AN-321

Configuring ICT Readers for OSDP Communication

Application Note

Last Published: 01-Nov-22 9:12 AM

Contents

Introduction

OSDP (Open Supervised Device Protocol) is an industry standard communications protocol, developed to improve interoperability among access control and security products. Unlike older standards such as Wiegand, OSDP utilizes a two-way channel and encrypted communications between the reader and the expander module, known as secure channel communication.

ICT card readers support communication using OSDP, implementing OSDP standard 2.2. Each card reader operates as an OSDP client when connected to an OSDP server.

This document outlines the configuration and programming requirements to enable OSDP communication, and specifies the communication packets supported by the ICT card reader.

Protege GX and Protege WX systems can be programmed for OSDP communication with ICT card readers and compatible third-party readers. For programming information and requirements, see Application Note 254: Configuring OSDP Readers in Protege.

Prerequisites

The following prerequisites are required to configure and communicate with ICT readers using OSDP.

- ICT card readers require firmware version 1.04.277 or higher.
- Only ICT card readers which support **Bluetooth**® Wireless Technology or 13.56MHz **NFC** communication are capable of being programmed for OSDP communication.
- A mobile device running the **Protege Config App** is required to configure readers via Bluetooth®.
- A correctly encoded MIFARE **config card** is required to configure readers via 13.56MHz NFC.

Note that it is **not** possible to configure readers for OSDP communication using a 125kHz programming card.

To enable OSDP communication, readers will need to be programmed for OSDP Output Mode (see page 7).

Supported Hardware

Only ICT card readers that support Bluetooth® or 13.56MHz communication are capable of OSDP communication.

Readers which support only 125kHz (or 125kHz and keypad PIN entry) **cannot** be configured to use OSDP.

OSDP **cannot** be used on card readerss with PSK hardware. This includes:

- PRX-TSEC-STD-B-PSK
- PRX-TSEC-STD-KP-B-PSK

The maximum version of reader firmware supported by readers with PSK hardware is 1.04 260.

Supported Card Types with OSDP

The OSDP protocol is used by the wired serial communication interface of the card reader, and does not affect the ability of the reader to read cards. The reader is capable of processing up to 13 bytes (104 bits) of data from a single card, regardless of the protocol used on its wired communication interface.

Reader Connection

When using OSDP mode, the ICT reader should be connected to the OSDP server system using an RS-485 wiring configuration. The example diagram below shows a reader correctly connected to a Protege reader expander.
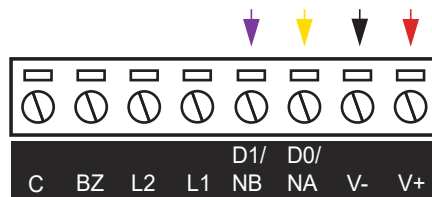
Wiring Connections

The wires of the ICT reader should be connected to the OSDP server system using the RS-485 configuration outlined in the table below.

Color	Reader Wire	Description	OSDP Server System Connection
🔴	Red	**12VDC+** positive	**V+** 12VDC positive
⚫	Black	**12VDC-** negative	**V-** 12VDC negative
🟡	Yellow	RS-485 **A**	RS-485 **A**
🟣	Violet	RS-485 **B**	RS-485 **B**
🟣	Shield	Shield (drain)	Frame grounded at one point only

Connecting OSDP readers to a Protege system requires additional hardware configuration and system programming. For more information, see Application Note 254: Configuring OSDP Readers in Protege.

Enabling Readers for OSDP Operation

For ICT card readers to use the OSDP communication protocol, OSDP needs to be enabled on each reader by programming the OSDP **Output Mode** TLV.

ICT card readers can be programmed using:

- A mobile device running the Protege Config App
- A correctly encoded MIFARE config card

For information on programming ICT card readers, including using the Protege Config App, see the ICT Card Reader Configuration Guide, available from the ICT website.

Config App

To enable OSDP using the Config App, you need to enable OSDP Output Mode.

1. Log in to the Protege Config App, using your app account.
2. Select your **Credential Profile**.
3. **Add** a new **Reader Configuration** called Enable OSDP Output Mode.
4. Tap the **Add TLV** dropdown and select the **Output Mode** option.
5. Tap the dropdown and select **OSDP**.
6. Tap **Save**.

You can now apply the configuration to the required reader(s). Power cycle the reader and select and apply your new Enable OSDP Output Mode config within two minutes of startup.

Config Card

MIFARE config cards can be ordered from ICT (Ordering code: PRX-ISO-CONFIG), or programmed using the ICT Encoder Client. For Encoder Client card programming instructions, see the ICT Encoder Client User Guide.

To program a config card to enable OSDP, you need to create a reader configuration and click the **Import** button to enter a **Custom Format** with the OSDP Output Mode Hex code `0B0104`.

OSDP Baud Rate Requirement

For a card reader operating in OSDP mode to communicate with an OSDP server, the reader must have the same baud rate setting as the reader port it is connected to. The default reader baud rate is 38400.

ICT card readers support the following baud rates:

Supported Baud Rates
4800 baud
9600 baud
19200 baud
38400 baud (default)
57600 baud
115200 baud

The card reader baud rate can be programmed using:

- A mobile device running the Protege Config App.

