

GlobalPlatform Technology

APDU Transport over SPI / I2C

Version 0.0.0.39

Public Review

July 2019

Document Reference: GPC_SPE_172

Copyright © 2017-2019 GlobalPlatform, Inc. All Rights Reserved.

Recipients of this document are invited to submit, with their comments, notification of any relevant patents or other intellectual property rights (collectively, "IPR") of which they may be aware which might be necessarily infringed by the implementation of the specification or other work product set forth in this document, and to provide supporting documentation. This document is currently in draft form, and the technology provided or described herein may be subject to updates, revisions, extensions, review, and enhancement by GlobalPlatform or its Committees or Working Groups. Prior to publication of this document by GlobalPlatform, neither Members nor third parties have any right to use this document for anything other than review and study purposes. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.

THIS SPECIFICATION OR OTHER WORK PRODUCT IS BEING OFFERED WITHOUT ANY WARRANTY WHATSOEVER, AND IN PARTICULAR, ANY WARRANTY OF NON-INFRINGEMENT IS EXPRESSLY DISCLAIMED. ANY IMPLEMENTATION OF THIS SPECIFICATION OR OTHER WORK PRODUCT SHALL BE MADE ENTIRELY AT THE IMPLEMENTER'S OWN RISK, AND NEITHER THE COMPANY, NOR ANY OF ITS MEMBERS OR SUBMITTERS, SHALL HAVE ANY LIABILITY WHATSOEVER TO ANY IMPLEMENTER OR THIRD PARTY FOR ANY DAMAGES OF ANY NATURE WHATSOEVER DIRECTLY OR INDIRECTLY ARISING FROM THE IMPLEMENTATION OF THIS SPECIFICATION OR OTHER WORK PRODUCT.

Contents

1	Introduction	6
1.1	Audience	6
1.2	IPR Disclaimer	6
1.3	References	6
1.4	Terminology and Definitions	7
1.5	Abbreviations and Notations	10
1.6	Revision History	12
2	Overview	13
3	Physical Interfaces	14
3.1	SPI Interface	14
3.1.1	Description	14
3.1.2	Physical Layer	14
3.1.2.1	Signal Conventions	14
3.1.2.2	Transmission of Data	15
3.1.2.3	Data Fragmentation / SPI Fragments	16
3.1.2.4	Half Duplex Usage	16
3.1.3	Activation Sequence	16
3.1.4	Detecting SE Ready to Receive Data	16
3.1.5	Detecting SE Ready to Send Data	17
3.1.5.1	Polling Mechanism	17
3.1.5.2	Interrupt Mechanism	18
3.1.6	Receiving Data from SE	18
3.1.7	Default Parameter Values / Ranges	19
3.2	I ² C Interface	20
3.2.1	Description	20
3.2.2	Physical Layer	20
3.2.3	Activation Sequence	21
3.2.4	Detecting SE Ready to Receive Data	21
3.2.5	Sending Data to SE	22
3.2.6	Detecting SE Ready to Send Data	23
3.2.7	Receiving Data from SE	25
3.2.8	Default Parameter Values / Ranges	28
4	Data Link Layer	29
4.1	T=1' Protocol	29
4.2	Block Format	30
4.2.1	Node Address Byte (NAD) Field Format	30
4.2.2	Protocol Control Byte (PCB) Field Format	31
4.2.3	Length (LEN) Field Format	32
4.2.4	Information (INF) Field Format	32
4.2.5	Epilogue Field Format	32
4.3	Communication Interface Parameters	33
4.3.1	CIP – Common Structure	33
4.3.2	CIP – Specific Parameters for Data Link Layer	33
4.3.3	CIP – Specific Parameters for SPI Physical Layer	34
4.3.4	CIP – Specific Parameters for I ² C Physical Layer	35
5	Power Saving Policy	36

Tables

Table 1-1: Normative References.....	6
Table 1-2: Informative References	7
Table 1-3: Common – Terminology and Definitions	7
Table 1-4: SPI – Terminology and Definitions	9
Table 1-5: I ² C – Terminology and Definitions	10
Table 1-6: Common – Abbreviations & Notations	10
Table 1-7: SPI – Abbreviations & Notations	11
Table 1-8: I ² C – Abbreviations & Notations	12
Table 1-9: Revision History	12
Table 3-1: SPI – Default Parameter Values / Ranges	19
Table 3-2: I ² C – Default Parameter Values / Ranges.....	28
Table 4-1: Block Format	30
Table 4-2: NAD Format.....	30
Table 4-3: Protocol Control Byte (PCB).....	31
Table 4-4: Information (INF) Field Format	32
Table 4-5: CIP – Common Structure	33
Table 4-6: CIP – Specific Parameters for Data Link Layer.....	33
Table 4-7: CIP – Specific Data for SPI Physical Layer.....	34
Table 4-8: CIP – Specific Parameters for I ² C Physical Layer	35

Figures

Figure 3-1: SPI Physical Lines	14
Figure 3-2: SPI Communication	15
Figure 3-3: Physical-Layer Fragmentation with Respect to SEAL Size	16
Figure 3-4: Level-Sensitive Interrupt Mechanism	18
Figure 3-5: Simplified I ² C Schematics	20
Figure 3-6: HD Detecting SE Ready to Receive Data	22
Figure 3-7: HD Sends Data to SE	23
Figure 3-8: HD Polling SE for Response Data	24
Figure 3-9: HD Receives Data from SE using a Single I ² C Message	26
Figure 3-10: HD Receives Data from SE using Multiple I ² C Messages	27

1 Introduction

More and more devices like mobile devices, wearables, or other IoT (Internet of Things) devices are now using soldered Secure Elements (SEs). This has generated new needs to support physical interfaces such as SPI or I²C in lieu of the former ISO/IEC 7816-3 layer. This specification describes how APDUs (as defined in [7816-3]) may be conveyed over these alternative physical interfaces.

This new protocol allows transferring longer payloads and is meant to adapt to the specific features of the underlying physical interfaces, e.g. to convey the length of the payload in a separate block ahead of the actual payload.

1.1 Audience

This specification is intended primarily for:

- Device Manufacturers who wish to embed a Secure Element into their solution.
- Secure Element OS developers who wish to provide support for APDU transport over alternative physical interfaces in their products.

It is assumed that the reader is familiar with the ISO/IEC 7816-3 T=1 smart card protocol.

1.2 IPR Disclaimer

Attention is drawn to the possibility that some of the elements of this GlobalPlatform specification or other work product may be the subject of intellectual property rights (IPR) held by GlobalPlatform members or others. For additional information regarding any such IPR that have been brought to the attention of GlobalPlatform, please visit <https://globalplatform.org/specifications/ip-disclaimers/>. GlobalPlatform shall not be held responsible for identifying any or all such IPR, and takes no position concerning the possible existence or the evidence, validity, or scope of any such IPR.

1.3 References

Table 1-1: Normative References

Standard / Specification	Description	Ref
ISO/IEC 7816-3:2006	Identification cards – Integrated circuit cards – Part 3: Cards with contacts – Electrical interface and transmission protocols	[7816-3]
ISO/IEC 7816-4	Identification cards – Integrated circuit cards – Part 4: Organization, security and commands for interchange	[7816-4]

Table 1-2: Informative References

Standard / Specification	Description	Ref
Motorola SPI Block Guide	SPI Block Guide v03.06, Motorola Inc. 04 February 2003	[SPI]
NXP I ² C manual	UM10204I2C-bus specification and user manual	[NXP_I2C]
BSI-CC-PP-0084	Common Criteria Protection Profile Security IC Platform Protection Profile with Augmentation Packages	[PP-0084]
ISO/IEC 13239	Information technology — Telecommunications and information exchange between systems — High-level data link control (HDLC) procedures	[ISO 13239]

1.4 Terminology and Definitions

Common terms and definitions are listed in the following table.

