PKOC over OSDP Specification

Security Classification:	Protected
Version:	1.63
Revision:	Rev C2
Control:	Uncontrolled when printed
Date	03/22/2024

Document History

Version	Date	Author	Description
1.23	Sep 11, 2023	R. Thayer, M. Zercher, M. de Olde	*shared at GSX 2023*
1.24	Oct 6, 2023	R. Thayer	*fixed typo's in 1.23*
1.30	Oct 14, 2023	R. Thayer	*added transaction id sequence number, sorted messages, corrected "blah" typo*
1.31	Oct 14, 2023	R. Thayer	*minor formatting changes, removed multi-part headerfrom OSDP_PKOC_CARD_PRESENT response*
1.40	Nov 29, 2023	R. Thayer	*updated error TLV description and use; reused tag 0xFC for card present payload, added card present payload wrapper TLV*
1.41	Dec, 2023	R. Thayer	*correct mfg/mfgrep header to include fragment size; specify PSIA OUI add transaction id and field to auth response transaction id field in auth request usage updated correct and add tag values*
1.50	Dec, 2023	R. Thayer	*editorial changes to text; removed redundant transaction identifier tag; removed osdp_RAW message; remove PD-side transaction ID generation; added glossary; clarify reader ID TLV use; add transaction sequence to auth response*
1.60	Mar 12, 2024	R. Thayer	*fix OUI reference in the appendix and the example(s).*
1.61	Mar 13, 2024	R. Thayer	*add clarification of various use cases (ACU aware, ACU unaware, etc.) add option for null field in NEXT_TRANSACTION. added more flow diagrams pulled the multipart header options (not used here) added version tags and logic*
1.62	Mar 14, 2024	R. Thayer	*incorporate changes from 20240314 meeting*
1.63	Mar 19, 2024	R. Thayer	*put offsets in all messages (reverses offset removal in 1.62)*

Disclaimer

THIS DOCUMENT IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, OR ANY WARRANTY OTHERWISE ARISING OUT OF ANY PROPOSAL, SPECIFICATION OR SAMPLE. Without limitation, PSIA disclaims all liability, including liability for infringement of any proprietary rights, relating to use of information in this specification and to the implementation of this specification, and PSIA disclaims all liability for cost of procurement of substitute goods or services, lost profits, loss of use, loss of data or any incidental, consequential, direct, indirect, or special damages, whether under contract, tort, warranty or otherwise, arising in any way out of use or reliance upon this specification or any information herein. You are hereby granted a license to copy and distribute (but not to modify) the information set forth in this document; and to make and sell, including commercially, products using the specification. Any rights that PSIA has not expressly granted are hereby reserved. PSIA encourages you to explore membership in the organization to obtain the full set of benefits to be received from use of its specification.

Table of Contents

Introduction

This document describes alternatives to process PKOC cards for access control. It is assumed that these would be considered as an alternative to a reader that handles the complete PKOC operation and just returns a cardholder number to the ACU as an “integrated PKOC reader”. This document describes processing PKOC cards with the work on the ACU “on-loaded” (from the ACU’s point of view), not off-loaded to the PD.

These all assume the standard OSDP manufacturer specific command format. This specification further adopts the multi-part message format proposed by Integrated Engineering for PIV.

Use of a PKOC card will require multiple card operations and so the osdp_KEEPACTIVE command is recommended to ensure the reader maintains the link to the card during the entire card processing operation. Since these messages are likely larger than the minimum size OSDP message it is recommended the ACU send an osdp_ACURXSIZE command with a size of at least 1024 bytes.

PKOC credential processing is either “synchronous”, meaning the ACU generates the necessary parameters at the time the card is presented, or “pre-loaded”, meaning the ACU generates these parameters in advance thus reducing the number of message exchanges needed during card read operations.

This spec is mean to be used in conjunction with the main PKOC card spec [PKOC]. It is assumed the then-current protocol version from that document applies. For guidance on formats, credential length, version and other protocol details refer to [PKOC].