  The Config App **Reader Configuration** will need a config with the **Uart Configuration** TLV selected, with the **Baud** set to match the connected reader port.

- A correctly encoded MIFARE config card programmed to configure the reader baud rate to the same setting as the connected reader port.

  A suitably configured MIFARE config card can be ordered from the ICT customer services team, or programmed using the ICT Encoder Client.

Reader Addressing

For a card reader operating in OSDP mode to be recognized on a third-party system, the reader address may need to be configured to meet the third-party system's addressing requirements.

For the tSec range of card readers the address and addressing options are determined by the reader's wiring configuration. When the reader is powered up it checks the configuration to determine its address.

1. If the reader's green and orange wires are **not** connected together it uses address 0 as its default address, unless it has been programmed with a specific address.

   The reader's address can be programmed using:

   - A mobile device running the Protege Config App.

     The Config App **Reader Configuration** will need a config with the **Reader Address** TLV selected, with the address set as required for the third-party system.

   - A correctly encoded MIFARE config card programmed to configure the necessary reader address.

     A suitably configured MIFARE config card can be ordered from the ICT customer services team, or programmed using the ICT Encoder Client.

2. If the reader's green and orange wires are connected together it is hardwired to **always** use 1 as its address. The address is not programmable.

Secure Channel Communication

Secure channel is the two-way encryption and authentication scheme used by OSDP devices to protect communication between controllers and readers, by requiring them to establish a secure session.

A secure channel session is initiated with a handshake that involves two command-reply transactions between the controller and reader, which perform mutual authentication and establish an encrypted session using a shared AES-128 key to secure the communication between the two devices.

Once the communication session between the two devices is secured the reader will not accept communication from another device without a new secure session being established.

Unencrypted Communication

While it is not recommended for live operating environments, ICT readers will accept unencrypted connections by default and can be connected to third-party OSDP systems without configuring secure channel communication.

This is compliant with the OSDP 2.2 'basic' profile, but not with the 'secure' profile.

Configuring Secure Channel Communication

There are two methods for establishing a secure channel communication session between an OSDP server and ICT reader. The session key may be preconfigured, or randomly generated using OSDP installation mode.

It is recommended that you validate the readers are working with unencrypted communications before configuring secure channel.

Installation Mode

OSDP installation mode allows you to establish a secure session with a default key, then negotiate a shared key during the secure session. ICT readers are in installation mode by default, and will allow a secure channel session to be established using the default key, until they have been paired. Once paired, the reader will automatically disable installation mode and will only accept secure communications with the correct encryption key.

The process of pairing the ICT reader with the OSDP server is initiated from the OSDP server using the Default Secure Channel Base Key SCBK-D. For more information see the Secure Channel Protocol section (see page 21).

Once a secure session is established the OSDP server can initiate negotiation of a new key within the secure session at any time. The reader does not need to be placed in installation mode again.

To connect the ICT reader to a new device once it has been paired, installation mode will need to be enabled.

ICT readers can be placed into installation mode by applying a **Hex** TLV with the Hex code **080103**, or with the Protege Config App **Device Mode** TLV set to **OSDP Install Mode**.

Session Key Programming

The reader can be preconfigured with an encryption key which matches the key assigned in the OSDP server system programming. The OSDP server can then establish a secure channel session using the predefined key.

ICT readers can be configured by applying a **Hex** TLV with the Hex code **0311<SessionKey>FF**. For example, for key FC9905847CC465FD827530AD3B194213 apply TLV **0311**FC9905847CC465FD827530AD3B194213**FF**.

Once a secure session is established, a new key can be programmed in the third-party OSDP system at any time and updated to the reader within the existing secure session. A new secure session is then established using the new key. The reader does not need to be manually configured with the new key.

OSDP Communication

The following communication packets are supported by the ICT card reader as an OSDP client when connected to an OSDP server.

OSDP Packet Format

Packets created according to the OSDP 2.2 standard use the following format:

Byte	Name	Description	Value
0	SOM	Start of message	0x53
1	ADDR	Physical address of the device	0x00-0x7E
2	LEN_LSB	Packet length least significant byte	0x00-0xFF
3	LEN_MSB	Packet length most significant byte	0x00-0xFF
4	CTRL	Message control information	See Message Control Format table below
	SEC_BLK_LEN	Length of security control block	0x00-0xFF
	SEC_BLK_TYPE	Security block type	See Security Block (see page 22)
	SEC_BLK_DATA	Security block data	See Security Block (see page 22)
	CMND/REPLY	Command or reply code	
	DATA	Data block (optional)	
	MAC [0]	MAC. Present if SCB bit set in CTRL	See MAC Generation (see page 26)
	MAC [1]		
	MAC [2]		
	MAC [3]		
	CKSUM/CRC_LSB	Checksum/CRC-16 least significant byte	
	CRC_MSB	CRC-16 most significant byte (optional)	

Message Control (CTRL) Format

Bit	Mask	Name	Description
0-1	0x03	SQN	Message sequence number. Used for delivery confirmation and error recovery
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
3	0x08	SCB	Set - Security control block is present in the message
			Clear - No security control block in the message
4-6	0x70		Not used

Supported OSDP Packet Types

As an OSDP client, the card reader will receive a command, then send a reply. The following commands types are supported.

