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)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

About the IEC
The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications
The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

IEC Customer Service Centre - webstore.iec.ch/csc
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

Electropedia - www.electropedia.org
The world's leading online dictionary on electrotechnology, containing more than 22 000 terminological entries in English and French, with equivalent terms in 16 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
67 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

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)

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_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_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

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*

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

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.

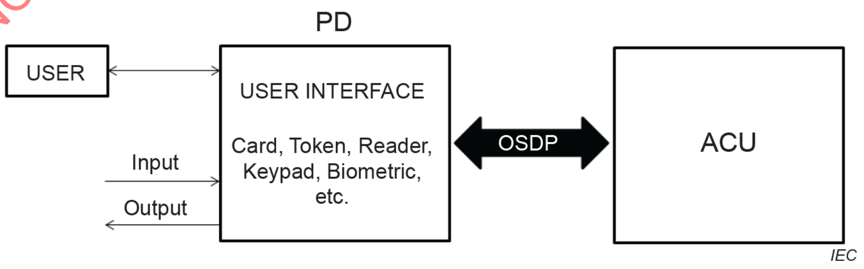

Figure 1 – Schematic overview of an OSDP connection

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).

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.

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

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

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;

- 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.

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.

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.

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.

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).

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

Table 16 – Temporary control code values

Temporary control code value	Meaning
0x00	NOP – do not alter this LED's temporary settings. The remaining values of the temporary settings record are ignored.
0x01	Cancel any temporary operation and display this LED's permanent state immediately
0x02	Set the temporary state as given and start timer immediately.

Table 17 – Permanent control code values

Permanent control code value	Meaning
0x00	NOP – do not alter this LED's permanent settings
0x01	Set the permanent state as given.

Table 18 – Color values

Color value	Meaning
0	Black (off/unlit)
1	Red
2	Green
3	Amber
4	Blue
The reply can be any of the following: • osdp_ACK as described in 7.2, • osdp_NAK as described in 7.3.	

Examples:

To cause the first LED on the first reader to flash red (100 ms) / black (200 ms) for 3 s, then resume its current display mode:

0, 0, 2, 1, 2, 1, 0, 30, 0, 0, 0, 0, 0, 0

To set the reader's second LED to display a steady green output

0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 2, 2

6.11 Reader buzzer control command (osdp_BUZ)

This command defines commands to a single, monotone audible annunciator (beeper or buzzer) that may be associated with a reader.

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

A record that contains an invalid reader number will result in a 0x09 error reply.

Refer to Table 19.

Table 19 – Reader buzzer control command (osdp_BUZ)

Packet format field	Code	Name	Meaning
CMND	0x6A	osdp_BUZ	
DATA 5 bytes repeated 1 or more times.	0x00 = First reader 0x01 = Second reader etc.	Reader number	
	0x00 = no tone 0x01 = off 0x02 = default tone	Tone code	Requested tone state
	0x00 – 0xFF	On time	The ON duration of the sound, in units of 100 ms
	0x00 – 0xFF	OFF time	The OFF duration of the sound, in units of 100 ms
	0x00 – 0xFF	Count	The number of times to repeat the ON/OFF cycle. 0 = tone continues until another tone command is received

6.12 Reader text output command (osdp_TEXT)

This command defines a string to be shown on a simple character-oriented text display organized in a row and column format. The PD is assumed to have limited text capability and so only small display sizes are supported.

Text will be written at the given starting position. If necessary, and if allowed by the command, the text may wrap to the next line. If the text message is used to represent calendar date and time then the format “GeneralizedTime” as defined in ISO 8601 should be used.

“Temp text” overwrites a text field for a specified time period after which the permanent text field is restored.

The "temp text time" field indicates the duration of the temp display in seconds. This field has a different meaning when used with a permanent text command. In that case, if the temp text time is zero then any active temp text shall be allowed to complete. A non-zero temp text time means that any active temp text shall be aborted and the permanent text shall be displayed immediately.

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

Commands issued to elements that are non-existent, will receive a NAK response. Refer Table 20.

Table 20 – Reader text output command (osdp_TEXT)

Packet format field	Code	Name	Meaning
CMND	0x6B	osdp_TEXT	
DATA	0x00 = First reader 0x01 = Second reader etc.	Reader number	
	See Table 21	Text command	How to treat the text
	0x00 – 0xFF	Temp text time	The duration to display temporary text, in seconds
	0x00 – 0xFF	Row	The row where the first character will be displayed. 0x01 = top row
	0x00 – 0xFF	Column	The column where the first character will be displayed 0x01 = leftmost column
	0x00 – 0xFF	Text length	Number of characters in the string
	0x20 to 0x7E	String	The string to display PD shall implement the minimum printable ASCII character set

Table 21 – Text command values

Text command value	Meaning
0x01	permanent text, no wrap
0x02	permanent text, with wrap
0x03	temp text, no wrap
0x04	temp text, with wrap

6.13 Communication configuration command (osdp_COMSET)

This command sets the PD's communication parameters. The settings will take effect AFTER the PD has completed its response to this command. It is recommended that communication parameters set by this command (address, baud rate) are non-volatile.

If the PD is unable to comply, it will return the values that it will use after the completion of this reply.

Refer to Table 22.

Table 22 – Communication configuration command (osdp_COMSET)

Packet format field	Code	Name	Meaning
CMND	0x6E	osdp_COMSET	
DATA 5 bytes	0x00 – 0x7E	Address	Unit ID to which this PD will respond after the change takes effect
	0x00 – 0xFF	Baud rate LSB	The baud rate is expressed as a 32-bit integer holding the actual value of the baud rate to use, such as 9 600, 38 400, etc.
	0x00 – 0xFF	Baud rate	
	0x00 – 0xFF	Baud rate	
	0x00 – 0xFF	Baud rate MSB	

6.14 Scan and send biometric data (osdp_BIOREAD)

This command instructs the reader to perform a fingerprint scan and return the scan data to the ACU as a poll response in osdp_BIOREADR. The type, format and quality of the scan are specified in the command structure. The reader shall restore the display to its previous state when finished processing the user input.

Table 23 – Scan and send biometric data (osdp_BIOREAD)

Packet format field	Code	Name	Meaning
CMND	0x73	osdp_BIOREAD	
DATA 4 bytes	0x00 = First reader 0x01 = Second reader etc.	Reader number	
	See Table 24	BIO_TYPE	Type/body part to scan
	See Table 25	BIO_FORMAT	Format of data to be returned
	0x00 – 0xFF	BIO_QUALITY	Normalised

Table 24 – Biometric types

Value	Meaning
0x00	Not specified – default –
0x01	Right thumb print
0x02	Right index finger print
0x03	Right middle finger print
0x04	Right ring finger print
0x05	Right little finger print
0x06	Left thumb print
0x07	Left index finger print
0x08	Left middle finger print
0x09	Left ring finger print
0x0A	Left little finger print
0x0B	Right iris scan
0x0C	Right retina scan
0x0D	Left iris scan
0x0E	Left retina scan
0x0F	Full face image
0x10	Right hand geometry
0x11	Left hand geometry

Table 25 – Fingerprint formats

Value	Meaning
0x00	Not specified – use default method to scan, then report format used
0x01	Send raw fingerprint data as a PGM
0x02	ANSI/INCITS 378 Fingerprint template 84

6.15 Scan and match biometric template (osdp_BIOMATCH)

If the reader supports biometric template matching, this command should be used instead of BIOREAD to improve performance. This packet instructs the reader to perform a biometric scan and to match it against the template provided in the data section of this packet and return the results to the ACU as a poll response in osdp_BIOMATCHR. The reader should restore the display to its previous state when done processing the user input. See Table 26.

Table 26 – Command structure: 6-byte header followed by a variable length template

Packet format field	Code	Name	Meaning
CMND	0x74	osdp_BIOMATCH	
DATA 5 bytes	0x00 = First reader 0x01 = Second reader etc.	Reader number	
	See Table 24	BIO_TYPE	Type/body part to scan
	See Table 25	BIO_FORMAT	Format of attached template
	0x00 – 0xFF	BIO_QUALITY	Threshold required for accepting the bio match, normalized
	0x00 – 0xFF	BIO_LENGTH (LSB)	Template length, least significant byte
	0x00 – 0xFF	BIO_LENGTH (MSB)	Template length, most significant byte
Data array	0x00 – 0xFF	BIO_DATA	Array of template data of BIO_LENGTH

6.16 Encryption key set (osdp_KEYSET)

This command transfers an encryption key from the ACU to a PD.

Refer to D.2.1.

6.17 Challenge and secure session initialization request (osdp_CHLNG)

This command is the first in the secure channel session connection sequence (SCS-CS).

Refer to D.2.2.

6.18 Server's random number and server cryptogram (osdp_SCRYPT)

This command transfers a block of data used for encryption synchronization.

Refer to D.2.3.

6.19 Manufacturer specific command (osdp_MFG)

This command is intended to allow manufacturer specific commands to be embedded within this protocol. The data content of this command is not defined in this document beyond the following formatting guidelines. The PD may use the vendor code and other content dependent values to confirm that the command contains the expected structure. Refer to Table 27.

Table 27 – Manufacturer specific commands (osdp_MFG)

Packet format field	Code	Name	Meaning
CMND	0x80	osdp_MFG	Command ID specifically defined for this vendor
DATA 3 bytes	0x00 – 0xFF	vendor code 1st	IEEE assigned OUI, "first octet"
	0x00 – 0xFF	vendor code 2nd	IEEE assigned OUI, "second octet"
	0x00 – 0xFF	Vendor code 3rd	IEEE assigned OUI, "third octet"
Data array	0x00 – 0xFF	DATA	Vendor defined
Reply: osdp_ACK, osdp_NAK, osdp_MFGREP – Manufacturer specific reply			

1) The PD shall use the four bytes formed by the three byte VendorCode and the Command_ID to interpret the command and its associated data. As with the “public” (non vendor specific) commands, content dependent values may be used to confirm that the data component of the command contains the expected structure.

2) A vendor is free to define any number of “Command_ID”-s and associated data structures without any obligation to or authorization by the OSDP community.

6.20 ACU receive size (osdp_ACURXSIZE)

This command informs the PD of the maximum size message the ACU can receive. Refer to Table 28.

Table 28 – ACU receive size (osdp_ACURXSIZE)

Packet format field	Code	Name	Meaning
CMND	0x7B	osdp_ACURXSIZE	
DATA 2 Bytes	0x00 – 0xFF	ACURX_BUFSIZE_LSB	ACU max receive buffer
	0x00 – 0xFF	ACURX_BUFSIZE_MSB	

6.21 Keep reader active (osdp_KEEPACTIVE)

This command instructs the PD to continue reader operations for the specified time limit to maintain communications with the credential. Refer to Table 29.

