



Lite-On Custom PiP User Manual



80179403-001 Rev. A
26 December 2022

ID TECH
10721 Walker Street, Cypress, CA 90630-4720
Tel: (714) 761-6368 Fax (714) 761-8880
www.idtechproducts.com

Copyright © 2022 International Technologies and Systems Corporation. All rights reserved.

ID TECH
10721 Walker Street
Cypress, CA 90630 USA

This document, as well as the hardware and software it describes, is furnished under license and may only be used in accordance with the terms of such license. The content of this paper is furnished for informational use, subject to change without notice, and not to be construed as a commitment by ID TECH. ID TECH assumes no responsibility or liability for any errors or inaccuracies that may appear in this document.

Except as permitted by such license, no part of this publication may be reproduced or transmitted by electronic, mechanical, recorded, or any other method, or translated into another language or language form without the express written consent of ID TECH. ID TECH is a registered trademark of International Technologies and Systems Corporation. ViVOpay and Value through Innovation are trademarks of International Technologies and Systems Corporation. Other trademarks are the property of the respective owner.

Warranty Disclaimer: The services and hardware are provided "as is" and "as-available," and the use of these services and hardware are at the user's own risk. ID TECH does not make, and hereby disclaims, any and all other express or implied warranties, including, but not limited to warranties of merchantability, title, fitness for a particular purpose, and any warranties arising from any course of dealing, usage, or trade practice. ID TECH does not warrant that the services or hardware will be uninterrupted, error-free, or completely secure.

Federal Communication Commission Interference Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Radiation Exposure Statement:

The product complies with the FCC portable RF exposure limit set forth for an uncontrolled environment and are safe for intended operation as described in this manual. The further RF exposure reduction can be achieved if the product can be kept as far as possible from the user body or set the device to lower output power if such function is available.

This module is intended for OEM integrators only. Per FCC KDB 996369 D03 OEM Manual v01 guidance, the following conditions must be strictly followed when using this certified module:

KDB 996369 D03 OEM Manual v01 rule sections:

2.2 List of applicable FCC rules

This module has been tested for compliance to FCC Part **15**

2.3 Summarize the specific operational use conditions

The module is tested for standalone mobile RF exposure use condition. Any other usage conditions such as co-location with other transmitter(s) or being used in a portable condition will need a separate reassessment through a class II permissive change application or new certification.

2.4 Limited module procedures

Not applicable.

2.5 Trace antenna designs

Not applicable.

2.6 RF exposure considerations

This equipment complies with FCC mobile radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20cm between the radiator & your body. If the module is installed in a portable host, a separate SAR evaluation is required to confirm compliance with relevant FCC portable RF exposure rules.

2.7 Antennas

The following antennas have been certified for use with this module; antennas of the same type with equal or lower gain may also be used with this module. The antenna must be installed such that 20 cm can be maintained between the antenna and users.

Antenna Type	Loop Antenna
Antenna connector	N/A

2.8 Label and compliance information

The final end product must be labeled in a visible area with the following: “Contains **FCC ID: WQJ-PIPOEM**”. The grantee's FCC ID can be used only when all FCC compliance requirements are met.

2.9 Information on test modes and additional testing requirements

This transmitter is tested in a standalone mobile RF exposure condition and any co-located or simultaneous transmission with other transmitter(s) or portable use will require a separate class II permissive change re-evaluation or new certification.

2.10 Additional testing, Part 15 Subpart B disclaimer

This transmitter module is tested as a subsystem and its certification does not cover the FCC Part 15 Subpart B (unintentional radiator) rule requirement applicable to the final

host. The final host will still need to be reassessed for compliance to this portion of rule requirements if applicable.

As long as all conditions above are met, further transmitter test will not be required. However, the OEM integrator is still responsible for testing their end-product for any additional compliance requirements required with this module installed.

IMPORTANT NOTE: In the event that these conditions can not be met (for example certain laptop configurations or co-location with another transmitter), then the FCC authorization is no longer considered valid and the FCC ID can not be used on the final product. In these circumstances, the OEM integrator will be responsible for re-evaluating the end product (including the transmitter) and obtaining a separate FCC authorization.

Manual Information To the End User

The OEM integrator has to be aware not to provide information to the end user regarding how to install or remove this RF module in the user's manual of the end product which integrates this module.

The end user manual shall include all required regulatory information/warning as show in this manual.

OEM/Host manufacturer responsibilities

OEM/Host manufacturers are ultimately responsible for the compliance of the Host and Module. The final product must be reassessed against all the essential requirements of the FCC rule such as FCC Part 15 Subpart B before it can be placed on the US market. This includes reassessing the transmitter module for compliance with the Radio and EMF essential requirements of the FCC rules. This module must not be incorporated into any other device or system without retesting for compliance as multi-radio and combined equipment.

Industry Canada statement:

This device complies with ISED's licence-exempt RSSs. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Le présent appareil est conforme aux CNR d'ISED applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

Radiation Exposure Statement:

The product comply with the Canada portable RF exposure limit set forth for an uncontrolled environment and are safe for intended operation as described in this manual. The further RF exposure reduction can be achieved if the product can be kept as far as possible from the user body or set the device to lower output power if such function is available.

Déclaration d'exposition aux radiations:

Le produit est conforme aux limites d'exposition pour les appareils portables RF pour les Etats-Unis et le Canada établies pour un environnement non contrôlé.