Commands Received by the Reader

Name	Value	Description	Data
osdp_POLL	0x60	Poll	None
osdp_ID	0x61	ID report request	Reply type
osdp_CAP	0x62	Device capabilities request	Reply type
osdp_LSTAT	0x64	Local status report request	None
osdp_LED	0x69	Reader LED control command	LED settings
osdp_BUZ	0x6A	Reader buzzer control command	Buzzer settings
osdp_COMSET	0x6E	Attempt to change address or baud rate	Communication settings
osdp_SCRYPT	0x77	Server cryptogram	Encryption data
osdp_KEYSET	0x75	Encryption key set command	Encryption key
osdp_CHLNG	0x76	Challenge and secure session initialization request	Challenge data

Replies Sent by the Reader

Name	Value	Description	Data
osdp_ACK	0x40	Command accepted. Nothing else to report	None
osdp_NAK	0x41	Command not processed	Reason for rejecting command
osdp_PDID	0x45	Device ID report	Report data
osdp_PDCAP	0x46	Device capabilities report	Report data
osdp_LSTATR	0x48	Local status report	Report data
osdp_RAW	0x50	Reader data. Raw bit image of card data	Card data
osdp_KPD	0x53	Keypad data	Keypad data
osdp_COM	0x54	Address and baud rate used by reader	Communication settings
osdp_CCRYPT	0x76	Client's ID, random number and cryptogram	Encryption data
osdp_RMAC_I	0x78	Initial R-MAC	Encryption data

Command Packets Explained

osdp_POLL

The **osdp_POLL** command serves as a general enquiry.

- The reader may reply with any of the following packet types:
  - **osdp_ACK**
  - **osdp_RAW**
  - **osdp_KPD**

osdp_ID

The **osdp_ID** command requests an ID report from the reader, containing manufacturer and version information.

- The reader will reply with the packet type **osdp_PDID**
- Command data structure: 1 byte
- Command data:

Request Code	Description
0x00	Send standard reply

osdp_CAP

The **osdp_CAP** command requests the reader to return a list of its functional capabilities.

- The reader will reply with the packet type **osdp_PDCAP**
- Command data structure: 1 byte
- Command data:

Request Code	Description
0x00	Send standard reply

osdp_LSTAT

The **osdp_LSTAT** command requests a local status report from the reader, containing power and tamper status information.

- The reader will reply with the packet type **osdp_LSTATR**

osdp_LED

The **osdp_LED** command is the LED control command, which controls the operation of the reader's LED.

- The reader will reply with the packet type **osdp_ACK**
- Command data structure: 14 byte element, repeated 1 or more times

- Command data:

Byte	Name	Description	Value
0	Reader Number	Not used	0x00-0xFF
1	LED Number	Always 0 for ICT card readers	0x00
		Temporary Settings	
2	Control Code	The mode to enter temporarily	See table below
3	ON Time	The ON duration of the flash, in units of 100ms	0x00-0xFF
4	OFF Time	The OFF duration of the flash, in units of 100ms	0x00-0xFF
5	ON Color	The color to set during the ON time	See table below
6	OFF Color	The color to set during the OFF time	See table below
7	Timer LSB	Least significant byte, in units of 100ms	0x00-0xFF
8	Timer MSB	Most significant byte, in units of 100ms	0x00-0xFF
		Permanent Settings	
9	Control Code	The mode to return to after the timer expires	See table below
10	ON Time	The ON duration of the flash, in units of 100ms	0x00-0xFF
11	OFF Time	The OFF duration of the flash, in units of 100ms	0x00-0xFF
12	ON Color	The color to set during the ON time	See table below
13	OFF Color	The color to set during the OFF time	See table below

For commands that control temporary settings, once the temporary command's timer expires, the LED will revert to the last permanent state set. A timer value of zero specifies zero duration.

Behavior of the keypad backlight cannot be controlled through OSDP.

Temporary LED Control Codes

Control Code	Description
0x00	Do not alter the temporary settings of the LED
0x01	Cancel any temporary operation and display this LED's permanent state
0x02	Set the temporary state given in the packet and start the timer immediately

Permanent LED Control Codes

Control Code	Description
0x00	Do not alter the permanent settings of the LED
0x01	Set the permanent state given in the packet

LED Color Codes

Color Code	Description
0x00	Turn LED off
0x01	Red
0x02	Green
0x03	Amber
0x04	Blue
0x05	Magenta
0x06	Cyan
0x07	White *

* White is not a supported color. The reader will respond with **osdp_NAK**, error code 0x09.

The LED will flash, alternating between the color specified for ON and the color specified for OFF, at a rate specified by the corresponding ON and OFF times in the packet.

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.

Example

To cause the LED to flash red and green for 3 seconds, then resume its permanent display mode:

- **Reader Number**: 0x00
- **LED Number**: 0x00
- **Temporary Control Code**: 0x02
- **Temporary ON Time**: 0x01
- **Temporary OFF Time**: 0x02
- **Temporary ON Color**: 0x01
- **Temporary OFF Color**: 0x02
- **Timer LSB**: 0x1E
- **Timer MSB**: 0x00
- **Permanent Control Code**: 0x00
- **Permanent ON Time**: 0x00
- **Permanent OFF Time**: 0x00
- **Permanent ON Color**:0x00
- **Permanent OFF Color**: 0x00

This packet does not modify the permanent LED state.

osdp_BUZ

The **osdp_BUZ** command controls the reader buzzer.