Table 29 – Keep reader active (osdp_KEEPACTIVE)

Packet format field	Code	Name	Meaning
CMND	0xA7	osdp_KEEPACTIVE	
DATA 2 Bytes	0x00 – 0xFF	KP_ACT_TIME (LSB)	Card keep-alive time in milliseconds
	0x00 – 0xFF	KP_ACT_TIME (MSB)	

6.22 Abort current operation (osdp_ABORT)

This command instructs the PD to abort the current operation. Refer to Table 30.

Table 30 – Abort current operation (osdp_ABORT)

Packet format field	Code	Name	Meaning
CMND	0xA2	osdp_ABORT	
DATA	Omitted		

6.23 Get PIV data (osdp_PIVDATA)

This command instructs the PD to return the selected contents of a PIV card. The byte ordering of certain fields is MSB first to match the card contents. Refer to Table 31.

Table 31 – Get PIV data (osdp_PIVDATA)

Packet format field	Code	Name	Meaning
CMND	0xA3	osdp_PIVDATA	
DATA 5 Bytes	0x00 – 0xFF	PIV-OBJECT-ID 1st	PIV object per SP 800-73-4 Part 1
	0x00 – 0xFF	PIV-OBJECT-ID 2nd	
	0x00 – 0xFF	PIV-OBJECT-ID 3rd	
	0x00 – 0xFF	PIV element ID	
	0x00 – 0xFF	Data offset	Offset within requested field

6.24 General authenticate (osdp_GENAUTH)

This command instructs the PD to direct a PIV credential to perform a general authenticate operation. The message detail is the cryptographic challenge payload. This sends an encrypted payload and expects a decrypted response. The algorithm and key are only sent one time per message and subsequent fragments (if needed) do not include these. Refer to Table 32.

Table 32 – General authenticate (osdp_GENAUTH) fragment

Packet format field	Code	Name	Meaning
CMND	**0xA4**	**osdp_GENAUTH**	
DATA	0x00 – 0xFF	TOTAL (LSB)	whole message length
	0x00 – 0xff	TOTAL (MSB)	
	0x00 – 0xff	OFFSET (LSB)	offset within whole message
	0x00 – 0xff	OFFSET (MSB)	
	0x00 – 0xff	DATA_LEN (LSB)	length of this fragment
	0x00 – 0xff	DATA_LEN (MSB)	
	0x00 – 0XFF	Algorithm and Key	Selected algorithm and key (first fragment only) NIST SP800-78-4, Table 6-2
	0x00 – 0xFF	Challenge	Cryptographic challenge payload fragment

6.25 Authentication challenge (osdp_CRAUTH)

This command instructs the PD to perform a cryptographic challenge/response sequence. The challenge data is in the payload of this message. This sends an unencrypted payload and expects an encrypted response. The algorithm and key are only sent one time per message and subsequent fragments (if needed) do not include these. Refer to Table 33.

Table 33 – Authentication challenge (osdp_CRAUTH) fragment

Packet format field	Code	Name	Meaning
CMND	**0xA5**	**osdp_CRAUTH**	
DATA	0x00 – 0xFF	TOTAL (LSB)	whole message length
	0x00 – 0xff	TOTAL (MSB)	
	0x00 – 0xff	OFFSET (LSB)	offset within whole message
	0x00 – 0xff	OFFSET (MSB)	
	0x00 – 0xff	DATA_LEN (LSB)	length of this fragment
	0x00 – 0xff	DATA_LEN (MSB)	
	0x00 – 0XFF	Algorithm and key	Selected algorithm and key (first fragment only) NIST SP800-78-4, Table 6-2
	0x00 – 0xFF	Challenge	Cryptographic challenge payload fragment

6.26 File transfer command (osdp_FILETRANSFER)

This command is used to transfer a block of data, called a "file", from the ACU to the PD. This is intended for use for firmware update, configuration changes, and other applications. There will in general be more than one osdp_FILETRANSFER message/reply pairs. The first one shall use the default message size (128 bytes) or a message no larger than the value returned in osdp_PDCAP. The PD response will contain control details including status. osdp_FILETRANSFER messages are continued until the PD sends an abort or the transfer is complete. Subsequent osdp_FILETRANSFER messages shall have increasing offsets. Refer to Table 34.

Table 34 – File transfer command

Packet format field	Code	Name	Meaning
CMND	0x7C	osdp_FILETRANSFER	
DATA		FtType	File transfer type 1= opaque file contents recognizable by this specific PD 2..127 = Reserved for future use 128..255 = Reserved for private use
	0x00-0xFF	FtSizeTotal (LSB)	File size (4 bytes,) little-endian format.
	0x00-0xFF	FtSizeTotal	
	0x00-0xFF	FtSizeTotal	
	0x00-0xFF	FtSizeTotal (MSB)	
	0x00-0xFF	FtOffset (LSB)	Offset in file of current message. Shall be monotonically increasing.
	0x00-0xFF	FtOffset	
	0x00-0xFF	FtOffset	
	0x00-0xFF	FtOffset (MSB)	
	0x00-0xFF	FtFragmentSize (LSB)	Size of fragment (2 bytes)
	0x00-0xFF	FtFragmentSize (MSB)	
	0x00-0xFF	FtData	File transfer fragment (optional)

The reply will be osdp_FTSTAT or osdp_NAK. The osdp_FTSTAT response dictates whether you send another osdp_FILETRANSFER command.

6.27 Extended write data (osdp_XWR)

6.27.1 General

This command implements extended write mode to facilitate communications with an ISO 7816-4 based credential. See 5.11 for a description of transparent mode.

Command Structure: 2 byte command structure, followed by an optional data block. Refer to Table 35.

Table 35 – Extended write command structure

Packet format field	Code	Name	Meaning
CMND	0xA1	osdp_XWR	
DATA	0 or 1	XRW_MODE	Extended READ/WRITE mode. Details below in 6.27.2 to 6.27.8
		XWR_PCMND	XRW_MODE dependent command code. Details below in 6.27.2 to 6.27.8
	0x00-0xFF	XWR_PDATA	Optional – XWR_PCMND dependent data
The reply can be any of the following: osdp_ACK, osdp_NAK, osdp_XRD.			

6.27.2 Mode set command

The Mode-00 set command sets and configures the background behaviour mode.

Command structure: 2 byte mode and command spec, 1 byte mode code and 1 optional byte for configuration. In the absence of the configuration byte, 0x00 is used. Refer to Table 36.

Table 36 – Mode set command

Size (in bytes)	Name	Meaning
1	XRW_MODE	0x00 = Mode 0
1	XRW_PCMND	0x01 = Request the PD to return the current XRW_MODE in effect 0x02 = Set the mode and config 0x03 – 0xFF = Reserved for future use
1	Mode code	0x00 = Mode 0 0x01 = Mode 1
1	Mode config	0x00 = Disable read card info report response 0x01 = Enable read card info report response (Mode 0 only)

The mode config values to set mode 0 are as listed in Table 37.

Table 37 – Mode 0 configuration

Bit values	Meaning
0 (LSBit)	1 = Enable the mode 0 extended read card info report response 0 = Disable
1-7	Shall be zero

The mode config values to set mode 1 are as listed in Table 38.

Table 38 – Mode 1 configuration

Bit values	Meaning
0-7	Shall be zero
The reply can be: osdp_ACK, osdp_NAK.	

6.27.3 Mode-00 read setting

The mode-00 read setting command is a request to the PD to return its current background behaviour mode setting.

Command structure: 2 byte mode and command spec, no additional command data structure. Refer to Table 39.

Table 39 – Read setting request

Packet format field	Code	Name	Meaning
MODE	0x00	XRW_MODE	This is a Mode-00 command
PCMND	0x01	XRW_PCMND	Read mode setting
The reply can be one of: osdp_XRD (XRW_Mode=0, XRD_REPLY=0x01), osdp_NAK.			

6.27.4 Mode specific command codes for XRW_MODE=1

Mode 1 specific commands instruct the reader to perform certain operations. Refer to Table 40.

Table 40 – Mode specific command codes

XWR_PCMND	Meaning
0x01	Pass the APDU embedded in this command to the specified reader
0x02	Notifies the designated reader to terminate its connection to the smart card
0x03	Instructs the designated reader to perform “secure PIN entry”
0x04	Instructs the designated reader to perform a smart card scan
0x05	Rserved for future use.

6.27.5 Mode-01 transparent content send request

The mode-01 XMIT send request command passes a data packet to the PD (reader) to pass on the smart card.

Command structure: 2 byte mode and command spec, 1 byte reader number, 1 byte destination, followed by an APDU structure. Refer to Table 41.

Table 41 – Transparent content send request

Size (in bytes)	Name	Meaning
1	XRW_MODE	This is a mode-01 command
1	XWR_PCMND	0x01 = Transparent content send command
1	Reader number	0 = First reader
N	APDU	Valid APDU to send to the smart card
The reply can be one of: osdp-ACK, osdp_NAK.		

6.27.6 Mode-01 connection done

The mode-01 smartcard connection done command instructs the PD (reader) to disconnect from the smartcard.

Command structure: 2 byte mode and command spec, 1 byte reader number, no additional command data structure. Refer to Table 42.

Table 42 – Smartcard connection done

Size (in bytes)	Name	Meaning
1	XRW_MODE	This is a mode-01 command
1	XWR_PCMND	0x02 = smart card connection done
1	Reader number	0 = first reader

6.27.7 Mode-01 request secure PIN entry command

The mode-01 secure PIN entry command instructs the PD (reader) to perform a local secure PIN entry sequence with the smart card. It also includes an APDU for the smart Card. When the reader receives this packet, it autonomously prompts the user for their PIN, inserts the PIN into the APDU and sends it to the smart card. The reader should restore the display to its previous state when done processing the user input.

While processing this message, the reader should not add any keys to the keypad buffer.

Command structure: a 22-byte header followed by a variable-length APDU. Refer to Table 43.

