BS EN IEC 60839-11-5:2020

BSI Standards Publication

Alarm and electronic security systems

Part 11-5: Electronic access control systems — Open Supervised Device Protocol (OSDP)

Documents
Document Sharing Hub

Full document details: BS EN IEC 60839-11-5:2020

National foreword

This British Standard is the UK implementation of EN IEC 60839-11-5:2020. It is identical to IEC 60839-11-5:2020.

The UK participation in its preparation was entrusted to Technical Committee GW/1/8, Access control.

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

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 2020
Published by BSI Standards Limited 2020

ISBN 978 0 580 98835 6

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 30 September 2020.

Amendments/corrigenda issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: BS EN IEC 60839-11-5:2020

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN IEC 60839-11-5

September 2020

ICS 13.320

English Version

Alarm and electronic security systems - Part 11-5: Electronic access control systems - Open Supervised Device Protocol (OSDP) (IEC 60839-11-5:2020)

Systèmes d'alarme et de sécurité électroniques - Partie 11-5: Systèmes de contrôle d'accès électronique - Protocole ouvert d'appareil supervisé (OSDP) (IEC 60839-11-5:2020)

Alarmanlagen - Teil 11-5: Elektronische Zutrittskontrollanlagen - Open Supervised Device Protocol (OSDP) (IEC 60839-11-5:2020)

This European Standard was approved by CENELEC on 2020-08-12. 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, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, 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: Rue de la Science 23, B-1040 Brussels

© 2020 CENELEC All rights of exploitation in any form and by any means reserved worldwide for CENELEC Members.

Ref. No. EN IEC 60839-11-5:2020 E

Documents
Document Sharing Hub

Full document details: BS EN IEC 60839-11-5:2020

European foreword

The text of document 79/634/FDIS, future edition 1 of IEC 60839-11-5, prepared by IEC/TC 79 "Alarm and electronic security systems" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN IEC 60839-11-5:2020.

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) 2021-05-12
- latest date by which the national standards conflicting with the document have to be withdrawn (dow) 2023-08-12

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

Endorsement notice

The text of the International Standard IEC 60839-11-5:2020 was approved by CENELEC as a European Standard without any modification.

Documents
Document Sharing Hub

Full document details: BS EN IEC 60839-11-5:2020

Annex ZA
(normative)

Normative references to international publications with their corresponding European publications

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.

NOTE 1 Where 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
IEC 60839-11-1	2013	Alarm and electronic security systems - Part 11-1: Electronic access control systems - System and components requirements	EN 60839-11-1	2013
-	-		+ AC	2015
IEC 60839-11-2	2014	Alarm and electronic security systems - Part 11-2: Electronic access control systems - Application guidelines	EN 60839-11-2	2015
-	-		+ AC	2015

Documents
Document Sharing Hub

Full document details: BS EN IEC 60839-11-5:2020

This page deliberately left blank

Documents
Document Sharing Hub

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

AVA Documents
Document Sharing Hub

Full document details: BS EN IEC 60839-11-5:2020

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

AVA Documents
Document Sharing Hub
Full document details: BS EN IEC 60839-11-5:2020

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_SCRYPT) 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

AVA Documents Document Sharing Hub

Full document details: BS EN IEC 60839-11-5:2020

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

AVA Documents
Document Sharing Hub

Full document details: BS EN IEC 60839-11-5:2020

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

AVA Documents
Document Sharing Hub

Full document details: BS EN IEC 60839-11-5:2020

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

Documents
Document Sharing Hub
Full document details: BS EN IEC 60839-11-5:2020

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.

AVA Documents Document Sharing Hub

Full document details: BS EN IEC 60839-11-5:2020

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.

Documents
Document Sharing Hub

Full document details: BS EN IEC 60839-11-5:2020

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.

Documents
Document Sharing Hub

Full document details: BS EN IEC 60839-11-5:2020

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*

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

For the purposes of this document the terms and definitions given in IEC 60839-11-1 and IEC 60839-11-2, as well as the following, 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
client
service requester

EXAMPLE User interface, etc.

