



# INTERNATIONAL STANDARD

# NORME INTERNATIONALE

---

**Alarm and electronic security systems –  
Part 11-5: Electronic access control systems – Open supervised device protocol  
(OSDP)**

**Systèmes d'alarme et de sécurité électroniques –  
Partie 11-5: Systèmes de contrôle d'accès électronique – Protocole ouvert  
d'appareil supervisé (OSDP)**

INTERNATIONAL  
ELECTROTECHNICAL  
COMMISSION

COMMISSION  
ELECTROTECHNIQUE  
INTERNATIONALE

---

ICS 13.320

ISBN 978-2-8322-9993-7

**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, definitions and abbreviated terms .....	11
3.1 Terms and definitions.....	11
3.2 Abbreviated terms.....	12
4 Overview .....	12
5 Communication settings.....	13
5.1 Physical interface .....	13
5.2 Signaling.....	13
5.3 Character encoding.....	13
5.4 Channel access .....	13
5.5 Multi-byte data encoding .....	13
5.6 Packet size limits .....	14
5.7 Timing.....	14
5.8 Message synchronization.....	14
5.9 Packet format .....	15
5.10 Multi-part messages.....	17
5.10.1 General .....	17
5.10.2 Multi-part message usage rules .....	17
5.11 Smartcard handling.....	18
6 Commands .....	19
6.1 General.....	19
6.2 Poll request (osdp_POLL).....	19
6.3 ID report request (osdp_ID) .....	19
6.4 Peripheral device capabilities request (osdp_CAP) .....	20
6.5 Local status report request (osdp_LSTAT) .....	20
6.6 Input status report request (osdp_ISTAT).....	20
6.7 Output status report request (osdp_OSTAT) .....	21
6.8 Reader status report request (osdp_RSTAT).....	21
6.9 Output control command (osdp_OUT) .....	21
6.10 Reader LED control command (osdp_LED) .....	22
6.11 Reader buzzer control command (osdp_BUZ) .....	24
6.12 Reader text output command (osdp_TEXT).....	25
6.13 Communication configuration command (osdp_COMSET).....	26
6.14 Scan and send biometric data (osdp_BIOREAD).....	27
6.15 Scan and match biometric template (osdp_BIOMATCH).....	28
6.16 Encryption key set (osdp_KEYSET) .....	29
6.17 Challenge and secure session initialization request (osdp_CHLNG).....	29
6.18 Server's random number and server cryptogram (osdp_SCRYPT).....	29
6.19 Manufacturer specific command (osdp_MFG) .....	29
6.20 ACU receive size (osdp_ACURXSIZE) .....	30
6.21 Keep reader active (osdp_KEEPACTIVE).....	30
6.22 Abort current operation (osdp_ABORT).....	31
6.23 Get PIV data (osdp_PIVDATA).....	31

6.24	General authenticate (osdp_GENAUTH) .....	31
6.25	Authentication challenge (osdp_CRAUTH) .....	32
6.26	File transfer command (osdp_FILETRANSFER) .....	33
6.27	Extended write data (osdp_XWR) .....	33
6.27.1	General .....	33
6.27.2	Mode set command .....	34
6.27.3	Mode-00 read setting .....	35
6.27.4	Mode specific command codes for XRW_MODE=1 .....	35
6.27.5	Mode-01 transparent content send request .....	35
6.27.6	Mode-01 connection done .....	35
6.27.7	Mode-01 request secure PIN entry command .....	36
6.27.8	Mode-01 smartcard scan .....	37
7	Replies .....	37
7.1	General .....	37
7.2	General acknowledge – Nothing to report (osdp_ACK) .....	38
7.3	Negative acknowledge – Error response (osdp_NAK) .....	38
7.4	Device identification report (osdp_PDID) .....	39
7.5	Device capabilities report (osdp_PDCAP) .....	40
7.6	Local status report (osdp_LSTATR) .....	41
7.7	Input status report (osdp_ISTATR) .....	41
7.8	Output status report (osdp_OSTATR) .....	41
7.9	Reader tamper status report (osdp_RSTATR) .....	42
7.10	Card data report, raw bit array (osdp_RAW) .....	42
7.11	Card data report, character array (osdp_FMT) .....	43
7.12	Keypad data report (osdp_KEYPAD) .....	43
7.13	Communication configuration report (osdp_COM) .....	44
7.14	Scan and send biometric data (osdp_BIOREADR) .....	44
7.15	Scan and match biometric template (osdp_BIOMATCHR) .....	45
7.16	Client's ID and client's random number (osdp_CCRYPT) .....	45
7.17	Client cryptogram packet and the initial R-MAC (osdp_RMAC_I) .....	46
7.18	Manufacturer specific reply (osdp_MFGREP) .....	46
7.19	PD busy reply (osdp_BUSY) .....	46
7.20	PIV data reply (osdp_PIVDATAR) .....	46
7.21	osdp_GENAUTHR .....	47
7.22	Response to challenge (osdp_CRAUTHR) .....	47
7.23	Manufacturer specific status reply (osdp_MFGSTATR) .....	48
7.24	Manufacturer specific error reply (osdp_MFGERRR) .....	48
7.25	File transfer status (osdp_FTSTAT) .....	48
7.26	Extended read reply (osdp_XRD) .....	49
7.26.1	General .....	49
7.26.2	Mode specific reply codes for XRW_MODE=0 .....	50
7.26.3	Mode-00 error reply (osdp_PR00ERROR) .....	50
7.26.4	Mode setting report (osdp_PR00REQR) .....	50
7.26.5	Card information report (osdp_PR00CIRR) .....	51
7.26.6	Mode specific reply codes for XRW_MODE=1 .....	51
7.26.7	Mode-01 NAK or error reply (osdp_PR01ERROR) .....	52
7.26.8	Card present notification reply (osdp_PR01PRES) .....	52
7.26.9	Transparent card data reply (osdp_PR01SCREP) .....	52
7.26.10	Secure PIN entry complete reply (osdp_PR01SPER) .....	53

