Google SmartTap 2.1 in ViVOpay™ Devices

Rev. G

January 4, 2019

ID TECH
10721 Walker St.
Cypress, CA 90630

Table of Contents

1. Introduction

Various contactless card readers produced by ID TECH under the ViVOpay name support Google's SmartTap loyalty technology. This document describes ID TECH's SmartTap 2.1 implementation as it applies to ViVOpay devices, and serves as a guide for integrators who wish to take advantage of this technology.

Note that the ultimate source of authoritative information on SmartTap is Google. SmartTap is a Google proprietary technology, the internal details of which are confidential. We recommend you obtain available SmartTap documentation from Google online before proceeding, as a good understanding of SmartTap concepts and data representations is necessary to fully understand this document.

In this document, we describe the ViVOpay device configuration options that pertain to SmartTap, and the data flows that occur during a transaction involving SmartTap. The business logic that might apply to "value added" data is beyond the scope of this document. What we describe below are the ways in which applicable ViVOpay devices convey value-added services (VAS) data in the course of a "tap" (or user session). What you do with the data is up to you.

2. SmartTap 2.1 High Level overview

SmartTap 2.1 is a contactless (NFC) card emulation protocol for providing value-added services (VAS).

The Google SmartTap specification allows a Google Pay wallet to exchange added value information with a host system (POS, phone, tablet) which, in turn, may convey that info to a store server, or other back-end system. VAS data is requested at "tap" time using the standard Start Transaction payment command (with optional TLVs included in the request). The transaction can be payment-only, VAS-only, or a combination (see discussion below).

In this document, we will focus on the value added (VAS) side of Google Pay – having to do with loyalty, coupons, discounts, "points," etc. – and only deal with the payment side when it intersects with the value added side. We use the generic term VAS (Value Added Services) for all functions and explanations related to the non-financial-card aspects of the wallet functionality.

To function properly, the ViVOpay reader needs to be initially setup with the correct configuration parameters. It is the merchant's responsibility to obtain required configuration information (such as the Collector ID) from Google, and properly configure the reader with that information using the appropriate APIs described below. Generally speaking, this is a one-time setup operation that does not need to be repeated once a reader has been deployed in the field. (The only configuration item that might need to be revisited in the field is the Long Term Private Key, which may need to be rotated periodically.)

Once the reader is configured, certain parameters must be included in the transaction step to indicate to the reader that the transaction type should be of a VAS type.

The key elements of the communication between the reader and the wallet are:

1) The reader and the wallet will use asymmetric elliptical-curve cryptography (ECC) to protect the data in transit between the phone and the reader. Security is based on an ECC256 key pair where the private key (LTPK – Long Term Private Key) is stored in the reader, and the public key is part of the wallet.

2) The data exchanged between the reader and the wallet follow an NFC Data Exchange Format (NDEF) structure. (Online, see https://nfc-forum.org/our-work/specifications-and-application-documents/specifications/nfc-forum-technical-specifications/.) The ViVOpay reader will deliver this data wrapped in a TLV structure. (See examples below.) The reader is agnostic with respect to NDEF content; that is, the ViVOpay device itself does not "know" anything special about NDEF data. It's just another form of data that the device conveys from the card to the host.

2.1 Types of Transactions

ID TECH's ViVOpay readers allow payment/VAS interactions with the wallet to be performed using an Activate Transaction command (sometimes also called Start Transaction).

For SmartTap 2.1, the possible transaction modes are:

1) Payment only (No VAS interaction)
2) VAS only (No payment, read the VAS data)
3) VAS and Payment (Allow both VAS and Payment to be performed with the wallet)
4) VAS over Payment (If VAS data is available, get VAS with no Payment; if and only if there is no VAS, perform payment if available)

The wallet can also receive data from the POS (or host) via a Push VAS command.

Conversely, ID TECH readers provide the ability to output the VAS data to the POS in any of several modes:

1) In the clear (as NDEF) with no encryption of the data fields (USB-HID)
2) With encryption of sensitive fields (as defined by Google), as NDEF encrypted using the reader's Data Encryption Key (USB-HID)
3) Using a simplified mode (using USB-KB, aka "keyboard device" USB), on applicable readers. One or several service objects are extracted from the NDEF structure and provided to the back end without any other data

ID TECH readers also provide the ability to rotate the LTPK (Long Term Private Key) for readers in the field, using a secure protocol.

Note: Simplified mode supports Get VAS Only and Secure Get VAS Only. Activate Transaction using other modes will be rejected (response status code 0C/05).

3. SmartTap 2.1: Supported Products

ID TECH supports SmartTap 2.1 on the following ViVOpay products:

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

3.1 Product Differences

Note that most of the above-listed products use ID TECH's NEO-series firmware, whereas VP8800 utilizes AR-series firmware. The Activate Transaction command (and certain other commands) will thus be different for VP8800 than for other products. (On NEO devices, Activate Transaction is typically the 02-40 command, whereas on AR devices it is 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 SmartTap works in the various devices. The same TLVs, payload semantics, configuration requirements, and interaction flows will occur on NEO devices as on AR devices.

4. SmartTap 2.1 Configuration

Before a device can participate in SmartTap transactions, it must be configured with various parameters. Broadly, this means TLV-based parameters that fall into one of two categories:

- Non-security-related parameters having to do with Collector ID (and reader capabilities) – see next section
- Security-related parameters (see further below)

The the two main items of information you will need to supply (initially, at setup time) in order to do SmartTap transactions are the Collector ID (Google's terminology for merchant ID) and the long-term private key (or LTPK). You will set the Collector ID via tag DFEE3B (as mentioned in the next section) using command 04-03 (when assigning it to groups other than the default Group of 8E). The command for injecting the LTPK is discussed in Section 4.2 further below.

In addition, you may *optionally* want to customize certain aspects of SmartTap transaction behavior using configuration tags. (This would only apply if the default out-of-the-box behaviors are not exactly what your app needs.) Out of the box, all ViVOpay readers that support SmartTap have the SmartTap 2.1 AID (A000000476D0000111) already loaded, as a System AID, set up to use contactless configuration Group 0x8E (decimal 142) by default. If you decide to customize your reader so that SmartTap utilizes a *custom* group or dataset (instead of 0x8E), you can do this using command 04-03. However, if you do not need to customize any behaviors, SmartTap 2.1 should work (using the default parameters in Group 0x8E) out of the box.

Consult your *Interface Developer's Guide* (IDG), applicable to NEO or AR, as appropriate, for additional information about managing configuration options involving AIDs, groups, and/or datasets. In particular, read about command 04-03.

4.1. Non-Security Parameters

Below is the list of non-security-related parameters and the corresponding tags that can be used to configure the reader for SmartTap. These TLVs will be sent to the reader at configuration time to establish persistent settings. They may optionally be sent at Activate Transaction time to override any configurations on a per-transaction basis. Note that of the first four parameters (having to do with the merchant and terminal), only the Collector ID is required to be non-empty. In general, tags that show no

default value in the table below are optional.

