Apple VAS in ViVOpay™ Devices
User Guide

12 May 2022

Rev. J

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

ID TECH
10721 Walker St.
Cypress, CA 90630

This document, as well as the software and hardware described in it, is furnished under license and may be used or copied online in accordance with the terms of such license. The content of this document is furnished for information use only, is subject to change without notice, and should not be construed as a commitment by ID TECH. Reasonable effort has been made to ensure the accuracy of information provided herein. However, ID TECH assumes no responsibility or liability for any unintentional errors or inaccuracies that may appear in this document.

Warranty Disclaimer: The services and hardware are provided "as is" and "as-available" and the use of the services and hardware is at its 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, fitness for a particular purpose, title, and any warranties arising from a 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.

Revision History

Rev	Date	Changes	By
F	03/23/2020	ACT Command: Added Payment Only Mode to Tag 9F26	CB
G	10/27/2021	Updated Apple VAS Examples: DEK VAS Encryption	CB
H	11/05/2021	Restored Set Private Key (C7-66) command. Note that this command is valid only for Demo readers.	CB
J	05/12/2022	Updated Set Private Key (C7-66), Set Configuration (04-00), and Apple VAS setup flow and Tag DFED3F.	CB

Table of Contents

1. Introduction

Various contactless card readers ID TECH produces under the ViVOpay name support Apple VAS loyalty technology. This document describes ID TECH's Apple VAS implementation as it applies to ViVOpay devices and serves as an integration guide.

Note that Apple is the authoritative source of information on Apple VAS. Apple VAS is an Apple proprietary technology, the internal details of which are confidential. Developers should obtain available Apple VAS online documentation from Apple to gain an understanding of Apple VAS concepts and data representations before using this document.

This document describes the ViVOpay device configuration options that pertain to Apple VAS and the data flows that occur during an Apple VAS transaction. The business logic that applies to "value added" data is beyond the scope of this document. The guide below describes the ways applicable ViVOpay devices convey value-added services (VAS) data in the course of a "tap" (or user session).

1.1. Apple VAS High Level Overview

Apple VAS is a contactless (NFC) card emulation protocol for providing value-added services (VAS). Apple VAS functions as part of Apple’s Pass system, in which developer accounts create and publish passes for customers to download to the Apple Wallet app. Developers manage and push passes to phones in their own API via the Apple PassKit interface with no interaction on Apple’s part. Passes are created as Pass packages, which contain all the images and code that comprise a pass. Each pass has identifiers, details, and credentials managed in JSON fields. For specific information on the Pass system and loyalty programs, see Apple’s Developer Site.

2. Apple VAS Supported Products

ID TECH supports Apple VAS on the following ViVOpay products:

- VP 3300 (BT, USB-HID, AJ)
- VP 8300
- Kiosk III and Kiosk IV
- Vendi
- VP8800
- VP5300
- VP3600
- VP6300
- PiP*

***Note:** PiP **only** works for VAS programs; it does not support payments.

2.1. Product Differences

Note that most of the above-listed products use ID TECH's NEO-series firmware, whereas the VP8800 utilizes AR-series firmware. The **Activate Transaction** command (and some others) are different for VP8800 devices; on NEO devices, **Activate Transaction** is typically the **02-40** command, whereas on AR devices use the **02-05** command.

Likewise, NEO devices use a slightly different command protocol (ViVOtech2) than AR 3.0 products (which use ViVOpayV3). These differences, which are documented in detail in the *Interface Developer's Guides* (IDG) for NEO and AR, have no bearing on how Apple VAS works. The same TLVs, payload semantics, configuration requirements, and interaction flows occur in both NEO and AR devices. Contact your ID TECH representative to receive a copy of the *Interface Developer's Guide* (IDG) you need for development.

3. Apple VAS Configuration

Use the following commands to configure ViVOpay devices for Apple VAS. See Apple VAS Transaction Flow for details on when to call these commands. See Apple VAS Examples for request and response examples.

3.1. Basic Apple VAS Setup Flow

Apple VAS setup uses the following commands in sequence:

1. **Set Merchant Record (04-11)** sets the reader's merchant record ID, which Apple VAS uses to determine what loyalty program to access.
2. Use **set Configuration command (04-00)** to set tags DFED3F and DFED49 in Group 0 to manage VAS Encryption.
3. Set **Poll on Demand Mode (01-01)** to set the reader to auto-poll or poll on demand for a phone tap.
4. Set **Set Data Output Mode (01-0C)** to select normal or simplified output mode.