Annex A (normative) Command and reply code numbers commands .....	54
A.1    Commands .....	54
A.2    Replies .....	55
Annex B (normative) Function code definitions list .....	56
B.1    General.....	56
B.2    Function code 1 – Contact status monitoring.....	56
B.3    Function code 2 – Output control .....	57
B.4    Function code 3 – Card data format .....	57
B.5    Function code 4 – Reader LED control.....	57
B.6    Function code 5 – Reader audible output .....	58
B.7    Function code 6 – Reader text output.....	58
B.8    Function code 7 – Time keeping .....	58
B.9    Function code 8 – Check character support .....	58
B.10   Function code 9 – Communication security .....	59
B.11   Function code 10 – Receive bufferSize .....	59
B.12   Function code 11 – Largest combined message size.....	59
B.13   Function code 12 – Smart card support.....	59
B.14   Function code 13 – Readers .....	60
B.15   Function code 14 – Biometrics .....	60
B.16   Function code 15 – Secure PIN entry support .....	60
B.17   Function code 16 – OSDP version .....	60
Annex C (normative) CRC definition .....	61
Annex D (normative) Encryption.....	64
D.1    Encryption method: OSDP-SC .....	64
D.1.1  General .....	64
D.1.2  Overview .....	65
D.1.3  The process.....	65
D.1.4  Secure channel session connection sequence (SCS-CS).....	65
D.1.5  Communication during a secure channel session.....	67
D.1.6  SCS_16 PD->ACU.....	67
D.1.7  SCS_17 ACU->PD .....	67
D.1.8  SCS_18 PD->ACU .....	67
D.2    Commands .....	67
D.2.1  Encryption key set (osdp_KEYSET).....	67
D.2.2  Challenge and secure session initialization request (osdp_CHLNG) .....	68
D.2.3  Server's random number and server cryptogram (osdp_SCRIPT) .....	68
D.3    Replies .....	68
D.3.1  Client's ID and client's random number (osdp_CCRYPT) .....	68
D.3.2  Client cryptogram packet and the initial R-MAC (osdp_RMAC_I) .....	69
D.4    Algorithms and support functions .....	69
D.4.1  Session key derivation.....	69
D.4.2  Key diversification .....	69
D.4.3  Client cryptogram .....	70
D.4.4  Server cryptogram .....	70
D.4.5  Padding .....	70
D.5    Message authentication code (MAC) generation .....	70
D.5.1  General .....	70
D.5.2  The wrap operation for security block types SCS_15, SCS-16, SCS_17, and SCS_18 .....	71