Le produit est sûr pour un fonctionnement tel que décrit dans ce manuel. La réduction aux expositions RF peut être augmentée si l'appareil peut être conservé aussi loin que possible du corps de l'utilisateur ou que le dispositif est réglé sur la puissance de sortie la plus faible si une telle fonction est disponible.

This device is intended only for OEM integrators under the following conditions: (For module device use)

1) The transmitter module may not be co-located with any other transmitter or antenna.

As long as **the condition above is** met, further transmitter test will not be required. However, the OEM integrator is still responsible for testing their end-product for any additional compliance requirements required with this module installed.

Cet appareil est conçu uniquement pour les intégrateurs OEM dans les conditions suivantes: (Pour utilisation de dispositif module)

1) Le module émetteur peut ne pas être coïmplanté avec un autre émetteur ou antenne.

Tant que **la condition** ci-dessus sont remplies, des essais supplémentaires sur l'émetteur ne seront pas nécessaires. Toutefois, l'intégrateur OEM est toujours responsable des essais sur son produit final pour toutes exigences de conformité supplémentaires requis pour ce module installé.

IMPORTANT NOTE:

In the event that these conditions can not be met (for example certain laptop configurations or co-location with another transmitter), then the Canada authorization is no longer considered valid and the IC ID can not be used on the final product. In these circumstances, the OEM integrator will be responsible for re-evaluating the end product (including the transmitter) and obtaining a separate Canada authorization.

NOTE IMPORTANTE:

Dans le cas où ces conditions ne peuvent être satisfaites (par exemple pour certaines configurations d'ordinateur portable ou de certaines co-localisation avec un autre émetteur), l'autorisation du Canada n'est plus considéré comme valide et l'ID IC ne peut pas être utilisé sur le produit final. Dans ces circonstances, l'intégrateur OEM sera chargé de réévaluer le produit final (y compris l'émetteur) et l'obtention d'une autorisation distincte au Canada.

End Product Labeling

The product can be kept as far as possible from the user body or set the device to lower output power if such function is available. The final end product must be labeled in a visible area with the following: "Contains IC:9847A-PIPOEM".

Plaque signalétique du produit final

L'appareil peut être conservé aussi loin que possible du corps de l'utilisateur ou que le dispositif est réglé sur la puissance de sortie la plus faible si une telle fonction est disponible. Le produit final doit être étiqueté dans un endroit visible avec l'inscription suivante: "Contient des IC: 9847A-PIPOEM".

Manual Information To the End User



The OEM integrator has to be aware not to provide information to the end user regarding how to install or remove this RF module in the user's manual of the end product which integrates this module.

The end user manual shall include all required regulatory information/warning as show in this manual.

Manuel d'information à l'utilisateur final

L'intégrateur OEM doit être conscient de ne pas fournir des informations à l'utilisateur final quant à la façon d'installer ou de supprimer ce module RF dans le manuel de l'utilisateur du produit final qui intègre ce module. Le manuel de l'utilisateur final doit inclure toutes les informations réglementaires requises et avertissements comme indiqué dans ce manuel.

Cautions and Warnings

	Caution: The LITE-ON CUSTOM PIP should be mounted 1-2 feet away from other PiPs. Can be adjusted based on lane setup.
	Warning: Avoid close proximity to radio transmitters which may reduce the capability of the reader.

Revision History

Date	Rev	Changes	By
12/26/2022	A	Initial release	EC

Table of Contents

1. OVERVIEW	9
1.1. Universal SDK	9
1.2. Encryption	9
1.3. Features.....	9
1.4. Approvals.....	9
1.5. Regulatory	9
1.6. Model Number	10
2. LITE-ON CUSTOM PIP SPECIFICATIONS	11
3. LITE-ON CUSTOM PIP INSTALLATION	11
3.1. Parts List	11
3.2. Mounting the Lite-On Custom PiP.....	12
3.2.1. Mounting Screws.....	12
3.3. Connecting to Power	12
3.4. Connecting to the Data Port.....	12
3.5. Using the LITE-ON CUSTOM PIP for Value-Added Services	12
3.6. Making a VAS Transaction	12
3.7. Notes on Installation Locations.....	13
4. LITE-ON CUSTOM PIP LED STATUS INDICATOR	14
5. RF INTERFERENCE	14
6. FIRMWARE COMMANDS.....	16
6.1. ECC Key Management	16
6.1.1. ECC Key Pair.....	16
6.1.2. How to Create an ECC Key Pair Using Open-SSL.....	16
6.1.3. How To Extract Key Data To Load In The Lite-On Custom PiP	17
6.2. Google Pay Smart Tap 2.1 Commands	18
6.2.1. Set Configurable Group (04-03)	18
6.2.2. Set SmartTap LTPK (C7-65)	19
6.3. Apple VAS Firmware Commands.....	21
6.3.1. Set Merchant Record (04-11)	21
6.3.2. Set Private Key (C7-66)	23
6.3.3. Set Configuration (04-00)	24
6.4. Lite-On Custom PiP Firmware Commands for Both Platforms.....	26
6.5. Poll On Demand and Auto Poll Settings	26
6.6. Non-Payment Card Switching Support.....	26
7. FIRMWARE UPGRADE	28
8. CUSTOMER SUPPORT.....	29

1. Overview

The ID TECH PIP OEM is a compact, standalone NFC device, designed to support loyalty programs that register via NFC phones. It is also great as an access control device as it supports Apple VAS and Google Smart Tap as well as Mifare and other closed-loop protocols.