Tag	Length (bytes)	Name	Default Value
DFEE3B	Maximum 8	Collector ID (mandatory), only the rightmost 4 bytes will be used. Tag length will be 4 in most cases.	00bc614e is the default, but you should plan on replacing this with your own unique 4-byte identifier.
DFEE3C	Up to 32	Store Location ID	Empty.
DFEE3D	Up to 32	Terminal ID	Empty.
DFEF25	Up to 32	Merchant Name	Empty.
DFED01	4	Merchant Category	Empty.
DFED02	5	POS Capabilities Bitmaps (see table below)	0000000001
DFED03	1	Retry Times	Empty.
DFED04	1	Select OSE support	01
DFED05	1	Skip Second Select support	01
DFED06	1	Stop payment if SmartTap 2.1 failed	Empty.
DFED07	1	Pre-Signed Support	Empty.
DFED27*	1	Delimiter for Service Objects*	0D
DFEF77*	1	Enable/Disable Multiple Service Objects*	Empty.

*Valid only for Simplified Output mode.

NOTE: The default value for DFED27 is 0x0D (CR).Tag DEEF77 value can be set as 0x00(Disable) or 0x01(Enable). If the function is disabled, the reader returns only the first service object in the NDEF record.

DFED02 (POS Capabilities): 5 bytes with flags as follows (1 = ON, 0 = OFF)

Byte	Bit 1	bit 2	bit 3	bit 4	bit 5	bit 6	bit 7	bit 8
System	Standalone	Semi-integrated	Unattended	Online	Offline	MMP	zlib support	RFU
UI	Printer	Printer graphics	Display	Images	Audio	Animation	Video	RFU
Checkout	Support payment	Support digital receipt	Support Service issuance	Support OTA POS data	RFU	RFU	RFU	RFU

CVM	Online PIN	CD PIN	Signature	No CVM	Device generated code	SP generated code	ID capture	Biometric
Tap	VAS Only	Payment Only	VAS and Payment	VAS over Payment	RFU	RFU	RFU	RFU

Example 04-03 configuration command (for NEO-series firmware):

5669564f7465636832000403004 4ffe4018edfee3b0400bc614edfee3c00dfee3d00dfef2500dfed0100dfed0
2050000000001dfed0300dfed040101dfed050101dfed0600dfed0700dfed27010ddfef77001082

Parsed:

56 69 56 4F 74 65 63 68 32 00 – ViVOTech2\0 header

04 03 – command

00 44 – length (less CRC)

FFE4-- Group Number / Fallback Group

DFEE3B -- TAC - Default

DFEE3C -- TAC - Denial

DFEE3D -- Terminal ID

DFEF25 -- Output Data Format Select

DFED01 -- Merchant Category

DFED02 -- POS Capabilities Bitmaps

DFED03 -- Retry Times

DFED04 -- Select OSE support

DFED05 -- Skip Second Select support

DFED06 -- Stop Payment if SmartTap2.1 failed support

DFED07 --Pre-Signed support

DFEF77 --Timeout for waiting next command

10 82 – CRC16

The above example assumes that a NEO-firmware device is used. In the case of an AR-firmware device (e.g. VP8800), the same command is used, but it will be wrapped in the device-appropriate protocol (i.e., ViVOpayV3) and will produce responses, likewise, that conform to that protocol.

4.2. Security Parameters

Secure interaction between the reader and the wallet requires a LTPK (Long Term Private Key). The ECC key-pair (consisting of a 32-byte LTPK private key, and corresponding public key) must be customer-generated (see Appendix). It will need to be injected into the ViVOpay device via the key injection firmware command as outlined in the next section. Note that because the LTPK is used only for non-financial-card, non-EMV purposes, it falls outside of PCI scope.

Devices in the field can have keys rotated via RKI (remote key injection); contact ID TECH for more information on this process.

Encrypted vs. Non-Encrypted Session Data

The reader can apply (or not apply) encryption to the VAS payload (separate from the financial transaction payload) depending on what you specify at transaction time. Use value 01 in tag DFED3F to indicate that encryption should be applied to the VAS payload. Use value 00 to indicate that the VAS data should not be encrypted. This choice will not have any effect on whether financial data are encrypted. It will only affect whether or not VAS data will be similarly encrypted. The default is 0x00 (off).

4.2.1. Direct Injection of LTPK

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

Command: **C7-65**

The data field will be 36 bytes long:

Version info: 4 bytes

Long term private key: 32 bytes

Example (using NEO firmware):

Request: 56 69 56 4F 74 65 63 68 32 00 **C7 65** 00 24 00 00 00 01 82 6D 17 E5 07 67 B1 65 B0 E4 D9 E3 32 F8 D1 D1 E2 02 24 28 4F B4 DA F1 E5 0A 03 24 6E 70 79 7D 71 B8

Parsed request:

56 69 56 4F 74 65 63 68 32 00 – ViVOTech2\0 header

C7 65 – command

00 24 – Length of payload

00 00 00 01 – version

82 6D 17 E5 07 67 B1 65 B0 E4 D9 E3 32 F8 D1 D1

E2 02 24 28 4F B4 DA F1 E5 0A 03 24 6E 70 79 7D – 32-byte key (LTPK)

71 B8 – CRC

NOTE: If the device is a NEO or AR device using ViVOtech2 protocol, the 2-byte CRC should be sent to the device in little-endian byte order. Any CRC received from the device will be in big-endian order.

Response: 56 69 56 4F 74 65 63 68 32 00 C7 00 00 00 86 6E

(00 00 indicates no error)

4.2.2. Remote Key Injection

For products supporting the symmetric key RKI method, the LTPK will be remotely injected from the ID TECH RKI host. (Please contact ID TECH for details on the protocol.) The LTPK will use the same commands as any other key; and it will use a TR-31 block to carry the key.

5. SmartTap 2.1 Device Transaction commands

5.1. ACT Command (Activate Transaction)

The Smart Tap Options tag, FFEE08, must be provided in the Activate Transaction (ACT) command if a Smart Tap 2.1 transaction is desired. The presence of this tag means the transaction will try to utilize Smart Tap if SmartTap is present on the target device.

Note that FFEE08 is a constructed (group) tag, which means it must contain at least one other TLV.

The terminal mode of the transaction will be conveyed in tag DFEF1A as defined below. (This is the only mandatory tag inside a FFEE08 Group Tag.)

Tag DFEF1A: Terminal Mode

b8	b7	b6	b5	b4	b3	b2	b1	Description
0	0	0	0					RFU

				x	x	x	x	0000: VAS OVER Payment Mode 0001: VAS AND Payment Mode 0010: VAS Only Mode 0011: Payment Mode Only 0101: Push VAS AND Payment Mode 0110: Push VAS Only Mode 1000: Secure Get VAS OVER Payment Mode 1001: Secure Get VAS AND Payment Mode 1010: Secure Get VAS Only Mode

The FFEE08 tag may optionally contain configuration tags (Section 4.1) that override any parameters configured earlier. Those parameters will be valid for one transaction only.