Table 43 – Request secure PIN entry command

Size (in bytes)	Name	Meaning
1	XRW_MODE	0x01 = This is a mode-01 command
1	XRW_PCMND	0x03 = Secure PIN entry request
1	Reader number	0 = First reader
1	bTimeOut	timeout in s (00 means use default timeout)
1	bTimeOut2	timeout in s after first key stroke
1	bmFormatString	Formatting USB_CCID_PIN_FORMAT_xxx
1	bmPINBlockString	Bits 7-4 – bit size of PIN length in APDU bits 3-0 – PIN block size in bytes after justification and formatting
1	bmPINLengthFormat	bits 7-5 reserved for future use, bit 4 set if system units are bytes clear if system units are bits. bits 3-0 PIN length position in system units
1	wPINMaxExtraDigit (MSB)	XXYY, where XX is minimum PIN size in digits, YY is maximum
1	wPINMaxExtraDigit (LSB)	
1	bEntryValidationCondition	Conditions under which PIN entry should be considered complete
1	bNumberMessage	Number of verification messages to display for PIN
1	wLangId (MSB)	Language for messages
1	wLangId (LSB)	
1	bMsgIndex	Message index (should be 00)
3	bTeoPrologue	(3 bytes) T=1 I-block prologue field to use (fill with 00)
2	ulDataLength (MSB)	length of APDU to be sent to the smart card
	ulDataLength (LSB)	
N	aPDUData	APDU data to be sent to the smart card
The reply can be one of: osdp_ACK, or osdp_NAK.		

Below is an example of how this data structure is built on the host:

```
PIN_VERIFY_STRUCTURE *pin_verify;

pin_verify = (PIN_VERIFY_STRUCTURE *)bSendBuffer;

/* PC/SC v2.02.05 Part 10 PIN verification data structure */
pin_verify -> bTimerOut = 0x00;
pin_verify -> bTimerOut2 = 0x00;
pin_verify -> bmFormatString = 0x82; /* ascii, left justified, 0 offset from Lc,
                                            system unit bytes */
pin_verify -> bmPINBlockString = 0x08;
pin_verify -> bmPINLengthFormat = 0x00;
pin_verify -> wPINMaxExtraDigit = HOST_TO_CCID_16(0x0408); /* Min Max */
pin_verify -> bEntryValidationCondition = 0x02;  /* validation key pressed */
pin_verify -> bNumberMessage = 0x01;
pin_verify -> wLangId = HOST_TO_CCID_16(0x0904);
pin_verify -> bMsgIndex = 0x00;
pin_verify -> bTeoPrologue[0] = 0x00;
pin_verify -> bTeoPrologue[1] = 0x00;
pin_verify -> bTeoPrologue[2] = 0x00;
/* pin_verify -> ulDataLength = 0x00; we don't know the size yet */

/* APDU: 00 20 00 00 08 30 30 30 30 00 00 00 00 */
offset = 0;
pin_verify -> abData[offset++] = 0x00;/* CLA */
pin_verify -> abData[offset++] = 0x20;/* INS: VERIFY */
pin_verify -> abData[offset++] = 0x00;/* P1 */
pin_verify -> abData[offset++] = 0x80;/* P2 */
pin_verify -> abData[offset++] = 0x08;/* Lc: 8 data bytes */
pin_verify -> abData[offset++] = 0xff;
pin_verify -> abData[offset++] = 0xff;
pin_verify -> abData[offset++] = 0xff;
pin_verify -> abData[offset++] = 0xff;
pin_verify -> abData[offset++] = 0xff;
pin_verify -> abData[offset++] = 0xff;
pin_verify -> abData[offset++] = 0xff;
pin_verify -> abData[offset++] = 0xff;
pin_verify -> ulDataLength = HOST_TO_CCID_32(offset);  /* APDU size */

send_len = sizeof(PIN_VERIFY_STRUCTURE) + offset -1;
/* -1 because PIN_VERIFY_STRUCTURE contains the first byte of abData[] */
```

6.27.8 Mode-01 smartcard scan

This is used to identify if a smartcard is present at the reader. Refer to Table 44.

Table 44 – Smartcard scan

Size (in bytes)	Name	Meaning
1	XRW_MODE	This is a mode-01 command
1	XWR_PCMND	0x04 = Smart card scan
1	Reader number	0 = First reader
The reply can be one of: osdp_XRD (osdp_PR01PRES or osdp_PR01ERROR), osdp_NAK.		

7 Replies

7.1 General

The PD shall begin sending a reply less than REPLY_DELAY after it receives the last character of a valid command. If it cannot, it should send an osdp_BUSY.

If the ACU receives a packet with an invalid checksum/CRC it should re-transmit the command using the same SQN as the original request to have the PD resend the reply.

See Table A.2 for a quick reference showing numeric reply values.

7.2 General acknowledge – Nothing to report (osdp_ACK)

There is no reply structure associated with this reply. Sent in response to all valid commands that do not require a specific response or will not receive an immediate response. Refer to Table 45.

Table 45 – General acknowledge (osdp_ACK)

Packet format field	Code	Name	Meaning
CMND	0x40	osdp_ACK	
DATA	Omitted		

7.3 Negative acknowledge – Error response (osdp_NAK)

The optional completion code array may be omitted if none of the command records were processed either because the command had only one record, or because none of the records were processed due to invalid record sizing.

Bytes 1-N are present only for error codes that define its use. The optional completion code array may be omitted if none of the command records were processed either because the command had only one record, or because none of the records were processed due to invalid record sizing. Refer to Table 46.

Table 46 – Negative acknowledge (osdp_NAK)

Packet format field	Code	Name	Meaning
CMND	0x41	osdp_NAK	
DATA	See Table 47	Error code	Refer to Table 47
	0x00 – 0xFF	Data	Error code dependent, 1 – N

Table 47 – Error codes

Error code value	Meaning
0x00	No error
0x01	Message check character(s) error (bad cksum/crc)
0x02	Command length error
0x03	Unknown command code – Command not implemented by PD
0x04	Unexpected sequence number detected in the header
0x05	This PD does not support the security block that was received
0x06	Encrypted communication is required to process this command
0x07	BIO_TYPE not supported
0x08	BIO_FORMAT not supported
0x09	Unable to process command record 0x09 indicates that one or more command records had invalid parameters and was not processed which can be followed by an optional array, where each byte represents the completion code of the corresponding command record. A zero value indicates no error, and the value 0xFF indicates a generic error.

7.4 Device identification report (osdp_PDID)

Sent in response to an osdp_ID command. Refer to Table 48. Note also that the “cUID”, used in certain secure channel operations, is the first 8 bytes of the PDID response.

Reply Structure: 12-byte fixed record.

Table 48 – Device identification report (osdp_PDID)

Packet format field	Code	Name	Meaning
CMND	0x45	osdp_PDID	
DATA 12 bytes	0x00 – 0xFF	Vendor code 1st	IEEE assigned OUI The vendor code is a 24-bit identifier of the manufacturer. It is recommended that each manufacturer use its IEEE assigned organizationally unique identifier, the same 24 bits it uses to form the MAC addresses of its ethernet-based products.
	0x00 – 0xFF	Vendor code 2nd	
	0x00 – 0xFF	Vendor code 3rd	
	0x00 – 0xFF	Model number	Manufacturer's model number The model field is assigned by and managed by the Vendor. This field has no direct operational purpose.
	0x00 – 0xFF	Version	Manufacturer's version of this product The version number field is assigned by and managed by the vendor. This field has no direct operational purpose.
	0x00 – 0xFF	Serial number (LSB)	4-byte serial number The 32-bit serial number field is assigned and managed by the vendor. This field has no direct operational purpose.
	0x00 – 0xFF	Serial number	
	0x00 – 0xFF	Serial number	
	0x00 – 0xFF	Serial number (MSB)	
	0x00 – 0xFF	Firmware major	Firmware revision code The firmware revision fields are assigned and managed by the vendor. These fields have no direct operational purpose.
	0x00 – 0xFF	Firmware minor	
	0x00 – 0xFF	Firmware build	

7.5 Device capabilities report (osdp_PDCAP)

Sent in response to an osdp_CAP command. The device capabilities report message may contain multiple records of this form (3 bytes per record). Use the total message length to determine the number of records present.

The records may be in any order. If a function code is omitted from the list, The ACU may assume that the PD has no support for that function code. A list of function codes and their definition, and the corresponding compliance levels is incorporated as Annex B. Refer to Table 49.

Reply structure: 3-byte element, repeated one or more times

Table 49 – Device capabilities report (osdp_PDCAP)

Packet format field	Code	Name	Meaning
CMND	0x46	osdp_PDCAP	
DATA 3 Bytes	0x00 – 0xFF	Function code	Repeated once per capability. Refer to Table B.1
	0x00 – 0xFF	Compliance	
	0x00 – 0xFF	Number of	

7.6 Local status report (osdp_LSTATR)

Sent in response to an osdp_LSTAT command or as a "poll response".

The local status report applies to conditions directly monitored by the PD. Tamper status is detected by the PD by monitoring the enclosure tamper mechanism. Power monitor status can be derived from the status of the power supply. Normally this reply is sent in response to an osdp_POLL command if either status has changed since the last POLL. Refer Table 50.

Reply Structure: 2 status bytes.

Table 50 – Local status report (osdp_LSTATR)

Packet format field	Code	Name	Meaning
CMND	0x48	osdp_LSTATR	
DATA 2 Bytes	0x00 – normal 0x01 – tamper	Tamper status	Status of tamper circuit
	0x00 – normal 0x01 – power failure	Power status	Status of power

7.7 Input status report (osdp_ISTATR)

Sent in response to an osdp_ISTAT command or as a "poll response".

Normally, this reply is sent in response to an osdp_POLL command if the status of any of the inputs has changed since the last report. The status of all inputs will be returned in this reply. The array size is defined by the total message length. The order of the status bytes corresponds to the numbering of the inputs, e.g. the first status byte corresponds to the first input, etc. Refer to Table 51.

Reply structure: 1 status byte for each input.

Table 51 – Input status report (osdp_ISTATR)

Packet format field	Code	Name	Meaning
CMND	0x49	osdp_ISTATR	
DATA	0x00 Inactive 0x01 Active		One per input

7.8 Output status report (osdp_OSTATR)

Sent in response to an osdp_OSTAT command, an osdp_OUT command or as a "poll response"

Normally, this response is sent as a reply to an osdp_OUT command to indicate that the output(s) have changed state.

This reply can also be sent in response to an osdp_POLL if the status of any of the outputs has changed since the last report. The status of all outputs will be returned in this reply. The array size is defined by the total message length. The order of the status bytes corresponds to the numbering of the outputs, e.g. the first status byte corresponds to the first output, etc. Refer to Table 52.

Reply structure: 1 status byte for each output.

Table 52 – Output status report (osdp_OSTATR)

Packet format field	Code	Name	Meaning
CMND	0x4A	osdp_OSTATR	
DATA	0x00 Inactive 0x01 Active		One per output

7.9 Reader tamper status report (osdp_RSTATR)

Sent in response to an osdp_RSTAT command or as a "poll response".