1.1. Universal SDK

A feature-rich Windows-based Universal SDK is available to aid rapid development of applications that talk to PIP OEM. The SDK is available for the C# language on Windows and comes with sample code for demo apps. To obtain the SDK and other useful utilities, demos, and downloads, be sure to check the Downloads link on the [ID TECH Knowledge Base](#) (no registration required).

1.2. Encryption

LITE-ON CUSTOM PIP supports ECC.

1.3. Features

LITE-ON CUSTOM PIP supports the following:

- Apple VAS
- Google Pay Smart Tap
- Mifare 1K/4K, Plus, DesFire, Ultralight
- UART
- Suitable for retail, entertainment, and other locations that use loyalty value-added services but do not require payment
- Consumer Intuitive: Equipped with an LED and sound to provide visual and audible cues to enable a smooth and seamless experience
- Buzzer sound notification

This document assumes that users are familiar with their host systems and all related functions.

1.4. Approvals

- Apple VAS & Google SmartTap

1.5. Regulatory

- FCC Part 15
- CE Mark
- UL certified(PCB material to be UL approved and with UL marking)
- REACH
- PMN: PIPOEM

1.6. Model Number

- IDP-05-L1

2. Lite-On Custom PiP Specifications

Hardware	
MTBF	50,000 POH (Minimum)
Transmitter Frequency	13.56 MHz +/- 0.01%
Transmitter Modulation	ISO 14443-2 Type A Rise/Fall Time: 2-3 µsec. Rise, < 1 µsec fall ISO14443-2 Type B Rise/Fall Time: < 2 µsec. each; 8% - 14% ASK
Receiver Subcarrier Frequency	847.5 KHz
Receiver Subcarrier Data	ISO 14443-2 Type A: Modified Manchester ISO 14443-2 Type B: NRZ-L, BPSK ISO 18092 ISO 21481 (PCD & NFC) ISO 15693 (under evaluation / Hardware Ready)
Typical Read Range	0-4cm, depends on card type, setup environment
Physical	
Length	78 mm
Width	53mm
Depth	4.8mm
Environmental	
Operating Temperature	-40°C to 85°C (-40°F to 185°F) [non-condensing]
Storage Temperature	-40°C to 85°C (-40°F to 185°F) [non-condensing]
Operating Humidity	Maximum 95% (non-condensing)
Storage Humidity	Maximum 95% (non-condensing)
Transit Humidity	Maximum 95% (non-condensing)
Operating Environment	Outdoor
IK Rating	N/A
IP Rating	N/A
Electrical	
Reader Input Voltage	+5V (UART port-powered)
Power Consumption	Idle mode: <1W Polling mode: <2.5W

3. LITE-ON CUSTOM PIP Installation

This section provides information on installing a Lite-On Custom PiP.

3.1. Parts List

Verify that you have the following hardware for installing the Lite-On Custom PiP:

- PIP OEM
- Customized UART cable

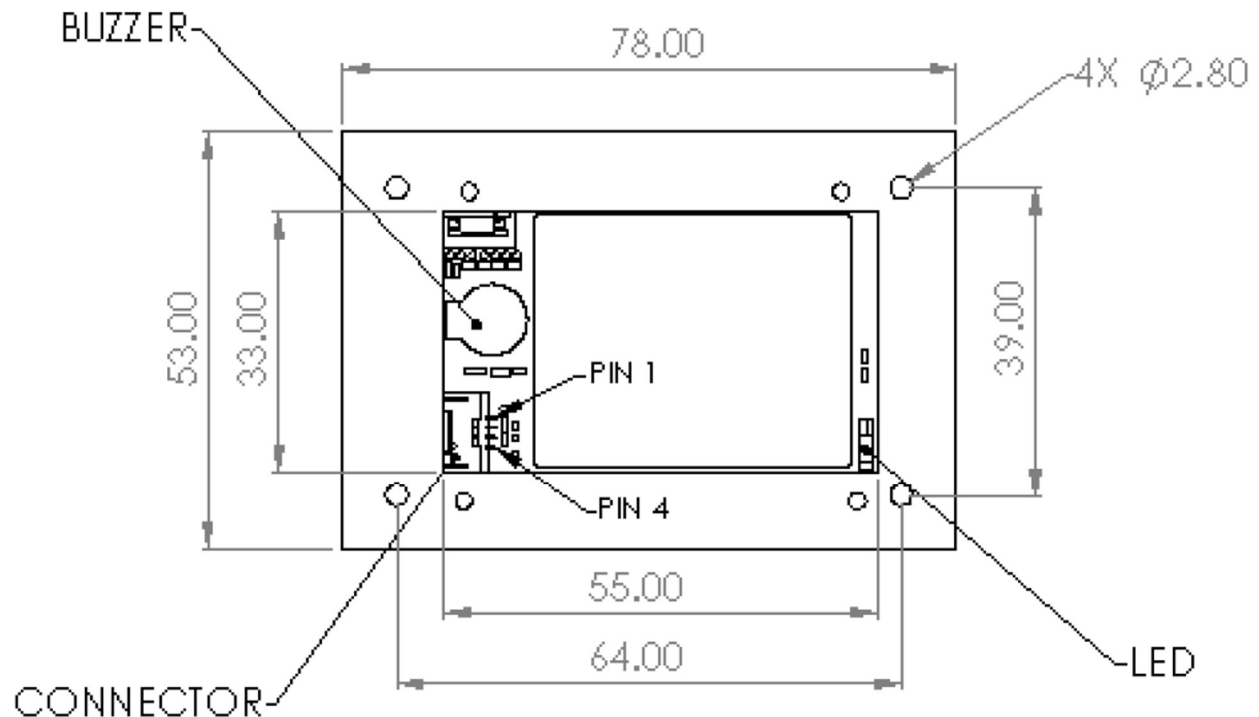
3.2. Mounting the Lite-On Custom PiP

Warning: The RF field of the LITE-ON CUSTOM PiP is sensitive to the proximity of metal. There are three options for mounting the LITE-ON CUSTOM PiP to a metal surface:

- Lite-On Custom PiP must not be installed behind any metal surfaces or materials that have metallic content, which blocks the RF field.
- Mount Lite-On Custom PiP a minimum of 2cm away from any metal surface.
- Keep the RF-emitting surface of Lite-On Custom PiP at least 2cm from any metal.

3.2.1. Mounting Screws

The back of the LITE-ON CUSTOM PiP has four holes for mounting screws (4X $\Phi 2.80$). Make sure that the depth of the screws used for mounting does not exceed 4mm.



3.3. Connecting to Power

The Lite-On Custom PiP is powered through the System connector.

3.4. Connecting to the Data Port

The Lite-On Custom PiP transfers data via the system connector by UART signal.

3.5. Using the LITE-ON CUSTOM PiP for Value-Added Services

This tests the Lite-On Custom PiP's ability to read an NFC phone or closed-loop tap card.

3.6. Making a VAS Transaction

The LITE-ON CUSTOM PiP allows for customer loyalty program services using Contactless (NFC) technology. To make a VAS transaction:









1. Present the phone in close proximity to the front portion of the PiP.
2. Orient the phone so that maximum surface area is parallel to the PiP.
3. The phone used for the test should display a rewards screen (steps for using that screen depend on the phone platform).
4. The Lite-On Custom PiP beeps once to indicate a successful VAS transaction.

3.7. Notes on Installation Locations

- The LITE-ON CUSTOM PIP is designed to be mounted on a surface and in close proximity to any internal motors and electrical devices that may be operating inside a point-of-sale area. However, the LITE-ON CUSTOM PIP is susceptible to RF and electromagnetic interference. It is important that the unit not be mounted near (within 3 or 4 feet) large electric motors, computer UPS systems, microwave transmitters (Wi-Fi routers), anti-theft devices, radio transmitters, communications equipment and so on.
- Tie all cables neatly with nylon cable-ties and route them so that they are inaccessible and invisible to customers.
- Test the LITE-ON CUSTOM PIP installation using a test card to perform an end-to-end VAS transaction. Even if the transaction is declined (as it should be with a test card), it will prove connectivity all the way through the system. If possible, a manager or some other responsible party should test each LITE-ON CUSTOM PIP on a regular basis (perhaps at the start of each day or at least once per week) with a test card to ensure continued operation and functionality. If the LITE-ON CUSTOM PIP is rebooted on a regular basis (such as every night), it is important to test the contactless reader as soon as possible afterwards to ensure continued communication to the LITE-ON CUSTOM PIP host.

4. LITE-ON CUSTOM PIP LED Status Indicator

The LITE-ON CUSTOM PIP has an LED indicator on the front of the device to indicate reader status.

	LED1 (Blue)	LED2 (Red)	Beeper
Ready for Transaction	 blink 5s	 off	Off
Transaction Started	 on	 off	Off
Transaction Successful	 blink	 on	Beeps Once
Transaction Failed	 off	 blink	Beeps Twice

5. RF Interference

Q. Why do I need to know about RF interference?

A. Contactless communication uses radio frequency technology to send phone data to a contactless terminal reader.

Q. How can RF interference affect contactless communication?

A. RF interference can cause data errors. If RF interference is present, contactless communication devices may operate intermittently or inconsistently.

Q. Where does RF interference come from?

A. Radio frequency interference (RFI) can originate from a wide number of sources at VAS-related locations. Some examples of sources of RF energy and RF interference include:

- AM/FM radio and TV transmitters
- 2-way radios and pagers
- Mobile telephones
- Power lines and transformers
- Medical equipment
- Microwaves
- Electromechanical switches

Q. What should I do if I suspect RF interference exists in my environment?

A. Begin by inspecting your environment for possible sources of RF interference.

Q. Do equipment manufacturers test their devices for RF interference?

A. Electronic equipment is tested for RFI sensitivity by the manufacturers. These tests are performed in a controlled laboratory environment and will often not replicate the types of devices that would be encountered in your point-of-sale (POS) environment.

Q. What RF levels will impact RF operations?

A. Factors that can cause RF interference vary case-by-case. There are no set rules defining a single RF level that will cause RFI. RFI depends on the sensitivity of the equipment under consideration, or how low an interpreting signal can be in the presence of the equipment and cause problems.

Equipment can be particularly sensitive to very low signal levels of one frequency and yet be quite immune to high signal levels of another frequency - so frequency is an important factor. Some electronic system components are internally shielded and have a very high immunity to interference; but generally, most equipment has not been so engineered.

6. Firmware Commands

The following firmware commands apply to LITE-ON CUSTOM PIP reader configuration. See the *NEO Interface Developer's Guide* for full details.

6.1. ECC Key Management

The section below describes ECC Key management for LITE-ON CUSTOM PIP devices.