D.5.3	The unwrap operation .....	72
D.6	Error recovery .....	72
D.7	Field deployment and configuration .....	72
Annex E (normative)	Test vectors .....	74
Annex F (informative)	Mapping of mandatory functions in IEC 60839-11-1 .....	75
Bibliography	.....	85
Figure 1 – Schematic overview of an OSDP connection .....		12
Figure D.1 – MAC algorithm .....		71
Table 1 – Packet format .....		15
Table 2 – Message control information .....		16
Table 3 – The security block (SB) .....		17
Table 4 – Multi-part message structure .....		17
Table 5 – Behaviour modes .....		18
Table 6 – Poll request .....		19
Table 7 – ID report request .....		20
Table 8 – Peripheral device capabilities request .....		20
Table 9 – Local status report request .....		20
Table 10 – Input status report request .....		20
Table 11 – Output status report request .....		21
Table 12 – Reader status report request .....		21
Table 13 – Output control command .....		22
Table 14 – Control code values .....		22
Table 15 – Reader LED control command .....		23
Table 16 – Temporary control code values .....		24
Table 17 – Permanent control code values .....		24
Table 18 – Color values .....		24
Table 19 – Reader buzzer control command (osdp_BUZ) .....		25
Table 20 – Reader text output command (osdp_TEXT) .....		26
Table 21 – Text command values .....		26
Table 22 – Communication configuration command (osdp_COMSET) .....		27
Table 23 – Scan and send biometric data (osdp_BIOREAD) .....		27
Table 24 – Biometric types .....		28
Table 25 – Fingerprint formats .....		28
Table 26 – Command structure: 6-byte header followed by a variable length template .....		29
Table 27 – Manufacturer specific commands (osdp_MFG) .....		30
Table 28 – ACU receive size (osdp_ACURXSIZE) .....		30
Table 29 – Keep reader active (osdp_KEEPACTIVE) .....		30
Table 30 – Abort current operation (osdp_ABORT) .....		31
Table 31 – Get PIV data (osdp_PIVDATA) .....		31
Table 32 – General authenticate (osdp_GENAUTH) fragment .....		32
Table 33 – Authentication challenge (osdp_CRAUTH) fragment .....		32

Table 34 – File transfer command .....	33
Table 35 – Extended write command structure .....	34
Table 36 – Mode set command .....	34
Table 37 – Mode 0 configuration .....	34
Table 38 – Mode 1 configuration .....	34
Table 39 – Read setting request .....	35
Table 40 – Mode specific command codes .....	35
Table 41 – Transparent content send request .....	35
Table 42 – Smartcard connection done .....	36
Table 43 – Request secure PIN entry command .....	36
Table 44 – Smartcard scan .....	37
Table 45 – General acknowledge (osdp_ACK) .....	38
Table 46 – Negative acknowledge (osdp_NAK) .....	38
Table 47 – Error codes .....	39
Table 48 – Device identification report (osdp_PDID) .....	40
Table 49 – Device capabilities report (osdp_PDCAP) .....	40
Table 50 – Local status report (osdp_LSTATR) .....	41
Table 51 – Input status report (osdp_ISTATR) .....	41
Table 52 – Output status report (osdp_OSTATR) .....	42
Table 53 – Reader tamper status report (osdp_RSTATR) .....	42
Table 54 – Card data report, raw bit array (osdp_RAW) .....	43
Table 55 – Card data report, character array (osdp_FMT) .....	43
Table 56 – Keypad data report (osdp_KEYPAD) .....	44
Table 57 – Communication configuration report (osdp_COM) .....	44
Table 58 – Scan and send biometric data (osdp_BIOREADR) .....	45
Table 59 – Scan and match biometric template (osdp_BIOMATCHR) .....	45
Table 60 – Manufacturer specific reply (osdp_MFGREP) .....	46
Table 61 – PD busy reply (osdp_BUSY) .....	46
Table 62 – PIV data reply (osdp_PIVDATAR) .....	47
Table 63 – General authenticate response (osdp_GENAUTHR) .....	47
Table 64 – Response to challenge (osdp_CRAUTHR) .....	48
Table 65 – Manufacturer specific status reply (osdp_MFGSTATR) .....	48
Table 66 – Manufacturer specific error reply (osdp_MFGERRR) .....	48
Table 67 – File transfer status (osdp_FTSTAT) .....	49
Table 68 – Extended read reply .....	50
Table 69 – Mode specific reply codes .....	50
Table 70 – Error reply .....	50
Table 71 – Mode setting report .....	51
Table 72 – Card information report .....	51
Table 73 – Mode specific reply codes .....	51
Table 74 – Error reply .....	52
Table 75 – Card present notification reply .....	52
Table 76 – Transparent card data reply .....	52