Normally, this reply is sent in response to an osdp_POLL if the status of any of the readers has changed since the last report. The tamper status of all readers will be returned in this reply. The array size is defined by the total message length. The order of the status bytes corresponds to the numbering of the readers, e.g. the first status byte corresponds to the first reader, etc.

The reader tamper is applicable only in cases where an external reader is attached to the PD, and the PD is able to monitor the status of the attached reader. (Certain readers can send periodic status messages.) Refer to Table 53.

Table 53 – Reader tamper status report (osdp_RSTATR)

Packet format field	Code	Name	Meaning
CMND	0x4B	osdp_RSTATR	
DATA	0x00 Normal 0x01 Not connected 0x02 Tamper		One per reader

7.10 Card data report, raw bit array (osdp_RAW)

Sent as a "poll response".

This reply is sent in response to an osdp_POLL command after a card was read but the raw data was not decoded into a character array. Unreported card data is deleted in case of, or during, a communication loss. Refer to Table 54.

Reply structure: 4-byte header, variable-length data.

Table 54 – Card data report, raw bit array (osdp_RAW)

Packet format field	Code	Name	Meaning
CMND	0x50	osdp_RAW	
DATA	0x00 – 0xFF	Reader number	0=First reader 1=Second reader
	0x00 = not specified, raw bit array 0x01 = P/data/P (wiegand)	Format code	Format of included data
	0x00 – 0xFF	Bit count (LSB)	2-byte size (in bits) of the data at the end of the record
	0x00 – 0xFF	Bit count (MSB)	
	0x00 – 0xFF	Data	8 bits of card data per data byte MSB to LSB (left justified)

7.11 Card data report, character array (osdp_FMT)

Sent as a "poll response".

This reply is sent in response to an osdp_POLL when decoded and formatted card data is available. Unreported card data is deleted in case of, or during, a communication loss. Refer to Table 55.

Reply structure: 3-byte header, variable-length data.

Table 55 – Card data report, character array (osdp_FMT)

Packet format field	Code	Name	Meaning
CMND	0x51	osdp_FMT	
DATA	0x00 – 0xFF	Reader number	0=First reader 1=Second reader
	0x00 = forward read 0x01 = reverse read	Read direction	Direction of data in array
	0x00 – 0xFF	Character count	Number of characters, including START, END, CKSUM
	0x00 – 0xFF	Data	Card data represented as ASCII characters

7.12 Keypad data report (osdp_KEYPAD)

Sent as a "poll response".

This reply is sent in response to an osdp_POLL if there is any data in the keypad buffer. It is applied when the keypad is in default operating mode. Unreported keypad data is deleted in case of, or during, a communication loss. Refer to Table 56.

Reply structure: 2-byte header, variable-length data.

Table 56 – Keypad data report (osdp_KEYPAD)

Packet format field	Code	Name	Meaning
CMND	0x53	osdp_KEYPAD	
DATA	0x00 – 0xFF	Reader number	0=First reader 1=Second reader
	0x00 – 0xFF	Digit count	Number of keypad digits to follow
	0x00 – 0xFF	Data	Card data represented as ASCII characters
The key encoding uses the following data representation: Digits 0 through 9 are reported as ASCII characters 0x30 through 0x39 The clear/delete/'*' key is reported as ASCII DELETE, 0x7F The enter/'#' key is reported as ASCII return, 0x0D Special/function keys are reported as upper case ASCII: A or F1 = 0x41, B or F2 = 0x42, C or F3 = 0x43, D or F4 = 0x44 F1 and F2 = 0x45, F2 and F3 = 0x46, F3 and F4 = 0x47, F1 and F4 = 0x48			

7.13 Communication configuration report (osdp_COM)

Sent in response to an osdp_COMSET command. This reply returns the communication parameters the PD will use after sending this reply. Refer to Table 57.

Reply structure: 5-byte record.

Table 57 – Communication configuration report (osdp_COM)

Packet format field	Code	Name	Meaning
CMND	0x54	osdp_COM	
DATA 5 bytes	0x00 – 0x7E	Address	Unit ID for this PD to respond to
	0x00 – 0xFF	Baud rate (LSB)	4 byte baud rate value
	0x00 – 0xFF	Baud rate	
	0x00 – 0xFF	Baud rate	
	0x00 – 0xFF	Baud rate (MSB)	

7.14 Scan and send biometric data (osdp_BIOREADR)

Sent as a "poll response".

The DATA section contains the scanned result in the requested format.

Reply structure: as defined below. Due to the template length, this reply may need to break up the data into multiple packets (See the “Multi-part messages” paragraph.) Refer to Table 58.

Table 58 – Scan and send biometric data (osdp_BIOREADR)

Packet format field	Code	Name	Meaning
CMND	0x57	osdp_BIOREADR	
DATA	0x00 – 0xFF	Reader number	0=First reader 1=Second reader
	0x00 – Success (rest of data fields are valid) 0x01 – Timeout 0x02 – 0xFE – Not used 0xFF – Unknown error	STATUS	
	See Table 24	BIO_TYPE	Bio template encoding type
	0x00 = worst 0xFF = best	BIO_QUALITY	Scan quality
	0x00 – 0xFF	BIO_LENGTH (LSB)	Template length, least significant byte
	0x00 – 0xFF	BIO_LENGTH (MSB)	Template length, most significant byte
	0x00 – 0xFF	BIO_TEMPLATE	Scan image or template

7.15 Scan and match biometric template (osdp_BIOMATCHR)

Sent as a "poll response".

Return the appropriate CODE and 1 byte of data indicating if the scanned body part matched the biometric template sent from the host. Refer to Table 59.

Reply structure: 1-byte reader number, 1-byte status code followed a 1-byte result code.

Table 59 – Scan and match biometric template (osdp_BIOMATCHR)

Packet format field	Code	Name	Meaning
CMND	0x57	osdp_BIOMATCHR	
DATA 3 Bytes	0x00 – 0xFF	Reader number	0=First reader 1=Second reader
	0x00 – Success (rest of data fields are valid) 0x01 – Timeout 0x02 – 0xFE – Not used 0xFF – Unknown error	STATUS	Results of requested command
	0x00 – No match 0xFF – Best match	SCORE	Result of the biometric match

7.16 Client's ID and client's random number (osdp_CCRYPT)

This reply sends a block of data used for encryption synchronization, sent in response to osdp_CHLNG command. Refer to D.3.1.

7.17 Client cryptogram packet and the initial R-MAC (osdp_RMAC_I)

This command transfers a block of data used for encryption synchronization, send in response to osdp_SCRYPT. Refer to D.3.2.

7.18 Manufacturer specific reply (osdp_MFGREP)

Sent in response to an osdp_MFGR command or as a "poll response".

This reply is intended to allow manufacturer specific messages to be embedded within this protocol. Refer to Table 60. The data content of this reply is not defined in this document beyond the following:

Table 60 – Manufacturer specific reply (osdp_MFGREP)

Packet format field	Code	Name	Meaning
CMND	0x90	osdp_MFGREP	
DATA	0x00 – 0xFF	Vendor code 1st	IEEE assigned OUI
	0x00 – 0xFF	Vendor code 2nd	
	0x00 – 0xFF	Vendor code 3rd	
	0x00 – 0xFF	Data	Vendor defined

7.19 PD busy reply (osdp_BUSY)

Sent in response to an osdp command if the PD is busy processing the previous command. This reply will use either checksum or CRC for message integrity even if the secure channel has been established and commands are exchanged using secure messaging. In other words, the busy reply is sent outside the secure channel and should not influence the secured messages that are sent before or after this reply.

The osdp_ACK is the appropriate response if the data requested by the command is not immediately available but will be returned in response to a subsequent osdp_POLL. Otherwise (meaning that a specific non-ACK response is required and the data is not available in time to meet the REPLY_TIMEOUT), the PD responds with osdp_BUSY until it is able to return the requested data. In this case, the ACU shall continue to repeat the command in its original form until the PD returns something other than osdp_BUSY. Refer to Table 61.

Table 61 – PD busy reply (osdp_BUSY)

Packet format field	Code	Name	Meaning
CMND	0x79	osdp_BUSY	
DATA	Omitted		
The sequence number of this ***reply*** will always be set to 0.			

7.20 PIV data reply (osdp_PIVDATAR)

Sent as a response to a PIV data request (osdp_PIVDATA). This message uses multi-part messaging as the entire response is assumed to be longer than one OSDP message. Refer to Table 62.

Table 62 – PIV data reply (osdp_PIVDATAR)

Packet format field	Code	Name	Meaning
CMND	0x80	osdp_PIVDATAR	
DATA	0x00 – 0xFF	TOTAL (LSB)	Whole message length
	0x00 – 0xFF	TOTAL (MSB)	
	0x00 – 0xFF	OFFSET (LSB)	Offset within whole message
	0x00 – 0xFF	OFFSET (MSB)	
	0x00 – 0xFF	DATA_LEN (LSB)	Length of this fragment
	0x00 – 0xFF	DATA_LEN (MSB)	
	0x00 – 0xFF	CARD_DATA	Requested data from cards

7.21 osdp_GENAUTHR

Sent as a response to a general authenticate request (osdp_GENAUTH.) This message uses multi-part messaging as the entire response is assumed to be longer than one OSDP message. Refer to Table 63.

Table 63 – General authenticate response (osdp_GENAUTHR)

Packet format field	Code	Name	Meaning
CMND	**0x81**	**osdp_GENAUTHR**	
DATA	0x00 – 0xFF	TOTAL (LSB)	Whole message length
	0x00 – 0xFF	TOTAL (MSB)	
	0x00 – 0xFF	OFFSET (LSB)	Offset within whole message
	0x00 – 0xFF	OFFSET (MSB)	
	0x00 – 0xFF	DATA_LEN (LSB)	Length of this fragment
	0x00 – 0xFF	DATA_LEN (MSB)	
	0x00 – 0xFF	AUTH_DATA	Response to general authenticate

7.22 Response to challenge (osdp_CRAUTHR)

Sent as a response to a cryptographic challenge (osdp_CRAUTH). This message uses multi-part messaging as the entire response is assumed to be longer than one OSDP message. Refer to Table 64.

Table 64 – Response to challenge (osdp_CRAUTHR)

Packet format field	Code	Name	Meaning
CMND	0x82	osdp_CRAUTHR	
DATA	0x00 – 0xFF	TOTAL (LSB)	whole message length
	0x00 – 0xFF	TOTAL (MSB)	
	0x00 – 0xFF	OFFSET (LSB)	offset within whole message
	0x00 – 0xFF	OFFSET (MSB)	
	0x00 – 0xFF	DATA_LEN (LSB)	Length of this fragment
	0x00 – 0xFF	DATA_LEN_MSB	
	0x00 – 0xFF	AUTH_DATA	Response to challenge

7.23 Manufacturer specific status reply (osdp_MFGSTATR)

Sent if there is a status condition requiring a manufacturer specific response. Refer to Table 65.