Table 1-3: Common – Terminology and Definitions

Term	Meaning
Assertion	Act of setting a signal from its inactive state to its active state.
Block	Smallest data unit that can be exchanged by the Data Link Layer. Used to convey application data and/or transmission control data.
Block Waiting Time (BWT)	Maximum delay between the leading edge of the last character of the command block received by the SE and the leading edge of the first character of the next response block transmitted by the SE. It represents the maximum time the SE may take to send its response. It is used to detect cases where the SE does not respond or takes too long to respond. The SE shall send a Waiting Time eXtension (WTX) signal if it wishes more time to process a command and build the corresponding response.
Communication Interface Parameters (CIP)	String of bytes returned by the Secure Element (SE) providing parameter values that the Hosting Device (HD) shall use to align with the SE's protocol and communication capabilities.
Cyclic Redundancy Check (CRC)	2-byte block error detection code (see [ISO 13239] for more information)
Data Link Layer	Protocol layer that manages the reliable point-to-point transfer of data over a physical interface. It provides data flow control, error correction, and addressing. It ensures that the incoming data is neither missing nor corrupted nor received in the incorrect order.
De-assertion	Act of setting a signal from its active state to its inactive state
Default Maximum Clock Frequency (DMCF)	Maximum clock frequency that shall be used by the HD when the CIP hasn't been received yet.
Epilogue Field	Last part of a Data Link Layer block, containing an error detection code computed over preceding block parts.

Term	Meaning
Hosting Device (HD)	The Hosting Device (aka Device Host) is a device connected to a Secure Element and acting as the SPI / I2C bus Master. It is generally seen as an IoT device, a mobile phone, or a wearable.
Information Block (I-Block)	Used to convey information for use by the application layer.
Information Field	Second part of a Data Link Layer block, containing application information for an I-Block or non-application information for an S-Block.
Information Field Size of the Hosting Device (IFSD)	Maximum size of the Information field of blocks that can be received by the Hosting Device (or sent by SE); above this limit, chaining shall be used.
Information Field Size of the SE (IFSC)	Maximum size of the Information field of blocks that can be received by the Secure Element (or sent by the HD); above this limit, chaining shall be used.
Inter Integrated Circuit bus (I2C)	Widespread bi-directional 2-wire physical serial interface allowing the connection of ICs.
Master	Device that initiates and controls the communication with slave device(s).
Node Address Byte (NAD)	Byte indicating the source and the destination of a Data Link Layer block.
Polling Time (POT)	Time interval between two polling requests made by the HD. This time interval shall be chosen by the HD based on the performance of the SE. The chosen value shall not be lower than the Minimum Polling Time (MPOT) communicated by the SE in the CIP.
Power Wake-Up Time (PWT)	Minimum time that the HD shall wait after having powered on the SE (i.e. after "VCC Valid" state has been reached) before initiating communications with the SE.
Prologue Field	First part of a Data Link Layer block, composed of 3 bytes: NAD, PCB, and LEN.
Protocol Control Byte (PCB)	Byte indicating the type of Data Link Layer block and conveys transmission control information.
Receive-Ready Block (R-Block)	Used to convey a positive or negative acknowledgement.
Secure Element (SE)	A tamper-resistant secure hardware component which is used in a device to provide the security, confidentiality, and multiple application environment required to support various business models. May exist in any form factor, such as embedded or integrated SE, SIM/UICC, smart card, smart microSD, etc.
Serial Clock Line (SCL)	Line that synchronizes the output of data bits from the master (HD) to the sampling of bits by the slave (SE). One bit of data is transferred in each clock cycle.
Serial Peripheral Interface (SPI)	Widespread 4(+)-wire physical serial interface allowing the connection of ICs.
Slave	Passive device which communicates with a Master device.
Supervisory Block (S-Block)	Used to exchange control information between the Hosting Device and the Secure Element.

Term	Meaning
Tamper-resistant secure hardware	Hardware designed to isolate and protect embedded software and data by implementing appropriate security measures. The hardware and embedded software meet the requirements of the latest Security IC Platform Protection Profile ([PP-0084]) including resistance to physical tampering scenarios described in that Protection Profile.

Additional terms and definitions relating to the SPI physical interface are listed in the following table.

Table 1-4: SPI – Terminology and Definitions

Term	Meaning
Clock Phase (CPHA)	Bit indicating when the sampling of data over the SPI MISO / MOSI lines shall occur.
Clock Polarity (CPOL)	Bit indicating whether the clock shall be inverted or not.
Default Wake-Up Time (DWUT)	Wake-Up Time that shall be used by the HD when the CIP hasn't been received yet.
Filling Byte	Same as Null-Byte.
Fragment	Piece of data exchanged during an SPI access (Length <= SEAL).
Master In / Slave Out line (MISO line)	Line used by the slave device to send data to the master device.
Master Out / Slave In line (MOSI line)	Line used by the master device to send data to the slave device.
Null-Byte	Byte value '00' sent by the HD or SE for one of the following purposes: <ul style="list-style-type: none"> As a filling byte on an SPI line; while meaningful data is conveyed on one line (MOSI or MISO), meaningless filling bytes are conveyed on the other. As a polling byte when the HD polls the SE for available data. As a wake-up byte when the HD wishes to wake up the SE from Power Saving Mode.
SE Access Length (SEAL)	2-byte length of the data that can be handled by the SE in one single SPI master (HD) access. It is required by the Hosting Device for data flow control purposes when sending data to and receiving data from the SE.
SE Guard Time (SEGT)	Time that the HD shall wait between two SPI accesses.
Serial Peripheral Interface (SPI)	Widespread physical serial interface allowing the connection of ICs.
Slave Select (SS)	Line used by the master (HD) to output the select signal towards the slave (SE) it wishes to exchange data with.
SPI Access	Transfer of data over the MOSI / MISO line, triggered by the Master.
SPI Interrupt line (SPI-IRQ)	Line asserted by the SE to inform the HD that a response is ready to be sent.
Wake-Up Byte	Same as Null Byte

Term	Meaning
Wake-Up Time (WUT)	Time taken by the SE to leave Power Saving Mode and get ready to receive data.

Additional terms and definitions relating to the I²C physical interface are listed in the following table.

Table 1-5: I²C – Terminology and Definitions

Term	Meaning
Idle Byte	Byte value 'FF' that may be sent by the SE to indicate that it is currently busy.
R/W Guard Time (RWGT)	Time that the HD shall wait before initiating an I ² C writing operation after an I ² C reading operation, and vice versa.
Serial Data Line (SDA)	I ² C data line allowing data to be transferred in both directions between a master (Hosting Device) and a slave (Secure Element).

1.5 Abbreviations and Notations

Common abbreviations and notations are listed in the following table.

Table 1-6: Common – Abbreviations & Notations

Abbreviation	Meaning
APDU	Application Protocol Data Unit
BWT	Block Waiting Time
CIP	Communication Interface Parameters
CLK	Clock line through which the HD provides the clock signal to the SE
CRC	Cyclic Redundancy Check
DAD	Destination Address
DMCF	Default Maximum Clock Frequency
EDC	Error Detection Code
HD	Hosting Device
I ² C	Inter Integrated Circuit bus
I-Block	Information Block
IFS	Information Field Size
IFSC	Information Field Size of the SE
IFSD	Information Field Size of the Hosting Device
IRQ	Interrupt Request
LEN	Length field of a Data Link Layer block
LSB	Least Significant Byte

Abbreviation	Meaning
lsb	Least Significant Bit
MCF	Maximum Clock Frequency
MPOT	Minimum Polling Time
MSB	Most Significant Byte
msb	Most Significant Bit
NAD	Node Address Byte
PCB	Protocol Control Byte
POT	Polling Time
PWT	Power Wake-Up Time
R-Block	Receive-Ready Block
SAD	Source Address
SCL	Serial Clock Line (a.k.a. SCKL or SCLK)
S-Block	Supervisory Block
SE	Secure Element
SPI	Serial Peripheral Interface
WTX	Waiting Time eXtension

Additional acronyms and abbreviations relating to the SPI physical interface are listed in the following table.