3.1.1. Set Configuration (04-00)

The **Set Configuration (04-00)** command sets or changes the values of the specified Tag Length Value (TLV) data objects in the reader. It can 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		

3.1.1.1. Tag DFED3F: VAS Encryption

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 Apple VAS encryption
- `BF 00` CRC16

3.1.2. Set Merchant Record (04-11)

The **Set Merchant Record** command sets the merchant the ViVOpay device 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			See data format in Apple VAS Examples		

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	var	The value of tag 9F29.
Length of Terminal Application Version Number	1	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	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, NEO 2 IDG	00	00		

3.1.3. Get Merchant Record (03-11)

The **Get Merchant Record** command retrieves the currently set merchant record.

Command Frame

Byte 0-9	Byte 10	Byte 11	Byte 12	Byte 13	Byte 14	Byte 15	Byte16
Header Tag & Protocol Version	Command	Sub-Command	Data length (MSB)	Data length (LSB)	Data	CRC (MSB)	CRC (LSB)
ViVOtech2\0	03	11h	01h		Merchant Record Index (1-6)		

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	03	See Status Code Table, NEO 2 IDG			See data format in Apple VAS Examples		

Data Field for Response Frame

Data Field	Length (bytes)	Description
Merchant Record Index	1	The valid value is 1--6. It can be set 6 records.
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	var	The value of tag 9F29.
Length of Terminal Application Version Number	1	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	The value of tag 9F22.

3.1.4. 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.

Apple VAS configuration settings are in Group 0.

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, NEO 2 IDG	00h	00h		

3.1.5. 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 Demo readers.

Command Frame

Byte 0-9	Byte 10	Byte 11	Byte 12	Byte 13	Byte 14	Byte 15	Byte16
Header Tag & Protocol Version	Command	Sub-Command	Data length (MSB)	Data length (LSB)	Data	CRC (MSB)	CRC (LSB)
ViVOtech2\0	C7	66h	20h		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: 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).

3.1.6. Set Poll Mode Command (01-01)

The **Set Poll Mode** command sets whether the ViVOpay devices uses Auto Poll or Poll on Demand.

Command Frame

Byte 0-9	Byte 10	Byte 11	Byte 12	Byte 13	Byte 14	Byte 15	Byte16
Header Tag & Protocol Version	Command	Sub-Command	Data length (MSB)	Data length (LSB)	Data	CRC (MSB)	CRC (LSB)
ViVOtech2\0	01	01h	00h	01h	Poll Mode		

Poll Mode:

00h = Auto Poll
01h = Poll on Demand

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	01	See Status Code Table, NEO 2 IDG	00h	00h			

3.1.7. Change USB Interface (01-0B)

The **Change USB Interface** command sets whether the ViVOpay device uses USB-HID or USB-KB. When USB-KB, Auto Poll, and Automatic Output On are all enabled, the payload output format changes to ASCII strings.

Command Frame

Byte 0-9	Byte 10	Byte 11	Byte 12	Byte 13	Byte 14	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	01h	0Bh	00h	01h	USB Interface		

Byte 1: USB Interface

00h = USB will change to USB-HID.
01h = USB will change to USB Keyboard.

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	01h	See Status Code Table, NEO 2 IDG	00h	00h		

3.1.8. Set Data Output Mode (01-0C)

The **Set Data Output Mode** command sets whether the output mode is normal, simplified, or tags only.

Command Frame

Byte 0-9	Byte 10	Byte 11	Byte 12	Byte 13	Byte 14	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	01h	0Ch	00h	01h	Mode		

Byte 1: Mode

Byte	Output Description	Terminal Type
00h = Normal mode	IDG header and trailer plus VAS data in tag.	Used in VAS Only, VAS-plus-payment, and payment-only terminals.
01h = Simplified output mode	VAS data not in tag, no IDG header and trailer.	Only used in VAS Only terminals.
02h = Tags only	VAS data in tag, no IDG header and trailer.	Used in VAS Only, VAS-plus-payment, and payment-only terminals.

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	01h	See Status Code Table, NEO 2 IDG	00h	00h		

3.1.9. Automatic Output for Auto Poll (01-0D)

The **Automatic Output for Auto Poll** command sets the device to output data automatically for Auto Poll mode.

Command Frame

Byte 0-9	Byte 10	Byte 11	Byte 12	Byte 13	Byte 14	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	01h	0Dh	00h	01h	Mode		

Byte 1: Mode

00h = Off

01h = On : output data on good reads

02h = On: output data on good and bad reads

Automatic mode sends out data without the **Get Transaction Results** command. The data is formatted according to the **Set Data Output Mode** command. This command only affects Auto Poll mode.