Data Format Conventions

In the following tables unless otherwise specified, when two or more TLV items are listed they are meant to be “stacked” one after the other. They are not wrapped with an outer TLV. These are meant to be in sync with the PKOC base specification’s notation.

Several new tags are introduced, see table 1. Error response codes are listed in table 2.

Additional TLV Tags

Tag	Contents
0xFA	PD supports synchronous PKOC OSDP ACU processing
0xFB	Error value
0xFC	Card Present Payload
0xFD	Transaction ID Sequence, Length 1 byte

Error Codes

Error Code	Meaning
0x00	No error
0x01	ISO 7816 status (two bytes follow, SW1/SW2)
0x02	Timeout accessing card.
0x03	Reserved for future use.
0x04	Missing TLV in data.
0x05	TLV out of bounds.
0x06	Missing data to complete request.
0x07	Invalid data.
0x08	Multipart out of sequence.
0x09	Multipart out of bounds.
0x0A-0x8F	Reserved for future use.
0x80-0xFF	Reserved for private use.

Note one code, 0x01, has two bytes of detail. Other defined error codes have no detail bytes.

PKOC Card Usage Variations

There are several possible scenarios:

1. The ACU is unaware or is configured to not directly handle PKOC credential processing. It just accepts (card lengths of 64 or greater.)
2. The ACU is configured to use PKOC OSDP ACU processing and will activate this capability. To identify this:
   - for preloading the transaction identifier, the ACU will send NEXT TRANSACTION with a transaction identifier.
   - for synchronous operation the ACU will send NEXT TRANSACTION with an empty payload.
3. The ACU is configured to use PKOC OSDP ACU processing if the PD indicates it is configured to do so. The PD in this case must send an OSDP_PKOC_TRANSACTION_REFRESH to indicate to the ACU it has this capability.
   - If the PD is capable of handling transaction identifer pre-loading it specifies a “pre-load OK” status in the TRANSACTION_REFRESH payload
   - If the PD expects synchronous operation only the TRANSACTION_REFRESH payload must be empty (or 0x00 0x00.)

Message Flow

PD with integrated PKOC support

In this case all PKOC processing happens within the PD. The ACU ***should*** send an OSDP_PKOC_NEXT_TRANSACTION command to confirm the PD is not expecting some other mode of operation. The ACU should be using osdp_ACURXSIZE and osdp_KEEPACTIVE in any case since there is expected to be smartcard bidirectional processing.

- the ACU should declares it's max receive message size using osdp_ACURXSIZE
- the ACU ***should*** use osdp_KEEPACTIVE to direct the PD to keep the 13.56 radio active during card processing.
- the ACU ***should*** send an OSDP_PKOC_NEXT_TRANSACTION command.
- the PD responds with a NAK to indicate the command cannot be processed.
- a card is presented
- the card is processed by the PD
- the PD delivers the card number to the ACU

Message Exchanges - PD with integrated PKOC

```
EAC ACU     PD    CARD
--- ---    ---    ----
 |   |      |      |
EAC initiates OSDP communications
 |   |      |      |
      ----->
      osdp_ACURXSIZE
 |   |      |      |
      ----->
      osdp_KEEPACTIVE
 |   |      |      |
      ----->
    Next Txn (any variant)
 |   |      |      |
      <-----
      osdp_NAK
      ...
      Poll/Ack Traffic
      ...
 |   |      |      |
             <-----
             card is presented
 |   |      |      |
             ----->
       Auth Request
 |   |      |      |
             <-----
             Auth Response
 |   |      |      |
      <-----
      Card data
 |   |      |      |
  <--
  Card data
 |   |      |      |
      ----->
      osdp_KEEPACTIVE
```

ACU-initiated pre-load

In this case the ACU initiate the use of PKOC OSDP ACU processing. The ACU ***must*** send an OSDP_PKOC_NEXT_TRANSACTION command to confirm the PD is not expecting some other mode of operation.