- The reader will reply with the packet type **osdp_ACK**
- Command data structure: 5 byte element

- Command data:

Byte	Name	Description	Value
0	Reader Number	Not used	0x00-0xFF
1	Tone Code	Not used	0x00-0xFF
2	ON Time	The ON duration of the beep, in units of 100ms	0x00-0xFF
3	OFF Time	The OFF duration of the beep, in units of 100ms	0x00-0xFF
4	Count	The number of times to repeat the ON/OFF cycle. A value of 0x00 means the beep will continue until another osdp_BUZ packet is received.	0x00-0xFF

The buzzer frequency is **not** configurable through OSDP. Buzzer tones will sound at the default frequency of 3378Hz.

osdp_COMSET

The **osdp_COMSET** command attempts to change the reader's address and baud rate. The reader will reply with the address and baud rate that it will use.

The reader currently **does not support** changing the address and baud rate using the **osdp_COMSET** command. If an **osdp_COMSET** command is sent the reader will reply with an **osdp_COM** command containing the address and baud rate it is currently using (and will continue to use). For instructions on changing reader address and baud rate, see the OSDP Baud Rate Requirement (see page 8) and Reader Addressing (see page 8) sections.

- The reader will reply with the packet type **osdp_COM**
- Command data structure: 1 byte address, 4 bytes baud rate
- Command data:

Byte	Name	Description	Value
0	Address	The address to attempt to set the reader to	0x00-0x7E
1	Baud Rate LSB	The baud rate to attempt to set the reader to (low byte)	0x00-0xFF
2	Baud Rate	The baud rate to attempt to set the reader to	0x00-0xFF
3	Baud Rate	The baud rate to attempt to set the reader to	0x00-0xFF
4	Baud Rate MSB	The baud rate to attempt to set the reader to (high byte)	0x00-0xFF

osdp_SCRYPT

The **osdp_SCRYPT** command transfers a block of data used for encryption synchronization.

For more information, see Server Cryptogram (page 25).

- The reader will reply with one of the following packet types:
  - **osdp_RMAC_I**
  - **osdp_NAK**
- Command data structure: 16 byte cryptogram array

osdp_KEYSET

The **osdp_KEYSET** command transfers an encryption key from the OSDP server to the reader.

- The reader will reply with one of the following packet types:
  - **osdp_ACK**
  - **osdp_NAK**
- Command data structure: 2 byte header followed by key

  The key should be AES128 (16 bytes in length).

- Command data:

Byte	Name	Description	Value
0	Key_Type	See Secure Channel Session Connection Sequence (see page 23)	0x00 – Default secure channel base key
			0x01 – Secure channel base key
1	Length	Length of the Key	0x10 (Key should be AES128)
2-17	Data	Key	0x00-0xFF

The **osdp_KEYSET** command will only be accepted by the reader during a secure channel session, encrypted with either **SCBK** or **SCBK-D**. For more information, see Secure Channel Protocol (page 21).

osdp_CHLNG

The **osdp_CHLNG** command is the first in the Secure Channel Session Connection Sequence (see page 23).

It delivers a random challenge to the reader and requests the reader to initialize a secure session.

- The reader will reply with one of the following packet types:
  - **osdp_ACK**
  - **osdp_NAK**
  - **osdp_CCRYPT**
- Command data structure: 8 byte random number (the "**challenge**")
- Command data:

Byte	Name	Description	Value
0-7	Random Number	Random number generated by the OSDP server (RND.A)	0x00-0xFF

Reply Packets Explained

osdp_ACK

The **osdp_ACK** reply is a general acknowledgement, sent in response to all valid commands that do not require a specific response. There is no reply data associated with this reply.

osdp_NAK

The **osdp_NAK** reply is a negative acknowledgement.

- Reply data structure: 1 byte
- Reply data:

Error Code	Description
0x01	Message integrity check failure (e.g. bad checksum)
0x02	Packet length error
0x03	Command not supported by the reader
0x04	Unexpected sequence number in command packet header
0x05	Security block not supported by the reader
0x06	Encrypted communication is required to process this command
0x09	Command parameter values not supported by the reader

osdp_PDID

The **osdp_PDID** reply is sent in response to an **osdp_ID** command.

- Reply data structure: 12 bytes
- Reply data:

Byte	Name	Description	Value
0-2	Vendor Code	Organizationally Unique Identifier (OUI) assigned by the IEEE	0x001BC2
3	Model Number	Product model identifier	0x00-0xFF
4	Version Number	Product version identifier	0x00-0xFF
5-8	Serial Number	Serial number unique to each individual product unit	0x00000000-0xFFFFFFFF
9	Firmware Version	Decimal representation of the major/minor firmware version (e.g. 0x68 represents version 1.04)	0x64-0xFF
10	Firmware Build MSB	Build number, most significant byte	0x00-0xFF
11	Firmware Build LSB	Build number, least significant byte	0x00-0xFF

osdp_PDCAP

The **osdp_PDCAP** reply is sent in response to an **osdp_CAP** command.