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	01h	See Status Code Table in NEO/NEO 2 IDG	00h	00h		

3.2. Remote Key Injection

For products supporting the symmetric key RKI method, the ID TECH RKI host directly injects the LTPK. Contact ID TECH for details on the protocol. The LTPK uses the same commands as any other key and a TR-31 block to carry the key.

4. Apple VAS Device Transaction commands

The following section describes transaction commands used for Apple VAS.

4.1. ACT Command (Activate Transaction)

The Activate Transaction (ACT) parameters required for ApplePay VAS functionality are communicated via the ApplePay VAS Container TLV (tag FFEE06). To make an ApplePay VAS transaction, provide the FFEE06 TLV in the ACT command (02-01 or 02-40).

Data Element	Presence	Description
9F26	Required	ApplePay Terminal Capabilities Information, an ApplePay VAS proprietary data element. Communicates the ViVOpay reader's capabilities to the iPhone. Byte 1: RFU Byte 2: RFU Byte 3: RFU Byte 4: Terminal Capabilities Set #1 87654321 ------00 Terminal in VAS App OR Payment Mode ------01 Terminal in VAS App AND Payment Mode ------10 Terminal in VAS App Only Mode ------11 Terminal in Payment Only Mode 0------- Last Get VAS Data Command (dynamic, do not set) 1------- More get VAS Data commands coming (dynamic, do not set) X-----xx Bits b7-b3 shall be set to 0
9F22	Optional	ApplePay Terminal Application Version Number, an ApplePay VAS proprietary data element. Per Apple, this is presently set to '0100'. Byte 1: '01' Byte 2: '00'
9F2B	Optional	ApplePay VAS Filter. The iPhone will not perform filtering without this tag. For details on the filtering function, see Apple's "NFC Value Added Service Protocol Specification." Apple is not using this parameter at the date of this document's release.
DFEE01	Optional	ApplePay VAS Protocol. Defines the desired protocol, reader UI, and communication error handling. Byte 1 87654321 -------0 URL VAS Protocol -------1 FULL VAS Protocol ------0- UI controlled by POS. For a VAS Only Transaction, the POS is responsible in this mode for the audio and UI display the transaction completion. ------1-- UI automatic. For a VAS Only Transaction, the reader beeps and displays "Card Read OK" at the end of the transaction. -----0-- EMEA Comm Err. For an ApplePay VAS transaction, a communications Error will be handled as defined in the EMEA UI Format (see NEO 2 IDG). -----1-- Silent Comm Err. For an ApplePay VAS transaction, in this mode a Communication Error will not beep.

		NOTE: This setting is handy as the iPhone generates communications errors as part of normal operations. xxxxx--- All other values are RFU If not provided, the following settings are used by default: Full VAS protocol No beeps for VAS EMEA Communications Error Handling

Tag 9F26 ApplePay Terminal Capabilities Information

Byte 1: Format

b8	b7	b6	b5	b4	b3	b2	b1	Description
x	x	x	x	x	x	x	x	RFU, Bits b8-b1 shall be set to 0

Byte 2: Format

b8	b7	b6	b5	b4	b3	b2	b1	Description
x	x	x	x	x	x	x	x	RFU, Bits b8-b1 shall be set to 0

Byte 3: Format

b8	b7	b6	b5	b4	b3	b2	b1	Description
x	x	x	x	x	x	x	x	RFU, Bits b8-b1 shall be set to 0

Byte 4: Terminal Capabilities Set

b8	b7	b6	b5	b4	b3	b2	b1	Description
						0	0	Terminal in VAS App OR Payment Mode
						0	1	Terminal in VAS App AND Payment Mode
						1	0	Terminal in VAS App Only Mode
						1	1	Terminal in Payment Only Mode
0								Last GET VAS DATA command
1								More GET VAS DATA command(s) forthcoming
x	0	0	0	0	0	x	x	Bits b7-b3 shall be set to 0
								All other values are RFU

4.2. VAS Encryption tags

Tag DFED3F controls Apple VAS output data by DEK encryption. It can also set tag 9F27 for Apple VAS to decrypt by private key.

Set this tag in 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

4.3. VAS Only Global Override

Tag DFED49 sets a device to VAS Only mode. Devices in VAS Only mode do not attempt to perform payments if VAS fails. Set this Tag in Group 0.

DFED49 (Optional)	VAS Only global override
Bit 0	Terminal will be VAS only
Bit 1 to 7	RFU

4.4. Status Code

Tag DFED5F is the transaction status code as defined in the *NEO Interface Developer's Guide*. This tag is mandatory for Tags Only mode.