If a Push is scheduled, the data to be sent to the wallet will be included in a Tag DFEF1B. The data is the Push Service NDEF record as defined in the Push SmartTap data request.

NOTE: Tag DFEF1B can contain up to 2560 bytes (maximum), on supported devices.

If Service Type Requests are included in the Get SmartTap data, those will be included in a Tag DFED28. The data will be part of the Get SmartTap data request and constitute the Service List NDEF record as defined in the Get SmartTap data request.

Service Type Byte

Value	Description
0x00	All services
0x01	All services except PPSE
0x02	PPSE
0x03	Loyalty
0x04	Offer
0x05	Gift Card
0x06	Private Label Card
0x07	Event Ticket
0x08	Flight
0x09-0x0F	RFU TWI
0x10	Cloud Based Wallet
0x11	Mobile Marketing Platform
0x0C-0x3F	RFU TWI
0x40	Wallet Customer
0x41-0x6F	RFU Wallet-specific
0x70-0x9F	RFU Merchant-specific

If the device will use encryption, the appropriate Activate Transaction command is 02-40.

Consult the Interface Developer's Guide (IDG) for your product, for more information on the Activate Transaction command.

5.2. Response

SmartTap payloads contain NDEF (NFC Data Exchange Format) records. The VAS NDEF structure(s) returned in a Smart Tap interaction will be embedded in Tag DFEF76. The details of the NDEF structures used by SmartTap are provided by Google under NDA and cannot be shared by ID TECH. Please contact Google directly if low-level details are needed.

If the standard Get mode is used, the VAS data will come back unencrypted, and all fields will be in the clear.

If the secure Get mode is used, the VAS data will come back encrypted using the DEK (Data Encryption Key) standard to the reader.

For examples, see the section below called SmartTap 2.1 Examples.

5.2.1 UID

Responses that contain the user's UID will have that UID in tag DFED44. The response will contain:

FFEE0E <length> <Error_Code> <Card_Type> <TLV_UID Card_Data>

where TLV_UID is:

Tag: DF ED 44

Length: Length of UID

Value: UID

Below is a response example:

56 69 56 4F 74 65 63 68 32 00 02 00 00 6C 00 00 00 FF EE 0E 59 E0 04 DF ED 44 07 04 30 42 F2 9F 43 80 01 F2 9F 43 80 AE 48 00 00 00 00 00 00 02 00 00 10 0D 0A 03 00 00 00 00 02 00 00 10 00 06 01 10 11 FF 00 00 0D 0A 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0D 0A 09 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0D 0A 9F 41 04 00 00 00 06 DF EE 26 01 41 01 3C

6. Simplified Output

When a device is operating in USB-KB (keyboard) mode, simplified output occurs. For simplified output, the reader will output the content of the Service Object NDEF records without any formatting (header, trailer), in an ASCII encoding appropriate to a keyboard device.

There are two modes that can be configured with Tag DFEF77.

- One (0x00) outputs the first Service Number NDEF record (first field after ObjectID) of the first Service Object following the Customer NDEF record. (The Customer NDEF record will always be ignored.)
- The second (0x01) outputs all Service Number NDEF records of all Service Objects (first field after ObjectID ObjectID) following the Customer NDEF record which is ignored and without the service

issuer NDEF record. Each data record is separated by the delimiter defined by tag DEED27, and the string will be completed by the delimiter.

The format byte will be removed from the output.

7. SmartTap 2.1 Examples

Note that the examples shown below are for NEO devices and thus use the ViVOtech2 protocol. For the VP8800 device, which uses AR firmware, the relevant commands and protocols should be substituted. (The 04-03 command exists in NEO as well as AR, but the protocol framing differs.In examples that use Activate Transaction, the ACT command is 02-40 on NEO devices and 02-05 on AR devices. Consult the appropriate IDG for detailed information about these commands.)

7.1. Configuring the Terminal for SmartTap - Loading the parameters

Request: Use the 04-03 command to set the Collector ID (a 4-byte value, in this example, 00 BC 61 4E).

Command:

5669564f74656368320004030044ffe4018edfee3b0400bc614edfee3c00dfee3d00dfef2500dfed0100dfed02050000000001dfed0300dfed040101dfed050101dfed0600dfed0700dfed27010ddfef77001082

Parsed:

56 69 56 4F 74 65 63 68 32 00 – ViVOTech2\0 header

04 03 – command

00 44 – length (less CRC)

FFE4-- Group Number / Fallback Group

DFEE3B -- TAC - Default

DFEE3C -- TAC - Denial

DFEE3D -- Terminal ID

DFEF25 -- Output Data Format Select

DFED01 -- Merchant Category

DFED02 -- POS Capabilities Bitmaps

DFED03 -- Retry Times

DFED04 -- Select OSE support

DFED05 -- Skip Second Select support

DFED06 -- Stop Payment if SmartTap2.1 failed support

DFED07 --Pre-Signed support

DFEF77 --Timeout for waiting next command

10 82 – CRC16

Response:

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

7.2. Get VAS only Transaction

Issue the Start Transaction command, specifying Get VAS only**.** In this terminal mode, only VAS data is requested. No payment data is requested.

Command (NEO firmware):

56 69 56 4F 74 65 63 68 32 00 02 40 00 1B 30 9F 02 06 00 00 00 00 00 01 9C 01 00 FF EE 08 0A DF EF 1A 01 02 DF ED 28 01 00 F4 19

Parsed:

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

02 40 – Start Transaction Command

00 1B – Length of payload

30 – Timeout value

9F 02 – Authorized Amount

06 00 00 00 00 00 01 – Length (06) and data

9C – Transaction Type

01 00 – Length (01) and data

FF EE 08 – Configuration Tags container

0A – Length (10 bytes)

DF EF 1A – Terminal Mode

01 02 – Length (01) and flag data (02 means VAS Only)

DF ED 28 – Service Type Requests

01 00 – Length (01) and data

F4 19 – CRC16

Response:

56 69 56 4F 74 65 63 68 32 00 02 57 00 7C 01 FF EE 08 66 DF EF 76 62 94 03 2F 61 73 76 94 01 06 69 04 02 71 79 79 71 54 03 1F 63 75 73 94 03 06 63 69 64 04 12 34 56 78 90 19 01 03 03 54 63 70 6C 00 65 6E 54 03 02 63 75 74 04 7B 54 03 27 61 73 76 94 01 05 69 05 01 F7 97 98 54 02 19 6C 79 94 03 09 6F 69 64 04 AC 80 1C BF CA 8D 5C 3A 54 01 06 6E 05 F3 24 23 42 34 9F 39 01 07 FF EE 01 04 DF 30 01 00 DF EE 26 01 01 0F D3