- the ACU should declares it's max receive message size using osdp_ACURXSIZE
- the ACU ***should*** use osdp_KEEPACTIVE to direct the PD to keep the 13.56 radio active during card processing.
- the ACU sends an OSDP_PKOC_NEXT_TRANSACTION command. It contains a Transaction ID to indicate pre-loaded identifiers are to be used.
- a card is presented
- an Auth Request is immediately sent to to the card. The PD does not need to wait for a transaction identifier, it was previously supplied.
- the card responds with an Auth response (this might take more than one OSDP poll cycle i.e. 200 ms.) This is processed into a cardholder number and passed to the ACU.

Message Exchanges - ACU-Initiated pre-load

```
EAC ACU     PD    CARD
--- ---    ---    ----
 |   |      |      |
EAC initiates OSDP communications
 |   |      |      |
      ----->
      osdp_ACURXSIZE
 |   |      |      |
      ----->
      osdp_KEEPACTIVE
 |   |      |      |
      ----->
    Next Txn (transaction id payload)
 |   |      |      |
      ...
      Poll/Ack Traffic
      ...
 |   |      |      |
             <-----
             card is presented
 |   |      |      |
             ----->
       Auth Request
 |   |      |      |
      ...
      Poll/Ack Traffic
      ...
 |   |      |      |
             <-----
             Auth Response
 |   |      |      |
      <-----
      Auth Response
 |   |      |      |
  <--
  Card data
 |   |      |      |
      ----->
      osdp_KEEPACTIVE
 |   |      |      |
      ----->
    Next Txn
```

ACU-initiated synchronous operation

In this case the ACU initiates the use of PKOC OSDP ACU processing.

- the ACU should declares it’s max receive message size using osdp_ACURXSIZE
- the ACU ***should*** use osdp_KEEPACTIVE to direct the PD to keep the 13.56 radio active during card processing.
- the ACU sends an OSDP_PKOC_NEXT_TRANSACTION command. this contains an empty payload to indicate synchronous processing is to be used.
- a card is presented
- a CARD PRESENT message is sent to the ACU
- the ACU sends an auth request to the PD including a transaction id
- the PD sends the auth request to the card
- some time later, the card responds with a response
- the card response is sent from the PD to the ACU
- the ACU processes the card number.

Message Exchange - ACU-Initiated Synchronous

```
EAC ACU     PD    CARD
--- ---    ---    ----
 |   |      |      |
EAC initiates OSDP communications
 |   |      |      |
      ----->
      osdp_ACURXSIZE
      ----->
      osdp_KEEPACTIVE
      ----->
    Next Txn (empty payload)
 |   |      |      |
             <-----
             card is presented
 |   |      |      |
      <-----
      Card present (as MFG Response)
 |   |      |      |
      ----->
Auth Request
 |   |      |      |
             ----->
       Auth Request
 |   |      |      |
      ...
      Poll/Ack Traffic
      ...
 |   |      |      |
             <-----
             Auth Response
 |   |      |      |
      <-----
      Auth Response
 |   |      |      |
  <--
  Card data
 |   |      |      |
      ----->
      osdp_KEEPACTIVE
```

PD-initiated pre-load operation

In this case the PD requests a transaction refresh thereby indicating to the ACU that it uses PKOC OSDP ACU processing.

- the PD sends an OSDP_PKOC_TRANSACTION_REFRESH response indicating a request for a transaction ID.
- to prepare to perform PKOC processing the ACU sends ACURXSIZE and KEEPACTIVE.
- the ACU sends an OSDP_PKOC_NEXT_TRANSACTION command with a transaction id.
- a card is presented
- an Auth Request is immediately sent to to the card. The PD does not need to wait for a transaction identifier, it was previously supplied.
- some time later, the card responds with a response
- the card response is sent from the PD to the ACU
- the ACU processes the card number.