DFED5F (Required)	Status Code; mandatory for Tags Only mode
	Refer to NEO IDG Status Codes table.

4.5. VAS Encryption Status

Tag DFED60 checks the VAS data's encryption status as configured by Tag DFED3F.

DFED60 (Optional)	VAS encryption status
Bit 0	VAS data encrypted with device's data encryption key
Bit 1	Apple VAS decrypted data with Apple VAS private key
Bit 2 to 7	RFU

4.6. CRC of TLV Tags

Tag DFED61 is the CRC of the TLV tags used in Tags Only mode. Use this tag to ensure data integrity.

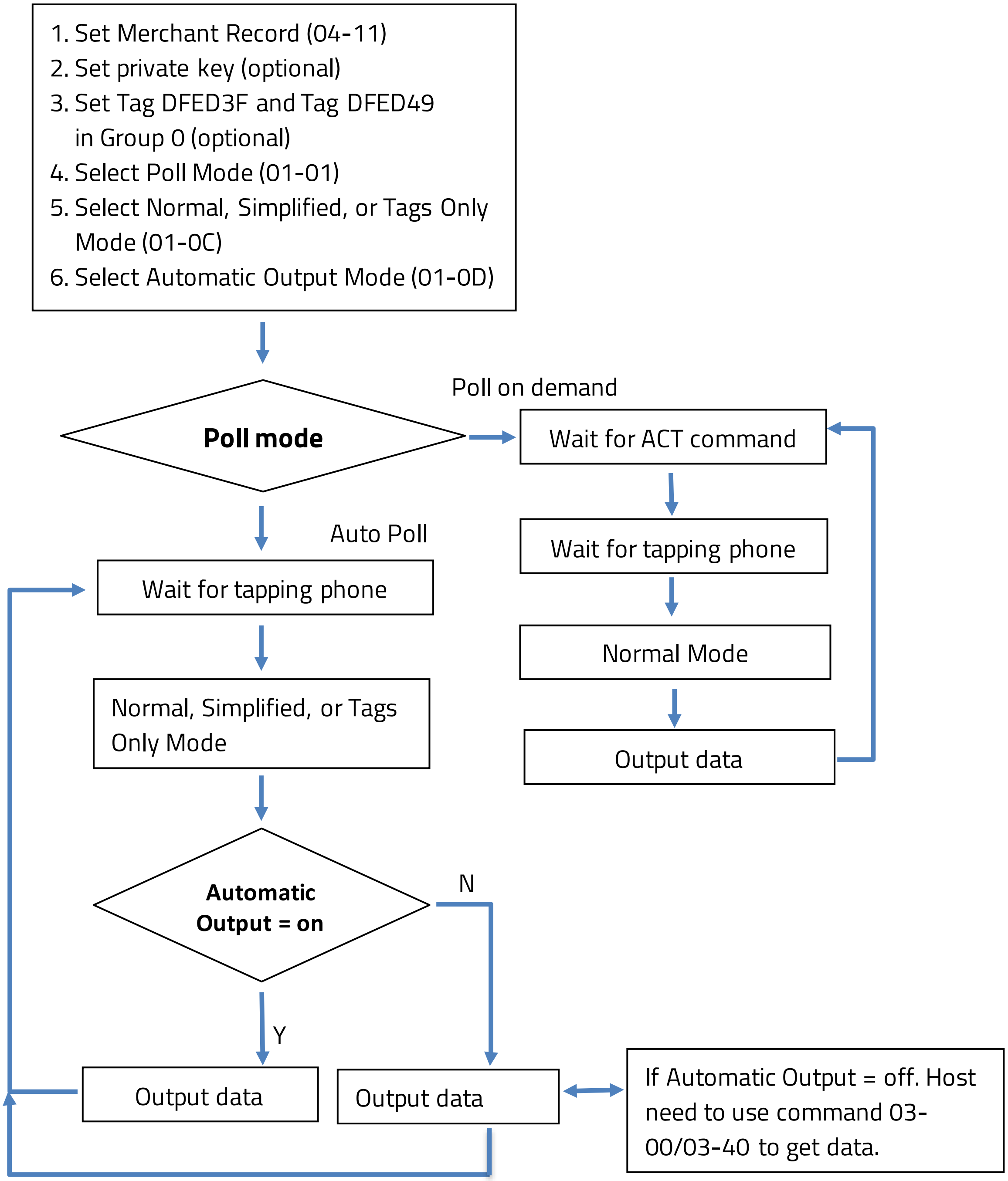
DFED61 (Optional)	2 bytes CRC

4.7. Tags Only Mode Settings

Tag DFED62 configures Tags Only mode options. Set this Tag in Group 0.