3.1.2
server
service provider

Documents
Document Sharing Hub

Full document details: BS EN IEC 60839-11-5:2020

EXAMPLE Access control unit, etc.

3.1.3
peripheral device
I/O device connected via OSDP to the access control unit

EXAMPLE Token reader, card reader, biometric reader, client, etc.

3.2 Abbreviated terms

For the purposes of this document, the abbreviated terms given in IEC 60839-11-1 and IEC 60839-11-2, as well as the following apply.

ACU	Access Control Unit
AES	Advanced Encryption Standard
APDU	Application Protocol Data Unit
CBC	Cypher Block Chaining
C-MAC	Command MAC (for packets from ACU to PD)
cUID	Client's Unique Identifier
ICV	Initial Chaining Vector
MAC	Message Authentication Code
MK	Master Key
PD	Peripheral Device
PGM	Portable Grey Map
R-MAC	Reply MAC (for packets from PD to ACU)
SCBK	Secure Channel Base Key
SCS	Secure Channel Session
S-ENC	Session Key for ensuring data confidentiality (message encryption)
S-MAC1	Session Key for Message Authentication, key 1
S-MAC2	Session Key for Message Authentication, key 2
SPE	Secure PIN Entry

4 Overview

This document defines the protocol for connecting an ACU to peripheral devices including communication settings, commands and replies as shown in Figure 1.

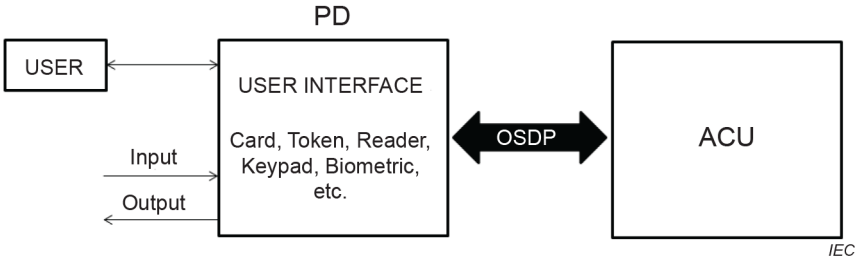

Figure 1 – Schematic overview of an OSDP connection

Documents
Document Sharing Hub
Full document details: BS EN IEC 60839-11-5:2020

5 Communication settings

5.1 Physical interface

The physical interface shall be a half-duplex RS-485 communication bus using one twisted pair of wires with shield/signal ground.

5.2 Signaling

The signaling port shall be half-duplex asynchronous serial with following settings:

- 8 data bits,
- 1 stop bit,
- no parity bits,
- at least one of 9 600, 19 200,38 400, 57 600, 115 200, 230 400 baud.

5.3 Character encoding

Data encoding shall be compliant with UTF-8 (ISO/IEC 10646:2017).

5.4 Channel access

The communication channel is used in the “interrogation/reply” mode. Only the ACU may spontaneously send a message. Each message sent by the ACU is addressed to one and only one PD. The “broadcast message”, as described in Table 1, assumes that there is only one PD connected to the ACU.

The PD shall send a single reply message to each message addressed to it within the specified MAX_REPLY_DELAY, as defined in 5.7.

Special case: if the PD is unable to accept the command for processing due to temporary unavailability of a resource required to process the command, then the PD shall send the osdp_BUSY reply as defined in 7.19. When the ACU receives the osdp_BUSY reply, it may, at its discretion, choose to re-send the same command as it would if the command delivery timed out. If the ACU elects to re-send the command that caused the osdp_BUSY reply, it may do so right away, or at its option may service other PDs before re-sending the command. If, on the other hand, the ACU elects to abandon the command that received the BUSY reply, the PD shall recognize this condition (new sequence number) and shall process the new command.

Commands which request specific data from the PD shall be limited to data that is expected to be immediately available. Following that guideline, applications where the ACU needs to request data that may take some time before it is available shall implement the operation in two distinct steps. The ACU shall issue a command requesting the data. The acceptance of that command shall be indicated by osdp_ACK. On completion of the operation, the PD shall return the matching reply in response to osdp_POLL.