Table 77 – Transparent card data reply.....	53
Table A.1 – Commands code numbers.....	54
Table A.2 – Replies code numbers.....	55
Table B.1 – Function codes .....	56
Table D.1 – SEC_BLK_TYPE assignment.....	64
Table D.2 – Command structure: 2-byte header followed by variable length data .....	67
Table D.3 – Command structure: 8-byte random number as the “challenge” .....	68
Table D.4 – Command structure: 16-byte server cryptogram.....	68
Table D.5 – Command structure: 32-byte structure .....	69
Table D.6 – Command structure: 16-byte structure .....	69
Table F.1 – Access point interface requirements.....	76
Table F.2 – Indication and annunciation requirements .....	77
Table F.3 – Recognition requirements.....	80
Table F.4 – Duress signalling requirements .....	81
Table F.5 – Overriding requirements.....	81
Table F.6 – System self-protection requirements .....	82

## INTERNATIONAL ELECTROTECHNICAL COMMISSION

### ALARM AND ELECTRONIC SECURITY SYSTEMS –

#### Part 11-5: Electronic access control systems – Open supervised device protocol (OSDP)

#### 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 60839-11-5 has been prepared by IEC technical committee 79: Alarm and electronic security systems.

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

FDIS	Report on voting
79/634/FDIS	79/636/RVD

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

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



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 "<http://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.

## INTRODUCTION

This document describes the communication protocol for interfacing one or more Peripheral Devices (PD) to an Access Control Unit (ACU). This document specifies the protocol implementation over a two-wire RS-485 multi-drop serial communication channel.

This document is based upon the work done by the Security Industry Association OSDP Working Group.

## **ALARM AND ELECTRONIC SECURITY SYSTEMS –**

### **Part 11-5: Electronic access control systems – Open supervised device protocol (OSDP)**

#### **1 Scope**

This part of IEC 60839 specifies the Open supervised device protocol (OSDP) for electronic access control systems. This includes communication settings, commands and replies between the ACU and the peripheral devices. It also includes a mapping of mandatory and optional requirements as per IEC 60839-11-1:2013 as covered by Annex F.

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

This document does not in any way limit a manufacturer to add other commands to the protocol defined here.

#### **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*

## SOMMAIRE

AVANT-PROPOS .....	92
INTRODUCTION.....	94
1 Domaine d'application .....	95
2 Références normatives .....	95
3 Termes, définitions et termes abrégés .....	95
3.1 Termes et définitions .....	95
3.2 Termes abrégés .....	96
4 Vue d'ensemble .....	96
5 Paramètres de communication.....	97
5.1 Interface physique .....	97
5.2 Signalisation .....	97
5.3 Codage de caractères .....	97
5.4 Accès au canal .....	97
5.5 Codage de données à octets multiples .....	97
5.6 Limites de taille de paquet .....	98
5.7 Cadencement.....	98
5.8 Synchronisation de message .....	98
5.9 Format de paquet.....	99
5.10 Messages en plusieurs parties .....	102
5.10.1 Généralités .....	102
5.10.2 Règles d'utilisation des messages en plusieurs parties .....	103
5.11 Manipulation de carte à puce .....	103
6 Instructions.....	104
6.1 Généralités .....	104
6.2 Demande d'interrogation (osdp_POLL) .....	105
6.3 Demande de rapport d'ID (osdp_ID).....	105
6.4 Demande de fonctionnalités de l'appareil périphérique (osdp_CAP).....	105
6.5 Demande de rapport d'état local (osdp_LSTAT).....	105
6.6 Demande de rapport d'état d'entrée (osdp_ISTAT) .....	106
6.7 Demande de rapport d'état de sortie (osdp_OSTAT) .....	106
6.8 Demande de rapport d'état de lecteur (osdp_RSTAT) .....	106
6.9 Instruction de commande de sortie (osdp_OUT).....	107
6.10 Instructions de commande de LED du lecteur (osdp_LED).....	108
6.11 Instruction de commande de ronfleur du lecteur (osdp_BUZ) .....	110
6.12 Instruction de sortie de texte du lecteur (osdp_TEXT) .....	111
6.13 Instruction de configuration de communication (osdp_COMSET) .....	112
6.14 Numérisation et envoi des données biométriques (osdp_BIOREAD) .....	113
6.15 Numérisation et concordance de modèle biométrique (osdp_BIOMATCH).....	114
6.16 Jeu de clés de cryptage (osdp_KEYSET).....	115
6.17 Demande de mise à l'épreuve et d'initialisation de session sécurisée (osdp_CHLNG) .....	115
6.18 Nombre aléatoire du serveur et cryptogramme de serveur (osdp_SCRIPT).....	115
6.19 Instruction spécifique au fabricant (osdp_MFG) .....	115
6.20 Taille de réception de l'ACU (osdp_ACURXSIZE) .....	116
6.21 Maintenir le lecteur actif (osdp_KEEPACTIVE).....	116
6.22 Abandonner opération en cours (osdp_ABORT).....	117