Parsed response:

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

02 – Command group

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

00 7C – Length

01 – Attribution byte (01: Contactless card)

FF EE 08 -- Configuration Tags container

66 – Length

DF EF 76 – SmartTap data (NDEF records)

62 – Length

94 03 2F 61 73 76 94 01 06 69 04 02 71 79 79 71 54 03 1F 63 75 73 94 03 06 63 69 64 04 12 34 56 78 90 19 01 03 03 54 63 70 6C 00 65 6E 54 03 02 63 75 74 04 7B 54 03 27 61 73 76 94 01 05 69 05 01 F7 97 98 54 02 19 6C 79 94 03 09 6F 69 64 04 AC 80 1C BF CA 8D 5C 3A 54 01 06 6E 05 F3 24 23 42 34 –

NDEF Data as follows:

Record .1:
HEADER: 0x94 (MB:1, ME:0, CF:0, SR:1, IL:0, TNF:4)
TYPE LENGTH: 0x3
PAYLOAD LENGTH: 0x2f
ID LENGTH: No ID LENGTH field
TYPE: 0x617376 ("asv")
ID: No ID field
PAYLOAD: 0x940106690402717979715403 1f6375739403066369640412345678901901030354637 06c00656e540302637574047b
Payload as Ascii: " i qyyqT cus cid 4Vx Tcpl enT cut {"

Payload is a NDEF Message:

Record .1.1:
HEADER: 0x94 (MB:1, ME:0, CF:0, SR:1, IL:0, TNF:4)
TYPE LENGTH: 0x1
PAYLOAD LENGTH: 0x6
ID LENGTH: No ID LENGTH field
TYPE: 0x69 ("i")
ID: No ID field
PAYLOAD: 0x040271797971

Record .1.2:
HEADER: 0x54 (MB:0, ME:1, CF:0, SR:1, IL:0, TNF:4)
TYPE LENGTH: 0x3
PAYLOAD LENGTH: 0x1f
ID LENGTH: No ID LENGTH field
TYPE: 0x637573 ("cus")
ID: No ID field
PAYLOAD: 0x940306636964041234567890190103035463706c00656e540302637574047b
Payload as Ascii: " cid 4Vx Tcpl enT cut {"

Payload is a NDEF Message:

Record .1.2.1:
HEADER: 0x94 (MB:1, ME:0, CF:0, SR:1, IL:0, TNF:4)
TYPE LENGTH: 0x3
PAYLOAD LENGTH: 0x6
ID LENGTH: No ID LENGTH field
TYPE: 0x636964 ("cid")
ID: No ID field
PAYLOAD: 0x041234567890

Record .1.2.2:
HEADER: 0x19 (MB:0, ME:0, CF:0, SR:1, IL:1, TNF:1)
TYPE LENGTH: 0x1
PAYLOAD LENGTH: 0x3
ID LENGTH: 0x3
TYPE: 0x54 ("T")
ID: 0x63706c ("cpl")
PAYLOAD: 0x00656e
Payload as Ascii: " en"

Record .1.2.3:
HEADER: 0x54 (MB:0, ME:1, CF:0, SR:1, IL:0, TNF:4)
TYPE LENGTH: 0x3
PAYLOAD LENGTH: 0x2
ID LENGTH: No ID LENGTH field
TYPE: 0x637574 ("cut")
ID: No ID field
PAYLOAD: 0x047b

Record .2:
HEADER: 0x54 (MB:0, ME:1, CF:0, SR:1, IL:0, TNF:4)
TYPE LENGTH: 0x3
PAYLOAD LENGTH: 0x27
ID LENGTH: No ID LENGTH field
TYPE: 0x617376 ("asv")
ID: No ID field
PAYLOAD: 0x940105690501f797985402196c799403096f696404ac801cbfca8d5c3a5401066e05f324234234

Payload is an NDEF Message:

Record .2.1:
HEADER: 0x94 (MB:1, ME:0, CF:0, SR:1, IL:0, TNF:4)
TYPE LENGTH: 0x1
PAYLOAD LENGTH: 0x5
ID LENGTH: No ID LENGTH field
TYPE: 0x69 ("i")
ID: No ID field
PAYLOAD: 0x0501f79798

Record .2.2:
HEADER: 0x54 (MB:0, ME:1, CF:0, SR:1, IL:0, TNF:4)
TYPE LENGTH: 0x2
PAYLOAD LENGTH: 0x19
ID LENGTH: No ID LENGTH field
TYPE: 0x6c79 ("ly")
ID: No ID field
PAYLOAD: 0x9403096f696404ac801cbfca8d5c3a5401066e05f324234234

Payload is an NDEF Message:

Record .2.2.1:
HEADER: 0x94 (MB:1, ME:0, CF:0, SR:1, IL:0, TNF:4)
TYPE LENGTH: 0x3
PAYLOAD LENGTH: 0x9
ID LENGTH: No ID LENGTH field
TYPE: 0x6f6964 ("oid")
ID: No ID field
PAYLOAD: 0x04ac801cbfca8d5c3a

Record .2.2.2:
HEADER: 0x54 (MB:0, ME:1, CF:0, SR:1, IL:0, TNF:4)
TYPE LENGTH: 0x1
PAYLOAD LENGTH: 0x6
ID LENGTH: No ID LENGTH field
TYPE: 0x6e ("n")
ID: No ID field
PAYLOAD: 0x05f324234234

9F 39 – POS Entry Mode per ISO-8583

01 07 – Length (01) and mode (07: Contactless EMV – see ISO-8583)

FF EE 01 – Clearing Record (Group Tag)

04 -- Length

DF 30 – Clearing Record

01 00 – Length (01) and data

DF EE 26 – Attribution byte (refer to NEO IDG)

01 01 – Length (01) and data (01: Contactless card)

0F D3 -- CRC16

7.3. Get VAS and Payment Transaction

VAS data is requested, followed by payment. Payment is always requested.