5.5 Multi-byte data encoding

Messages are constructed using a character stream model, meaning that all data shall be packed without any "alignment pad" characters.

Numeric data types that require more than 1 byte are stored with the least significant byte first ("little-endian" format).

Documents
Document Sharing Hub
Full document details: BS EN IEC 60839-11-5:2020

5.6 Packet size limits

The implementation of the standard message set requires all devices to be able to accept packets up to 128 bytes long and be able to tolerate messages addressed to other devices having a total length not exceeding 1 440 bytes.

If the packet was meant for another device, there should be no adverse condition created in the PD with the limitation. If the PD receives a packet specifically addressed to it which is greater than its reported RX buffer size, it would constitute a protocol error and respond with a NAK code 0x02.

This protocol's primary purpose is to support communication to simple devices on a shared (multi-dropped) channel. Large packets should be avoided.

5.7 Timing

The transmitting device shall guarantee an equivalent of two UTF-8 characters idle time before it may access the communication channel. This idle line delay is required to allow for signal converters and/or multiplexers to sense that the line has become idle.

The transmitting device shall drive the line to a marking state for a minimum time pause equivalent of one UTF-8 character before starting to send the first character of a message (this can be achieved by sending a character with all bits set to '1').

The transmitting device shall stop driving the line no longer than the equivalent time of one full UTF-8 character after the transmission of the stop bit of the last character of a message.

A device shall begin the transmission of its reply in less than the defined REPLY_DELAY from the last character of the message requesting the reply.

The REPLY_DELAY shall not exceed 200 ms. The REPLY_DELAY is defined as the time measured from the receipt of the checksum character of the command to the transmission of the first byte of the reply. The typical REPLY_DELAY should be less than 3 ms. If a device is overwhelmed, it can send a BUSY message(s) (The longest REPLY_DELAY occurs when local data is being processed, typically an infrequent event.)

The PD shall consider its communication "off-line" if the period between messages to which it responds exceeds 8 s. Both sides shall reset the connection state to “off-line” and reinitiate a new connect sequence.

If the ACU does not receive a reply before the REPLY_DELAY, the ACU moves to the next communication cycle.

5.8 Message synchronization

The general procedure for a peripheral device (PD) to obtain message synchronization is to wait for an inter-character timeout then look for a Start-Of-Message (SOM) code. The device should then receive and store at least the header fields while computing the checksum/CRC on the rest of the message. If the checksum is good, only the PD that matches the address field processes the message. All other PDs, however, should monitor the packet by counting the remaining portion of packet to be able to anticipate the start of the next packet.

If there is an inter-character timeout while receiving the message the PD shall abort the receive sequence. Once aborted, the PD should re-sync using the method described above.

The nominal value of the inter-character timeout shall be 20 ms. This parameter may need to be adjusted for special channel timing considerations.

AVA Documents
Document Sharing Hub

Full document details: BS EN IEC 60839-11-5:2020

5.9 Packet format

All messages, regardless of origin, shall follow the structure as defined in Table 1.

Table 1 – Packet format

Size (in bytes)	Name	Meaning	Value
1	SOM	Start of message NOTE 1 The constant value 0x53, begins each message header. This character is used for synchronization.	0x53
1	ADDR	Physical address of the PD NOTE 2 The 7 least significant bits of this character represent the address of the PD to which the message is directed, or the address of the PD sending the reply. The most significant bit is set to 0 in a command and 1 in a reply. Address 0x7F is reserved as a special "BROADCAST" address that each PD will accept and respond to, just as if it matched its communication address. The reply message will use 0x7F plus the reply flag (0x7F+0x80=0xFF) in its address field. Since each PD will respond to 0x7F, the use of the broadcast address should be limited to controlled (single PD) configurations.	0x00 – 0x7E 0x7F = broadcast
1	LEN_LSB	Packet length least significant byte NOTE 3 The value of the two-character length field is the total number of characters contained in the message, including the SOM through the CKSUM or CRC characters.	Any
1	LEN_MSB	Packet length most significant byte NOTE 4 The value of the two-character length field is the total number of characters contained in the message, including the SOM through the CKSUM or CRC characters.	Any
1	CTRL	Message control information	Refer to Table 2
1	SEC_BLK_LEN	(optional) Length of security control block	Any
1	SEC_BLK_TYPE	(optional) Security block type NOTE 5 The Security block (SB) is optional. Its presence is indicated by setting the CTRL::SBC flag. The purpose of the SB is to facilitate the implementation of data security within the OSDP framework. By itself, the SB does not define or specify the nature of the security methods used. Rather, the SB is available to support the use of various security methods as OSDP device capabilities and client security requirements change. See Annex D for further details.	Refer to Table 3
1	SEC_BLK_DATA	(optional) Security block data	Based on type
1	CMND/REPLY	Command or reply code NOTE 6 Commands and replies are the actual data block of the communication packets. A packet originated by the ACU is called a command, and a packet returned by the PD is called a reply. The purpose and meaning of each message packet is defined by its command or reply code. The actual codes and associated data blocks (if any) are specified in detail in the following sections. See Table A.1 for a quick reference for the numeric command values.	Refer to A.1 and A.2
1	DATA	(optional) data block	Based on CMD/REPLY