6.23	Obtenir données PIV (osdp_PIVDATA) .....	117
6.24	Authentification générale (osdp_GENAUTH) .....	117
6.25	Mise à l'épreuve d'authentification (osdp_CRAUTH) .....	118
6.26	Instruction de transfert de fichier (osdp_FILETRANSFER) .....	119
6.27	Données d'écriture étendues (osdp_XWR) .....	119
6.27.1	Généralités .....	119
6.27.2	Instruction de définition de mode .....	120
6.27.3	Paramètre de lecture Mode-00 .....	121
6.27.4	Codes d'instruction spécifiques au mode pour XRW_MODE=1 .....	121
6.27.5	Demande d'envoi de contenu transparent du Mode-01 .....	121
6.27.6	Connexion de Mode-01 achevée .....	122
6.27.7	Instruction de demande de saisie de PIN sécurisée du Mode-01 .....	122
6.27.8	Lecture de la carte à puce Mode-01 .....	124
7	Réponses .....	124
7.1	Généralités .....	124
7.2	Accusé de réception général – rien à signaler (osdp_ACK) .....	124
7.3	Accusé de réception négatif – Réponse d'erreur (osdp_NAK) .....	125
7.4	Rapport d'identification d'appareil (osdp_PDID) .....	125
7.5	Rapport de fonctionnalités d'appareil (osdp_PDCAP) .....	126
7.6	Rapport d'état local (osdp_LSTATR) .....	127
7.7	Rapport d'état d'entrée (osdp_ISTATR) .....	127
7.8	Rapport d'état de sortie (osdp_OSTATR) .....	128
7.9	Rapport d'état de fraude du lecteur (osdp_RSTATR) .....	128
7.10	Rapport de données de carte, matrice binaire brute (osdp_RAW) .....	129
7.11	Rapport de données de carte, matrice de caractères (osdp_FMT) .....	129
7.12	Rapport de données de clavier (osdp_KEYPAD) .....	130
7.13	Rapport de configuration de communication (osdp_COM) .....	131
7.14	Numérisation et envoi des données biométriques (osdp_BIOREADR) .....	131
7.15	Numérisation et concordance de modèle biométrique (osdp_BIOMATCHR) .....	132
7.16	ID de client et nombre aléatoire de clients (osdp_CCRYPT) .....	133
7.17	Paquet de cryptogramme de client et le R-MAC initial (osdp_RMAC_I) .....	133
7.18	Réponse spécifique au fabricant (osdp_MFGREP) .....	133
7.19	Réponse de PD occupé (osdp_BUSY) .....	133
7.20	Réponse de données de PIV (osdp_PIVDATAR) .....	134
7.21	osdp_GENAUTHR .....	134
7.22	Réponse à une mise à l'épreuve (osdp_CRAUTHR) .....	135
7.23	Réponse d'état spécifique au fabricant (osdp_MFGSTATR) .....	135
7.24	Réponse d'erreur spécifique au fabricant (osdp_MFGERRR) .....	136
7.25	Etat de transfert de fichier (osdp_FTSTAT) .....	136
7.26	Réponse de lecture étendue (osdp_XRD) .....	137
7.26.1	Généralités .....	137
7.26.2	Codes de réponse spécifiques au mode pour XRW_MODE=0 .....	138
7.26.3	Réponse d'erreur Mode-00 (osdp_PR00ERROR) .....	138
7.26.4	Rapport de paramètre de mode (osdp_PR00REQR) .....	138
7.26.5	Rapport d'informations de carte (osdp_PR00CIRR) .....	139
7.26.6	Codes de réponse spécifiques au mode pour XRW_MODE=1 .....	139
7.26.7	NAK ou réponse d'erreur de Mode-01 (osdp_PR01ERROR) .....	140
7.26.8	Réponse de notification de carte présente (osdp_PR01PRES) .....	140
7.26.9	Réponse de données de carte transparentes (osdp_PR01SCREP) .....	140