Command (NEO firmware):

56 69 56 4F 74 65 63 68 32 00 02 40 00 1B 30 9F 02 06 00 00 00 00 00 01 9C 01 00 FF EE 08 0A DF EF 1A 01 01 DF ED 28 01 00 14 D7

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

02 40 – Start Transaction Command

00 1B – Length of payload

30 – Timeout value

9F 02 – Amount, Authorized

06 – Length

00 00 00 00 00 01 – data for Amount

9C – Transaction Type

01 – Length

00 – data

FF EE 08 – Smart Tap Options (group tag)

0A – length

DF EF 1A – Terminal Mode for Smart Tap

01 – Length

01 – Data (Get VAS AND Payment Mode)

DF ED 28 – Service Type Request

01 – Length

00 – data

14 D7 -- CRC

Response:

56 69 56 4F 74 65 63 68 32 00 02 23 02 04 11 82 02 00 00 95 05 00 00 00 00 00 9A 03 14 08 10 9C 01 00 5F 2A 02 08 40 9F 02 06 00 00 00 00 00 01 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 12 03 03 9F 33 03 00 00 E8 9F 34 03 00 00 00 9F 35 01 22 9F 36 02 00 00 9F 37 04 06 C7 B7 BD 9F 39 01 91 9F 53 01 00 DF 81 29 08 30 F0 F0 00 30 F0 FF 00 FF 81 06 31 DF 81 2A 18 33 33 30 30 30 33 33 33 30 30 30 32 32 32 32 32 30 30 30 31 31 31 31 30 DF 81 2B 07 90 00 99 00 00 00 0F DF 81 15 06 00 00 00 00 00 FF FF 81 05 74 50 0A 4D 61 73 74 65 72 43 61 72 64 84 07 A0 00 00 00 04 10 10 9F 11 01 01 9F 6D 02 00 01 56 3E 42 35 34 31 33 31 32 33 34 35 36 37 38 34 38 30 30 5E 53 55 50 50 4C 49 45 44 2F 4E 4F 54 5E 31 39 30 36 31 30 31 33 33 37 38 30 33 33 33 30 30 30 32 32 32 32 32 33 31 33 31 31 31 31 38 9F 6B 13 54 13 12 34 56 78 48 00 D1 90 61 01 90 00 99 31 38 89 8F FF EE 01 2F DF 30 01 00 DF 31 18 33 33 30 30 30 33 33 33 30 30 30 32 32 32 32 32 30 30 30 31 31 31 31 30 DF 32 0D 39 30 30 30 39 39 30 30 30 30 30 30 30 FF EE 08 66 DF EF 76 62 94 03 2F 61 73 76 94 01 06 69 04 02 71 79 79 71 54 03 1F 63 75 73 94 03 06 63 69 64 04 12 34 56 78 90 19 01 03 03 54 63 70 6C 00 65 6E 54 03 02 63 75 74 04 7B 54 03 27 61 73 76 94 01 05 69 05 01 F7 97 98 54 02 19 6C 79 94 03 09 6F 69 64 04 6F 0A F4 F6 F6 56 63 21 54 01 06 6E 05 F3 24 23 42 34 DF EF 4C 06 00 27 00 00 00 00 DF EF 4D 27 3B 35 34 31 33 31 32 33 34 35 36 37 38 34 38 30 30 3D 31 39 30 36 31 30 31 39 30 30 30 39 39 33 31 33 38 38 39 38 3F DF EE 26 01 11 E6 C5

Parsed:

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

02 – Command

23 – Response

02 04 – Length of payload

11 – Attribution byte

82 -- Application Interchange Profile (AIP)

02 – Length

00 00 – Value

95 -- Terminal Verification Results (TVR)

05 – Length

00 00 00 00 00 – Value

9A -- Transaction Date

03 – Length

14 08 10 – Value

9C -- Transaction Type

01 – Length

00 – Value

5F 2A -- Transaction Currency Code

02 – Length

08 40 – Value

9F 02 -- Amount, Authorized

06 – Length

00 00 00 00 00 01 – Value

9F 03 -- Amount, Other

06 -- Length

00 00 00 00 00 00 – Value

9F 06 -- Application Identifier (AID)

07 – Length

A0 00 00 00 04 10 10 – Value

9F 09 -- Application Version Number

02 – Length

00 02 – Value

9F 1A -- Terminal Country Code

02 -- Length

08 40 – Value

9F 1E -- Interface Device (IFD) Serial Number

08 -- Length

30 30 30 30 30 30 30 30 – Value

9F 21 -- Transaction Time

03 – Length

12 03 03 – Value

9F 33 -- Terminal Capabilities

03 – Length

00 00 E8 – Value

9F 34 -- Cardholder Verification Method (CVM) Results

03 – Length

00 00 00 – Value

9F 35 -- Terminal Type

01 – Length

22 – Value

9F 36 -- Application Transaction Counter (ATC)

02 – Length

00 00 – Value

9F 37 -- Unpredictable Number (UN)

04 – Length

06 C7 B7 BD – Value

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

01 – Length

91 – Value

9F 53 -- Terminal Interchange Profile (dynamic)

01 – Length

00 – Value

DF 81 29 -- Outcome Parameter Set

08 – Length

30 F0 F0 00 30 F0 FF 00 – Value

FF 81 06 -- Discretionary Data

31 – Length

DF 81 2A -- DD Card (Track1)

18 – Length

33 33 30 30 30 33 33 33 30 30 30 32 32 32 32 32 30 30 30 31 31 31 31 30 – Value

DF 81 2B -- DD Card (Track2)

07 – Length

90 00 99 00 00 00 0F – Value

DF 81 15 -- Error Indication

06 – Length

00 00 00 00 00 FF – Value

FF 81 05 -- Data Record

74 – Length

50 -- Application Label

0A – Length

4D 61 73 74 65 72 43 61 72 64 – Value

84 -- Dedicated File (DF) Name

07 – Length

A0 00 00 00 04 10 10 – Value

9F 11 -- Issuer Code Table Index

01 – Length

01 – Value

9F 6D -- Kernel 4 Reader Capabilities

02 – Length

00 01 – Value

56 -- Track 1 Data

3E – Length

42 35 34 31 33 31 32 33 34 35 36 37 38 34 38 30 30 5E 53 55 50 50 4C 49 45 44 2F 4E 4F 54 5E 31 39 30 36 31 30 31 33 33 37 38 30 33 33 33 30 30 30 32 32 32 32 32 33 31 33 31 31 31 31 38 -- Value

9F 6B -- Track 2 Data

13 – Length

54 13 12 34 56 78 48 00 D1 90 61 01 90 00 99 31 38 89 8F – Value

FF EE 01 -- ViVOpay TLV Group Tag for Clearing Record

2F – Length

DF 30 -- Track Data Source

01 – Length

00 – Value

DF 31 -- DD Card Track 1

18 – Length

33 33 30 30 30 33 33 33 30 30 30 32 32 32 32 32 30 30 30 31 31 31 31 30 – Value

DF 32 -- DD Card Track 2

0D – Length

39 30 30 30 39 39 30 30 30 30 30 30 30 – Value

FF EE 08 – Smart Tap Result Set

66 – Length

DF EF 76 – NDEF data (See Get VAS Only Transaction for details.)