Table 1-7: SPI – Abbreviations & Notations

Abbreviation	Meaning
CPHA	Clock Phase
CPOL	Clock Polarity
MISO	Master In / Slave Out
MOSI	Master Out / Slave In
SEAL	SE Access Length
SEGT	Secure Element Guard Time
SPI	Serial Peripheral Interface
SPI-IRQ	SPI Interrupt line
SS	Slave Select line
WUT	Wake-Up Time

Additional acronyms and abbreviations relating to the I²C physical interface are listed in the following table.

Table 1-8: I²C – Abbreviations & Notations

Abbreviation	Meaning
SDA	Serial Data Line
RWGT	R/W Guard Time

1.6 Revision History

GlobalPlatform technical documents numbered *n.0* are major releases. Those numbered *n.1*, *n.2*, etc., are minor releases where changes typically introduce supplementary items that do not impact backward compatibility or interoperability of the specifications. Those numbered *n.n.1*, *n.n.2*, etc., are maintenance releases that incorporate errata and precisions; all non-trivial changes are indicated, often with revision marks.

Table 1-9: Revision History

Date	Version	Description
December 2018	0.0.0.28	Member Review
July 2019	0.0.0.39	Public Review
TBD	1.0	Public Release

2 Overview

This document specifies how to transport APDUs between a Hosting Device (HD) and a Secure Element (SE) using serial physical interfaces based on [SPI] or [NXP_I2C], which are very commonly used in the industry for connecting different electronic components.

Section 3 describes the Physical Layer that shall be implemented to access the physical interface. Section 4 describes the Data Link Layer (implemented over the Physical Layer) that shall be used to transport APDU commands and responses.

Section 5 describes the conditions under which the SE may enter Power Saving Mode.

3 Physical Interfaces

3.1 SPI Interface

3.1.1 Description

The Serial Peripheral Interface (SPI) described in [SPI] is a synchronous Serial Data Link that offers full-duplex communication. Devices communicate in master/slave mode whereby the master initiates the communication by sending data while the slave is able to send data at the same time. In this specification however, the SPI is only used for half-duplex communication.

Although multiple slave devices may be present, each one using its own individual Slave Select line (SS), this specification only describes the communication between one single master and one single slave device; the Hosting Device (HD) acts as master, the Secure Element (SE) acts as slave.

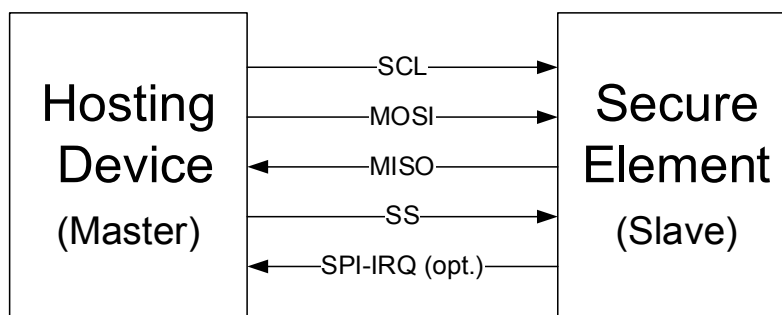
3.1.2 Physical Layer

The SPI bus specifies four mandatory physical signals/lines:

- SCL line: Serial Clock (output from HD)
- MOSI line: Master Out / Slave In (output from HD)
- MISO line: Master In / Slave Out (output from SE)
- SS line: Slave Select (active low, output from HD)

A supplementary SPI-IRQ physical line may be added.

Figure 3-1: SPI Physical Lines



When it is present, the SPI-IRQ line may be used by the SE to notify the HD that it is ready to send data, which is needed because only the HD (master) may initiate the communication. If the SPI-IRQ line is not available, the HD may instead poll the SE for incoming data. See section 3.1.5 for more details.

3.1.2.1 Signal Conventions

The SPI communication shall use the “mode 0” configuration as described below:

- The SPI Clock Polarity bit (CPOL) shall be 0 (non-inverted clock), meaning that the idle state of the clock is low and that trigger is initiated at a raising clock signal (Active-high clocks selected).
- The SPI Clock Phase bit (CPHA) shall be 0, meaning that the sampling of data occurs at a raising clock signal of the SCL signal. The data signals are set at chip selection and falling clock signals.

- The SCL frequency shall not exceed the Maximum Clock Frequency (MCF) defined by the CIP (see section 4.3). If the MCF is not known yet (i.e. CIP not retrieved yet), the Default Maximum Clock Frequency (DMCF) defined in section 3.1.7 shall be used.
- The number of bits transmitted via MOSI or MISO signal during a single SPI access shall be a multiple of eight.
- The Most Significant Byte / Bit (MSB / msb) shall be sent first.

3.1.2.2 Transmission of Data

Only the HD may initiate the transmission of data and it shall select the SE before it can exchange data with it, i.e. the HD shall pull down the SS line and provide a proper clock signal on the SCL line.

If the HD needs to send data to the SE, it shall provide such data on the MOSI line and ignore the data received on the MISO line. Conversely, if the HD needs to receive data from the SE, it shall provide filling bytes on the MOSI line and read the data received on the MISO line.

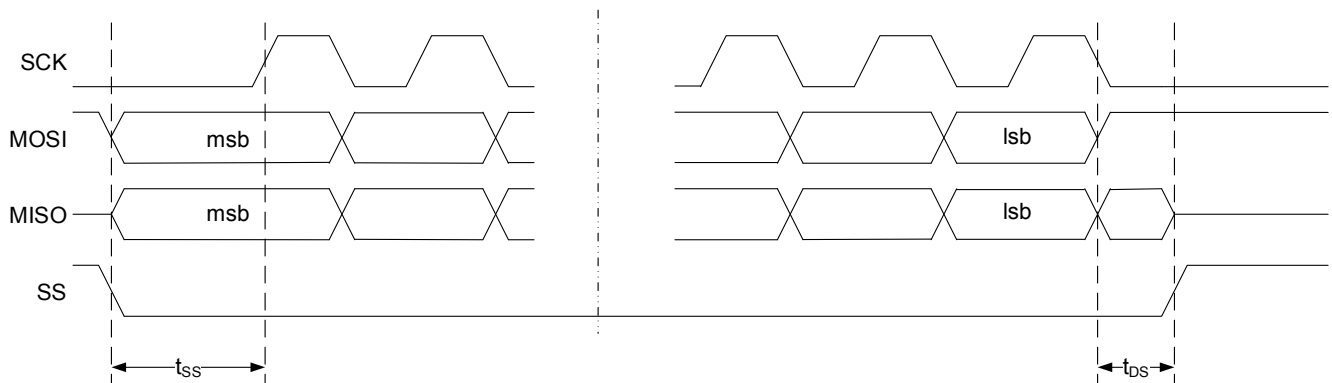
Similarly, the SE shall provide filling bytes on the MISO line when expecting meaningful data from the HD on the MOSI line, and shall ignore data on the MOSI line when sending data to the HD on the MISO line.

Once all data have been exchanged as expected, the HD shall stop the clock signal and de-select the SE.

Above rules are summarized in Figure 3-2 where:

- “msb” shows the position of the most significant bit of the first byte of the transmitted data.
- “lsb” shows the position of the least significant bit of the last byte.
- “ t_{ss} ” is the minimum time that the master shall wait after assertion of the SS line before starting the clock signal and transmitting the first bit of data. Its value remains out of scope of this specification.
- “ t_{ds} ” is the minimum time that the master shall wait after the transmission of the last bit of data before de-asserting the SS line (i.e. deselecting the slave). Its value remains out of scope of this specification.