AVA Documents Document Sharing Hub

Full document details: BS EN IEC 60839-11-5:2020

Size (in bytes)	Name	Meaning	Value
4	MAC	Present for secured messages NOTE 7 Optional 4 byte MAC if SBC bit set in CTRL.	
1	CKSUM/CRC_LSB	Checksum, or, CRC-16 least significant byte NOTE 8 OSDP supports two different forms of error detection as discussed in the CKSUM/CRC paragraph under CTRL. If the PD does not support the indicated checksum/CRC method, or if it gets a checksum/CRC error, then PD shall send an osdp_NAK response, error_code set to 0x01.	
1	CRC_MSB	(optional) CRC-16 most significant byte	

Table 2 – Message control information

BIT	MASK	NAME	Meaning
0-1	0x03	SQN	The sequence number of the message is used for message delivery confirmation and for error recovery. NOTE 1 The sequence number is incremented by the ACU from one command to the next, skipping zero: 0->1->2->3->1->... Non-zero sequence numbers support error recovery: the ACU acknowledges the last reply by sending the next command with the incremented sequence number, or it repeats the command without changing the sequence number to request the repeat of the last reply. This method allows the receiver to properly handle the command: process the command if it did not receive it correctly last time (error occurred on the command), or to simply repeat the reply it already made without executing the command again (error occurred in the reply). SQN zero should be used only for communication startup, at boot time or after a communications loss. Zero forces the PD to discard its last reply and to accept and process the current command.
2	0x04	CKSUM/ CRC	Set – 16-bit CRC is contained in the last 2 bytes of the message. Clear – 8-bit CHECKSUM is contained in the last byte of the message. NOTE 2 This setting defines the message check character(s) method used to provide error detection. The CKSUM value is the 8 least significant bits of the 2's complement value of the sum of all previous characters of the message. This mode is supported in order to allow for devices with limited resources, but new devices should use the CRC method. The CRC calculation is applied to all previous characters of the message. Refer to Annex C for the definition and sample code for the CRC algorithm.
3	0x08	SCB	Set – Security Control Block is present in the message Clear – No Security Control block in the message
4-7	0xF0		Shall be set to zero

Documents
Document Sharing Hub
Full document details: BS EN IEC 60839-11-5:2020

Table 3 – The security block (SB)

Size (in bytes)	Name	Meaning	Value
1	SEC_BLK_LEN	Length of the security control block NOTE 1 This field is set to the total byte count of the SB, including itself.	Any
1	SEC_BLK_TYPE	Security block type NOTE 2 This field defines the manner in which the security block applies to the rest of message (the optional sec_blk_data[] array , the command/reply, the optional data[] array, and the message check characters).	Defined in Table D.1
n	SEC_BLK_DATA	Variable length data (optional) NOTE 3 This section is an array whose size is (sec_blk_length-2). The data content is separately defined for each SEC_BLK_TYPE. A PD that receives an SB, but does not support the processing of the SB should return an osdp_NAK response, error code set to 0x05. A PD whose settings require an encrypted connection, and receives a command without the appropriate data security extension shall return an osdp_NAK response, error code set to 0x06.	Any

5.10 Multi-part messages

5.10.1 General

Under some conditions, it is necessary to send information that does not fit within one OSDP message. To support this capability certain messages as specified in Clauses 6 or 7 include control fields to support multi-part messages. This is intended for the transfer of data blocks that may exceed the maximum supported payload of a single OSDP message. See Table 4.