6.1.1. ECC Key Pair

Merchants or other administrators who wish to use SmartTap must create and manage the Elliptical Curve Cryptography (ECC) key pair used to for securing communication between the reader and the wallet.

- **Public Key:** administrators must communicate the public key to Google. It is public and can be visible to anyone.
- **Private Key:** the private key must be kept private and injected into the ViVOpay device, where it will be stored securely.

6.1.2. How to Create an ECC Key Pair Using Open-SSL

Users have several options for generating the ECC key pair (or the ECDSA digital signature key pair). The example below uses the freely available OpenSSL package to generate a prime256v1 Elliptical Curve Cipher key pair (and to sign messages).

To generate EC private key:

```
openssl> ecparam -out PRIVATE.key.pem -name prime256v1 -genkey
```

To generate EC public key from private key:

```
openssl> ec -in PRIVATE.key.pem -pubout -out PUBLIC.key.pem -conv_form  
compressed
```

Sign message:

```
openssl> dgst -sha256 -sign LONG_TERM_PRIVATE.pem message.txt >  
signature.bin
```

Verify message:

```
openssl> dgst -sha256 -verify LONG_TERM_PUBLIC.pem -signature  
signature.bin message.txt
```


Generate ECDH shared secret:

```
openssl> pkeyutl -derive -inkey TERMINAL_EPHEMERAL_PRIVATE.pem -  
peerkey HANDSET_EPHEMERAL_PUBLIC.pem -out secret.bin
```

6.1.3. How To Extract Key Data To Load In The Lite-On Custom PiP

Having generated the ECC Key Pair, the Lite-On Custom PiP requires the Private Key data to be loaded so that it can decrypt the pass information sent from the mobile device. To extract the required Key Data, use the following OpenSSL command line:

```
>openssl.exe ec -noout -text -in private_key.pem
```

This will output information to the screen. You should see the below as a minimum:

```
Private-Key: (256 bit)  
priv:  
  00:f5:36:87:08:93:39:20:55:3b:7b:9f:fb:16:ae:  
  ed:9c:77:d5:bf:d9:66:2a:f1:49:a6:b9:f9:65:b7:  
  3f:0c:ca
```

Copy the bytes of data and edit them to remove the colon characters. If, as in the example above, there are 33 bytes of data, remove the leading 00 to leave 32 bytes of key data. These are used in the **C7-65** and **C7-66** commands detailed later in this document.

6.2. Google Pay Smart Tap 2.1 Commands

The following commands apply to Google Pay Smart Tap 2.1.

6.2.1. Set Configurable Group (04-03)

The **Set Configurable Group** command creates or modifies a TLV Group. Configure a specific TLV Group by passing the TLVs with the desired functionality and a unique TLV Group Number to the reader. The Google Pay Smart Tap feature is controlled using the Configuration Group 142 (0x8E).

Command Frame

Byte 0-9	Byte 10	Byte 11	Byte 12	Byte 13	Byte 14 ... Byte 14+n-1	Byte 14+n	Byte 15+n
Header Tag & Protocol Version	Command	Sub- Command	Data Length (MSB)	Data Length (LSB)	Data	CRC (LSB)	CRC (MSB)
ViVOtech2\0	04h	03h			TLV Data Objects		

Response Frame

Byte 0-9	Byte 10	Byte 11	Byte 12	Byte 13	Byte 14	Byte 15
Header Tag & Protocol Version	Command	Status Code	Data Length (MSB)	Data Length (LSB)	CRC (MSB)	CRC (LSB)
ViVOtech2\0	04h	See Status Code Table	00h	00h		

6.2.1.1. Example Usage

Further information on the TLV Data Objects that can be set in the command frame are described in detail in the *Google Pay Smart Tap 2.1 In ViVOpay Devices* document. The settings used with ID TECH's Demo Pass are shown below:

FFE4018E..... Group Number 142 (0x8E)
DFEE3B0405318C74..... Collector ID (87133300)
DFEE3C00..... Store Location ID (Empty)
DFEE3D00 Terminal ID (Empty)
DFEF2500 Merchant Name (Empty)
DFED0100 Merchant Category (Empty)
DFED02050000000001 PoS Capability Bitmap
DFED030101 Retry Times (01)
DFED040101 Select OSE Support (01)
DFED050101 Skip Second Select Support (01)
DFED060100 Stop payment if SmartTap 2.1 failed (00)
DFED070100 Pre-signed support (00)
DFED27010D Delimiter for Service Objects (0x0D)
DFED3F0100..... VAS encryption flag (00)

DFED490100 VAS-only global override (00)
 DFEF770100 Multiple Service Objects enabled/disabled (00)

To set these default values in your Lite-On Custom PiP, use the USDK Demo App and select the “Send NEO Command option. Set the command fields as below, the press **Execute Command** to set the values:

- Cmd: 04
- Sub: 03
- Hex Data:
 FFE4018EDFEE3B0405318C74DFEE3C00DFEE3D00DFEF2500DFED0100DFED02
 050000000001DFED030101DFED040101DFED050101DFED060100DFED070100
 DFED27010DDFED3F0100DFED490100DFEF770100

6.2.2. Set SmartTap LTPK (C7-65)

For direct injection of the LTPK, send firmware command **C7-65** via serial connection to the (offline) device. Developers should observe good cryptographic practices by, for example, injecting devices in a secure setup.