DFED62 (Optional)	VAS Only global override
Bit 0	Enable CRC Tag DFED61
Bit 1	TLV-Only mode for MSR transactions
Bit 2 to 7	RFU

5. Apple VAS Transaction Flow



1. Set Merchant Record (04-11)
2. Set private key (optional)
3. Set Tag DFED3F and Tag DFED49 in Group 0 (optional)
4. Select Poll Mode (01-01)
5. Select Normal, Simplified, or Tags Only Mode (01-0C)
6. Select Automatic Output Mode (01-0D)

If Automatic Output = off. Host need to use command 03-00/03-40 to get data.

6. Output Formats

Note the following information about Apple VAS output formats:

- Poll on Demand only supports normal mode.
- Auto Poll supports normal, simplified, and tags only modes.
- For USB-KB, it is best to use Auto Poll mode, Tags Only mode, and Automatic Output on.
- In Auto Poll mode, the reader will look for the container tag FFEE06 in Group 0 for the Apple VAS parameters. If FFEE06 is in both Group 0 and the command, the FFEE06 in the command will be used.
- Configure tag DFED3F bit 1 to on in order to output the Apple VAS data in the clear in tag 9F27.
- The Apple VAS private key must be loaded into the reader for the decryption to work.

7. Apple VAS Examples

The following examples illustrate Apple VAS configuration and transactions.

7.1. Configuring the Terminal for Apple VAS

The example below illustrates Apple VAS terminal configuration.

Set Merchant Record command using the SDK:

```
idtVendi.device_sendDataCommand("04 11 01 01 3C C7 0E D8 9A 9D 43 54
BE 98 30 AB 58 D8 9C 6F E7 E6 2B AC A9 39 D2 A6 85 1D FC 60 2E A7 98
F7 16 77 77 77 2E 69 64 74 65 63 68 70 72 6F 64 75 63 74 73 2E 63 6F
6D 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00", false,
resDataStruct);
```

Set Merchant Record command via raw firmware commands:

```
56 69 56 4F 74 65 63 68 32 00 04 11 00 63 01 01 3C C7 0E D8 9A 9D 43
54 BE 98 30 AB 58 D8 9C 6F E7 E6 2B AC A9 39 D2 A6 85 1D FC 60 2E A7
98 F7 16 77 77 77 2E 69 64 74 65 63 68 70 72 6F 64 75 63 74 73 2E 63
6F 6D 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 91 0C
```

Breakdown of command sent:

56 69 56 4F 74 65 63 68 32 00: ViVOtech2\0 header

04: Set Merchant Command

11: Set Merchant Sub-Command

00 63: Data Length

01: Merchant Index number

01: Merchant ID is enabled

3C C7 0E D8 9A 9D 43 54 BE 98 30 AB 58 D8 9C 6F E7 E6 2B AC A9 39 D2 A6 85 1D FC 60 2E A7 98 F7: Merchant ID (this is the SHA-256 hash of the IDTech Pass having the name "pass.com.apple.wallet.vas.prodtest")

16: Length of VAS URL.

77 77 77 2E 69 64 74 65 63 68 70 72 6F 64 75 63 74 73 2E 63 6F 6D 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00: **URL in ASCII "www.idtechproducts.com"**

91 0C: CRC-16

Response:

56 69 56 4F 74 65 63 68 32 00 04 00 00 00 AE 16

Breakdown of Response:

56 69 56 4F 74 65 63 68 32 00: ViVOtech2\0 Header
04: Command
00: Status (see table "Status Codes for Protocol 2")
00 00: Data
AE 16: CRC

7.2. Get VAS Only Transaction

The example below illustrates getting a VAS Only transaction.

Example:

```
56 69 56 4F 74 65 63 68 32 00 02 40 00 29 30 9F 02 06 00 00 00 00 00
01 9C 01 00 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 01 33 FE
```

Command Sent Breakdown:

56 69 56 4F 74 65 63 68 32 00: ViVOTech2 header
02 40: Start transaction command
00 29: Data Length
30: Time out
9F 02 06 00 00 00 00 00 01: Transaction amount
9C 01 00: Transaction Type
FF EE 06: ApplePay VAS tag Container
18: length of ApplePay VAS tag Container
9F 22 02 01 00: ApplePay Terminal AVN
9F 26 04 00 00 00 02: ApplePay terminal Capabilities; 02 = VAS only
9F 2B 05 01 00 00 00 00: ApplePay VAS Filter (optional)
DF 01 01 01
33 FE: CRC-16