7.26.10	Réponse saisie de PIN sécurisée complète (osdp_PR01SPER).....	141
Annexe A (normative)	Numéros de code d’instruction et de réponses .....	142
A.1	Instructions .....	142
A.2	Réponses .....	143
Annexe B (normative)	Liste des définitions des codes de fonction.....	145
B.1	Généralités .....	145
B.2	Code de fonction 1 – Surveillance de l’état du contact .....	145
B.3	Code de fonction 2 – Commande de sortie.....	146
B.4	Code de fonction 3 – Format des données de la carte.....	146
B.5	Code de fonction 4 – Commande de LED du lecteur .....	146
B.6	Code de fonction 5 – Sortie audible du lecteur .....	147
B.7	Code de fonction 6 – Sortie texte du lecteur.....	147
B.8	Code de fonction 7 – Conservation du temps .....	147
B.9	Code de fonction 8 – Prise en charge du caractère de contrôle.....	147
B.10	Code de fonction 9 – Sécurité de communication .....	148
B.11	Code de fonction 10 – Taille du tampon de réception .....	148
B.12	Code de fonction 11 – Taille maximale de message combiné.....	148
B.13	Code de fonction 12 – Prise en charge de carte à puce .....	148
B.14	Code de fonction 13 – Lecteurs.....	149
B.15	Code de fonction 14 – Biométrie .....	149
B.16	Code de fonction 15 – Prise en charge de saisie de PIN sécurisée .....	149
B.17	Code de fonction 16 – Version OSDP .....	149
Annexe C (normative)	Définition du CRC .....	150
Annexe D (normative)	Cryptage .....	153
D.1	Méthode de cryptage: OSDP-SC.....	153
D.1.1	Généralités .....	153
D.1.2	Vue d’ensemble.....	154
D.1.3	Processus.....	154
D.1.4	Séquence de connexion de session à canal sécurisé (SCS-CS) .....	154
D.1.5	Communication pendant une session à canal sécurisé .....	156
D.1.6	SCS_16 PD->ACU .....	156
D.1.7	SCS_17 ACU->PD .....	156
D.1.8	SCS_18 PD->ACU .....	156
D.2	Instructions .....	157
D.2.1	Jeu de clés de cryptage (osdp_KEYSET).....	157
D.2.2	Demande de mise à l’épreuve et d’initialisation de session sécurisée (osdp_CHLNG) .....	157
D.2.3	Nombre aléatoire du serveur et cryptogramme de serveur (osdp_SCRIPT) .....	158
D.3	Réponses .....	158
D.3.1	ID de client et nombre aléatoire de clients (osdp_CCRYPT) .....	158
D.3.2	Paquet de cryptogramme de client et le R-MAC initial (osdp_RMAC_I) .....	158
D.4	Algorithmes et fonctions de prise en charge.....	159
D.4.1	Dérivation de la clé de session .....	159
D.4.2	Diversification de clé .....	159
D.4.3	Cryptogramme du client.....	159
D.4.4	Cryptogramme du serveur .....	159
D.4.5	Padding .....	160
D.5	Génération du code d’authentification de message (MAC) .....	160