Command Frame

Byte 0-9	Byte 10	Byte 11	Byte 12	Byte 13	Byte 14	Byte 15	Byte 16
Header Tag & Protocol Version	Command	Sub- Command	Data Length (MSB)	Data Length (LSB)	Data	CRC (LSB)	CRC (MSB)
ViVOtech2\0	C7h	65h	0x00	0x24	See Command Data Table		

Command Data

Data Item	Length (bytes)
Version	4
Long term private key	32

Response Frame

Byte 0-9	Byte 10	Byte 11	Byte 12	Byte 13	Byte 14	Byte 15
Header Tag & Protocol Version	Command	Status Code	Data Length (MSB)	Data Length (LSB)	CRC (MSB)	CRC (LSB)
ViVOtech2\0	C7h	See Status Code Table	00h	00h		

6.2.2.1. Example Usage

To load the Google Pay Long Term Private Key in your Lite-On Custom Lite-On Custom PiP for use with the ID TECH Demo Pass, the values used are shown below:

Version: 0000000A

Data:

F5368708933920553B7B9FFB16AEED9C77D5BFD9662AF149A6B9F965B73F0C
CA

The Data shown was obtained in Section 6.1.3.

To set these default values in your Lite-On Custom PiP, use the USDK Demo App and select the Send NEO Command option. Set the command fields as below, then press **Execute Command** to set the values:

- Cmd: C7
- Sub: 65
- Hex Data:
F5368708933920553B7B9FFB16AEED9C77D5BFD9662AF149A6B9F965B73F0CCA

6.3. Apple VAS Firmware Commands

The following commands apply to Apple VAS.

6.3.1. Set Merchant Record (04-11)

The **Set Merchant Record** command sets the merchant the PIP OEMreader uses for loyalty points.

Command Frame

Byte 0-9	Byte 10	Byte 11	Byte 12	Byte 13	Byte 14 ... Byte 14+n-1	Byte 14+n	Byte15+n
Header Tag & Protocol Version	Command	Sub- Command	Data length (MSB)	Data length (LSB)	Data	CRC (MSB)	CRC (LSB)
ViVOtech2\0	04	11h					

Data Field for Command Frame

Data Field	Length (bytes)	Description
Merchant Record Index	1	The valid value is 1-6. Up to 6 records can be set.
ID Present	1	1: The Merchant ID is valid. 0: The Merchant ID is not valid.
Merchant ID	32	The value of tag 9F25. SHA256 of pass name.
Length of Merchant URL	1	Can be zero, if no URL is used (real Merchant URL Length).
Merchant URL	64	The value of tag 9F29, padded with trailing zeroes to 64 bytes.
Length of Terminal Application Version Number	1	Optional. Can be zero, if no terminal application version number is used (terminal application version number buffer is 2 bytes).
ApplePay Terminal Application Version Number	var	Optional. The value of tag 9F22.

Response Frame

Byte 0-9	Byte 10	Byte 11	Byte 12	Byte 13	Byte 14	Byte 15
Header Tag & Protocol Version	Command	Status	Data length (MSB)	Data length (LSB)	CRC(MSB)	CRC(LSB)
ViVOtech2\0	04h	See Status Code Table	00	00		

6.3.1.1. Example Usage

Further information on the TLV Data Objects that can be set in the command frame are described in detail in the *Apple VAS In ViVOpay Devices* document. The settings used with ID TECH's Demo Pass are shown below:

- [illegible]

To set these default values in your Lite-On Custom Lite-On Custom PiP, use the SDK Demo App and select the Send NEO Command option. Set the command fields as below, then press Execute Command to set the values:

- [illegible]

6.3.2. Set Private Key (C7-66)

The **Set Private Key** command loads the private key associated with the Merchant's Apple VAS pass into the ViVOpay device. This allows the reader to decrypt the pass data.

Note: The **Set Private Key (C7-66)** command only works on non-SRED readers; Lite-On Custom PIP s are not SRED.

Command Frame

Byte 0-9	Byte 10	Byte 11	Byte 12	Byte 13	Byte 14 ... Byte 14+n-1	Byte 14+n	Byte15+n
Header Tag & Protocol Version	Command	Sub- Command	Data length (MSB)	Data length (LSB)	Data	CRC (MSB)	CRC (LSB)
ViVOtech2\0	C7	66h	0020h or 0021h		Data		

Command Frame Data Field

Data Field	Length (bytes)	Description
Merchant Record Index	1 or 0 (OTP)	If the Merchant Record Index does not exist, this Private Key is used by all Merchant IDs. If the Merchant Record Index exists, this Private Key is used for the specified Merchant ID. The valid value is 1-6. It can be set for 6 records.
Private Key	32	Apple VAS Private Key.

Response Frame

Byte 0-9	Byte 10	Byte 11	Byte 12	Byte 13	Byte 14 ... Byte 14+n-1	Byte 14+n	Byte15+n
Header Tag & Protocol Version	Command	Status	Data length (MSB)	Data length (LSB)	Data	CRC (MSB)	CRC (LSB)
ViVOtech2\0	C7	See Status Code Table, NEO 2 IDG	00h	00h			

Note 1: The private key should be 32 bytes long. If the private key is injected and tag DFED3F bit 2 set to **1**, the reader will decrypt VAS data (tag 9F27).