Figure 3-2: SPI Communication

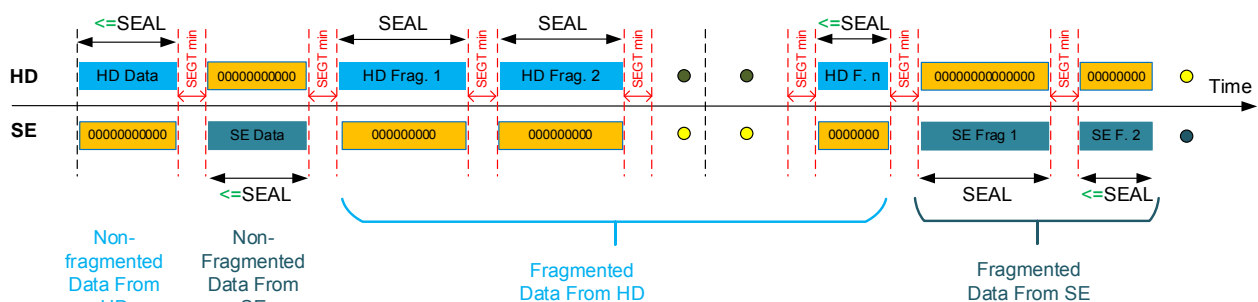


3.1.2.3 Data Fragmentation / SPI Fragments

The SPI bus is used to convey Data Link Layer blocks for which a data flow control is defined (see section 4). However, a first level of data flow control is implemented at the Physical Layer through the exchange of so-called SPI fragments. A block of data may be split in multiple SPI fragments. The fragmentation of data will depend on the size of the data that needs to be exchanged and the SE Access Length (SEAL).

When the HD needs to exchange data with the SE (send or receive) and the length of such data exceeds SEAL bytes, the HD shall fragment and exchange data so that the number of bytes conveyed during each SPI access does not exceed a maximum of SEAL bytes (in each direction). When possible, the HD shall maximize the number of bytes transferred per SPI access in order to minimize the number of SPI accesses. In addition, the HD shall pause for a duration of SE Guard Time (SEGT) between two consecutive SPI accesses. This process is summarized in Figure 3-3.

Figure 3-3: Physical-Layer Fragmentation with Respect to SEAL Size



3.1.2.4 Half Duplex Usage

Although the SPI bus allows full-duplex mode operation, this specification does not use such capabilities and the meaningful information is only communicated by the Data Link Layer in half-duplex mode (see section 4), meaning that HD and SE are only expected to send Data Link Layer blocks alternatively.

However, it may happen in a time-out situation that both HD and SE attempt to send data, in which case both HD and SE may receive Data Link Layer blocks at the same time (due to the full-duplex nature of the SPI bus). In such a case, the SE shall discard the remaining bytes of the block it started to send and shall process the block sent by the HD.

3.1.3 Activation Sequence

After having powered on the SE, the HD shall wait for a duration of Power Wake-Up Time (PWT) before initiating any communication with the SE. When initiating the communication with the SE, the HD shall ensure that the SE is ready to receive data following the procedure described in section 3.1.4.

The HD may then retrieve the CIP (see section 4.3). If the CIP has never been retrieved and/or the HD doesn't know which parameter values may be used, the HD shall use the default values (e.g. Default PWT) defined in section 3.1.7. Otherwise, it may use the parameter values previously read from the CIP.

The HD shall adapt its behavior according to the parameters specified by the CIP.

3.1.4 Detecting SE Ready to Receive Data

The SE may decide to enter some kind of Power Saving Mode in order to save battery (typically the host device battery), in which case it would not be able to receive data. The conditions under which an SE implementation may enter such a Power Saving Mode are described in Chapter 5.

When the HD wishes to send data and considers the SE has probably entered Power Saving Mode, it shall first make sure the SE is ready to receive data. To do so, the HD shall apply a so-called wake-up procedure.

Two wake-up procedures are described hereafter; however, this specification acknowledges the fact that it may not be possible to implement these procedures in some environments. Therefore, use of a proprietary wake-up procedure (known to both HD and SE) is permitted.

- Wake-Up Procedure 1 (a.k.a. SS-WUT-SCL):

The HD shall assert the SS line and wait for a duration of WUT (or DWUT if the CIP / WUT has never been retrieved from the SE) before applying the clock signal (SCL) and sending data.

In this procedure, the SS line is used as an interrupt line to wake up the SE and waiting WUT provides the SE with necessary time to wake up and get ready. For best performance, the HD should start sending data immediately after WUT. However, it may safely wait longer; keeping the SS line asserted prevents the SE from going back to Power Saving Mode.

- Wake-Up Procedure 2 (a.k.a. NB-WUT):

The HD shall send one Null-Byte (using the procedure described in section 3.1.2.2, i.e. ending a deselection of the SE) and then wait for a duration of WUT (or DWUT if the CIP / WUT has never been retrieved from the SE) before sending any significant data. When the SE detects that it is deselected for the first time since wake up, it shall discard any data previously received on the MOSI line.

In this procedure, waiting WUT provides the SE with necessary time to wake up and get ready and the deselection instructs the SE to discard any non-significant data initially received on the MOSI line. Note that to prevent the SE going back to Power Saving Mode (see Chapter 5), the HD shall take care not to wait too long.

In addition, when the SE expects a new Data Link Layer block (see section 4) and instead receives a single Null-Byte, the SE shall simply discard this Null-Byte and wait for further incoming data. This behavior is required to handle the case where the HD would incorrectly assess the SE as being in Power Saving Mode and unnecessarily apply the wake-up procedure.

In support of the above procedures, a Wake-Up Time (WUT) is defined as part of the CIP (see section 4.3.3) and a Default WUT (DWUT) is defined in section 3.1.7. The WUT found in the CIP may be ignored or used with another meaning if a proprietary wake-up procedure is implemented.

3.1.5 Detecting SE Ready to Send Data

To detect that the SE is ready to send data and initiate the retrieval of such data, the HD Physical Layer shall use one of the mechanisms described in the following sections. As such mechanisms correspond to different hardware architectures, the choice of using one or the other is implicit (i.e. the HD implicitly knows which one to use).

3.1.5.1 Polling Mechanism

When the HD and SE are configured to use the polling mechanism, the HD shall poll the SE for available data. To do so, it shall first decide a Polling Time (POT). The chosen POT shall be greater than the MPOT communicated by the CIP. Then, when the HD is expecting some response data, the HD shall poll the SE as follows:

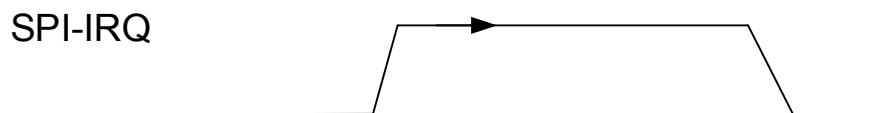
- The HD shall send one Null-Byte (using the procedure described in 3.1.2.2) to try receive a first meaningful byte from the SE (i.e. valid first byte of a Data Link Layer block).
- If a Null-Byte is received from the SE, the HD shall wait for a duration of POT and then try exchanging a Null-Byte again. The HD shall repeat this procedure until it receives a meaningful byte from the SE or until the HD Data Link Layer determines that a timeout has occurred.

- If a meaningful byte is received from the SE, the HD shall wait for a duration of SEGT before carrying on receiving remaining block data.

3.1.5.2 Interruption Mechanism

When the HD and SE are configured to use the interruption mechanism, the dedicated SPI-IRQ line shall be asserted by the SE when response data is available. A Level-Sensitive mechanism shall be implemented where the interruption shall be triggered by setting the SPI-IRQ line to an active high voltage level. The SE shall clear the interruption as soon as the SS line is asserted by the HD.

Figure 3-4: Level-Sensitive Interrupt Mechanism



To prevent communication errors and allow safe retrieval of data by the HD, the SE shall only assert the SPI-IRQ line when consistent data are actually ready for sending, that is, when SEAL bytes of meaningful data or the end of or a complete Data Link Layer block shorter than SEAL bytes is ready for sending.

3.1.6 Receiving Data from SE

Because receiving data from the SE may only be initiated and driven by the HD (master), the HD needs to know the size of data that shall be retrieved from the SE. To enable this, after detecting that the SE is ready to send data (see section 3.1.5), the HD may safely expect to receive a Data Link Layer block (see section 4) from the SE. From the prologue field of that block, the HD may learn how much data shall be received.