62 – Length

94 03 2F 61 73 76 94 01 06 69 04 02 71 79 79 71 54 03 1F 63 75 73 94 03 06 63 69 64 04 12 34 56 78 90 19 01 03 03 54 63 70 6C 00 65 6E 54 03 02 63 75 74 04 7B 54 03 27 61 73 76 94 01 05 69 05 01 F7 97 98 54 02 19 6C 79 94 03 09 6F 69 64 04 6F 0A F4 F6 F6 56 63 21 54 01 06 6E 05 F3 24 23 42 34 – Value

DF EF 4C -- MSR Equivalent Data Length Values (for data returned in DFEF4D)

06 – Length

00 27 00 00 00 00 – Value

DF EF 4D -- MSR Equivalent Data (Track Data and/or PAN, encrypted)

27 – Length

3B 35 34 31 33 31 32 33 34 35 36 37 38 34 38 30 30 3D 31 39 30 36 31 30 31 39 30 30 30 39 39 33 31 33 38 38 39 38 3F -- Value

DF EE 26 -- Encryption Status Information

01 – Length

11 – Value (same as Attribution byte)

E6 C5 – CRC

7.4. Push VAS AND Pay Activate Transaction

Command (NEO firmware):

56 69 56 4F 74 65 63 68 32 00 02 40 01 5F 30 9F 02 06 00 00 00 00 00 01 9C 01 00 FF EE 08 82 01 4C DF EF 1A 01 05 DF EF 1B 82 01 41 14 03 65 73 73 72 94 03 03 6F 69 64 04 23 34 54 03 56 73 75 67 01 99 01 19 03 54 73 75 74 02 65 6E 52 65 77 61 72 64 20 50 72 6F 67 72 61 6D 20 41 70 70 6C 69 65 64 59 01 2C 03 54 73 75 64 02 65 6E 31 30 20 70 6F 69 6E 74 73 20 68 61 76 65 20 62 65 65 6E 20 61 64 64 65 64 20 74 6F 20 79 6F 75 72 20 61 63 63 6F 75 6E 74 54 03 65 73 73 72 94 03 03 6F 69 64 04 16 2E 54 03 56 73 75 67 01 99 01 19 03 54 73 75 74 02 65 6E 52 65 77 61 72 64 20 50 72 6F 67 72 61 6D 20 41 70 70 6C 69 65 64 59 01 2C 03 54 73 75 64 02 65 6E 31 30 20 70 6F 69 6E 74 73 20 68 61 76 65 20 62 65 65 6E 20 61 64 64 65 64 20 74 6F 20 79 6F 75 72 20 61 63 63 6F 75 6E 74 54 03 65 73 73 72 94 03 03 6F 69 64 04 04 D2 54 03 56 73 75 67 01 99 01 19 03 54 73 75 74 02 65 6E 52 65 77 61 72 64 20 50 72 6F 67 72 61 6D 20 41 70 70 6C 69 65 64 59 01 2C 03 54 73 75 64 02 65 6E 31 30 20 70 6F 69 6E 74 73 20 68 61 76 65 20 62 65 65 6E 20 61 64 64 65 64 20 74 6F 20 79 6F 75 72 20 61 63 63 6F 75 6E 74 1D 44

Parsed Command:

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

02 40 – Command (Activate Transaction)

01 5F – Length of payload

30 – Timeout value

9F 02 – Amount, Authorized

06 – Length

00 00 00 00 00 01 – Value

9C – Transaction Type

01 00 – Length and data

FF EE 08 – Configuration Container

82 – Overflow flag (0x80) and "length of length" (0x02)

01 4C -- Length

DF EF 1A – Terminal Mode

01 – Length

05 – Mode

DF EF 1B – Outgoing NDEF Service Record

82 – Overflow flag and "length of length"

01 41 – Length

NDEF Service Record of length 01 41:

14 03 65 73 73 72 94 03 03 6F 69 64 04 23 34 54 03 56 73 75 67 01 99 01 19 03 54 73 75 74 02 65 6E 52 65 77 61 72 64 20 50 72 6F 67 72 61 6D 20 41 70 70 6C 69 65 64 59 01 2C 03 54 73 75 64 02 65 6E 31 30 20 70 6F 69 6E 74 73 20 68 61 76 65 20 62 65 65 6E 20 61 64 64 65 64 20 74 6F 20 79 6F 75 72 20 61 63 63 6F 75 6E 74 54 03 65 73 73 72 94 03 03 6F 69 64 04 16 2E 54 03 56 73 75 67 01 99 01 19 03 54 73 75 74 02 65 6E 52 65 77 61 72 64 20 50 72 6F 67 72 61 6D 20 41 70 70 6C 69 65 64 59 01 2C 03 54 73 75 64 02 65 6E 31 30 20 70 6F 69 6E 74 73 20 68 61 76 65 20 62 65 65 6E 20 61 64 64 65 64 20 74 6F 20 79 6F 75 72 20 61 63 63 6F 75 6E 74 54 03 65 73 73 72 94 03 03 6F 69 64 04 04 D2 54 03 56 73 75 67 01 99 01 19 03 54 73 75 74 02 65 6E 52 65 77 61 72 64 20 50 72 6F 67 72 61 6D 20 41 70 70 6C 69 65 64 59 01 2C 03 54 73 75 64 02 65 6E 31 30 20 70 6F 69 6E 74 73 20 68 61 76 65 20 62 65 65 6E 20 61 64 64 65 64 20 74 6F 20 79 6F 75 72 20 61 63 63 6F 75 6E 74 (See Get VAS Only Transaction for details.)

1D 44 – CRC (little-endian)

Response:

56 69 56 4F 74 65 63 68 32 00 02 23 01 A2 11 82 02 00 00 95 05 00 00 00 00 00 9A 03 14 08 10 9C 01 00 5F 2A 02 08 40 9F 02 06 00 00 00 00 00 01 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 13 56 16 9F 33 03 00 00 E8 9F 34 03 00 00

00 9F 35 01 22 9F 36 02 00 00 9F 37 04 96 B1 71 CF 9F 39 01 91 9F 53 01 00 DF 81 29 08 30 F0 F0 00 30 F0 FF 00 FF 81 06 31 DF 81 2A 18 33 33 30 30 30 33 33 33 30 30 30 32 32 32 32 32 30 30 30 31 31 31 31 30 DF 81 2B 07 90 00 99 00 00 00 0F DF 81 15 06 00 00 00 00 00 FF FF 81 05 74 50 0A 4D 61 73 74 65 72 43 61 72 64 84 07 A0 00 00 00 04 10 10 9F 11 01 01 9F 6D 02 00 01 56 3E 42 35 34 31 33 31 32 33 34 35 36 37 38 34 38 30 30 5E 53 55 50 50 4C 49 45 44 2F 4E 4F 54 5E 31 39 30 36 31 30 31 33 33 39 31 35 33 33 33 30 30 30 32 32 32 32 32 38 32 38 31 31 31 31 38 9F 6B 13 54 13 12 34 56 78 48 00 D1 90 61 01 90 00 99 82 84 82 8F FF EE 01 2F DF 30 01 00 DF 31 18 33 33 30 30 30 33 33 33 30 30 30 32 32 32 32 32 30 30 30 31 31 31 31 30 DF 32 0D 39 30 30 30 39 39 30 30 30 30 30 30 30 FF EE 08 04 DF EF 76 00 DF EF 4C 06 00 27 00 00 00 00 DF EF 4D 27 3B 35 34 31 33 31 32 33 34 35 36 37 38 34 38 30 30 3D 31 39 30 36 31 30 31 39 30 30 30 39 39 38 32 38 34 38 32 38 3F DF EE 26 01 11 75 25