6.3.2.1. Example Usage

To load the Apple VAS Private Key in your Lite-On Custom PiP for use with the ID TECH Demo Pass, the values used are shown below:

- **Data:**
F5368708933920553B7B9FFB16AEED9C77D5BFD9662AF149A6B9F965B73F0C
CA

The Data shown was obtained in Section 6.1.3.

To set these default values in your Lite-On Custom PiP, use the USDK Demo App and select the Send NEO Command option. Set the command fields as below, then press Execute Command to set the values:

- **Cmd:** C7
- **Sub:** 66
- **Hex Data:**
0000000AF5368708933920553B7B9FFB16AEED9C77D5BFD9662AF149A6B9F965B
73F0CCA

6.3.3. Set Configuration (04-00)

Use this command to set or change the values of the specified Tag Length Value (TLV) data objects in the reader. It can be used to set parameters for Auto Poll as well as Poll on Demand Mode.

When the reader receives this command, it extracts the TLV encoded parameters from the data portion of the command and saves them to the default TLV Group in non-volatile memory. If a TLV data object is incorrectly formatted, the reader stops processing the object. A single command may contain more than one TLV data object. This command can be used to set any EMV TLV object in the reader.

Note: The **Set Configuration** command is the only mechanism for setting global configuration parameter values.

Command Frame

Byte 0-9	Byte 10	Byte 11	Byte 12	Byte 13	Byte 14 ... Byte 14+n-1	Byte 14+n	Byte 15+n
Header Tag & Protocol Version	Command	Sub- Command	Data Length (MSB)	Data Length (LSB)	Data	CRC (LSB)	CRC (MSB)
ViVotech2\0	04h	00h			TLV Data Objects		

Response Frame

Byte 0-9	Byte 10	Byte 11	Byte 12	Byte 13	Byte 14	Byte 15
Header Tag & Protocol Version	Command	Status Code	Data Length (MSB)	Data Length (LSB)	CRC (MSB)	CRC (LSB)

ViVOtech2\0	04h	See Status Code Table	00h	00h		
-------------	-----	--------------------------	-----	-----	--	--

6.3.3.1. Tag DFED3F: VAS Encryption

Tag DFED3F controls VAS encryption options. The Tag is set to Group 0.

DFED3F	Optional	VAS encryption on/off flag Bit 0: Encrypt VAS data with device's data encryption key Bit 1: Decrypt Apple VAS data with Apple VAS private key Bit 2 to 7: RFU
--------	----------	--

For example:

- 56 69 56 4F 74 65 63 68 32 00 ViVOtech2\0
- 04 00 Set configuration
- 00 05 Data length
- DF ED 3F 01 01 Enable both the encryption of Smart Tap and Apple VAS
- BF 00 CRC16

6.4. Lite-On Custom PiP Firmware Commands for Both Platforms

The following applies to both Google Pay Smart Tap 2.1 and Apple VAS. Refer to “NEO IDG(NEO Interface Developers Guide)_Rev 165.4” document.



NEO IDG_Rev
165.4.pdf

6.5. Poll On Demand and Auto Poll Settings

For Poll On Demand, the Apple VAS & Google Pay Smart Tap 2.1 container tags must be included in the parameters for the **Activate Contactless Transaction** command. When using Auto Poll, the container tags must be set in Configuration Group 0.

Apple VAS: FF EE 06 18 9F 22 02 01 00 9F 26 04 00 00 00 02 9F 2B 05 01 00
00 00 00 DF 01 01 03

Google Pay Smart Tap 2.1: FF EE 08 0A DF EF 1A 01 0A DF ED 28 01 00

6.6. Non-Payment Card Switching Support

Lite-On Custom PiP can read several card formats without needing to be manually switched.

The ACT command and the template in the FFEE0E Tag handles reading EMV cards and Mifare cards using a single command.

Note: The FFEE0E container tag is used in the same manner as FFEE06 and FFEE08 for Apple VAS and Google Pay Smart Tap 2.1 in relation to Poll On Demand/Auto Poll behavior.

Tags used:

- **FFEE0E** provides the template, which includes DFED3A, DFED3B, and DFED3C.
 - **DFED3A** defines which blocks to read. One block is a byte. For example, **DFED3A 04 02 12 18 22** reads blocks 02, 12, 18, and 22.
 - **DFED3C** defines the block and the corresponding data to write to it. For example, **DFED3C 11 06 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10** means write data "01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10" into block 06.
 - **0801FFFFFFFF** means from block 08, key-A, use "FFFFFFFF". Mode 01 is **KEY-A**, 02 is **KEY-B**.

Example:

ACT(02 40): 0A 9C 01 00 9F 02 06 00 00 00 00 15 00 FF EE 06 18 9F 22 02 01
 00 9F 26 04 00 00 00 01 9F 2B 05 01 00 00 00 00 DF 01 01 01 FF EE 08
 02 81 00 FF EE 0E 41 DF ED 3B 08 01 01 FF FF FF FF FF FF DF ED 3B 08
 04 01 FF FF FF FF FF FF DF ED 3B 08 08 01 FF FF FF FF FF FF DF ED 3C
 11 06 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 DF ED 3A 04 01
 03 07 09

This ACT parameter defines the following operations:

- Read blocks 01, 03, 07, and 09
- Write to block 06 with "01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10" as the data
- The key from block 01 is KEY-A "FFFFFFFFFFFFFF"
- The key from block 04 is KEY-A "FFFFFFFFFFFFFF"
- The key from block 08 is KEY-A "FFFFFFFFFFFFFF"

Return Data: FFEE0E length Error_Code Card_Type TLV_UID Card_Data
 Where **length** is the length of [Error_Code Card_Type Card_Data].