NOTE: When the polling mechanism described in section 3.1.5.1 is used to detect that the SE is ready to send data, the first valid (non-null) byte returned by the SE indicates the end of the polling procedure and is the first byte of the Data Link Layer block the SE intends to send. When the interrupt mechanism is used, the HD has not received any byte yet and shall retrieve the entire Data Link Layer block.

NOTE: Data transfer and communication performance may be optimized by having the HD always immediately retrieve not just the prologue field of a Data Link Layer block but rather a common short block size (e.g. 6 bytes) or even slightly more (e.g. 8 bytes). If the HD tries to retrieve more data than is made available by the SE, the HD should only receive additional filling bytes (common behavior in SPI implementations), which should not be an issue: Either the HD received a complete Data Link Layer block (that it may check and use), or it received an incomplete block and remaining data may be retrieved with more SPI accesses.

3.1.7 Default Parameter Values / Ranges

The following table defines SPI parameter values (or ranges) that shall be used by default.

Table 3-1: SPI – Default Parameter Values / Ranges

Parameter	Description	Unit	Minimum	Maximum
DPWT	Default Power Wake-Up Time	ms	25	-
DMCF	Default Maximum Clock Frequency	kHz	-	1000
DMPOT	Default Minimum Polling Time	ms	5	-
DSEGT	Default SE Guard Time	μs	10	-
DWUT	Default Wake-Up Time	μs	25	-

NOTE: The HD shall instead use the parameter values (or ranges) specified by the CIP (see section 4.3) once it's been retrieved from the SE.

3.2 I²C Interface

3.2.1 Description

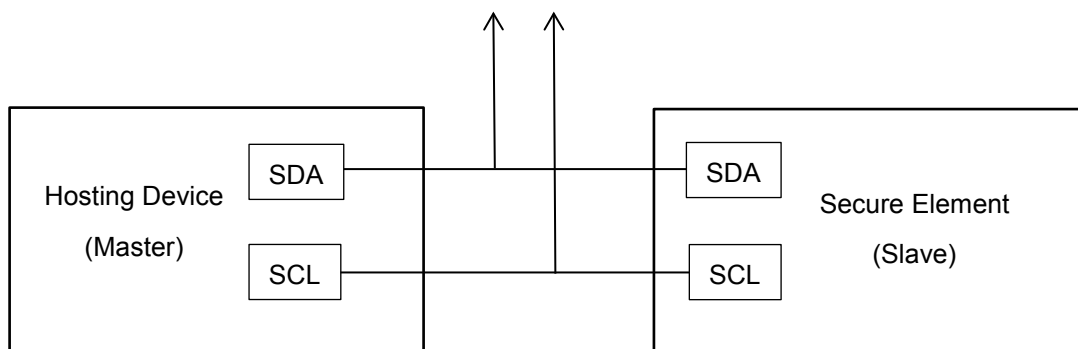
The Inter Integrated Circuit (I²C) bus described in [NXP_I2C] allows establishing half-duplex communications between one or several master(s) and one or several slave(s). Although multiple master devices may be present, this specification only describes communications involving a single master device. The HD acts as master, the SE(s) act(s) as slave(s).

3.2.2 Physical Layer

The I²C bus comprises two signal lines:

- Serial Clock Line (SCL)
- Serial Data Line (SDA)

Figure 3-5: Simplified I²C Schematics



Only the following options of I²C are used:

- Support of 7-bit Addressing only
- Single-Master / Multi-Slave configuration
- Maximum Clock Frequency (specified in CIP; see section 4.3.4)
 - 400 kHz for Fast Mode
 - 1000 kHz for Fast Mode Plus
 - 3400 kHz for HS Mode
- Clock Stretching mandatory for HD and optional for SE (specified in CIP; see section 4.3.4)

3.2.3 Activation Sequence

After having powered on the SE, the HD shall wait for a duration of Power Wake-Up Time (PWT) before initiating any communication with the SE. When initiating the communication with the SE, the HD shall ensure that the SE is ready to receive data following the procedure described in section 3.2.4.

The HD may then retrieve the CIP (see section 4.3). If the CIP has never been retrieved and/or the HD doesn't know which parameter values may be used, the HD shall use the default values (e.g. Default PWT) defined in section 3.1.7. Otherwise, it may use parameter values previously read from the CIP.

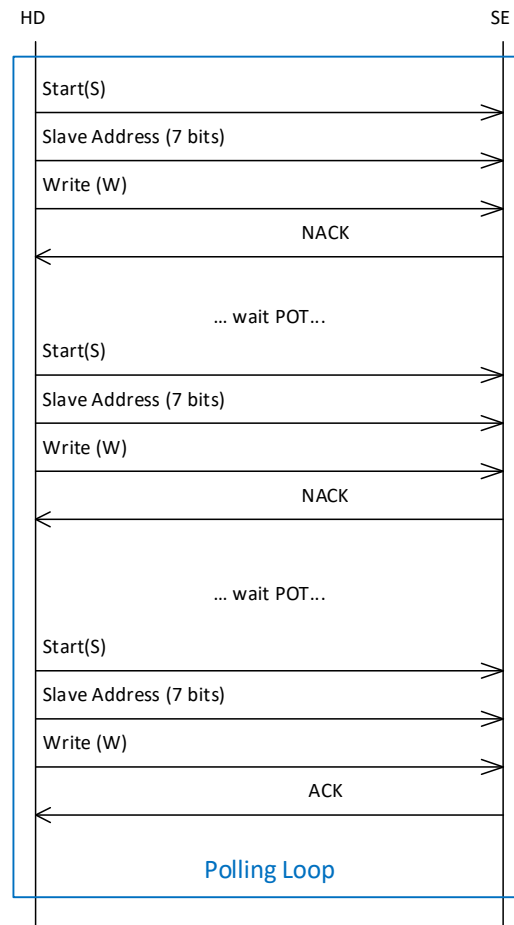
The HD shall adapt its behavior according to the parameters specified by the CIP.

3.2.4 Detecting SE Ready to Receive Data

The SE may decide to enter some kind of Power Saving Mode in order to save battery (typically the host device battery), in which case it would not be able to receive data. The conditions under which an SE implementation may enter such a Power Saving Mode are described in Chapter 5.

When the HD wishes to send data and considers that the SE has probably entered Power Saving Mode, it shall first make sure the SE is ready to receive data. To do so, the HD shall periodically poll the SE by sending a start condition and a 1-byte write request to the SE (see

Figure 3-6) and shall ignore and retry (after a duration of POT) if the SE rejects (NACK) the I²C write request (to indicate it is not ready). The polling time (POT) used by the HD shall be greater than the MPOT communicated by the CIP.

Figure 3-6: HD Detecting SE Ready to Receive Data

3.2.5 Sending Data to SE

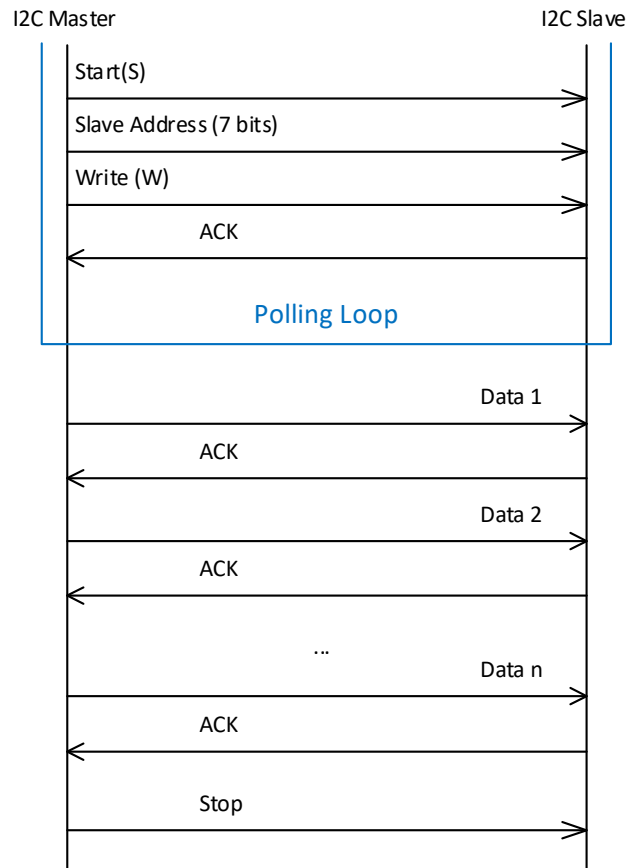
When the SE is in RECEIVING state, it is idle and waiting for a Data Link Layer block from the HD. In RECEIVING state, the SE shall:

- Acknowledge (ACK) any I²C write request from HD

The HD shall follow the sequence below to send an I²C message to the SE:

- 1) Send I²C start bit
- 2) Send the I²C address of the SE with the R/W bit low (Write to SE)
- 3) Send data (i.e. Data Link Layer block)
- 4) Send I²C stop bit

This is illustrated in Figure 3-7. The HD shall send a complete Data Link Layer block in one I²C message; however, it may abort the message transmission anytime by sending an I²C stop bit. The HD shall not use repeated start condition. The HD shall wait RWGT (Read Write Guard Time) before initiating any new I²C read requests.

Figure 3-7: HD Sends Data to SE

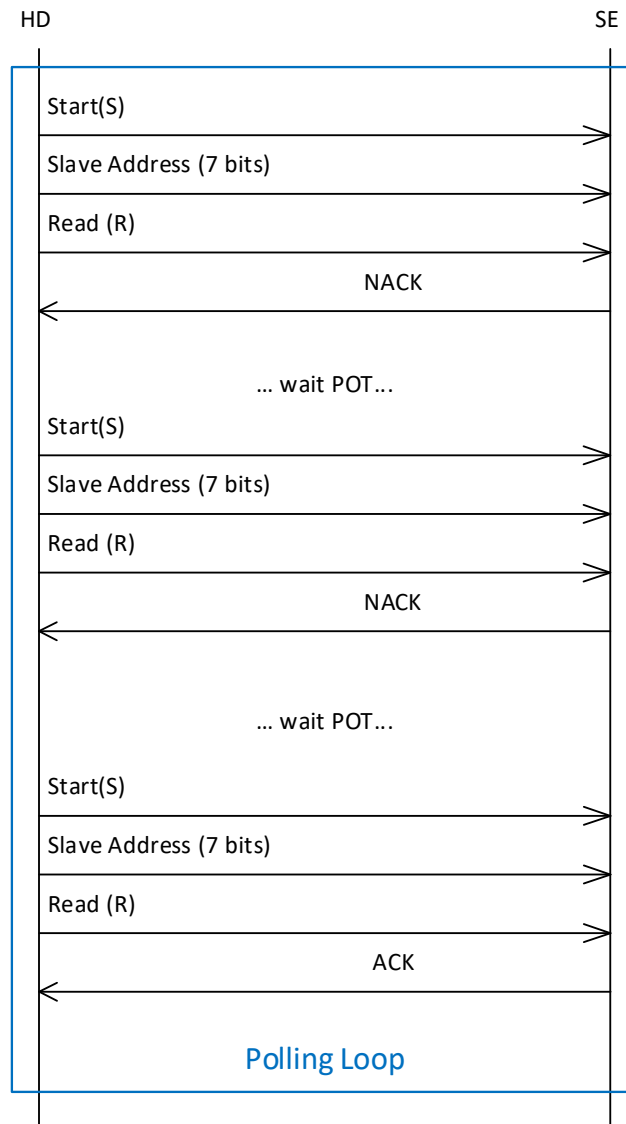
3.2.6 Detecting SE Ready to Send Data

When the HD has finished sending an I²C message (i.e. the SE has received the I²C stop bit), the SE shall switch from RECEIVING state to PROCESSING state. In PROCESSING state, the SE is busy processing the command sent by the HD and shall:

- Reject (NACK) any I²C write request from HD
- Reject (NACK) any I²C read request from HD

The HD shall periodically poll the SE for response data by sending a 1-byte read request to the SE (see Figure 3-8) and shall ignore and retry (after a duration of POT) if the SE rejects (NACK) the I²C read request (to indicate it is busy). The polling time (POT) used by the HD shall be greater than the MPOT communicated by the CIP.

Figure 3-8: HD Polling SE for Response Data



3.2.7 Receiving Data from SE

When the SE has finished processing the Data Link Layer command block sent by the HD and it is ready to send a Data Link Layer response block, the SE shall switch from RECEIVING to SENDING state. In SENDING state, the SE shall:

- Acknowledge (ACK) any I²C read request from the HD.

The HD shall follow the sequence below to receive an I²C message from the SE:

- 1) Send I²C start bit
- 2) Send the I²C address of the SE with the R/W bit high (Read from SE)
- 3) Receive data
- 4) Send I²C stop bit

The HD may read the response bytes using a single I²C message or multiple I²C messages. This is illustrated in Figure 3-9 and Figure 3-10. The HD shall not use a repeated start condition. The HD shall wait RWGT (Read Write Guard Time) before initiating any new I²C write requests.

The SE shall remain in SENDING state until all response bytes have been read by the HD or until the HD sends a new I²C write request (see section 3.2.5). As the HD may safely expect to receive a Data Link Layer block (see section 4) from the SE, the HD may learn from the prologue field of that block how much data shall be received. If the HD attempts to read more data than was made available by the SE, the SE shall answer with Idle Bytes to indicate it doesn't have data to send anymore.