D.5.1	Généralités .....	160
D.5.2	Opération d'inclusion pour les types de blocs de sécurité SCS_15, SCS-16, SCS_17 et SCS_18 .....	161
D.5.3	Opération d'annulation de l'inclusion .....	162
D.6	Reprise sur erreur .....	162
D.7	Déploiement et configuration sur le terrain .....	162
Annexe E (normative)	Vecteurs d'essai .....	164
Annexe F (informative)	Mapping des fonctions obligatoires dans l'IEC 60839-11-1 .....	165
Bibliographie	.....	177
Figure 1	– Vue d'ensemble schématique d'une connexion OSDP .....	96
Figure D.1	– Algorithme du MAC .....	161
Tableau 1	– Format de paquet .....	99
Tableau 2	– Informations de contrôle de message .....	101
Tableau 3	– Le bloc de sécurité (SB) .....	102
Tableau 4	– Structure de message en plusieurs parties .....	102
Tableau 5	– Modes de comportement .....	103
Tableau 6	– Demande d'interrogation .....	105
Tableau 7	– Demande de rapport d'ID .....	105
Tableau 8	– Demande de fonctionnalités de l'appareil périphérique .....	105
Tableau 9	– Demande de rapport d'état local .....	106
Tableau 10	– Demande de rapport d'état d'entrée .....	106
Tableau 11	– Demande de rapport d'état de sortie .....	106
Tableau 12	– Demande de rapport d'état de lecteur .....	106
Tableau 13	– Instruction de commande de sortie .....	107
Tableau 14	– Valeurs du code de commande .....	108
Tableau 15	– Instruction de commande de LED de lecteur .....	109
Tableau 16	– Valeurs de code de commande temporaire .....	110
Tableau 17	– Valeurs du code de commande permanent .....	110
Tableau 18	– Valeurs de couleur .....	110
Tableau 19	– Instruction de commande de ronfleur du lecteur (osdp_BUZ) .....	111
Tableau 20	– Instruction de sortie de texte du lecteur (osdp_TEXT) .....	112
Tableau 21	– Valeurs d'instruction de texte .....	112
Tableau 22	– Instruction de configuration de communication (osdp_COMSET) .....	113
Tableau 23	– Numérisation et envoi des données biométriques (osdp_BIOREAD) .....	113
Tableau 24	– Types biométriques .....	114
Tableau 25	– Formats d'empreinte digitale .....	114
Tableau 26	– Structure d'instruction: en-tête de 6 octets suivi d'un modèle de longueur variable .....	115
Tableau 27	– Instructions spécifiques au fabricant (osdp_MFG) .....	116
Tableau 28	– Taille de réception de l'ACU (osdp_ACURXSIZE) .....	116
Tableau 29	– Maintenir le lecteur actif (osdp_KEEPACTIVE) .....	117
Tableau 30	– Abandonner opération en cours (osdp_ABORT) .....	117

Tableau 31 – Obtenir données PIV (osdp_PIVDATA) .....	117
Tableau 32 – Fragment d’authentification générale (osdp_GENAUTH).....	118
Tableau 33 – Fragment de mise à l’épreuve d’authentification (osdp_CRAUTH) .....	118
Tableau 34 – Instruction de transfert de fichier .....	119
Tableau 35 – Structure d’instruction d’écriture étendue.....	120
Tableau 36 – Instruction de définition de mode .....	120
Tableau 37 – Configuration du mode 0 .....	120
Tableau 38 – Configuration du mode 1 .....	121
Tableau 39 – Demande de lecture de paramètre.....	121
Tableau 40 – Codes d’instruction spécifiques au mode .....	121
Tableau 41 – Demande d’envoi de contenu transparent.....	122
Tableau 42 – Connexion avec la carte à puce achevée.....	122
Tableau 43 – Instruction de demande de saisie de PIN sécurisée .....	123
Tableau 44 – Lecture de la carte à puce .....	124
Tableau 45 – Accusé de réception général (osdp_ACK).....	124
Tableau 46 – Accusé de réception négatif (osdp_NAK).....	125
Tableau 47 – Codes d’erreur.....	125
Tableau 48 – Rapport d’identification d’appareil (osdp_PDID).....	126
Tableau 49 – Rapport de fonctionnalités d’appareil (osdp_PDCAP) .....	127
Tableau 50 – Rapport d’état local (osdp_LSTATR).....	127
Tableau 51 – Rapport d’état d’entrée (osdp_ISTATR) .....	128
Tableau 52 – Rapport d’état de sortie (osdp_OSTATR).....	128
Tableau 53 – Rapport d’état de fraude du lecteur (osdp_RSTATR) .....	129
Tableau 54 – Rapport de données de carte, matrice binaire brute (osdp_RAW) .....	129
Tableau 55 – Rapport de données de carte, matrice de caractères (osdp_FMT) .....	130
Tableau 56 – Rapport de données de clavier (osdp_KEYPAD).....	130
Tableau 57 – Rapport de configuration de communication (osdp_COM).....	131
Tableau 58 – Numérisation et envoi des données biométriques (osdp_BIOREADR).....	132
Tableau 59 – Numérisation et concordance de modèle biométrique (osdp_BIOMATCHR).....	132
Tableau 60 – Réponse spécifique au fabricant (osdp_MFGREP).....	133
Tableau 61 – Réponse de PD occupé (osdp_BUSY) .....	134
Tableau 62 – Réponse de données de PIV (osdp_PIVDATAR).....	134
Tableau 63 – Réponse d’authentification générale (osdp_GENAUTHR) .....	135
Tableau 64 – Réponse à une mise à l’épreuve (osdp_CRAUTHR) .....	135
Tableau 65 – Réponse d’état spécifique au fabricant (osdp_MFGSTATR).....	136
Tableau 66 – Réponse d’erreur spécifique au fabricant (osdp_MFGERRR).....	136
Tableau 67 – Etat de transfert de fichier (osdp_FTSTAT).....	137
Tableau 68 – Réponse de lecture étendue .....	138
Tableau 69 – Codes de réponse spécifiques au mode .....	138
Tableau 70 – Réponse d’erreur.....	138
Tableau 71 – Réponse de paramètre de mode.....	139
Tableau 72 – Rapport d’informations de carte .....	139