Error_Code is defined as:

0xE0	#define ERROR_NO_ERROR
0xE1	#define ERROR_TIMEOUT_ERROR
0xE2	#define ERROR_AUTHENTICATE_ERROR
0xE3	#define ERROR_READ_ERROR
0xE4	#define ERROR_WRITE_ERROR

Card_Type is defined as:

0x03	Classic Mifare
0x04	MifareUltraLight
0x05	Mifare Plus (PiP support and read UID only)
0x06	Mifare Desfire (PiP support and read UID only)

TLV_UID: DFED44

Card_Data is the data read from the card designated by DFED3A. The delimiter is **[0D 0A]**.

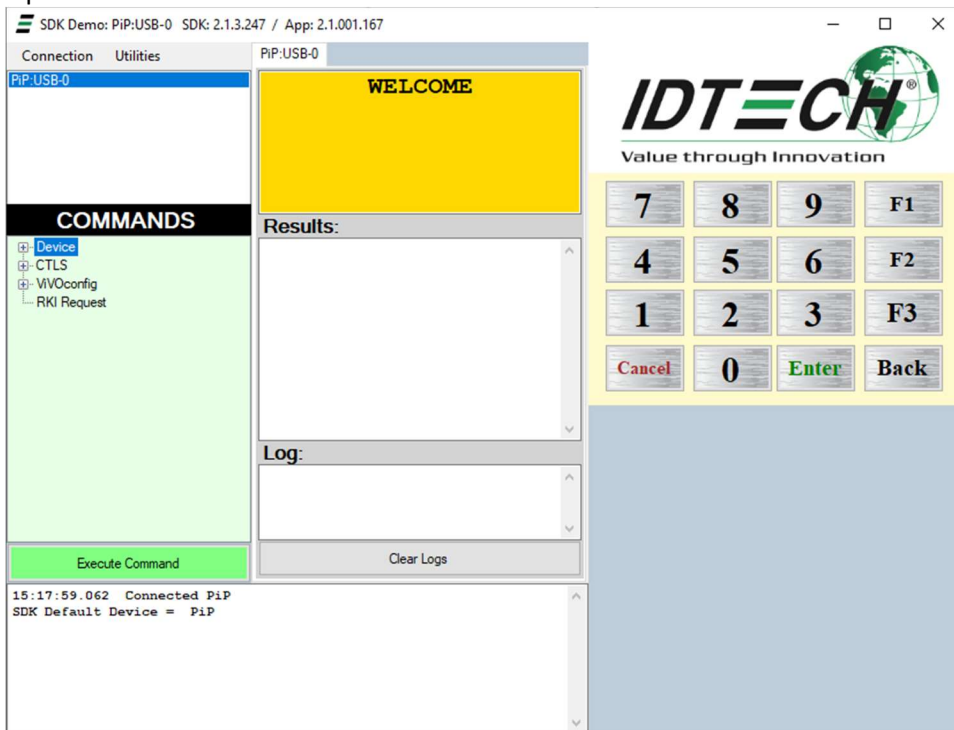
For the ACT command, if a key is not necessary or the key is KEY-A "FF FF FF FF FF FF", Tag DFED3B can be omitted.

7. Firmware Upgrade

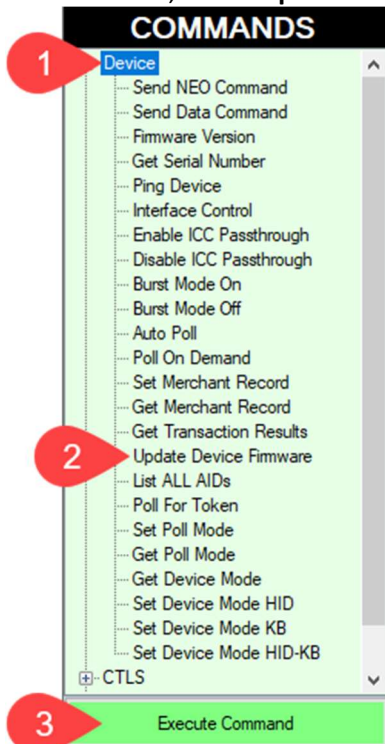
The steps below describe the process for updating LITE-ON CUSTOM PIP firmware via the Universal SDK Demo.

Note: Before you begin, contact your ID TECH representative to receive the most recent Lite-On Custom PiP firmware. Download the ZIP file and extract it to your computer.

1. Connect the LITE-ON CUSTOM PIP to your PC via serial port.
2. Download and install the latest [USDK Demo](#) app from the ID TECH Knowledge Base (if you cannot access the link, please [contact support](#)).
3. Open the USDK demo from the Windows Start menu.



4. Under **Device**, select **Update Device Firmware**, then click **Execute Command**.



5. Navigate to and select the LITE-ON CUSTOM PIP firmware you downloaded earlier and click **Open**.
6. The LITE-ON CUSTOM PIP will reboot and enter the bootloader, at which point the USDK demo begins updating the device.
7. When the firmware update completes, the LITE-ON CUSTOM PIP will reboot again and the USDK demo will prompt **Firmware Update Successful**.

8. Customer Support

If you are unable to resolve any technical issues, please contact support@idtechproducts.com (sending an e-mail to this address will automatically open a support ticket).