Parsed Response:

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

02 23 – Command and response

01 A2 – Length

11 – Attribution byte

82 – Application Interchange Profile tag

02 -- Length

00 00 – Value

95 – Terminal Verification Results tag

05 – Length

00 00 00 00 00 -- Value

9A – Transaction Date

03 – Length

14 08 10 -- Value

9C – Transaction Type

01 – Length

00 – Value

5F 2A – Transaction Currency Code

02 – Length

08 40 – Value

9F 02 – Amount, Authorized

06 – Length

00 00 00 00 00 01 – Value

9F 03 – Amount, Other

06 – Length

00 00 00 00 00 00 – Value

9F 06 – Application Identifier (AID)

07 – Length

A0 00 00 00 04 10 10 – Value

9F 09 – Application Version Number

02 – Length

00 02 – Value

9F 1A – Terminal Country Code

02 – Length

08 40 -- Value

9F 1E – IFD Serial Number

08 – Length

30 30 30 30 30 30 30 30 – Value

9F 21 – Transaction Time

03 – Length

13 56 16 -- Value

9F 33 – Terminal Capabilities

03 – Length

00 00 E8 -- Value

9F 34 – CVM Results

03 – Length

00 00 00 -- Value

9F 35 – Terminal Type

01 – Length

22 -- Value

9F 36 – Application Transaction Counter

02 – Length

00 00 -- Value

9F 37 – Unpredictable Number

04 – Length

96 B1 71 CF – Value

9F 39 – POS Entry Mode

01 – Length

91 – Value

9F 53 – Terminal Interchange Profile

01 – Length

00 – Value

DF 81 29 – Outcome Parameter Set

08 – Length

30 F0 F0 00 30 F0 FF 00

FF 81 06 – Discretionary Data (Group Tag)

31 – Length

DF 81 2A – Track 1 Discretionary Data

18 -- Length

33 33 30 30 30 33 33 33 30 30 30 32 32 32 32 32 30 30 30 31 31 31 31 30 – Value

DF 81 2B – Track 2 Discretionary Data

07 – Length

90 00 99 00 00 00 0F – Value

DF 81 15 – Error Indication

06 – Length

00 00 00 00 00 FF – Value

FF 81 05 – Data Record (Group Tag)

74 -- Length

50 – Application Label

0A – Length

4D 61 73 74 65 72 43 61 72 64 – Value

84 – Dedicated File Name

07 – Length

A0 00 00 00 04 10 10 – Value

9F 11 – Issuer Code Table Index

01 – Length

01 – Value

9F 6D – Kernel Reader Capabilities

02 – Length

00 01 – Value

56 – Track 1 Data

3E -- Length

42 35 34 31 33 31 32 33 34 35 36 37 38 34 38 30 30 5E 53 55 50 50 4C 49 45 44 2F 4E 4F 54 5E 31 39 30 36 31 30 31 33 33 39 31 35 33 33 33 30 30 30 32 32 32 32 32 38 32 38 31 31 31 31 38 – Value

9F 6B – Track 2 Data

13 -- Length

54 13 12 34 56 78 48 00 D1 90 61 01 90 00 99 82 84 82 8F – Value

FF EE 01 – Group Tag for Clearing Record

2F -- Length

DF 30 – Track Data Source

01 – Length

00 – Value

DF 31 – DD Track 1

18 – Length

33 33 30 30 30 33 33 33 30 30 30 32 32 32 32 32 30 30 30 31 31 31 31 30 – Value

DF 32 – DD Track 2

0D – Length

39 30 30 30 39 39 30 30 30 30 30 30 30 – Value

FF EE 08 – Masked Tags

04 -- Length

DF EF 76 – NDEF

00 – Length (no Value)

DF EF 4C -- MSR Equivalent Data Length Values (for data returned in DFEF4D)

06 – Length

00 27 00 00 00 00 -- Value

DF EF 4D -- MSR Equivalent Data

27 -- Length

3B 35 34 31 33 31 32 33 34 35 36 37 38 34 38 30 30 3D 31 39 30 36 31 30 31 39 30 30 30 39 39 38 32 38 34 38 32 38 3F -- Value

DF EE 26 – Attribution

01 – Length

11 -- Value

75 25 -- CRC

7.5. Push VAS Only Activate Transaction:

Command:

56 69 56 4F 74 65 63 68 32 00 02 40 00 CA 30 9F 02 06 00 00 00 00 00 01 9C 01 00 FF EE 08 81 B8 DF EF 1A 01 06 DF EF 1B 81 AE 14 03 67 73 73 72 94 03 05 6F 69 64 04 98 76 67 89 54 03 56 73 75 67 01 99 01 19 03 54 73 75 74 02 65 6E 52 65 77 61 72 64 20 50 72 6F 67 72 61 6D 20 41 70 70 6C 69 65 64 59 01 2C 03 54 73 75 64 02 65 6E 31 30 20 70 6F 69 6E 74 73 20 68 61 76 65 20 62 65 65 6E 20 61 64 64 65 64 20 74 6F 20 79 6F 75 72 20 61 63 63 6F 75 6E 74 54 03 3B 6E 73 72 01 99 01 15 03 54 6E 73 74 02 65 6E 4D 79 20 6C 6F 79 61 6C 74 79 20 70 72 6F 67 72 61 6D 59 01 15 03 55 6E 73 75 00 65 78 61 6D 70 6C 65 2E 63 6F 6D 2F 76 61 6C 75 61 62 6C 65 1C 31

Parsed command:

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

02 40 – Command (Activate Transaction)

00 CA – Length of payload

30 – Timeout value

9F 02 – Amount, Authorized

06 – Length

00 00 00 00 00 01 – Value

9C – Transaction Type

01 – Length

00 – Value

FF EE 08 – Configuration Container Tag

81 – Overflow (because length > 127) and "length of length"

B8 -- Length

DF EF 1A – Terminal Mode

01 – Length

06 – Value (0110: Push VAS Only)

DF EF 1B – Push Service NDEF Record

81 – Overflow flag and "length of length"

AE -- Length

14 03 67 73 73 72 94 03 05 6F 69 64 04 98 76 67 89 54 03 56 73 75 67 01 99 01 19 03 54 73 75 74 02 65 6E 52 65 77 61 72 64 20 50 72 6F 67 72 61 6D 20 41 70 70 6C 69 65 64 59 01 2C 03 54 73 75 64 02 65 6E 31 30 20 70 6F 69 6E 74 73 20 68 61 76 65 20 62 65 65 6E 20 61 64 64 65 64 20 74 6F 20 79 6F 75 72 20 61 63 63 6F 75 6E 74 54 03 3B 6E 73 72 01 99 01 15 03 54 6E 73 74 02 65 6E 4D 79 20 6C 6F 79 61 6C 74 79 20 70 72 6F 67 72 61 6D 59 01 15 03 55 6E 73 75 00 65 78 61 6D 70 6C 65 2E 63 6F 6D 2F 76 61 6C 75 61 62 6C 65
(See Get VAS Only Transaction for details.)