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

Byte	Description	Value
0	Function Code	See table below
1	Level of compliance with the above function	
2	Number of objects of this type	

Function Codes

Code	Compliance Level Supported by the Reader	Number of Objects Supported by the Reader
0x03 Card Data Format	0x01 Reader sends card data to the OSDP server as an array of bits, not exceeding 1024 bits *	0x01 Reader is a single card reader
0x04 LED control	0x04 Reader supports timed LED commands with a tri-color LED	0x01 Reader has one LED controllable through OSDP
0x05 Audible Output	0x02 Reader supports timed buzzer commands	0x01 Reader has one buzzer controllable through OSDP
0x08 Check Character Support	0x01 Reader supports a CRC-16 check character	0x00 Not applicable. The reader will return 0
0x09 Communication Security	0x01 Reader supports AES128 encryption	0x00 Reader supports encrypted communications with a 16 bit CRC
0x0A Receive Buffer Size	0x80 Reader's receive buffer size is 128 bytes (low byte)	0x00 Reader's receive buffer size is 128 bytes (high byte)
0x10 OSDP Version	0x02 Reader complies with SIA OSDP 2.2	0x00 Not applicable. The reader will return 0

* The reader is internally limited to processing 104 bytes of card data, as specified in Supported Card Types with OSDP (see page 5).

osdp_LSTATR

The **osdp_LSTATR** reply is sent in response to an **osdp_LSTAT** command.

- Reply data structure: 2 bytes
- Reply data:

Byte	Name	Description	Value
0	Tamper Status	0x00 if normal, 0x01 if tamper	0x00-0x01
1	Power Status	0x00 if normal, 0x01 if power failure	0x00-0x01

osdp_RAW

The **osdp_RAW** reply is sent in response to an **osdp_POLL** command.

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

Byte	Name	Description	Value
0	Reader Number	Always 0x00 in the case of the readers	0x00
1	Format Code	Always 0x01 in the case of the readers	0x01
2	Bit Count LSB	Card data in bit length (least significant byte)	0x00-0xFF
3	Bit Count MSB	Card data in bit length (least significant byte)	0x00
4-n	Card	Card data (big endian)	0x00-0xFF

osdp_KPD

The **osdp_KPD** reply is sent in response to an **osdp_POLL** command.

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

Byte	Name	Description	Value
0	Reader Number	Always 0x00 in the case of the readers	0x00
1	Digit Count	The number of keypad digits to follow	0x00-0xFF
2-n	Keypad Data	Digits from the keypad buffer, in the order they were entered	See below

- Digits **0 to 9** are reported as ASCII characters 0x30 to 0x39
- The **Enter** key is reported as ASCII return, 0x0D.

If a user enters a **PIN**, the reader will buffer the key codes (including 0x0D for the enter key), and send them immediately after the user presses **Enter**.

The reader will not send a code for the **Clear** key. When a user presses the clear key, the reader will simply clear its internal buffer.

osdp_COM

The **osdp_COM** reply is sent in response to an **osdp_COMSET** command. The reply data contains the address and baud rate that the reader will use.

> The reader currently **does not support** changing the address and baud rate using the **osdp_COMSET** command. If the reader receives an **osdp_COMSET** command it will reply with an **osdp_COM** command containing the address and baud rate it is currently using (and will continue to use). For instructions on changing reader address and baud rate, see the OSDP Baud Rate Requirement (see page 8) and Reader Addressing (see page 8) sections.

- Reply data structure: 1 byte address, 4 bytes baud rate
- Reply data:

Byte	Name	Description	Value
0	Address	The address the reader will use	0x00-0x7E
1	Baud Rate LSB	The baud rate the reader will use (low byte)	0x00-0xFF
2	Baud Rate	The baud rate the reader will use	0x00-0xFF
3	Baud Rate	The baud rate the reader will use	0x00-0xFF
4	Baud Rate MSB	The baud rate the reader will use (high byte)	0x00-0xFF

osdp_CCRYPT

The **osdp_CCRYPT** reply is a block of data used for encryption synchronization. This is sent in response to an **osdp_CHLNG** command.

- Reply data structure: 8 byte ID, 8 byte random number, 16 byte cryptogram array byte structure
- Reply data:

Byte	Name	Description	Value
0-7	cUID	Unique identifier of the reader	0x00-0xFF
8-15	RND.B	Random number generated by the reader	0x00-0xFF
16-31	Cryptogram	Cryptogram array generated by the reader	0x00-0xFF

osdp_RMAC_I

The **osdp_RMAC_I** reply is a block of data used for encryption synchronization. This is sent in response to an **osdp_SCRYPT** command.

- Reply data structure: 16 byte MAC array
- Reply data:

Byte	Name	Description	Value
0-15	MAC_I	Initial MAC value generated by the reader	0x00-0xFF

Secure Channel Protocol

The card reader can optionally implement the Secure Channel Protocol specified in the OSDP standard.

The reader will operate with secure channel mode **disabled** until the secure channel is initialized.

To initialize secure channel mode on the reader it must be programmed with the Secure Channel Base Key (**SCBK**), a secure key shared between the OSDP server and the reader to establish encrypted communication sessions.