Figure 3-9: HD Receives Data from SE using a Single I²C Message

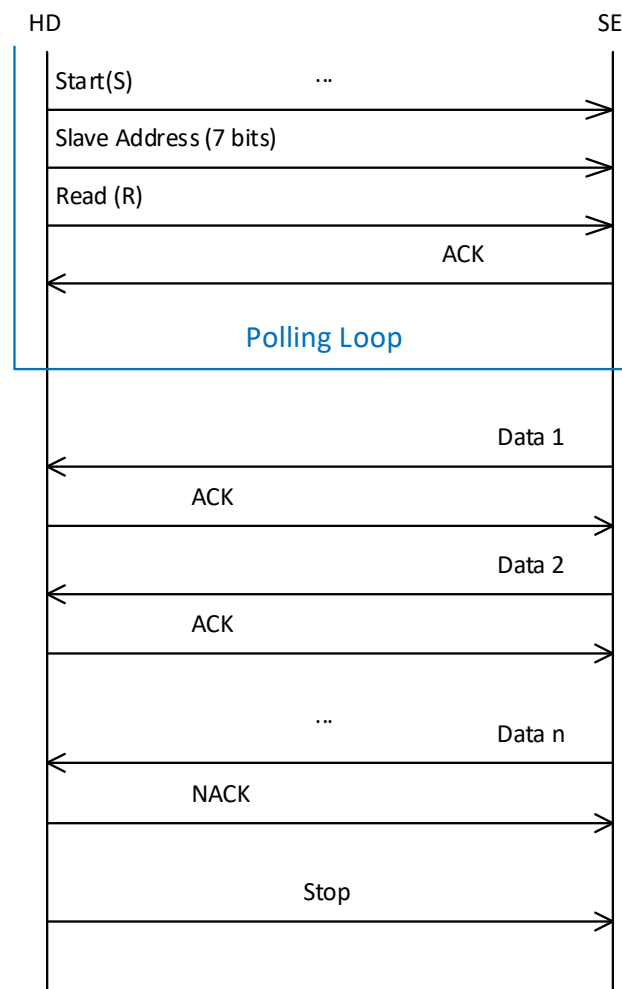
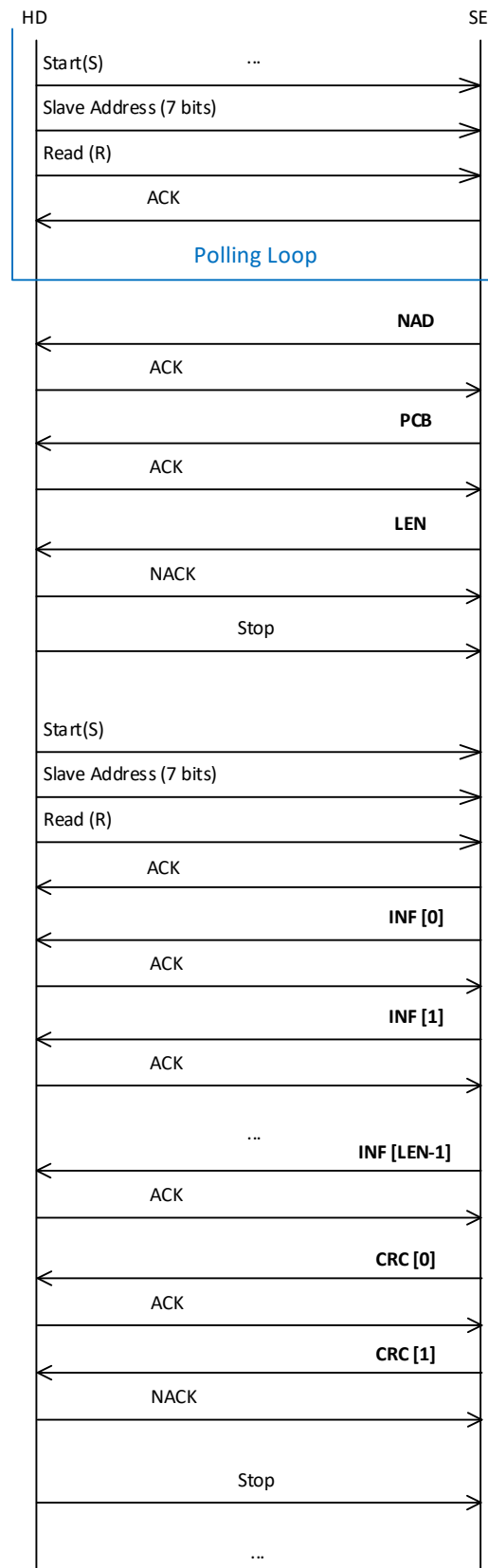


Figure 3-10: HD Receives Data from SE using Multiple I²C Messages

3.2.8 Default Parameter Values / Ranges

The following table defines I²C parameter values (or ranges) that shall be used by default.

Table 3-2: I²C – Default Parameter Values / Ranges

Parameter	Description	Unit	Minimum	Maximum
DPWT	Default Power Wake-Up Time	ms	25	-
DMCF	Default Maximum Clock Frequency	kHz	-	400
DMPOT	Default Minimum Polling Time	ms	5	-
DRWGT	Default R/W Guard Time	μs	10	-

NOTE: The HD shall instead use the parameter values (or ranges) specified by the CIP (see section 4.3) once it's been retrieved from the SE.

4 Data Link Layer

The Data Link Layer uses one of the Physical Layers described in section 3 to transfer blocks of data between the HD and the SE. Such blocks may only be sent alternatively by the HD and SE (i.e. half-duplex communication) and may convey application data or transmission control data. The protocol that shall be implemented by the Data Link Layer is very similar to the T=1 protocol described in [7816-3] and therefore is simply called T=1'.

4.1 T=1' Protocol

The T=1' protocol builds upon the T=1 protocol described in [7816-3] with the following differences:

- The general block structure is the same but the LEN field of the prologue is coded on 2 bytes.
- Additional rules are defined for the value of the NAD field.
- 2-byte CRC is retained as the unique EDC algorithm that shall be used.
- The S(IFS xxx) block may contain a value coded on 1 or 2 bytes.
- Additional S-Blocks are defined (with no direct impact on the protocol).

More explanations are given throughout section 4.2.

The rules for error free operation described in [7816-3] section 11.6.2.3 and the example scenarios described in [7816-3] Annex A.2 still apply. The error handling rules described in [7816-3] section 11.6.3 and the example scenarios described in [7816-3] Annex A.3 still apply.

4.2 Block Format

The general block structure used by the T=1' protocol is the same as the one described in [7816-3] for the T=1 protocol; however, the LEN field is coded on 2 bytes as shown in Table 4-1.

Table 4-1: Block Format

Prologue Field (mandatory)			Information Field (optional)	Epilogue Field (mandatory)
NAD (1 byte)	PCB (1 byte)	LEN (2 byte)	INF (LEN bytes)	CRC (2 bytes)

4.2.1 Node Address Byte (NAD) Field Format

The NAD field specifies the source and the intended destination of the block.

Table 4-2: NAD Format

Destination Address (DAD)	Source Address (SAD)
8 – 5b	4 – 1b

The following restrictions apply to NAD values:

- To facilitate the detection of the NAD byte (i.e. start of a block vs. non-significant byte), values 0000b and 1111b are forbidden for the DAD and SAD.
- To facilitate the detection of the direction of a block (e.g. HD to SE or SE to HD), the DAD and SAD shall never have the same value.

This specification specifies the following values for SAD and DAD:

- 0001b: Host Device (HD)
- 0010b: Secure Element (SE)

The values above shall be used for configurations involving a single master and single slave. Configurations involving more than one master or slave may define and use supplementary values.

4.2.2 Protocol Control Byte (PCB) Field Format

The PCB field defines the type of the block and includes transmission control data.

The T=1' protocol introduces the following new block types:

- S(CIP request): Requests the SE to return the CIP.
- S(CIP response): Answers an S(CIP request) block containing the CIP (see section 4.3).
- S(RELEASE request): Releases the SE, i.e. the HD indicates that it doesn't matter if the SE goes to Power Saving Mode at that time. See Chapter 5 for more details.
- S(RELEASE response): Acknowledges an S(RELEASE request) block.
- S(SWR request): Requests the SE to perform a software reset, which shall be interpreted by the SE as a “warm reset” of the communication interface. The impact of this “warm reset” for the software executed by the SE is out of scope of this specification.
- S(SWR response): Acknowledges an S(SWR request) block after software reset.

The encoding of the PCB field is described in Table 4-3.

Table 4-3: Protocol Control Byte (PCB)

Type	Sub-Type	b8	b7	b6	b5	b4	b3	b2	b1
I-Block	Application Data	0	N(S)	M-bit	0	0	0	0	0
R-Block	Error-free acknowledgement	1	0	0	N(R)	0	0	0	0
	CRC error	1	0	0	N(R)	0	0	0	1
	Other error	1	0	0	N(R)	0	0	1	0
S-Block	RESYNCH request	1	1	0	0	0	0	0	0
	RESYNCH response	1	1	1	0	0	0	0	0
	IFS request	1	1	0	0	0	0	0	1
	IFS response	1	1	1	0	0	0	0	1
	ABORT request	1	1	0	0	0	0	1	0
	ABORT response	1	1	1	0	0	0	1	0
	WTX request	1	1	0	0	0	0	1	1
	WTX response	1	1	1	0	0	0	1	1
	CIP request	1	1	0	0	0	1	0	0
	CIP response	1	1	1	0	0	1	0	0
	RELEASE request	1	1	0	0	0	1	1	0
	RELEASE response	1	1	1	0	0	1	1	0
	SWR request	1	1	0	0	1	1	1	1
	SWR response	1	1	1	0	1	1	1	1

4.2.3 Length (LEN) Field Format

The LEN field encodes the length of the INF field of the block.

The following values shall be considered as invalid by the receiver:

- Values exceeding the current IFS value of the receiver (i.e. IFSC for SE, IFSD for HD)
- Values beyond '0FF9' (4089) (see explanations in section 4.2.5)

4.2.4 Information (INF) Field Format

The content of the INF field depends on the block type.