Message Exchange - PD-initiated pre-load

```
EAC ACU     PD    CARD
--- ---    ---    ----
 |   |      |      |
EAC initiates OSDP communications
 |   |      |      |
      <-----
      Xtn Refresh
      ----->
      osdp_ACURXSIZE
      ----->
      osdp_KEEPACTIVE
      ----->
 |   |      |      |
      ----->
    Next Txn with transaction id
 |   |      |      |
      ...
      Poll/Ack Traffic
      ...
 |   |      |      |
             <-----
             card is presented
 |   |      |      |
             ----->
       Auth Request
 |   |      |      |
             <-----
             Auth Response
 |   |      |      |
      <-----
      Auth Response
 |   |      |      |
  <--
  Card data
 |   |      |      |
      ----->
      osdp_KEEPACTIVE
      ----->
    Next Txn
```

PD-initiated synchronous operation

In this case the PD requests a transaction refresh thereby indicating to the ACU that it uses PKOC OSDP ACU processing. The transaction refresh response contains an empty payload indicating synchronous operation is to be used.

- the PD sends an OSDP_PKOC_TRANSACTION_REFRESH response with an empty payload
- to prepare to perform PKOC processing the ACU sends ACURXSIZE and KEEPACTIVE.
- the ACU sends an OSDP_PKOC_NEXT_TRANSACTION command with an empty payload
- a card is presented
- a CARD PRESENT message is sent to the ACU
- the ACU sends an auth request to the PD including a transaction id
- the PD sends the auth request to the card
- some time later, the card responds with a response
- the card response is sent from the PD to the ACU
- the ACU processes the card number.

Message Exchanges - PD-initiated synchronous

```
EAC ACU     PD    CARD
--- ---    ---    ----
 |   |      |      |
EAC initiates OSDP communications
 |   |      |      |
      <-----
      Xtn Refresh
      ----->
      osdp_ACURXSIZE
      ----->
      osdp_KEEPACTIVE
      ----->
      ----->
    Next Txn with empty payload
 |   |      |      |
      Poll/Ack Traffic
      ...
             <-----
             card is presented
 |   |      |      |
      <-----
      Card present (as MFG Response)
 |   |      |      |
      ----->
Auth Request
 |   |      |      |
             ----->
       Auth Request
 |   |      |      |
             <-----
             Auth Response
 |   |      |      |
      <-----
      Auth Response
 |   |      |      |
  <--
  Card data
 |   |      |      |
      ----->
      osdp_KEEPACTIVE
      ----->
    Next Txn
```

Transaction Identifier Set-up

The PD needs the Transaction Identifier ('transaction ID') to perform the Authentication Request. This value can be provided by the ACU in response to an OSDP_PKOC_CARD_PRESENT response, or provided in advance of a card read using the OSDP_PKOC_NEXT_TRANSACTION command. The PD may request a pre-defined transaction id by using the OSDP_PKOC_TRANSACTION_REFRESH response. A sequence number may also be provided with the transaction ID. This is useful for case where the ACU is periodically sending transaction identifiers and there is a need to know which one the PD is using. It is assumed the PD uses the last transaction identifier sent. If the PD provides a transaction identifier sequence number in the OSDP_PKOC_AUTH_RESPONSE the ACU must use the corresponding transaction identifier in the validation process. If the ACU is pre-loading transaction identifiers and a card has not been processed by the PD within a suitable time interval then the ACU must send a new transaction identifier (in an OSDP_PKOC_NEXT_TRANSACTION command) so as to ensure freshness of the entropy used. Transaction identifiers are to be used for only one credential operation. Refer to [PKOC] for guidance on the transaction id lifetime. Note that unless the PD supports integrated PKOC credential processing the transaction ID is always generated by the ACU.