Tableau 73 – Codes de réponse spécifiques au mode .....	140
Tableau 74 – Réponse d'erreur.....	140
Tableau 75 – Réponse de notification de carte présente .....	140
Tableau 76 – Réponse de données de carte transparentes .....	141
Tableau 77 – Réponse de données de carte transparentes .....	141
Tableau A.1 – Numéros de code des instructions.....	142
Tableau A.2 – Numéros de code des réponses .....	143
Tableau B.1 – Codes de fonction .....	145
Tableau D.1 – Attribution SEC_BLK_TYPE .....	153
Tableau D.2 – Structure d'instruction: en-tête de 2 octets suivi de données de longueur variable.....	157
Tableau D.3 – Structure d'instruction: Nombre aléatoire de 8 octets en tant que "mise à l'épreuve" .....	157
Tableau D.4 – Structure d'instruction: Cryptogramme du serveur de 16 octets .....	158
Tableau D.5 – Structure d'instruction: Structure de 32 octets .....	158
Tableau D.6 – Structure d'instruction: Structure de 16 octets .....	158
Tableau F.1 – Exigences concernant l'interface de point d'accès .....	166
Tableau F.2 – Exigences concernant l'indication et l'annonce .....	167
Tableau F.3 – Exigences concernant la reconnaissance .....	171
Tableau F.4 – Exigences concernant le signalement d'agression .....	172
Tableau F.5 – Exigences concernant la neutralisation.....	173
Tableau F.6 – Exigences concernant l'autoprotection du système (1 sur 3).....	174

## COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

### SYSTÈMES D'ALARME ET DE SÉCURITÉ ÉLECTRONIQUES –

#### Partie 11-5: Systèmes de contrôle d'accès électronique – Protocole ouvert d'appareil supervisé (OSDP)

##### 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 et de ne pas avoir signalé leur existence.

La Norme internationale IEC 60839-11-5 a été établie par le comité d'études 79 de l'IEC: Systèmes d'alarme et de sécurité électroniques.

La présente version bilingue (2021-07) correspond à la version anglaise monolingue publiée en 2020-07.

La version française de cette norme n'a pas été soumise au vote.

Ce document a été rédigé selon les Directives ISO/IEC, Partie 2.

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

Le comité a décidé que le contenu de ce document ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous "<http://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.

## INTRODUCTION

Le présent document décrit le protocole de communication pour interfacier un ou plusieurs appareils périphériques (PD) avec une unité de contrôle d'accès (ACU). Le présent document spécifie la mise en œuvre du protocole par le biais d'un canal de communication série à branchements multiples RS-485 bifilaire.

Le présent document repose sur les travaux menés par le Groupe de travail OSDP de la Security Industry Association.

## **SYSTÈMES D'ALARME ET DE SÉCURITÉ ÉLECTRONIQUES –**

### **Partie 11-5: Systèmes de contrôle d'accès électronique – Protocole ouvert d'appareil supervisé (OSDP)**

#### **1 Domaine d'application**

La présente partie de l'IEC 60839 spécifie le protocole ouvert d'appareil supervisé (OSDP) pour les systèmes de contrôle d'accès électronique. Cela inclut les paramètres de communication, les instructions et les réponses entre l'ACU et les appareils périphériques. Elle contient également un mapping entre les exigences obligatoires et facultatives selon l'IEC 60839-11-1:2013 telles qu'elles sont couvertes par l'Annexe F.

Le présent document s'applique uniquement à la sécurité physique. La sécurité physique empêche le personnel non autorisé, les agresseurs ou les intrus accidentels d'accéder physiquement à un bâtiment, une pièce, etc.

Le présent document ne restreint aucunement l'ajout par un fabricant d'instructions supplémentaires au protocole défini ici.

#### **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*