Table 65 – Manufacturer specific status reply (osdp_MFGSTATR)

Packet format field	Code	Name	Meaning
CMND	0x83	osdp_MFGSTATR	
DATA	0x00-0xFF	Data	Vendor defined

7.24 Manufacturer specific error reply (osdp_MFGERRR)

Sent if there is an error condition requiring a manufacturer specific response. Refer to Table 66.

Table 66 – Manufacturer specific error reply (osdp_MFGERRR)

Packet format field	Code	Name	Meaning
CMND	0x84	osdp_MFGERRR	
DATA	0x00-0xFF	Manufacturer specific	Details

7.25 File transfer status (osdp_FTSTAT)

Sent in response to an osdp_FILETRANSFER command. This message is the response to an osdp_FILETRANSFER request. If the file transfer is acceptable FtStat will be 0. If the file transfer is unacceptable FtStat will be a negative number. Use of secure channel or interleaved messages is indicated in FtAction. If an alternative message size is available, it is indicated in FtUpdateMsgMax. Some PD's require time delays due to the special nature of file transfer. In this case the FtDelay value is set to a non-zero value. If the PD responds with an FTSTAT of (3) – “finishing” then the ACU is to send an “idling” FILETRANSFER message with the total size set, the offset set to the total size, and the fragment size set to zero. Refer to Table 67.

Table 67 – File transfer status (osdp_FTSTAT)

Packet format field	Code	Name	Meaning
CMND	0x7A	osdp_FTSTAT	
DATA 7 bytes	0x00-0xFF	FtAction	Control flags. Bit 0: 1=OK to interleave; 0=dedicate for filetransfer. Bit 1: 1=shall leave secure channel for file transfer. 0= stay in secure channel if SC is active. Bit 2: 1=A separate poll response is available 0=no other activity.
	0x00-0xFF	FtDelay (LSB)	Requested ACU time delay in milliseconds before next osdp_FILETRANSFER message. 2 bytes, little endian. 0=no delay required.
	0x00-0xFF	FtDelay (MSB)	
	0x00-0xFF	FtStatusDetail (LSB)	File transfer status. This is a signed little-endian number. 0= ok to proceed. 1= file contents processed. 2= rebooting now, expect full communications reset. 3= PD is finishing file transfer. ACU shall send “idle” (FtFragmentSize=0) osdp_FILETRANSFER messages until status changes to another value. 4..32767=Reserved for future use -1= abort file transfer -2= unrecognized file contents -3=f ile data unacceptable (malformed) -4..-32768=Reserved for future use
	0x00-0xFF	FtStatusDetail (MSB)	
	0x00-0xFF	FtUpdateMsgMax (LSB)	Alternate maximum message size for osdp_FILETRANSFER messages for this transfer. 2 bytes, little endian. 0=no change requested, otherwise use this value as the maximum value for FtFragmentSize in the next osdp_FILETRANSFER message. This value may change from message to message.
	0x00-0xFF	FtUpdateMsgMax (MSB)	

7.26 Extended read reply (osdp_XRD)

7.26.1 General

Sent in response to an osdp_XWR command, or as a “poll response”.

Reply structure: 2 byte reply structure, followed by an optional data block. Refer to Table 68.

Table 68 – Extended read reply

Packet format field	Code	Name	Meaning
CMND	0xB1	osdp_XRD	
DATA	0 or 1	XRW_MODE	Extended READ/WRITE Mode. Refer to 7.26.2 and 7.26.6
		XRD_PREPLY	XRW_MODE dependent reply code. Refer to Table 69 to Table 77
	0x00 – 0xFF	XWR_PDATA	Optional – XWR_PCMND dependent data.

7.26.2 Mode specific reply codes for XRW_MODE=0

Refer to Table 69.

Table 69 – Mode specific reply codes

Code Value	Meaning
0x00	General error indication: PD was unable to process the command
0x01	Returns the current XRW_MODE in effect
0x02	Returns a card information report when a smart card is detected

7.26.3 Mode-00 error reply (osdp_PR00ERROR)

This may be sent as a poll response, or in response to any Mode-00 command (osdp_XWR | XRD_MODE = 0 | XWR_PCMND = any) to return an error or negative acknowledge (NAK) condition.

Reply structure: 2 byte mode and command spec followed by a single byte error code. Refer to Table 70.

Table 70 – Error reply

Size (in bytes)	Name	Meaning
1	XRW_MODE	0x00 = This is a mode-00 reply
1	XRD_PREPLY	0x00 = This is an extended read/write operation related error report
1	Error code	Various transparent mode error conditions

7.26.4 Mode setting report (osdp_PR00REQR)

This reply is sent in response to sdp_XWR|XRD_MODE=0|XWR_PCMND=osdp_PR00REQ and it returns its current background behaviour mode setting and configuration in response to the request.

Command structure: 2 byte mode and reply spec, plus 1 byte mode code, 1 byte config. Refer to Table 71.

Table 71 – Mode setting report

Size (in bytes)	Name	Meaning
1	XRW_MODE	0x00 = This is a mode-00 reply
1	XRD_PREPLY	0x01 = This is a mode setting report
1	Mode code	XRW_MODE in use for background operation
1	Mode config	The XRW_MODE configuration

7.26.5 Card information report (osdp_PR00CIRR)

Sent as a "poll response".

When enabled, this reply is sent in response to an osdp_POLL command after a smart card is detected that may require additional processing in an alternate mode.

Command structure: 2 byte mode and reply spec, followed by the card info report. Refer to Table 72.

Table 72 – Card information report

Size (in bytes)	Name	Meaning
1	XRW_MODE	0x00 = This is a mode-00 Reply
1	XRD_REPLY	0x02 = Card info report
1	Reader number	0= First reader 1=Second reader
1	Protocol	Detected card protocol 0 = Contact T0T1 1 = 14443 A/B 2 = reserved for future use
1	Length of CSN	Byte size of the CSN (0 = no data)
1	Length of protocol data	Byte size of the protocol data (0 = no data)
N	CSN data	Card serial number
N	Protocol data	Protocol specific data Protocol 0: ATR Protocol 1: ATS/ATQB

7.26.6 Mode specific reply codes for XRW_MODE=1

Refer to Table 73.

Table 73 – Mode specific reply codes

Code Value	Meaning
0x00	Card not present
0x01	Card present – Interface not specified
0x02	Card present on contactless interface
0x03	Card present on contact interface
0x04	reserved for future use

7.26.7 Mode-01 NAK or error reply (osdp_PR01ERROR)

This may be sent as a poll response, or in response to any mode-01 command (osdp_XWR | XRD_MODE = 1 | XWR_PCMND = any) to return an error or negative acknowledge (NAK) condition.

Reply structure: 2 byte mode and command spec followed by a single byte error code. Refer to Table 74.

Table 74 – Error reply

Size (in bytes)	Name	Meaning
1	XRW_MODE	0x01 = This is a mode-01 reply
1	XRD_PREPLY	0x00 = This is an extended read/write operation related error report
1	Error code	Various transparent mode error conditions

7.26.8 Card present notification reply (osdp_PR01PRES)

This reply is sent in response to an osdp_PR01SCSCAN indicating the resulting smart card connection status.

Command structure: 2 byte mode and reply spec, 1 byte reader number, 1 byte status. Refer to Table 75.

Table 75 – Card present notification reply

Size (in bytes)	Name	Meaning
1	XRW_MODE	0x01 = This is a mode-01 reply
1	XRD_PREPLY	0x01 = This is a “card present” reply
1	Reader number	0 = First reader
1	Status	Smart card present status

7.26.9 Transparent card data reply (osdp_PR01SCREP)

This reply is sent in response to an osdp_POLL reporting a data packet received from a smart card by a reader set to operate in background mode = 1.

Command structure: 2 byte mode and command spec, 1 byte reader number, 1 byte status, followed by an APDU structure. Refer to Table 76.

Table 76 – Transparent card data reply

Size (in bytes)	Name	Meaning
1	XRW_MODE	0x01 = This is a mode-01 reply
1	XRD_PREPLY	0x02 = This is a “card data” reply
1	Reader number	0 = First reader
1	Status	Results of requested command
N	APDU	APDU data from the card

7.26.10 Secure PIN entry complete reply (osdp_PR01SPER)

This reply is sent in response to an osdp_POLL indicating that a secure PIN entry sequence has completed. This reply is used by smart card readers set to operate in background Mode = 1.

Command structure: 2 byte mode and reply spec, 1 byte reader number, 1 byte status, 1 byte tries. Refer to Table 77.

Table 77 – Transparent card data reply

Size (in bytes)	Name	Meaning
1	XRW_MODE	0x01 = This is a mode-01 reply
1	XRD_PREPLY	0x03 = This is a “PIN entry complete” reply
1	Reader number	0 = First reader
1	Status	Results of the SPE sequence
1	Tries	Number of attempts before card “locks” itself

Annex A
(normative)

Command and reply code numbers commands

A.1 Commands

Table A.1 shows the code numbers for all commands supported by the protocol.

Table A.1 – Commands code numbers

Name	Value	Meaning	Data
osdp_POLL	0x60	Poll	None
osdp_ID	0x61	ID report request	Id type
osdp_CAP	0x62	PD capabilities request	Reply type
osdp_LSTAT	0x64	Local status report request	None
osdp_ISTAT	0x65	Input status report request	None
osdp_OSTAT	0x66	Output status report request	None
osdp_RSTAT	0x67	Reader status report request	None
osdp_OUT	0x68	Output control command	Output settings
osdp_LED	0x69	Reader led control command	LED settings
osdp_BUZ	0x6A	Reader buzzer control command	Buzzer settings
osdp_TEXT	0x6B	Text output command	Text settings
osdp_COMSET	0x6E	PD communication configuration command	Com settings
osdp_DATA	0x6F	Data transfer command	Raw data
osdp_BIOREAD	0x73	Scan and send biometric data	Requested return format
osdp_BIOMATCH	0x74	Scan and match biometric template	Biometric template
osdp_KEYSET	0x75	Encryption key set command	Encryption key
osdp_CHLNG	0x76	Challenge and secure session initialization Rq.	Challenge data
osdp_SCRYPT	0x77	Server cryptogram Refer to Table D.2	Encryption data
osdp_ACURXSIZE	0x7B	Max ACU receive size	Buffer size
osdp_FILETRANSFER	0x7C	Send data file to PD	File contents
osdp_MFG	0x80	Manufacturer specific command	Any
osdp_XWR	0xA1	Extended write data	APDU and details
osdp_ABORT	0xA2	Abort PD operation	None
osdp_PIVDATA	0xA3	Get PIV data	Object details
osdp_GENAUTH	0xA4	Request authenticate	Request details

Name	Value	Meaning	Data
osdp_CRAUTH	0xA5	Request crypto response	Challenge details
osdp_MFGSTAT	0xA6	Mfg specific status request	Request details
Osdp_KEEPACTIVE	0xA7	PD read activation	Time duration

A.2 Replies

The Table A.2 shows the code numbers for all replies supported by the protocol.