Table 4 – Multi-part message structure

Size (in bytes)	Code	Name	Meaning
2	0x00 – 0xFF	MpSizeTotal (LSB)	Total size of all fragments which make up the multi-part message data
	0x00 – 0xFF	MpSizeTotal (MSB)	
2	0x00 – 0xFF	MpOffset (LSB)	Byte offset of the data in this fragment
	0x00 – 0xFF	MpOffset (MSB)	
2	0x00 – 0xFF	MpFragmentSize (LSB)	The number of bytes of data in this fragment
	0x00 – 0xFF	MpFragmentSize (MSB)	

5.10.2 Multi-part message usage rules

Even though the message structure supports otherwise, the following rules shall apply:

- the data array shall be transferred in sequential order, without any gaps;
- the first message of a multi-part message shall always have MpOffset set to zero;

Documents
Document Sharing Hub
Full document details: BS EN IEC 60839-11-5:2020

- the transfer of a multi-part message may be terminated by the sender early by setting MpOffset to equal or greater than MpSizeTotal and setting MpFragmentSize to zero. Conversely, the receiving device shall recognize this condition as an early termination of the multi-part transfer;
- the transfer sequence of multi-part messages may not be interrupted to interleave other messages.
  - the case of multi-part commands is simple: once the ACU begins, the transfer of a multi-part message, it shall not send any other commands to the PD until the entire transfer has completed; (It has the option to send the “abort” packet to terminate early.)
  - of course, the ACU may interleave a multi-part transfer sequence to a PD with messages to other PDs without any impact on the multi-part transfer;
  - the PD can reject a multi-part command by sending a NAK reply with reply code 0x09. This reply shall cause the ACU to abort the mutlti-part sequence;
- in case the PD is unable to process the current frame of a multi-part command because of a temporary busy condition, it shall use the osdp_BUSY reply per 5.4 and 7.19;
- the ACU is in control of the retrieval of replies from a PD, therefore no special provisions are required to throttle multi-packet replies.

5.11 Smartcard handling

OSDP includes a set of messages for use in communicating directly with Smartcards. This is referred to as “transparent mode”. A PD that supports smartcards (see the PDCAP entry for smartcard support) will have several “behaviour modes”. These are described in Table 5.

Table 5 – Behaviour modes

XRW_MODE	Behaviour mode description
0x00	Default – no specific behaviour mode is in effect. osdp_XWR commands support the read back and the setting of the PD’s behaviour mode.
0x01	Transparent smart card interface support. This behaviour mode supports transparent operations between the ACU and a smart Card.
0x02-0xFF	Reserved for future use.

The combination of **XRW_MODE** and **XWR_PCMND** are both required to uniquely identify the command, and the combination of **XRW_MODE** and **XRD_REPLY** are both required to uniquely identify the reply. Therefore for clarity, they should be handled and referenced as pairs.

This specification allows for the condition where a given PD may support several modes, and it may even support those several modes simultaneously. The guideline regarding multiple modes is that the PD shall process all mode specific commands that it is capable of processing. If these commands create a conflict, then the PD shall return an error code in response.

Certain behaviour modes may enable background operations that return data as an osdp_XRD reply to an osdp_POLL. Mode 0 commands are available in all modes. Mode specific commands should only be executed after successfully switching to the corresponding mode.

AVA Documents
Document Sharing Hub

Full document details: BS EN IEC 60839-11-5:2020

6 Commands

6.1 General

The following commands can be sent from the ACU to the PD. The value listed in this clause below goes in the message CMND field. Values 0x40 through 0x7F are reserved for core commands. Values outside this range can be used for application specific and/or proprietary implementations. Messages from 0x40 through 0x7F shall follow the command structure specified within the protocol.