Reader Identifier Set-up

The reader may or may not generate the "Reader Identifier". If it does generate it, a TLV with a length of 0 shall be returned to the ACU in the OSDP_PKOC_CARD_PRESENT response. If the ACU is to generate the reader ID, it shall provide it in the OSDP_AUTH_REQUEST command, otherwise the OSDP_AUTH_REQUEST command must not include a Reader ID TLV.

Manufacturer Messages

To implement these operations OSDP's manufacturer-specific message mechanism is used. Commands and responses are defined here. These use the PSIA OUI, 1A-90-21 to uniquely identify PKOC OSDP operations. This follows the migration style of the OSDP standard in order to facilitate future migration into the OSDP mainline specification.

Request values for MFG and MFGREP

Name	Value
OSDP_PKOC_CARD_PRESENT	0xE0
OSDP_PKOC_AUTH_REQUEST	0xE1
OSDP_PKOC_AUTH_RESPONSE	0xE2
OSDP_PKOC_NEXT_TRANSACTION	0xE3
OSDP_PKOC_TRANSACTION_REFRESH	0xE4
OSDP_PKOC_READER_ERROR	0xFE

Credential Processing Considerations

The crypto operation on a PKOC card may take longer than the available time after an Authentication Request is sent. Implementations must not assume that an OSDP_PKOC_AUTH_REQUEST or other messages will elicit an immediate response. It should be expected that in general commands will be responded to with a plain acknowledgement (osdp_ACK) and one or more OSDP poll/ack cycles (200 ms max per the OSDP spec) may occur before there is a response from the card.

OSDP_PKOC_AUTH_REQUEST

This REQUEST is sent by the ACU so that the PD may issue an Authentication Request to the card. This contains the protocol version, transaction ID, and “reader” identifier. The order of these fields does not matter, the TLV tags identify them. If the transaction ID has been previously provided the “Transaction ID TLV” field must be present and use a length of 0. If the transaction id was previously allocated, it’s corresponding sequence number may also be sent.

OSDP_PKOC_AUTH_REQUEST MFG Payload

Offset	Contents
0	Manufacturer OUI (3 octets)
3	0xE1 (Mfg Request Code)
4	Total request payload size (Least Significant Octet)
5	Total request payload size (Most Significant Octet)
6	Offset in request (Least Significant Octet)
7	Offset in request (Most Significant Octet)
8	Command fragment length (Least Significant Octet)
9	Command fragment length (Most Significant Octet)
10	Auth Command Parameter 1 (“P1”) - 1 octet (only in first fragment)
11	Auth Command Parameter 2 (“P2”) - 1 octet (only in first fragment)
12-n	Protocol Version TLV Transaction ID TLV (see description for use.) Reader Identifier TLV (or indicated to be omitted) Transaction ID Sequence TLV (optional)

OSDP_PKOC_AUTH_RESPONSE

This RESPONSE consists of an osdp_MFGREP response. It is sent in response to an osdp_POLL command. This response is sent after the Authentication Response is received from the card by the reader. Note this response is definitely longer than the minimum OSDP packet size and so may be sent in fragments by the PD.

OSDP_PKOC_AUTH_RESPONSE

Offset	Contents
0	Manufacturer OUI (3 octets)
3	0xE2 (Mfg Response Code)
4	Total request payload size (Least Significant Octet)
5	Total request payload size (Most Significant Octet)
6	Offset in request (Least Significant Octet)
7	Offset in request (Most Significant Octet)
8	Command fragment length (Least Significant Octet)
9	Command fragment length (Most Significant Octet)
10-n	PKOC Authentication Response TLV (contains Public Key and Digital Signature TLV) Transaction ID TLV (optional) Transaction ID Sequence TLV (optional) Error TLV (optional, do not send if no error.)

OSDP_PKOC_CARD_PRESENT

This RESPONSE is sent by the reader to the ACU so that the ACU may specify the Authentication Request transaction ID. It returns the “supported protocol versions” TLV structure as received by the reader in the select response. It can optionally include a transaction sequence value, so that the ACU can maintain sync with respect to ACU-supplied transaction id’s.