Table A.2 – Replies code numbers

Name	Value	Meaning	Data
osdp_ACK	0x40	Command accepted, nothing else to report	None
osdp_NAK	0x41	Command not processed	Reason for rejecting command
osdp_PDID	0x45	PD ID report	Report data
osdp_PDCAP	0x46	PD capabilities report	Report data
osdp_LSTATR	0x48	Local status report	Report data
osdp_ISTATR	0x49	Input status report	Report data
osdp_OSTATR	0x4A	Output status report	Report data
osdp_RSTATR	0x4B	Reader status report	Report data
osdp_RAW	0x50	Reader data – Raw bit image of card data	Card data
osdp_FMT	0x51	Reader data – Formatted character stream	Card data
osdp_KEYPAD	0x53	Keypad data	Keypad data
osdp_COM	0x54	PD communications configuration report	Comm data
osdp_BIOREADR	0x57	Biometric data	Biometric data
osdp_BIOMATCHR	0x58	Biometric match result	Result
osdp_CCRYPT	0x76	Client's ID, Random number, and cryptogram Refer to D.3.1 Client's ID and client's random number (osdp_CCRYPT)	Encryption data
osdp_BUSY	0x79	PD is busy reply	
osdp_RMAC_I	0x78	Initial R-MAC	Encryption data
osdp_FTSTAT	0x7A	File transfer status	Status details
osdp_PIVDATAR	0x80	PIV data reply	credential data
osdp_GENAUTHR	0x81	Authentication response	Response details
osdp_CRAUTHR	0x82	Response to challenge	Response details
osdp_MFGSTATR	0x83	MFG specific status	Rtatus details
osdp_MFGERRR	0x84	MFG specific error	Error details
osdp_MFGREP	0x90	Manufacturer specific reply	Any
osdp_XRD	0xB1	Extended read response	APDU and details

Annex B
(normative)

Function code definitions list

B.1 General

This annex refers to message type osdp_PDCAP. See Table B.1.

Table B.1 – Function codes

Byte	Name	Meaning	Value
0	Function code	Function/feature code	See function codes below
1	Compliance	Level of compliance with above function	See compliance levels in the function codes below
2	Number of	Number of objects of this type	See Number of objects in the function codes below

B.2 Function code 1 – Contact status monitoring

This function indicates the ability to monitor the status of a switch using a two-wire electrical connection between the PD and the switch. The on/off position of the switch indicates the state of an external device.

The PD may simply resolve all circuit states to an open/closed status, or it may implement supervision of the monitoring circuit. A supervised circuit is able to indicate circuit fault status in addition to open/closed status.

Compliance levels:

01 – PD monitors and reports the state of the circuit without any supervision. The PD encodes the circuit status per its default interpretation of contact state to active/inactive status.

02 – Like 01, plus: The PD accepts configuration of the encoding of the open/closed circuit status to the reported active/inactive status. (User may configure each circuit as "normally closed" or "normally open".)

03 – Like 02, plus: PD supports supervised monitoring. The operating mode for each circuit is determined by configuration settings.

04 – Like 03, plus: the PD supports custom end-of-line settings within the manufacturer's guidelines.

The end-of-line circuit parameters are defined by the manufacturer of the PD.

Number of: The number of inputs.

B.3 Function code 2 – Output control

This function provides a switched output, typically in the form of a relay. The output has two states: active or inactive. The ACU can directly set the output's state, or, if the PD supports timed operations, the ACU can specify a time period for the activation of the output.

Compliance levels:

01 – The PD is able to activate and deactivate the output per direct command from the ACU.

02 – Like 01, plus: The PD is able to accept configuration of the output driver to set the inactive state of the output. The typical state of an inactive output is the state of the output when no power is applied to the PD and the output device (relay) is not energized. The inverted drive setting causes the PD to energize the output during the inactive state and de-energize the output during the active state.

This feature allows the support of "fail-safe/fail-secure" operating modes.

03 – Like 01, plus: The PD is able to accept timed commands to the output. A timed command specifies the state of the output for the specified duration.

04 – Like 02 and 03 – normal/inverted drive and timed operation.

Number of: The number of outputs.

B.4 Function code 3 – Card data format

This capability indicates the form of the card data is presented to the control panel.

Compliance levels:

01 – the PD sends card data to the ACU as array of bits, not exceeding 1 024 bits.

02 – the PD sends card data to the ACU as array of BCD characters, not exceeding 256 characters.

03 – the PD can send card data to the ACU as array of bits, or as an array of BCD characters.

Number of: N/A, set to 0.

B.5 Function code 4 – Reader LED control

This capability indicates the presence of and type of LEDs.

Compliance levels:

01 – the PD support on/off control only

02 – the PD supports timed commands

03 – like 02, plus bi-color LEDs

04 – like 02, plus tri-color LEDs

Number of: The number of LEDs per reader.

B.6 Function code 5 – Reader audible output

This capability indicates the presence of and type of an audible annunciator (buzzer or similar tone generator)

Compliance levels:

01 – the PD supports on/off control only

02 – the PD supports timed commands

Number of: The number of audible annunciators per reader.

B.7 Function code 6 – Reader text output

This capability indicates that the PD supports a text display emulating character-based display terminals.

Compliance levels:

00 – The PD has no text display support

01 – The PD supports 1 row of 16 characters

02 – the PD supports 2 rows of 16 characters

03 – the PD supports 4 rows of 16 characters

04 – FF reserved for future use

80 – FF reserved for private use

Number of: Number of textual displays per reader.

B.8 Function code 7 – Time keeping

This capability indicates that the type of date and time awareness or time keeping ability of the PD.

Compliance levels:

00 – The PD does not support time/date functionality

02 – The PD is able to locally update the time and date

Number of: N/A, set to 0.

B.9 Function code 8 – Check character support

All PDs shall be able to support the checksum mode. This capability indicates if the PD is capable of supporting CRC mode.

Compliance levels:

00 – The PD does not support CRC-16, only checksum mode.

01 – The PD supports the 16-bit CRC-16 mode.

Number of: N/A, set to 0.

B.10 Function code 9 – Communication security

This capability indicates the extent to which the PD supports communication security as defined in Annex D.

Compliance levels:

This field is a bit map of the supported encryption algorithms

0x01 – (Bit-0) AES128 support

0x02 – (Bit-1) Not used

This field is encoded to represent the key exchange capabilities

0x01 – (Bit-0) default AES128 key, as defined in Annex D.

0x02 – (Bit-1) Not used

Number of: N/A, set to 0.

B.11 Function code 10 – Receive bufferSize

This capability indicates the maximum size single message the PD can receive.

Compliance levels:

This field is the LSB of the buffer size.

Number of:

This field is the MSB of the buffer size.

B.12 Function code 11 – Largest combined message size

This capability indicates the maximum size multi-part message which the PD can handle.

Compliance levels:

This field is the LSB of the combined buffer size.

Number of:

This field is the MSB of the combined buffer size.

B.13 Function code 12 – Smart card support

This capability indicates what kind of smartcard support is available for communicating directly with a smart card.

Compliance levels:

Bit 0 (mask 0x01) – PD supports transparent reader mode

Bit 1 (mask 0x02) – PD supports extended packet mode.

Either one or both modes may be supported.

B.14 Function code 13 – Readers

This capability indicates the number of credential reader devices present. Compliance levels are bit fields to be assigned as needed.

Compliance levels:

Bits 0 to 7- Reserved for future use

Number of:

Indicates the number of readers only. Compliance level is reserved for future use.

B.15 Function code 14 – Biometrics

This capability indicates the ability of the reader to handle biometric input

Compliance levels:

0 – No biometric

1 – Fingerprint, Template 1

2 – Fingerprint, Template 2

3 – Iris, Template 1

B.16 Function code 15 – Secure PIN entry support

This capability indicates if the reader is capable of supporting secure PIN entry (SPE) for smart cards. Secure PIN entry is used with ISO 7816 (Smartcards). It is assumed the osdp_KEYPAD message will be used if the keypad is to be read by the ACU.

Compliance levels:

0 = does not support SPE

1 = supports SPE

B.17 Function code 16 – OSDP version

This capability indicates the version of OSDP this PD supports.

Compliance levels:

0	= unspecified (also used for pre-IEC 60839-11-5 implementations)
1	= IEC 60893-11-5
2-0x7F	= Reserved for future use
0x80-0xFF	= reserved for private use

Annex C
(normative)

CRC definition

All devices shall be able to support the simple checksum defined earlier in this document. The preferred implementation uses the more robust error checking technique offered by a 16-bit cyclic redundancy check character.

There are several well-documented algorithms in the public domain. The implementation selected for this protocol is commonly referred to as CRC16-CCITT. It is based on the polynomial of X**16 + X**12 + X**5 + X**0, or more commonly represented as 0x1021.

A straightforward shift–and–xor algorithm for computing the CRC requires an initial value of the CRC register to be all ones. The data bytes are passed through the CRC register most significant bit first. The message is always augmented with 16 zero bits. This CRC algorithm is thoroughly addressed in the public domain.