Several of the commands are specified to support multiple records. The effect of having "*n*" records in a command is the same as issuing "*n*" commands in the same order as the records, except for timing. The number of records contained in those commands shall be computed by dividing the length of the DATA block by the size of the command record defined for the specific CMND code in the message.

Commands containing multiple records shall not request the return of any specific data message. The PD shall return an osdp_ACK response if each command record was accepted by the PD, otherwise, the PD shall return an osdp_NAK reply with the error code set to 0x09 "bad command record(s)," which may be followed by an array of one-byte completion codes, one entry per command record received.

A non-zero remainder of this division indicates a command format error. In this case the PD shall assume that the ACU is not using the same template size for this command as the PD is prepared to process and therefore it shall abandon processing any part of the command ad will return an osdp_NAK reply with the error code set to 0x09 "Unable to process command record." In this case, the PD does not include an array of completion codes for individual command records because it did not attempt to process any.

If the number of command records appears to be acceptable, then the PD shall begin processing the command records in the order they appear. If all command records are acceptable then the PD shall return an osdp_ACK reply. Otherwise, the PD shall return an osdp_NAK reply with the error code set to 0x09 "Unable to process command record" followed by an array of completion codes for the individual command records processed. The value zero indicates no error, and the value 0x01 indicates a generic error. The remaining values are reserved for future definition.

See Annex A for a quick reference with the numeric command values.

6.2 Poll request (osdp_POLL)

This command serves as a general inquiry. The PD may return any reply that is marked as a possible "poll response". Normally, the PD will return any unreported input data or status change information as a poll response. Refer to Table 6.

Table 6 – Poll request

Packet format field	Code	Name
CMND	0x60	osdp_POLL
DATA	Omitted	

6.3 ID report request (osdp_ID)

This command requests the return of the PD ID report. The ID request code parameter may request the extended form of the PD ID block. Refer to Table 7.

Documents
Document Sharing Hub
Full document details: BS EN IEC 60839-11-5:2020

Table 7 – ID report request

Packet format field	Code	Name
CMND	0x61	osdp_ID
DATA	0x00	Send Standard PD ID Block

The reply is formatted as described in 7.4.

6.4 Peripheral device capabilities request (osdp_CAP)

This command requests the PD to return a list of its functional capabilities, such as the type and number of input points, outputs points, reader ports, etc. Refer to Table 8.

Table 8 – Peripheral device capabilities request

Packet format field	Code	Name
CMND	0x62	osdp_CAP
DATA	0x00	Send standard reply

The reply is formatted as described in 7.5.

6.5 Local status report request (osdp_LSTAT)

This command instructs the PD to reply with a local status report. Refer to Table 9.

Table 9 – Local status report request

Packet format field	Code	Name
CMND	0x64	osdp_LSTAT
DATA	Omitted	

The reply is formatted as described in 7.6.

6.6 Input status report request (osdp_ISTAT)

This command instructs the PD to reply with an input status report. Refer to Table 10.

Table 10 – Input status report request

Packet format field	Code	Name
CMND	0x65	osdp_ISTAT
DATA	Omitted	

The reply is formatted as described in 7.7.

Documents
Document Sharing Hub

Full document details: BS EN IEC 60839-11-5:2020

6.7 Output status report request (osdp_OSTAT)

This command instructs the PD to reply with an output status report. Refer to Table 11.

Table 11 – Output status report request

Packet format field	Code	Name
CMND	0x66	osdp_OSTAT
DATA	Omitted	

The reply is formatted as described in 7.8.

6.8 Reader status report request (osdp_RSTAT)

This command instructs the PD to reply with a reader status report. Refer to Table 12.

Table 12 – Reader status report request

Packet format field	Code	Name
CMND	0x67	osdp_RSTAT
DATA	Omitted	

The reply is formatted as described in 7.9.

6.9 Output control command (osdp_OUT)

This command can alter the permanent state of the output, or it can request a timed pulse output. The permanent command is volatile (does not transcend power cycles).