Note is expected the OSDP_PKOC_AUTH_REQUEST command will be sent soon after the OSDP_PKOC_CARD_PRESENT response is received by the ACU, but not necessarily as the next command. In general the next command after OSDP_PKOC_CARD_PRESENt is expected to be a poll.

Note this has no multipart header as the response will never exceed the minimum OSDP packet size. In addition, it does use an outer TLV to make PD-side processing easier.

OSDP_PKOC_CARD_PRESENT payload

Offset	Contents
0	Manufacturer OUI (3 octets)
3	0xE0 (Mfg Response Code)
4	Total request payload size (Least Significant Octet)
5	Total request payload size (Most Significant Octet)
6	Offset in request (Least Significant Octet)
7	Offset in request (Most Significant Octet)
8	Command fragment length (Least Significant Octet)
9	Command fragment length (Most Significant Octet)
10-n	Card Present TLV, contains: Supported Protocol Versions TLV Transaction Sequence TLV (optional) Error TLV (optional)

Example

```
1A9021E0FC065C0201004C00
```

meaning OUI 1A9021, OSDP_PKOC_CARD_PRESENT (0xE0), payload FC with length 6, Supported Protocol 0100, Transaction sequence empty (meaning not provided by PD)

OSDP_PKOC_NEXT_TRANSACTION

This COMMAND consists of an osdp_MFG command. It is sent to provide the PD with a transaction ID to be used in the next Authentication Request. This command may be sent at any time. The payload contents is either:

- an empty payload (0x00 0x00) to indicate "synchronous" operation is to be used
- a Transaction ID TLV optionally followed by a transaction sequence number. This "pre-loads" the PD with a transaction ID for more efficient operation. It is assumed the PD will track the sequence numbers in case more than one NEXT_TRANSACTION command is received before the next card read.

Under certain conditions the PD must return an OSDP negative acknowledgement (osdp_NAK).

The PD must return a NAK when: - it does no PKOC processing - it only does synchronous operation and a transaction ID was specified. - it does not work with any of the protocol versions listed in the command.

OSDP_PKOC_NEXT_TRANSACTION Payload

Offset	Contents
0	Manufacturer OUI (3 octets)
3	0xE3 (Mfg Command Code)
4	Total request payload size (Least Significant Octet)
5	Total request payload size (Most Significant Octet)
6	Offset in request (Least Significant Octet)
7	Offset in request (Most Significant Octet)
8	Command fragment length (Least Significant Octet)
9	Command fragment length (Most Significant Octet)
10-n	Transaction ID TLV Transaction ID Sequence TLV (optional) Protocol Version TLV (optional)

OSDP_PKOC_READER_ERROR

This RESPONSE consists of an osdp_MFGREP command and associated payload. It is sent in response to a poll when there is an error reading the card. The code 0xFE was selected as the format corresponds to response 0xFE in [2].

OSDP_PKOC_READER_ERROR payload

Offset	Contents
0	Manufacturer OUI (3 octets)
3	0xFE (Mfg Response Code)
4	Total request payload size (Least Significant Octet)
5	Total request payload size (Most Significant Octet)
6	Offset in request (Least Significant Octet)
7	Offset in request (Most Significant Octet)
8	Command fragment length (Least Significant Octet)
9	Command fragment length (Most Significant Octet)
10-n	Error TLV

OSDP_PKOC_TRANSACTION_REFRESH

This RESPONSE consists of an OSDP_MFGREP response. It is sent in response to an OSDP_POLL command. This response is sent when the PD wants to pre-load a transaction id for the next card read. It is also used to indicate to the ACU that this PD is configured for OSDP ACU PKOC exchanges. It is expected this would be generated within a few poll cycles after an OSDP_PKOC_AUTH_RESPONSE.

