relèvent pas du domaine d'application du présent document. Pour plus d'informations, se reporter à l'IEC 60839-11-31:2016.

Le présent document n'empêche en aucune façon un fabricant d'ajouter d'autres protocoles ou de développer le protocole défini ci-après. Pour plus d'informations sur les règles d'ajout ou d'extension, se reporter à l'IEC 60839-11-31:2016.

2 Références normatives

Les documents suivants sont cités dans le texte de sorte qu'ils constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

IEC 60839-11-1:2013, *Systèmes d'alarme et de sécurité électroniques – Partie 11-1: Systèmes de contrôle d'accès électronique – Exigences système et exigences concernant les composants*

IEC 60839-11-2:2014, *Systèmes d'alarme et de sécurité électroniques – Partie 11-2: Systèmes de contrôle d'accès électronique – Lignes directrices d'application*

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 60839-11-32:2016, *Systèmes d'alarme et de sécurité électroniques – Partie 11-32: Systèmes de contrôle d'accès électronique – Commande de contrôle d'accès en fonction des services Web*

ISO 16484-5:2017, *Building automation and control systems (BACS) – Part 5: Data communication protocol* (disponible en anglais seulement)

RFC 5545, *Internet Calendaring and Scheduling Core Object Specification (iCalendar)*
(disponible en anglais seulement)
(disponible à l'adresse <https://tools.ietf.org/html/rfc5545>)

RFC 5234, *Augmented BNF for Syntax Specifications: ABNF* (disponible en anglais seulement)
(disponible à l'adresse <https://tools.ietf.org/html/rfc5234>)