Response:

```
56 69 56 4F 74 65 63 68 32 00 02 57 00 8D 01 FF EE 06 82 00 75 9A 03
14 08 10 9F 21 03 12 01 58 9F 25 20 06 41 3B 95 7A 52 59 98 3B 60 8C
FC 89 CF B1 DA B9 0C E7 05 AD 8E FF 78 E9 DE 12 2C CF 8D 2C BF 9F 2A
00 9F 27 41 44 8D EC 4C 91 A8 36 55 88 BE 36 46 1B 14 68 38 7F 6F FC
0D 5E DC 01 7C 81 CF DC C1 FD B2 3A 51 77 31 1A C6 74 62 B8 F0 CA 84
70 22 EE 42 AB F8 17 C8 9A 53 29 74 AA 01 FE 7C 13 17 FD A1 D0 4D 0C
9F 39 01 07 FF EE 01 04 DF 30 01 00 DF EE 26 01 01 71 44
```

56 69 56 4F 74 65 63 68 32 00: ViVOTech2 header

02: Command group

57: Response code (57 means no payment occurred; VAS only)

00 8D: Length

01: Attribution byte (01: Contactless card)

FF EE 06: ApplePay VAS Container

82 00 75: Length

9A: Transaction Date

03: Length

14 08 10: Data

9F 21: Transaction time

03: Length

12 01 58: Data

9F 25: Merchant ID

20: Length

06 41 3B 95 7A 52 59 98 3B 60 8C FC 89 CF B1 DA B9 0C E7 05 AD 8E FF 78 E9 DE 12 2C CF 8D 2C BF: Data

9F 2A: Mobile token

00: Length

9F 27: VAS Data (Encrypted)

41: Length

44 8D EC 4C 91 A8 36 55 88 BE 36 46 1B 14 68 38 7F 6F FC 0D 5E DC 01 7C 81 CF DC C1 FD B2 3A 51 77 31 1A C6 74 62 B8 F0 CA 84 70 22 EE 42 AB F8 17 C8 9A 53 29 74 AA 01 FE 7C 13 17 FD A1 D0 4D 0C: Data

9F 39: Point of Service (POS) Entry Mode

01: Length

07: Data (Contactless EMV)

FF EE 01: ViVOpay TLV Group Tag

04: Length

DF 30: Track data source

01: Length

00: Data (Contactless (PICC))

DF EE 26: Encryption Status Information

01: Length

01: Data

71 44: CRC

Note: VAS data is encrypted and plaintext-only output in simplified output mode.

7.3. Get VAS and Payment Transaction

The example below illustrates getting a transaction with both VAS and a payment.

Example:

```
56 69 56 4F 74 65 63 68 32 00 02 40 00 31 30 9F 02 06 00 00 00 00 02
00 9C 01 00 9A 03 17 12 19 9F 21 03 09 58 08 FF EE 06 10 9F 26 04 00
00 00 01 9F 22 02 01 00 DF 01 01 03 DF EF 7A 01 01 58 01
```