There are two methods to program the reader with the SCBK and enable the secure channel protocol:

1. Configure the reader programming with the TLV: `0311xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxFF`

   Where xx is the 16-byte encryption key

2. Establish a secure session using the Default Secure Channel Base Key **SCBK-D**, and send the `osdp_KEYSET` command to set the SCBK during the session (see page 16).

The **SCBK-D** is a default key which can be used to establish a secure session to allow the reader to be programmed with the SCBK. The SCBK-D is published in the OSDP 2.2 specification as:

- {0x30, 0x31, 0x32, 0x33, 0x34, 0x35, 0x36, 0x37, 0x38, 0x39, 0x3A, 0x3B, 0x3C, 0x3D, 0x3E, 0x3F}

As the SCBK-D is publicly available, this encryption key should not be used for live site operations.

Summary

- By default, the reader will accept unencrypted connections or allow a secure channel to be established using SCBK-D.

  This behavior is defined as **Installation Mode** in the OSDP 2.2 specification.

- To enable secure channel protocol an SCBK must be programmed on the reader, using either the TLV configuration or sending the `osdp_KEYSET` command during an **SCBK-D** session.

- Once an SCBK key has been set and secure channel mode has been initialized the reader will automatically disable installation mode and will only accept secure communications with the correct encryption key.

- After an SCBK has been set, it is possible to put the reader back into installation mode by programming the TLV: `080103`, or with the Protege Config App **Device Mode** TLV set to **OSDP Install Mode**.

For information on programming card readers, including using the Protege Config App, see the ICT Card Reader Configuration Guide, available from the ICT website.

MIFARE config cards can be ordered from ICT (Ordering code: PRX-ISO-CONFIG), or programmed using the ICT Encoder Client. For Encoder Client card programming instructions, see the ICT Encoder Client User Guide.

Terminology

The following key terms will be used in explaining the secure channel communication process.

- **AES**: The Advanced Encryption Standard algorithm used for the secure channel.
- **CBC**: The Cipher Block Chaining mode of operation.
- **ICV**: Initial Chaining Vector, utilized by CBC.
- **SCS-SC**: Secure Channel Session Connection Sequence.
- **SCBK**: Secure Channel Base Key, used during session initialization.
- **SCBK-D**: Default Secure Channel Base Key, used during session initialization in installation mode.
- **MAC**: Message Authentication Code used during the secure channel session.
- **S-ENC**: Data Confidentiality Session Key, for ensuring data confidentiality (message encryption).
- **S-MAC1**: Secure Message Authentication Key 1, for message authentication.
- **S-MAC2**: Secure Message Authentication Key 2, for message authentication.
- **C-MAC**: Command MAC, sent from the OSDP server to the reader.
- **R-MAC**: Reply MAC, sent from the reader to the OSDP server.

Security Block

The Security Block (SB) is required when communicating through Secure Channel Protocol.

Its presence is indicated by setting the SCB flag of the CTRL byte in an OSDP packet. 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 security requirements change.

Security Block Structure

Byte	Name	Description	Value
0	SEC_BLK_LEN	Length of security block	0x00-0xFF
1	SEC_BLK_TYPE	Security block type	0x11-0x18
2-n	SEC_BLK_DATA	Variable length data (optional)	0x00-0xFF

Security Block Types

Name	Value	Description	Direction
SCS_11	0x11	Begin new secure connection sequence	OSDP server to reader
SCS_12	0x12	Secure connection sequence step 2	Reader to OSDP server
SCS_13	0x13	Secure connection sequence step 3	OSDP server to reader
SCS_14	0x14	Secure connection sequence step 4	Reader to OSDP server
SCS_15	0x15	Secure session message with MAC, no data security	OSDP server to reader
SCS_16	0x16	Secure session message with MAC, no data security	Reader to OSDP server
SCS_17	0x17	Secure session message with MAC and data security	OSDP server to reader
SCS_18	0x18	Secure session message with MAC and data security	Reader to OSDP server

Secure Channel Session Connection Sequence

Secure channel mode can be initialized through the Secure Channel Session Connection Sequence (SCS-CS) specified by the OSDP standard. The standard defines two keys for establishing a secure channel:

- **SCBK** (Secure Channel Base Key)
- **SCBK-D** (Default Secure Channel Base Key)

When initializing a secure channel session:

- SEC_BLK_DATA[0] is set to **1** to select **SCBK**.
- SEC_BLK_DATA[0] is set to **0** to select **SCBK-D**.
- SCBK-D can only be selected if the reader is in installation mode.
- Otherwise, if the OSDP server tries to select SCBK-D the reader will respond with **osdp_NAK** with error code **0x06**.

The message check method is 16-bit CRC (Cyclic Redundancy Check) during this sequence.

Initialize Secure Channel Session

To initialize a secure channel session, perform the below four steps in the following order:

- **SCS_11**: OSDP server to reader: command 0x76 (**osdp_CHLNG**)

  The OSDP server sends SCS_11 code in SEC_BLK_TYPE to begin a new SCS-CS.

  The command is **osdp_CHLNG** with an 8 byte random number as the server challenge.

- **SCS_12**: Reader to OSDP server: reply 0x76 (**osdp_CCRYPT**)

  The reader responds with SCS_12 to acknowledge that a new SCS-CS has begun.

  The reader performs the following operations:

  1. Generates its own 8 byte random number.
  2. Generates a set of session keys: S-ENC, S-MAC1, and S-MAC2, using the server's random number along with SCBK.