A faster alternative to the shift-and-xor algorithm is the direct table lookup algorithm, which is illustrated in the following C code.

```
typedef unsigned int uint16;

static uint16 nCrcTblValid = 0;     // preset: CRC Table not initialized
static uint16 cCrcTable[256];                 // CRC table – working copy

// generate the table for POLY == 0x1012
static int fCrcTblInit( uint16 *pTbl )
{       int ii, jj;
        uint16 ww;

        for (ii = 0; ii < 256; ii++) {
                ww = (uint16)(ii << 8);
                for (jj = 0; jj < 8; jj++) {
                        if ( ww & 0x8000 ) {
                                ww = (ww << 1) ^ 0x1021;
                        } else {
                                ww = (ww << 1);
                        }
                }
                pTbl[ii] = ww;
        }
        return 1;
}

// table based CRC – this is the "direct table" mode -
uint16 fCrcBlk( uint08 *pData, uint16 nLength)
{       uint16 nCrc;
        int ii;

        if ( nCrcTblValid == 0 ) {
                nCrcTblValid = fCrcTblInit(&cCrcTable[0]);
        }
        for ( ii = 0, nCrc = 0x1D0F; ii < nLength; ii++ ) {
                nCrc = (nCrc<<8) ^ cCrcTable[ ((nCrc>>8) ^ pData[ii]) & 0xFF];
        }
        return nCrc;
}
```

The CRC table uses 512 bytes (256 two-byte entries). Depending on limitations on system resources, some implementations may prefer to place a pre-built table into read only memory. Use the fCrcTblInit() function to generate the 256 entries, then format the output and place into the form of an initialized array, such as:

```
const uint16 CrcTable[256] =
{
0x0000, 0x1021, 0x2042, 0x3063, 0x4084, 0x50A5, 0x60C6, 0x70E7,
0x8108, 0x9129, 0xA14A, 0xB16B, 0xC18C, 0xD1AD, 0xE1CE, 0xF1EF,
0x1231, 0x0210, 0x3273, 0x2252, 0x52B5, 0x4294, 0x72F7, 0x62D6,
0x9339, 0x8318, 0xB37B, 0xA35A, 0xD3BD, 0xC39C, 0xF3FF, 0xE3DE,
0x2462, 0x3443, 0x0420, 0x1401, 0x64E6, 0x74C7, 0x44A4, 0x5485,
0xA56A, 0xB54B, 0x8528, 0x9509, 0xE5EE, 0xF5CF, 0xC5AC, 0xD58D,
0x3653, 0x2672, 0x1611, 0x0630, 0x76D7, 0x66F6, 0x5695, 0x46B4,
0xB75B, 0xA77A, 0x9719, 0x8738, 0xF7DF, 0xE7FE, 0xD79D, 0xC7BC,
0x48C4, 0x58E5, 0x6886, 0x78A7, 0x0840, 0x1861, 0x2802, 0x3823,
0xC9CC, 0xD9ED, 0xE98E, 0xF9AF, 0x8948, 0x9969, 0xA90A, 0xB92B,
0x5AF5, 0x4AD4, 0x7AB7, 0x6A96, 0x1A71, 0x0A50, 0x3A33, 0x2A12,
0xDBFD, 0xCBDC, 0xFBBF, 0xEB9E, 0x9B79, 0x8B58, 0xBB3B, 0xAB1A,
0x6CA6, 0x7C87, 0x4CE4, 0x5CC5, 0x2C22, 0x3C03, 0x0C60, 0x1C41,
0xEDAE, 0xFD8F, 0xCDEC, 0xDDCD, 0xAD2A, 0xBD0B, 0x8D68, 0x9D49,
0x7E97, 0x6EB6, 0x5ED5, 0x4EF4, 0x3E13, 0x2E32, 0x1E51, 0x0E70,
0xFF9F, 0xEFBE, 0xDFDD, 0xCFFC, 0xBF1B, 0xAF3A, 0x9F59, 0x8F78,
0x9188, 0x81A9, 0xB1CA, 0xA1EB, 0xD10C, 0xC12D, 0xF14E, 0xE16F,
0x1080, 0x00A1, 0x30C2, 0x20E3, 0x5004, 0x4025, 0x7046, 0x6067,
0x83B9, 0x9398, 0xA3FB, 0xB3DA, 0xC33D, 0xD31C, 0xE37F, 0xF35E,
0x02B1, 0x1290, 0x22F3, 0x32D2, 0x4235, 0x5214, 0x6277, 0x7256,
0xB5EA, 0xA5CB, 0x95A8, 0x8589, 0xF56E, 0xE54F, 0xD52C, 0xC50D,
0x34E2, 0x24C3, 0x14A0, 0x0481, 0x7466, 0x6447, 0x5424, 0x4405,
0xA7DB, 0xB7FA, 0x8799, 0x97B8, 0xE75F, 0xF77E, 0xC71D, 0xD73C,
0x26D3, 0x36F2, 0x0691, 0x16B0, 0x6657, 0x7676, 0x4615, 0x5634,
0xD94C, 0xC96D, 0xF90E, 0xE92F, 0x99C8, 0x89E9, 0xB98A, 0xA9AB,
0x5844, 0x4865, 0x7806, 0x6827, 0x18C0, 0x08E1, 0x3882, 0x28A3,
0xCB7D, 0xDB5C, 0xEB3F, 0xFB1E, 0x8BF9, 0x9BD8, 0xABBB, 0xBB9A,
0x4A75, 0x5A54, 0x6A37, 0x7A16, 0x0AF1, 0x1AD0, 0x2AB3, 0x3A92,
0xFD2E, 0xED0F, 0xDD6C, 0xCD4D, 0xBDAA, 0xAD8B, 0x9DE8, 0x8DC9,
0x7C26, 0x6C07, 0x5C64, 0x4C45, 0x3CA2, 0x2C83, 0x1CE0, 0x0CC1,
0xEF1F, 0xFF3E, 0xCF5D, 0xDF7C, 0xAF9B, 0xBFBA, 0x8FD9, 0x9FF8,
0x6E17, 0x7E36, 0x4E55, 0x5E74, 0x2E93, 0x3EB2, 0x0ED1, 0x1EF0
};
```

Annex D
(normative)

Encryption

D.1 Encryption method: OSDP-SC

D.1.1 General

OSDP supports a secure channel ("SC") mechanism to protect data exchanged between the PD and the ACU. This mechanism is based on the work in GlobalPlatform Inc's secure channel protocol 03, card specification 2.2, (2009 edition) Amendment D version 1.1.

A session is initiated by using CHLNG, CCRYPT, SCRYPT, and RMAC_I.

The initiation sequence is:

1) ACU sends osdp_CHLNG with an SCS-11 header
2) PD responds with osdp_CCRYPT with an SCS-12 header
3) ACU sends osdp_SCRYPT with an SCS-13 header
4) PD responds with osdp_RMAC_I with an SCS-14 header.

After the session is initiated messages include a MAC and an SCS header and if necessary, an encrypted payload. SCS-15 or 17 for commands from the ACU and SCS-16 or 18 for responses from the PD. The MAC processing applies to SCS message types 15,16,17,18. Encryption processing applies to message types 17 and 18.

Messages following this rule set are identified by the SEC_BLK_TYPE values assigned in this subclause. See Table D.1

Table D.1 – SEC_BLK_TYPE assignment

Name	Value	Meaning	Direction
SCS_11	0x11	Begin new secure connection sequence	ACU to PD
SCS_12	0x12	Secure connection sequence step 2	PD to ACU
SCS_13	0x13	Secure connection sequence step 3	ACU to PD
SCS_14	0x14	Secure connection sequence step 4	PD to ACU
SCS_15	0x15	Secure session msg. w. MAC, authenticated only or with non-encrypted data.	ACU to PD
SCS_16	0x16	Secure session msg. w. MAC, authenticated only or with non-encrypted data.	PD to ACU
SCS_17	0x17	Secure session msg. with MAC and data encryption	ACU to PD
SCS_18	0x18	Secure session msg. with MAC and data encryption	PD to ACU

OSDP-SC based communication security is established and maintained during a communication SESSION. Built on the AES algorithm using a set of 128-bit keys, OSDP-SC provides device authentication, data content security, and message authentication during the course of a session.

D.1.2 Overview

A secure connection using OSDP-SC is referred to as a “secure session”. A secure session established by a set of initialization messages which perform mutual authentication and establish a set of keys that shall be used for the remainder of the communication. These initialization messages are based on the secure channel base key (SCBK), known to both the ACU and the PD. The SCBK is used only during session initialization.

SCBKs are required to be unique to each PD in order to be secure. The SCBK value is either set by the ACU using osdp_KEYSET, set out of band (using a config card for example) or calculated based on a shared “Master Key” (MK). The preferred mechanism is for the ACU to use its own key management mechanism to create a key and set it via osdp_KEYSET.

With the SCBK shared between the ACU and PD, a set of three separate keys can be established for communication sessions: S-ENC, S-MAC1, and S-MAC2.

Each communication packet shall contain an encrypted message block for data privacy using S-ENC and authenticated using S-MAC1 and S-MAC2 and a per-message unique IV derived from the message stream. The message stream should use unique IV’s for each message.

(osdp_BUSY is the only exception.)

D.1.3 The process

In order to establish a session using the secure channel protocol, the client and the server shall be mutually authenticated with each other and in the same process, a set of keys are established for this session. The secure channel session is terminated and the session keys are destroyed whenever an error is detected in the secure channel protocol which indicates that encryption synchronization has been lost. (This condition would be indicated by a message containing the correct CRC with an invalid message authentication code (MAC)) For example, the secure channel session can be terminated by either party by forcing a timeout, or by simply sending an invalid MAC. A session is also closed when a new OSDP-SC secure channel session connection sequence (SCS-CS) begins.

The following steps define the OSDP-SC secure channel session connection sequence (SCS-CS), and also define the SEC_BLK_TYPE values assigned to each SCS step:

D.1.4 Secure channel session connection sequence (SCS-CS)

D.1.4.1 General

The following four steps initialize a secure channel session. For these two commands and two replies SEC_BLK_DATA[0] is used to select SCBK or SCBK-D for the connection sequence. SEC_BLK_DATA[0] is set to 1 to select SCBK, and is set to 0 to select SCBK-D.

D.1.4.2 SCS_11 ACU->PD

The ACU sends SCS_11 code in SEC_BLK_TYPE to begin a new SCS-CS. The SEC_BLK_DATA[0] is used to select SCBK or SCBK-D for the connection sequence. SEC_BLK_DATA[0] is set to 1 to select SCBK, and is set to 0 to select SCBK-D.

The CMND character is osdp_CHLNG with an 8-byte random number (RND.A[8]) as the server challenge.

If the PD does not support the security block, and/or specifically SCS_11, then the PD shall return the osdp_NAK response: error_code set to 0x05.

D.1.4.3 SCS_12 PD->ACU

The PD responds with SCS_12 to acknowledge beginning a new SCS-CS. The SEC_BLK_DATA[0] is used to select SCBK or SCBK-D for the connection sequence. SEC_BLK_DATA[0] is set to 1 to select SCBK, and is set to 0 to select SCBK-D.

The PD performs the following operations:

a) generates its own 8-byte random number (RND.B[8]), and

b) generates a set of session keys: S-ENC, S-MAC1, and MAC2, using the server's random number, RND.A[8], along with SCBK (or SCBK-D) -- see "**Session Key Derivation**" paragraph below, if necessary.

c) Generate the client cryptogram – see "**Client Cryptogram**" paragraph below.

The REPLY is osdp_CCRYPT, returning the PD's ID (cUID), its random number, and the client cryptogram. If the ACU detects the PD has responded on a different SCBK than what was used in SCS_11 then it may switch keys or, it may restart the sequence at SCS_11.