Table 4-4: Information (INF) Field Format

Type	Sub-Type	Information Field Usage
I-Block	Application Data	Application Data
R-Block	Error-free acknowledgement	Not Present
	CRC error	Not Present
	Other error	Not Present
S-Block	RESYNCH request	Not Present
	RESYNCH response	Not Present
	IFS request	1 or 2-byte IFS value (see explanations below)
	IFS response	Same INF field as preceding S(IFS request)
	ABORT request	Not Present
	ABORT response	Not Present
	WTX request	1-byte integer value multiple of BWT
	WTX response	Same INF field as preceding S(WTX request)
	CIP request	Not Present
	CIP response	Communication Interface Parameters (see section 4.3)
	SWR request	Not Present
	SWR response	Not Present

For the INF field of an S(IFS request) block:

- A value from '01' to 'FE' shall be coded on 1 byte.
- A value from '00FF' to '0FF9' (4089) shall be coded on 2 bytes.
- Values beyond '0FF9' (4089) are invalid (see details in section 4.2.5).

4.2.5 Epilogue Field Format

The Epilogue field conveys the Error Detection Code of the block.

In this version of the specification, a 2-byte CRC shall be used. Note that such a CRC can only efficiently protect ($2^{15} - 1$) bits (including itself) from 1, 2, and 3 bits corruption. For this reason, the size of INF fields in this protocol is limited to a maximum value of '0FF9' (4089) bytes.

4.3 Communication Interface Parameters

The CIP contains the communication interface parameters (i.e. both Physical Layer and Data Link Layer parameters) that the HD shall use to communicate with the SE, as well as Historical Bytes. To retrieve the CIP, the HD shall send an S(CIP request) block (see section 4.2) and receive an S(CIP response) block containing the CIP structure described in the following sections. This procedure may be used anytime (although rather expected to be used upon power on or after a warm reset).

In the following sections, all numerical values are encoded as unsigned integers.

4.3.1 CIP – Common Structure

This section describes the common structure of the CIP, irrespective of the Physical Layer that is used.

Table 4-5: CIP – Common Structure

Name	Length	Description
PVER	1	Protocol Version This version of the specification defines version '01' of the protocol.
RID	5	RID according to [7816-4]
PLID	1	Physical Layer ID: '01' for SPI / '02' for I ² C
Length of PLP	1	Length of Physical Layer Parameters
PLP	Var.	Physical Layer Parameters Either data describing the SPI Physical Layer, as defined in Table 4-7, or data describing the I ² C Physical Layer, as defined in Table 4-8.
Length of DLLP	1	Length of Data Link Layer Parameters
DLLP	Var.	Data Link Layer Parameters: See Table 4-6
Length of HB	1	Length of Historical Bytes
HB	Var.	Historical Bytes

4.3.2 CIP – Specific Parameters for Data Link Layer

This section describes the parameters provided by the CIP for the Data Link Layer.

Table 4-6: CIP – Specific Parameters for Data Link Layer

Name	Length	Description
BWT	2	Block Waiting Time (in ms)
IFSC	2	Maximum Information Field Size of the SE (in bytes) (i.e. initial value)

NOTE: To enable a certain level of compatibility with higher versions of the protocol (if any are defined in the future), HD implementations shall accept more data (not described in the table above) to be present at the end of Data Link Layer Parameters and ignore such data.

4.3.3 CIP – Specific Parameters for SPI Physical Layer

This section describes the parameters provided by the CIP when the SPI Physical Layer is used.

Table 4-7: CIP – Specific Data for SPI Physical Layer

Name	Length	Description	Presence
Configuration	1	RFU	Mandatory
PWT	1	Power Wake-Up Time (in ms; see section 3.1.3)	Mandatory
MCF	2	Maximum Clock Frequency (in kHz; see section 3.1.2.1)	Mandatory
PST	1	Power Saving Timeout (in ms; see Chapter 5)	Mandatory
MPOT	1	Minimum Polling Time (in ms; see NOTE 2 below)	Mandatory
SEGT	2	Secure Element Guard Time (in μ s; see section 3.1.2.3)	Mandatory
SEAL	2	Maximum SE Access Length (in bytes; see NOTE 3 below)	Mandatory
WUT	2	Wake-Up Time (in μ s; see section 3.1.4)	Mandatory

NOTE 1: To enable a certain level of compatibility with higher versions of the protocol (if any are defined in the future), HD implementations shall accept more data (not described in the table above) to be present at the end of Physical Layer Parameters and ignore such data.

NOTE 2: See section 3.1.5. If the Polling Mechanism is **not** used, MPOT shall be set to '00'.

NOTE 3: See section 3.1.2.3. A SEAL value set to 'FFFF' shall be interpreted as the SE leveraging Direct Memory Access (DMA), meaning the HD may virtually send any amount of data per SPI access. In such a case, the SE may indicate an appropriate SEGT value accordingly.

4.3.4 CIP – Specific Parameters for I²C Physical Layer

This section describes the parameters provided by the CIP when the I²C Physical Layer is used.

Table 4-8: CIP – Specific Parameters for I²C Physical Layer

Name	Length	Description	Presence
Configuration	1	Characteristics supported by SE: <ul style="list-style-type: none"> - b1 = 0: Clock stretching not supported - b1 = 1: Clock stretching supported - Other bits RFU 	Mandatory
PWT	1	Power Wake-Up Time (in ms; see section 3.2.3)	Mandatory
MCF	2	Maximum Clock Frequency (in kHz; see section 3.2.2)	Mandatory
PST	1	Power Saving Timeout (in ms; see Chapter 5)	Mandatory
MPOT	1	Minimum Polling Time (in ms; see sections 3.2.4 and 3.2.6)	Mandatory
RWGT	2	R/W Guard Time (in μ s; see sections 3.2.5 and 3.2.7)	Mandatory

NOTE: To enable a certain level of compatibility with higher versions of the protocol (if any are defined in the future), HD implementations shall accept more data (not described in the table above) to be present at the end of Physical Layer Parameters and ignore such data.

5 Power Saving Policy

The SE may decide to enter Power Saving Mode in order to save battery (typically the host device battery). The conditions under which an SE implementation would enter such a mode usually depend on high-level applicative use cases defining requirements regarding performance, availability, battery saving, etc. As it might be impossible to capture a set of such conditions that would fit all use cases, this specification acknowledges the fact that a particular SE implementation may decide to enter Power Saving Mode according to proprietary policies. Nevertheless, this document specifies the following interoperable policy for the SE:

- The SE may only enter Power Saving Mode
 - On receipt of an S(RELEASE request) block (see section 4.2.2) and after returning the corresponding S(RELEASE response) block, or
 - After a timeout if the HD didn't send any new Data Link Layer block after any of the following events:
 - Completion of boot (upon Power-On)
 - SE returned an R-block or S-block (including S(SWR response))
 - SE returned an I-block completing the sending of an APDU response (or last APDU response of a chain if APDU chaining is used).

While this policy guarantees that the SE will only enter Power Saving Mode when one of the above conditions are satisfied, the SE may choose not to do so (i.e. even if above conditions are satisfied) for other proprietary reasons.

- The SE shall indicate the applicable timeout value as part of the CIP (see section 4.3).
 - If the timeout value is set to '00', the SE indicates that it may actually enter Power Saving Mode whenever it wants. An SE that implements a proprietary policy should indicate this value. It is assumed that the HD implementation is aware of and can adapt its behavior to such a proprietary policy.
 - If the timeout value is set to 'FF', the SE indicates that it doesn't use this timeout value and therefore may only enter Power Saving Mode on receipt of an S(RELEASE request) block.
 - Any other value (from '01' to 'FE') shall be understood as a valid timeout value. Note that the HD should apply some margin when measuring timeouts.

Upon power-on, if the HD expects the SE to implement the above interoperable policy and is not aware of the applicable timeout value (e.g. CIP not retrieved yet), it shall assume that the SE may have already entered Power Saving Mode.

It is assumed that, in case the SE would implement a proprietary Power Saving Policy (or only partially behave according to the above interoperable policy), the HD would have enough knowledge of such a proprietary policy to adapt its own behavior.