     For more information, see Session Key Derivation (page 25).

  3. Generates the client cryptogram.

     For more information, see Client Cryptogram (page 26).

  The REPLY is **osdp_CCRYPT**, returning the reader's ID (cUID), its random number, and the client cryptogram.

- **SCS_13**: OSDP server to reader: command 0x77 (**osdp_SCRYPT**)

  The OSDP server continues by sending the SCS_13 code in SEC_BLK_TYPE.

  After receiving the **osdp_CCRYPT** in the SCS_12 reply, the OSDP server will generate:

  1. The reader's SCBK using a site-specific key.
  2. A set of session keys: S-ENC, S-MAC1, and S-MAC2, using the server's random number, RND.A[8], along with the SCBK number.
  3. The server cryptogram.

     For more information, see Server Cryptogram (page 25).

  The OSDP server then formats and sends command **osdp_SCRYPT**, posting the Server Cryptogram.

SCS_14: Reader to OSDP server

The reader responds with SCS_14.

The reader processes the **osdp_SCRYPT** command and verifies the server cryptogram:

a. If the server cryptogram is verified:

    1. SEC_BLK_DATA [0] is set to **0x01** indicating that the server cryptogram in SCS_Cryptogram in SCS_13 was accepted.

    2. Generates the initial MAC reply (**osdp_RMAC_I**), as defined for the osdp_RMAC_I reply.

b. If the server cryptogram test fails:

    1. 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.

        Both the OSDP server and the reader must begin a new secure connection sequence with SCS_11, possibly using SCBK-D.

    2. The REPLY code is set to the **osdp_NAK** response, with the error_code set to **0x05**.

Successful completion of the initialization steps confirms that the SCBK is valid, and that both sides have the full complement of the keys derived for this session: S-ENC, S-MAC1, and S-MAC2.

Secure Channel Session Communication

The successful completion of the synchronization sequence SCS_11 through SCS_14 is followed by continuing to exchange the following OSDP_SC packet types.

The message check method applied to all packets with SEC_BLK_TYPE set to SCS_ 15, 16, 17, and 18 is the first four bytes of the 16 byte MAC computed for the message, as defined in the Message Authentication Code Generation section (see next page).

Perform the below four steps in the following order:

- **SCS_15**: OSDP server to reader

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

  Note: This form provides message authentication, but no data security. Therefore, it should be used **ONLY** with the `osdp_POLL` command.

- **SCS_16**: Reader to OSDP server

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

  Note: This form provides message authentication, but no data security. Therefore, it should be used **ONLY** with the `osdp_ACK` reply.

- **SCS_17**: OSDP server to reader

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

  This form should be used with all non-poll commands.

- **SCS_18**: Reader to OSDP server

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

  This form should be used with all non-ACK replies.

Session Key Derivation

The SCBK will persist even if an individual secure communication session has ended.

For each session, a set of three keys are derived from the SCBK. Both the reader and the OSDP server should derive these three keys independently.

The derivation operation uses the SCBK and encrypts a data block generated for each key. The data block for each key is as follows:

- **S-ENC**: 0x01, 0x82, rnd[0], rnd[1], rnd[2], rnd[3], rnd[4], rnd[5], 0, 0, ...
- **S-MAC1**: 0x01, 0x01, rnd[0], rnd[1], rnd[2], rnd[3], rnd[4], rnd[5], 0, 0, ...
- **S-MAC2**: 0x01, 0x02, rnd[0], rnd[1], rnd[2], rnd[3], rnd[4], rnd[5], 0, 0, ...

The data fields rnd[0] through rnd[5] are the first 6 bytes of RND.A [8] (the 8 byte random number generated by the OSDP server). RND.A[8] is transferred to the reader while the secure connection is being established.

Server Cryptogram

The server cryptogram is computed by encrypting the concatenated RND.B [8] and A [8] using key S-ENC.

RND.A[8] is generated by the OSDP server and RND.B[8] is generated by the reader (client).

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

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 OSDP server and RND.B[8] is generated by the reader (client).

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

Padding

When used, padding shall be performed as follows:

- 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 evenly divisible by the block size of 16.

Message Authentication Code (MAC) Generation

The MAC is computed for and appended only to messages where:

- SEC_BLK_TYPE is SCS_15, SCS_16, SCS_17 or SCS_18,
- **and** the AES128 algorithm is applied in CBC mode using SMAC-1 as the key for all blocks except the last,
- **and** using SMAC-2 as the key for the last block.

ICV Values

The ICV (Initial Chaining Vector) is initialized by the reader during the secure connection sequence, and is passed to the OSDP server during SCS_14 in reply osdp_RMAC _I.

After the initial secure channel setup, in order to reduce message size and transmission time overhead, messages will contain only a partial MAC.

For messages whose SEC_BLK_TYPE is SCS_15, SCS_16, SCS_17 or SCS_18, only the first four bytes of the computed MAC are actually sent.