Response:

```
56 69 56 4F 74 65 63 68 32 00 02 23 02 2B 11 4F 07 A0 00 00 00 04 10
10 82 02 1B 00 95 05 00 00 00 00 00 9A 03 17 12 19 9C 01 00 5F 2A 02
08 40 5F 2D 02 65 6E 9F 02 06 00 00 00 00 02 00 9F 03 06 00 00 00 00
00 00 9F 06 07 A0 00 00 00 04 10 10 9F 09 02 00 02 9F 1A 02 08 40 9F
1E 08 30 30 30 30 30 30 30 30 9F 21 03 09 58 08 9F 33 03 00 00 E8 9F
34 03 00 00 00 9F 35 01 22 9F 36 02 00 90 9F 37 04 C4 8D C8 63 9F 39
01 91 9F 41 04 00 00 00 06 9F 53 01 00 DF 81 29 08 30 F0 F0 00 30 F0
FF 00 FF 81 06 3B DF 81 2A 18 30 30 30 30 30 30 30 30 30 30 30 30 30
30 30 30 30 30 30 30 30 30 30 30 DF 81 2B 07 00 00 00 00 00 00 0F DF
81 15 06 00 00 00 00 00 FF 9F 6E 07 08 40 00 00 30 39 00 FF 81 05 66
50 0A 4D 41 53 54 45 52 43 41 52 44 84 07 A0 00 00 00 04 10 10 9F 6D
02 00 01 56 34 42 35 32 30 34 32 34 30 32 35 30 34 34 31 39 36 36 5E
20 2F 5E 31 39 30 37 32 30 31 30 30 31 34 34 31 31 30 39 37 39 37 30
30 30 30 30 30 30 30 30 30 30 39 9F 6B 13 52 04 24 02 50 44 19 66 D1
90 72 01 00 14 42 09 97 97 9F FF EE 01 2F DF 30 01 00 DF 31 18 30 30
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 DF
32 0D 30 30 30 30 30 30 30 30 30 30 30 30 30 FF EE 06 82 00 75 9A 03
17 12 19 9F 21 03 09 58 08 9F 25 20 06 41 3B 95 7A 52 59 98 3B 60 8C
FC 89 CF B1 DA B9 0C E7 05 AD 8E FF 78 E9 DE 12 2C CF 8D 2C BF 9F 2A
00 9F 27 41 44 8D EC 4C AB 42 F2 15 02 6E 29 19 FE 3E 84 47 AC 22 7F
59 A2 70 A0 43 A5 9E D8 AB 36 B8 C0 AA 70 EE 34 12 80 34 F0 69 BE BD
7D A1 EB 85 63 12 2D CC AC E4 9A 8F 5E C4 D8 9D E3 2D E3 CA A2 2A 5F
DF EF 4C 06 00 27 00 00 00 00 DF EF 4D 27 3B 35 32 30 34 32 34 30 32
35 30 34 34 31 39 36 36 3D 31 39 30 37 32 30 31 30 30 31 34 34 32 30
39 39 37 39 37 39 3F DF EE 26 01 11 DF EF 7B 01 01 22 63
```

56 69 56 4F 74 65 63 68 32 00: ViVOtech2\0 header

02: Command

23: Response code

02 2B: Data length

11: Attribute byte

FF EE 06: ApplePay VAS Container

82 00 75: Length

9A: Transaction Date

03: Length

17 12 19: Data

9F 21: Transaction Time

03: Length

09 58 08: Data

9F25: Merchant ID

20: Length

06 41 3B 95 7A 52 59 98 3B 60 8C FC 89 CF B1 DA B9 0C E7 05 AD 8E FF 78 E9 DE 12 2C CF 8D 2C BF: Data

9F2A: Mobile token

00: Length

9F 27: VAS Data (Encrypted)

41: Length

44 8D EC 4C AB 42 F2 15 02 6E 29 19 FE 3E 84 47 AC 22 7F 59 A2 70 A0 43 A5 9E D8 AB 36 B8 C0 AA 70 EE 34 12 80 34 F0 69 BE BD 7D A1 EB 85 63 12 2D CC AC E4 9A 8F 5E C4 D8 9D E3 2D E3 CA A2 2A 5F DF EE 26: Encryption Status Information

01: Length

11: Data

DF EF 7B: VAS indicator

01: Length

01: ApplePay or Apple VAS

22 63: CRC

Note: The example above skips financial transaction tags and only parses tags related to Apple VAS.

7.4. Simplified Output

The example below illustrates a transaction with Simplified Output, which is used primarily in USB-KB mode, where the reader does not receive commands. Only VAS Only configuration uses Simplified Output. "Decrypt Apple VAS data with an Apple VAS private key" should be enabled and "Encrypt VAS data with the device's data encryption key" should be disabled. The response below contains decrypted VAS data.

Response:

```
324234242
```

7.5. Tags Only Output

The example below illustrates Tags Only Output, which is used primarily in USB-KB mode, where the reader does not receive commands. Any VAS configurations and VAS encryption settings can use Tags Only Output. The response below contains VAS data in tag form along with other tags.

Response:

```
DF ED 5F 01 57 FF EE 06 82 00 75 9A 03 14 08 10 9F 21 03 12 01 58 9F
25 20 06 41 3B 95 7A 52 59 98 3B 60 8C FC 89 CF B1 DA B9 0C E7 05 AD
8E FF 78 E9 DE 12 2C CF 8D 2C BF 9F 2A 00 9F 27 41 44 8D EC 4C 91 A8
36 55 88 BE 36 46 1B 14 68 38 7F 6F FC 0D 5E DC 01 7C 81 CF DC C1 FD
B2 3A 51 77 31 1A C6 74 62 B8 F0 CA 84 70 22 EE 42 AB F8 17 C8 9A 53
29 74 AA 01 FE 7C 13 17 FD A1 D0 4D 0C 9F 39 01 07 FF EE 01 04 DF 30
01 00 DF EE 26 01 01 DF ED 61 02 01 94
```