The payload contains one or more of these values:

- PKOC OSDP ACU enabled TLV
- Protocol Version TLV (as described in the PKOC spec.)
- 0x00 0x00 indicating synchronous use

The ACU is responsible for determining if the versions supported by the PD are acceptable for use.

OSDP_PKOC_TRANSACTION_REFRESH payload

Offset	Contents
0	Manufacturer OUI (3 octets)
3	0xE4 (Mfg Response Code)
4	Total request payload size (Least Significant Octet)
5	Total request payload size (Most Significant Octet)
6	Offset in request (Least Significant Octet)
7	Offset in request (Most Significant Octet)
8	Command fragment length (Least Significant Octet)
9	Command fragment length (Most Significant Octet)
10-n	OSDP PKOC ACU capability TLV Protocol Version (TLV as described in PKOC spec) -or- an empty DER value (tag 0 length 0 i.e. 0x00 0x00)

Appendix

Colophon

This document originated by Rodney Thayer (Smithee Solutions), Mike Zercher (Secure Element Solutions), and Mark de Olde (Integrated Engineering.) Additional instigation provided by Ed Chandler (Security by Design.)

Security Considerations

It is assumed all of this message traffic happens inside a proper OSDP secure channel using a unique paired (not the default) key.

To mitigate potential man-in-the-middle attacks, allocation of the transaction id is limited to the ACU and so is different from the way an autonomous PKOC-enabled PD would behave.

Assigned Numbers

This specification assumes certain numbers will be registered.

The OUI value (3-byte) is registered with the IEE and assigned to PSIA - the value is 1A-90-21.

The tag values used here are from a list managed by PSIA.

Glossary

7816 - ISO standard for Smart Card communications.

ACU - Access Control Unit. IEC/OSDP terminology for a “panel”.

Challenge - value provided to a key-pair holder to prove possession of the private key.

Command - message from an OSDP ACU to an OSDP PD.

EC - Elliptic Curve.

NAK - Negative Acknowledgement. A response from an OSDP PD back to the ACU indicating there was an issue with the command just receive. May optionally have an explanation (byte) attached.

NFC - Near-Field Communications.

OSDP - Open Supervised Device Protocol.

osdp_ACK, osdp_ACURXSIZE, osdp_KEEPACTIVE, osdp_MFG, osdp_MFGREP, osdp_POLL, osdp_RAW - specific commands and responses from the OSDP specification (IEC 60839-11-5 / SIA OSDP 2.2.)

OUI - Organizational Unit Identifier - IEEE terminology for their vendor registry.

Panel - access control device that controls readers.

PD - Peripheral Device. IEC/OSDP terminology for a "reader" or I/O device.

PIV - Personal Identification Verification. (NIST SP 800-73-4.)

PKOC - Public Key Open Credential.

PKOC Identifier

Pre-loaded operation - use of the NEXT TRANSACTION command to pre-load a transaction identifier into the PD.

Reader - Device that reads credentials (i.e. an ISO 14443 or Bluetooth transponder.)

Reader Identifier - PKOC data value providing identification of a PD for PKOC authentication.

Response - message from an OSDP PD to an OSDP ACU.

Secure Channel - OSDP encrypted connection between an ACU and a PD.

Synchronous operation - use of the AUTH REQUEST command to send a transaction identifier from the ACU to the PD at the time the card is read.

Tag - the identifying first octet of a TLV string.

TLV - Tag,Length,Value - variable size data format.

Transaction Identifier, Transaction ID - arbitrary value provide to the credential to be used in signature validation.

References

[PKOC] PKOC NFC Card Specification, Version 1.0 Rev0, 6/13/2023. Physical Security Interoperability Alliance.

[2] Integrated Engineering OSDP extensions, document 100-01G-PS-01-INID "Vendor Specific OSDP Extensions v10c".

[3] OSDP, IEC 60839-11-5

[4] ISO 7816-4-2020

END OF DOCUMENT