
Alarmni in elektronski varnostni sistemi - 11-5. del: Elektronski sistemi nadzora dostopa - Odprti protokol nadzora naprav (OSDP)

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

Ta slovenski standard je istoveten z: EN IEC 60839-11-5:2020

ICS:

13.320 Alarmni in opozorilni sistemi Alarm and warning systems

SIST EN IEC 60839-11-5:2020

en

iTeh STANDARD PREVIEW
(standards.iteh.ai)

<https://standards.iteh.ai/catalog/standards/sist/84a17e5-01b7-4cca-81c5-d1518c147408/sist-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

EN IEC 60839-11-5:2020 (E)**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.

STANDARD PREVIEW
(standards.iteh.ai)
SIST EN IEC 60839-11-5:2020
<https://standards.iteh.ai/catalog/standards/sist/844b17e5-01b7-4cca-81e5-d1518c147408/sist-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.

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

<https://standards.iteh.ai/catalog/standards/sist/84a17e5-01b7-4cca-81c5-d1518c147408/sist-en-iec-60839-11-5-2020>



IEC 60839-11-5

Edition 1.0 2020-07

INTERNATIONAL STANDARD

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

*Pre-Standard Preview
(standard.iec.ai)*
SIST EN IEC 60839-11-5:2020 -
<https://standards.iteh.ai/catalog/standards/sist/84a117e5-01b7-4cca-81e5-d1518c147408/sist-en-iec-60839-11-5-2020>

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 13.320

ISBN 978-2-8322-8480-3

Warning! Make sure that you obtained this publication from an authorized distributor.

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_SCRIPT).....	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

iTeh STANDARD PREVIEW
 (standards.iteh.ai)
 SIST EN IEC 60839-11-5:2020 -
<https://standards.iteh.ai/catalog/standards/sist/84a117e5-01b7-4cca-81e5-d1518c147408/sist-en-iec-60839-11-5-2020>