D.1.4.4 SCS_13 ACU->PD

The ACU continues by sending SCS_13 code in SEC_BLK_TYPE. The SEC_BLK_DATA[0] is used to select SCBK or SCBK-D for the connection sequence. SEC_BLK_DATA[0] is set to 1 to select SCBK, and is set to 0 to select SCBK-D. SEC_BLK_LEN is a 3, indicating there is a 1 byte data block in addition to the type and length fields.

After receiving the osdp_CCRYPT in the SCS_12 reply, the ACU will

a) calculate the client cryptogram to verify the PD's cryptogram matches the one calculated.

b) compute a set of session keys: S-ENC, S-MAC1, and MAC2, using cUID, RND.A[8], RND.B[8] and SCBK

c) derive the PD's SCBK (or SCBK-D.) If necessary, using its MK and cIUD (see "**Key Diversification**" paragraph below).

d) generate the server cryptogram – see "**Server Cryptogram**" paragraph below

The ACU then formats and sends CMND osdp_SCRYPT, posting the server cryptogram.

D.1.4.5 SCS_14 PD->ACU

The PD responds with SCS_14. Sec_blk_data [0] is set to 0 or 0xff to indicate status as described below.

The PD processes the osdp_SCRYPT command and verifies the server cryptogram:

a) if the server cryptogram is ok, then generates the initial MAC reply (osdp_RMAC_I) – as defined for the osdp_RMAC_I reply.

b) else (the server cryptogram test failed), then, then sec_blk_data[0] is set to "0xFF" indicating that the server cryptogram in SCS-13 was not accepted, and the secure connection sequence cannot proceed. Note it is also valid for the PD to return a NAK with a code of 5. As the secure connection sequence has failed to complete, the ACU shall start a new sequence if it wishes to establish a secure channel.

NOTE Successful completion of the first four steps confirms that the SCBK (or SCBK-D) is valid, and that both sides have the full complement of the keys derived for this session: S-ENC, S-MAC1, and S-MAC2. Also, the R-MAC is the initial ICV value that will be rolling throughout the session.

D.1.5 Communication during a secure channel session

D.1.5.1 General

The successful completion of the synchronization sequence SCS_11 through SCS_14 confirms that the ACU and PD established a valid secure channel session. In order to maintain the SCS, the ACU shall send each message with SEC_BLK_TYPE set to SCS_15 or SCS_17, and the PD shall send each if its replies with SEC_BLK_TYPE set to SCS_16 or SCS_18. All four security block types are formatted with a message authentication code appended to the message (see D.5). SCS_17 and SCS_18 also include encrypted message DATA.

D.1.5.2 SCS_15 ACU->PD

The DATA field is sent in plain text (unencrypted).

NOTE This form provides message authentication but does not contain encrypted DATA. It is intended to be used ONLY with commands that do not include a DATA field. Development and test modes can use this form for testing while containing an unencrypted DATA field, but an implementation rejects an unencrypted payload under normal production use.

D.1.6 SCS_16PD->ACU

The data field is sent in plain text (unencrypted).

NOTE This form provides message authentication but does not contain encrypted DATA. It is intended to be used ONLY with -reply messages that do not include a DATA field. Development and test modes can use this form for testing while containing an unencrypted DATA field, but an implementation rejects an unencrypted payload under normal production use.

D.1.7 SCS_17ACU->PD

The DATA block of the command is padded and encrypted using S-ENC key.

This form shall be used with all commands that contain a DATA field.

D.1.8 SCS_18PD->ACU

Data of the reply is padded and encrypted using S-ENC key.

This form shall be used with all replies that contain a DATA field.

D.2 Commands

D.2.1 Encryption key set (osdp_KEYSET)

This command transfers an encryption key from the ACU to a PD. Refer to Table D.2.

Table D.2 – Command structure: 2-byte header followed by variable length data

Byte	Name	Meaning	Value
0	Key_Type	Encryption method to use with this key	0x01 – Secure channel base key
1	Length	Number of bytes of key data	(Key Length in bits + 7) / 8
2 – (2+Length)	Data	Key data	Any
Reply: osdp_ACK, osdp_NAK			

NOTE The following notes apply to Key_Type = 0x01:

The Length indicates the number of bytes containing key data in the array Data[]. It is computed as the integer value of the quantity of key length in bits plus 7 divided by 8. For example, the Length is 16, and the data[] array contains the 128-bit secure channel base key (SCBK). For a 256-bit key the length would be 32.

This command shall be sent by the ACU and accepted by the PD only while the connection is “secure”. The “secure” connection in this context shall mean that either:

a) the current connection is encrypted, and the session keys are based on the current SCBK (or SCBK-D), or

b) that the connection is inherently secure via physical security, such as ACU/PD are connected via simple short cable. The “inherently secure” connection shall be asserted to the ACU and to the PD by setting the devices into a special installation setup mode. The devices should exit the setup mode automatically after a successful completion of this osdp_KEYSET command.

If this command is used with the “secure channel protocol 03” encryption mode to transfer the secure channel base key (SCBK). (See global platform secure channel protocol)

D.2.2 Challenge and secure session initialization request (osdp_CHLNG)

This command is the first in the secure channel session connection sequence (SCS-CS). It delivers a random challenge to the PD and it requests the PD to initialize for the secure session. Refer to Table D.3.

Table D.3 – Command structure: 8-byte random number as the “challenge”

Byte	Name	Meaning	Value
0 – 7	Random number	Random number generated by the ACU (RND.A)	Any
Command structure: none. Reply: osdp_NAK, osdp_CCRYPT.			

D.2.3 Server's random number and server cryptogram (osdp_SCRYPT)

This command transfers a block of data used for encryption synchronization. Refer to Table D.4.

Table D.4 – Command structure: 16-byte server cryptogram

Byte	Name	Meaning	Value
0 – 15	Cryptogram	16-byte server cryptogram array	Any. Refer to the server cryptogram paragraph below.
Reply: osdp_NAK, osdp_RMAC_I			

D.3 Replies

D.3.1 Client's ID and client's random number (osdp_CCRYPT)

This reply sends a block of data used for encryption synchronization, sent in response to osdp_CHLNG command. Refer to Table D.5.

Table D.5 – Command structure: 32-byte structure

Byte	Name	Meaning	Value
0 – 7	Client ID	Client's Unique Identifier (cUID)	any
8 – 15	Random number	PD’s random number generated, (RND.B)	any
16 – 31	Cryptogram	16-byte Client Cryptogram array	any

D.3.2 Client cryptogram packet and the initial R-MAC (osdp_RMAC_I)

This command transfers a block of data used for encryption synchronization, sent in response to osdp_SCRYPT. Refer to Table D.6.

Table D.6 – Command structure: 16-byte structure

Byte	Name	Meaning	Value
0 – 15	MAC_I	16-byte MAC array – initial MAC value	any

MAC_I is the initial value for the rolling MAC that is used during the secure channel session. It is computed by encrypting the server cryptogram received in osdp_SCRYPT using S-MAC1, then encrypting the result using S-MAC2.

D.4 Algorithms and support functions

D.4.1 Session key derivation

A set of three keys are derived and used for each secure communication session. The derivation operation uses the current SCBK and encrypts a data block generated for each key. The values are derived by encrypting these data blocks using the current SCBK.

S-ENC = Encrypt the string
(0x01,0x82,RND.A[0],RND.A[1],RND.A[2],RND.A[3],RND.A[4],RND.A[5],0,0,...) with SCBK.

S-MAC1 = Encrypt the string
(0x01,0x01,RND.A[0],RND.A[1],RND.A[2],RND.A[3],RND.A[4],RND.A[5],0,0,...) with SCBK.

S-MAC2 = Encrypt the string
(0x01,0x02,RND.A[0],RND.A[1],RND.A[2],RND.A[3],RND.A[4],RND.A[5],0,0,...) with SCBK.

RND.A[8] is an 8-byte random number generated by the ACU and is transferred to the PD during the SCS_11 step.

D.4.2 Key diversification

An optional mechanism is available to support site-based key management. To support site based key management where it is not feasible to distribute the PDs’ SCBKs to the ACUs, the following algorithm allows for computation of unique SCBKs for each PD based on the PD’s cUID and a site specific master key. The cUID is concatenated with its inverse value and that result is encrypted using the MK.

SCBK = Enc(cUID || (~cUID), MK)

The above equation means that the concatenated 8-byte cUID and the one's complement inverse of the cUID are encrypted by applying the AES128 algorithm using MK as the key. The nature of the AES block transform algorithm guarantees that the resultant SCBKs are unique as long as the cUIDs are unique.

If the KEYSET command is to be used the PD does not need this calculation and the ACU can use any formula for the SCBK calculation.

D.4.3 Client cryptogram

The client cryptogram is computed by encrypting the concatenated RND.A[8] and RND.B[8] using key S-ENC. RND.A[8] is generated by the ACU (server) and RND.B[8] is generated by the PD (client).

ClientCryptogram = ENC(RND.A[8] || RND.B[8], S-ENC)

D.4.4 Server cryptogram

The server cryptogram is computed by encrypting the concatenated RND.B[8] and RND.A[8] using key S-ENC. RND.A[8] is generated by the ACU (server) and RND.B[8] is generated by the PD (client).

ServerCryptogram = ENC(RND.B[8] || RND.A[8], S-ENC)

D.4.5 Padding

Padding is required because the AES-128 algorithm only operates on 16-byte blocks.

The padding of the message for MAC generation:

MAC is applied to is the entire message, starting with SOM, the security block, and if present the DATA block. Padding is applied only if the message is not evenly divisible by the encryption block size (16.) If it is required, then append the character 0x80 to the message, then continue to append as many characters of 0x00 as are required to make the size evenly divisible by the block size of 16.

The padding of the DATA field:

Append the character 0x80 to the data block, then continue to append as many characters of 0x00 as are required to make the size of the data block to be evenly divisible by the block size of 16. Padding is required even if the length of the original data block is evenly divisible by 16.

D.5 Message authentication code (MAC) generation

D.5.1 General

General: MAC is computed for and appended only to messages whose SEC_BLK_TYPE is SCS_15, SCS_16, SCS_17, and SCS_18. The AES algorithm is applied in CBC mode using S-MAC1 as the key for all blocks, except the last one, and using S-MAC2 as the key for the last block. If the message contains only one block, then only S-MAC2 is used.

ICV values: The ICV is initialized during the secure connection sequence by the PD and is passed to the ACU during SCS_14 in reply osdp_RMAC_I.

R-MAC – the ICV value for generating the R-MAC is the previously locally generated C-MAC.