The MAC verification should locally generate the full MAC[16] and compare the actual bytes that were received.
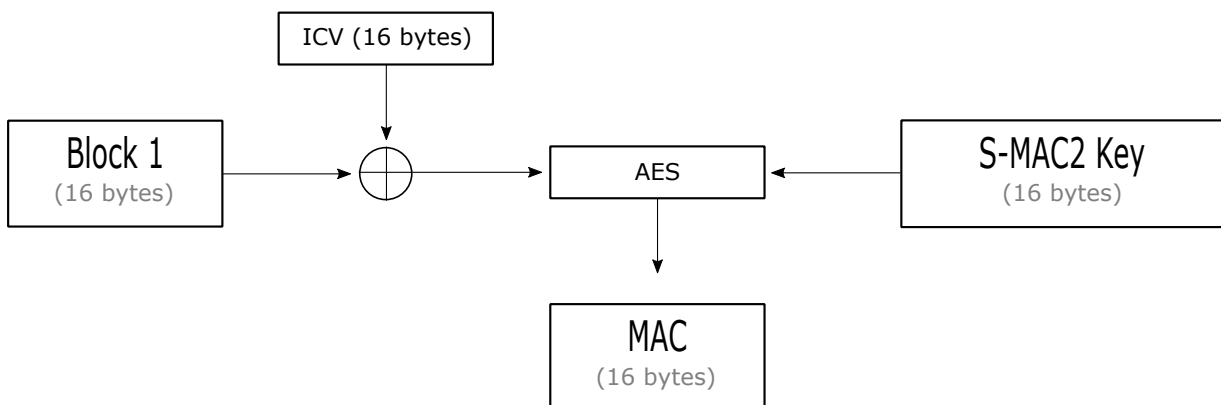
The MAC is generated from the entire OSDP packet including the SOM (0x53).

MAC Generation Diagram

The diagram below demonstrates the MAC generation process, where the AES algorithm is applied in CBC mode using S-MAC1 as the key for all blocks, except the last, where S-MAC2 is used.
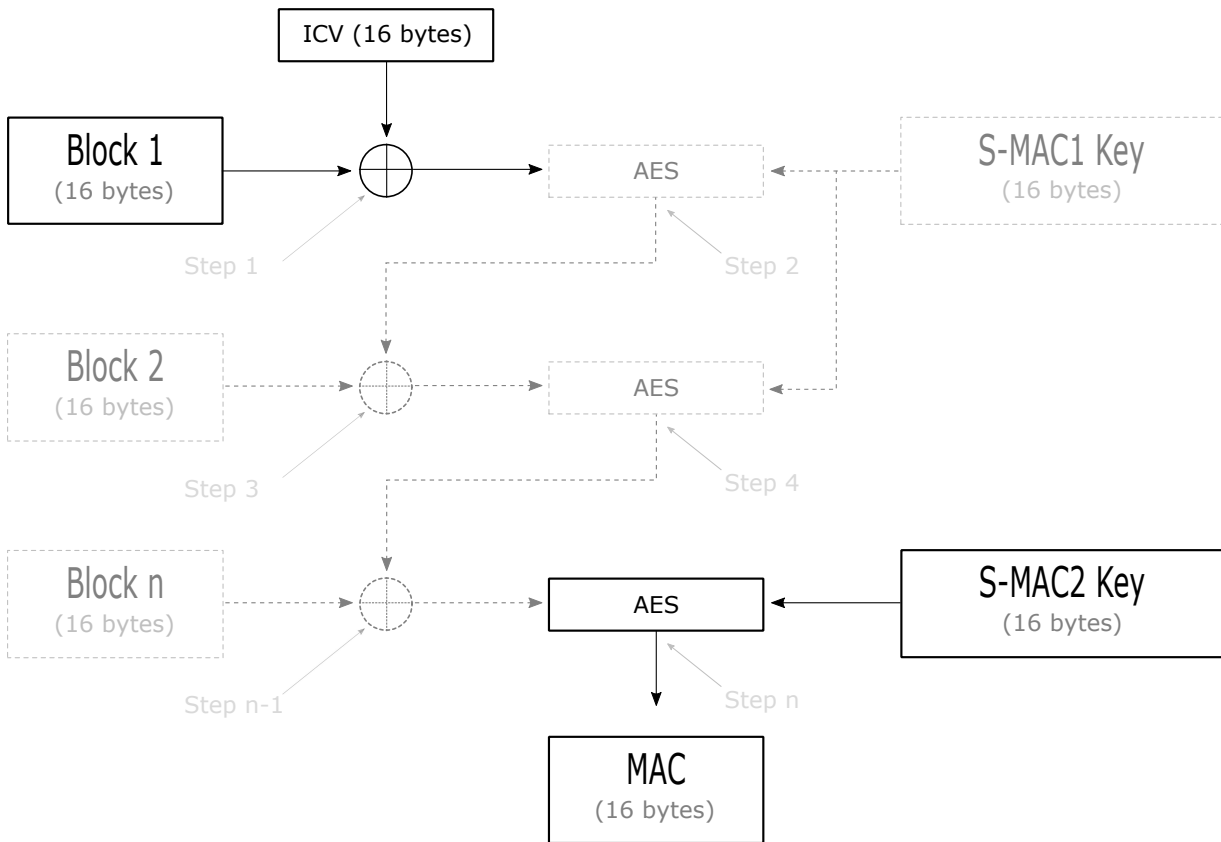
If the message size is 16 bytes (a single block) then only the S-MAC2 key will be used, as demonstrated in the diagram below.