DF ED 5F: Response code
01: Length
57: Response code (57 means no payment occurred; VAS only)
FF EE 06: ApplePay VAS Container
82 00 75: Length
9A: Transaction Date
03: Length
14 08 10: Data
9F 21: Transaction time
03: Length
12 01 58: Data
9F 25: Merchant ID
20: Length
06 41 3B 95 7A 52 59 98 3B 60 8C FC 89 CF B1 DA B9 0C E7 05 AD 8E FF 78 E9 DE 12 2C CF 8D 2C BF: Data
9F 2A: Mobile token
00: Length
9F 27: VAS Data (Encrypted)
41: Length
44 8D EC 4C 91 A8 36 55 88 BE 36 46 1B 14 68 38 7F 6F FC 0D 5E DC 01 7C 81 CF DC C1 FD B2 3A 51 77 31 1A C6 74 62 B8 F0 CA 84 70 22 EE 42 AB F8 17 C8 9A 53 29 74 AA 01 FE 7C 13 17 FD A1 D0 4D 0C: Data
9F 39: Point of Service (POS) Entry Mode
01: Length
07: Data (Contactless EMV)
FF EE 01: ViVOpay TLV Group Tag
04: Length
DF 30: Track data source

01: Length
00: Data (Contactless (PICC))
DF EE 26: Encryption Status Information
01: Length
01: Data
DF ED 60: VAS Encryption Status
01: Length
00: Data
DF ED 61: CRC
02: Length
01 94: Data

7.6. DEK VAS Encryption

The example below illustrates a transaction with DEK VAS encryption.

Note: Set **DFED3F** to **03** to turn on "VAS data encryption with the device's data encryption key" and "Decrypt Apple VAS data with an Apple VAS private key."

Example:

```
56 69 56 4F 74 65 63 68 32 00 02 40 00 29 30 9F 02 06 00 00 00 00 00
01 9C 01 00 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 01 33 FE
```

56 69 56 4F 74 65 63 68 32 00: ViVOTech2 header
02 40: Start transaction command
00 29: Data Length
30: Time out
9F 02 06 00 00 00 00 00 01: Transaction amount
9C 01 00: Transaction Type
FF EE 06: ApplePay VAS tag Container
18: length of ApplePay VAS tag Container
9F 22 02 01 00: ApplePay Terminal AVN
9F 26 04 00 00 00 02: ApplePay terminal Capabilities; 02 = VAS only
9F 2B 05 01 00 00 00 00: ApplePay VAS Filter (optional)
DF 01 01 01 33 FE: CRC-16

Response:

```
56 69 56 4F 74 65 63 68 32 00 02 57 00 64 C1 FF EE 12 0A 62 99 49 01
2C 00 04 60 00 02 FF EE 06 45 9A 03 14 08 10 9F 21 03 12 02 56 9F 25
20 3F A5 AA BE C7 27 53 35 18 F9 64 06 33 BC DA 51 F2 F0 19 D9 F5 37
67 54 BF 21 3F A3 47 05 B1 7D 9F 2A 00 9F 27 C1 10 10 62 DF C2 97 83
C3 E6 00 FA D7 82 A4 4E 51 8B 9F 39 01 07 FF EE 01 04 DF 30 01 00 44
6D
```

56 69 56 4F 74 65 63 68 32 00: ViVOTech2 header

02: Command group

57: Response code (57 means no payment occurred; VAS only)

00 64: Length

C1: Attribution byte

DF EE 12: KSN

0A: Length

62 99 49 01 2C 00 04 60 00 02: Data

FF EE 06: ApplePay VAS Container

45: Length

9A: Transaction Date

03: Length

14 08 10: Data

9F 21: Transaction time

03: Length

12 01 56: Data

9F 25: Merchant ID

20: Length

3F A5 AA BE C7 27 53 35 18 F9 64 06 33 BC DA 51 F2 F0 19 D9 F5 37 67 54 BF 21 3F A3 47 05 B1 7D: Data

9F 2A: Mobile token

00: Length

9F 27: VAS Data (Encrypted with DEK)

C1: Special (indicate data is encrypted by DEK)

10: Length

10 62 DF C2 97 83 C3 E6 00 FA D7 82 A4 4E 51 8B: Data

9F 39: Point of Service (POS) Entry Mode

01: Length

07: Data (Contactless EMV)

FF EE 01: ViVOpay TLV Group Tag

04: Length

DF 30: Track data source

01: Length

00: Data (Contactless (PICC))

44 6D: CRC