The output control command message packet may contain multiple 4-byte records. The PD should use the total message length to determine the number of records present. The number of 4-byte records should not exceed the number of outputs as reported in function code 2 (Annex B). Records containing an invalid output number or invalid control code will result in a 0x09 error reply. Refer to Table 13.

Documents
Document Sharing Hub
Full document details: BS EN IEC 60839-11-5:2020

Table 13 – Output control command

Packet format field	Code	Name	Meaning
CMND	0x68	osdp_OUT	
DATA 4 bytes repeated 1 or more times.	0x00 = First output 0x01 = Second output etc.	Output number	
	Refer to Table 14	Control code	Requested output state
	Refer to 6.9	Timer LSB	A 16 bit timer value, in units of 100 ms A zero value means “forever”
		Timer MSB	
The reply can be any of the following: • osdp_ACK as described in 7.2 • osdp_NAK as described in 7.3 • osdp_OSTATR as described in 7.8			

The PD may respond with a reply osdp_OSTATR to indicate that output(s) have changed state, or at the PD's option, it can return reply osdp_ACK, then send the output change report osdp_OSTATR later.

Table 14 – Control code values

Control code value	Meaning
0x00	NOP – do not alter this output
0x01	set the permanent state to OFF, abort timed operation (if any)
0x02	set the permanent state to ON, abort timed operation (if any)
0x03	set the permanent state to OFF, allow timed operation to complete
0x04	set the permanent state to ON, allow timed operation to complete
0x05	set the temporary state to ON, resume permanent state on timeout
0x06	set the temporary state to OFF, resume permanent state on timeout

6.10 Reader LED control command (osdp_LED)

This command controls the LEDs associated with one or more readers.

Once the temporary command's timer expires the LED will revert to the last permanent state set.

The permanent command is volatile (does not transcend power cycles).

The LED will flash, alternating between the color specified for ON and color specified for OFF at the rate specified by the corresponding timers. Setting both color codes to the same value will produce a steady (non-flashing) output.

The 16-bit timer applies to the temporary LED commands only.

The LED control command message packet may contain multiple 14-byte records. The PD should use the total message length to determine the number of records present. The number of records should not exceed the number of LEDs as reported in function code 4 (Annex B); however, the upper limit should not exceed the receive buffer size of the PD as reported in function code 10 (Annex B).

AVA Documents Document Sharing Hub

Full document details: BS EN IEC 60839-11-5:2020

Records containing an invalid Reader/LED number will result in a 0x09 error reply.

If the ACU sets a temporary setting and tries to establish another temporary setting, then a new temporary command should override a currently active temporary command.

The ON time OFF time values cannot both be set to zero. Refer to Table 15.

Table 15 – Reader LED control command

Packet format field	Code	Name	Meaning
CMND	0x69	osdp_LED	
DATA 14 bytes repeated 1 or more times.	0x00 = First reader 0x01 = Second reader etc.	Reader number	
	0x00 = first LED 0x01 = second LED etc.	LED number	
	Temporary settings		
	Refer to Table 16	Control code	The mode to enter temporarily
	0x00 – 0xFF	ON time	An 8 bit ON duration of the flash, in units of 100 ms A zero value means no duration
	0x00 – 0xFF	OFF time	An 8 bit OFF duration of the flash, in units of 100 ms A zero value means no duration
	Refer to Table 18	ON color	The color to set during the ON time
	Refer to Table 18	OFF color	The color to set during the OFF time
	Refer to 6.10	Timer (LSB)	A 16 bit timer value, in units of 100 ms A zero value means “forever”
	Refer to 6.10	Timer (MSB)	
	Permanent settings		
	Refer to Table 17	Control code	The mode to return to after the timer expires
	0x00 – 0xFF	ON time	An 8 bit ON duration of the flash, in units of 100 ms A zero value means no duration
	0x00 – 0xFF	OFF time	An 8 bit OFF duration of the flash, in units of 100 ms A zero value means no duration
	Refer to Table 18	ON color	The color to set during the ON time
	Refer to Table 18	OFF color	The color to set during the OFF time

Documents
Document Sharing Hub
Full document details: BS EN IEC 60839-11-5:2020