1C 31 – CRC (little-endian)

Response:

56 69 56 4F 74 65 63 68 32 00 02 57 00 1A 01 FF EE 08 04 DF EF 76 00 9F 39 01 07 FF EE 01 04 DF 30 01 00 DF EE 26 01 01 8A 23

Parsed response:

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

02 57 – Command and response

00 1A – Length of payload

01 – Attribution byte

FF EE 08 – Container

04 – Length

DF EF 76 – NDEF Record

00 – Length (no Value)

9F 39 – POS Entry Mode

01 – Length

07 – Value

FF EE 01 – Group Tag for Clearing Record

DF 30 – Track Data Source

01 -- Length

00 -- Value

DF EE 26 – Attribution Byte

01 -- Length

01 -- Value

8A 23 -- CRC

7.6. Encrypted VAS Only Activate Transaction:

Command (NEO firmware):

56 69 56 4F 74 65 63 68 32 00 02 40 00 1B 30 9F 02 06 00 00 00 00 00 01 9C 01 00 FF EE 08 0A DF EF 1A 01 0A DF ED 28 01 00 B6 14

Encryption Key parameters:

BDK: 0123456789ABCDEFFEDCBA9876543210

KSN: 629949012C0004600001 (will come back in response in tag FFEE12)

Response:

56 69 56 4F 74 65 63 68 32 00 02 57 00 95 C1 FF EE 12 0A 62 99 49 01 2C 00 04 60 00 01 FF EE 08 C1 70 76 FF C5 F9 BB A4 EC 34 FD 5C 9A D5 C5 9F 6C 7F 45 71 2F CC 1C F1 CC 7B 06 12 6B C4 FF 73 9A F2 13 EF 7D 70 AB 01 E9 EF EA 7B C7 8D B7 5F AC 9D AC 8E 9B 0D A7 78 9E 8C 53 2E A5 A0 7E 36 F3 84 4E CF 5A 24 91 12 A7 31 F9 3E A7 33 C1 F9 B1 7F F3 3A 38 AE 85 8F 05 18 9F EF 53 24 5B 00 9F 57 CD 35 4A CE 04 C0 D7 04 5B DD C0 E3 B0 FE 7E FF 9F 39 01 07 FF EE 01 04 DF 30 01 00 DF EE 26 01 C1 87 6F

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

02 57 – Command and response

00 95 – Length of payload

C1 – Attribution byte

FF EE 12 -- KSN

0A -- Length

62 99 49 01 2C 00 04 60 00 01 – Value of KSN

FF EE 08 – NDEF Container

C1 – 'C' means the contents are encrypted, '1' is the length of the length

70 – Length (original data length rounded up to multiple of 8, for TDES)

76 FF C5 F9 BB A4 EC 34 FD 5C 9A D5 C5 9F 6C 7F 45 71 2F CC 1C F1 CC 7B 06 12 6B C4 FF 73 9A F2 13 EF 7D 70 AB 01 E9 EF EA 7B C7 8D B7 5F AC 9D AC 8E 9B 0D A7 78 9E 8C 53 2E A5 A0 7E 36 F3 84 4E CF 5A 24 91 12 A7 31 F9 3E A7 33 C1 F9 B1 7F F3 3A 38 AE 85 8F 05 18 9F EF 53 24 5B 00 9F 57 CD 35 4A CE 04 C0 D7 04 5B DD C0 E3 B0 FE 7E FF

9F 39 – POS Entry Mode

01 – Length

07 -- Value

FF EE 01 – Container tag

04 – Length of container payload

DF 30 – Track Data Source

01 00 – Length (01) and Value (00)

DF EE 26 – Attribution byte

01 – Length

C1 – Value

87 6F – CRC

Note that using a BDK of 0123456789ABCDEFFEDCBA9876543210 and a KSN of 629949012C0004600001 results in a one-time DUKPT session (Data) key of AA9C25D7FE17CFC88033197D0304AEB3. (Use the free tool at https://www.idtechproducts.com/hosted-files/tools/encryptiondecryptiontool.html to derive DUKPT session keys and decrypt data.)

The encrypted NDEF payload (from tag FF EE 08), after decryption with the one-time key, will look as follows:

FF EE 08 66 DF EF 76 62 94 03 2F 61 73 76 94 01 06 69 04 02 71 79 79 71 54 03 1F 63 75 73 94 03 06 63 69 64 04 12 34 56 78 90 19 01 03 03 54 63 70 6C 00 7A 68 54 03 02 63 75 74 04 7B 54 03 27 61 73 76 94 01 05 69 05 01 F7 97 98 54 02 19 6C 79 94 03 09 6F 69 64 04 DC 14 8D 1A 6F A8 BB 4A 54 01 06 6E 05 F3 24 23 42 34 00 00 00 00 00 00

The correct native length is shown after FF EE 08 as 66. This length is the length of the native data; it makes it possible to parse out (remove) the 00 padding bytes that occur at the end, which were put there in order to facilitate block-ciphered TDES encryption.

7.7. Simplified Output

Example:

56 69 56 4F 74 65 63 68 32 00 02 01 00 1B 30 9F 02 06 00 00 00 00 00 01 9C 01 00 FF EE 08 0A DF EF 1A 01

02 DF ED 28 01 00 69 77

With DFEF77 set to 0

Response:

324234242

With DFEF77 set to 1 and delimiter set to 0x0D (CR)

Response:

324234244<CR>324234240<CR>324234238<CR>324234241<CR>324234237<CR>324234236<CR>324234243<CR>324234235<CR>324234242<CR>324234239<CR>324234234<CR>

In this example, there are 11 services objects: Loyalty “324234234”, Offer “324234235”, Offer “324234236”, Offer “324234237”, Offer “324234238”, Offer “324234239”, Offer “324234240” , Offer “324234241” , Offer “324234242” , Offer “324234243” , Offer “324234244”.

APPENDIX A: ECC Key Pair

The party that wishes to use SmartTap (typically a merchant) has the responsibility of creating and managing the ECC (Elliptical Curve Cryptography) key pair that will be used for the security of the communication between the reader and the wallet.

The public key must be communicated to Google. (It can be sent in the clear to anyone. It is a public key.)

The private key must be kept private. It will be injected into the ViVOpay device (where it will be stored securely).

How to create an ECC key pair using open-ssl

The ECC key pair (or the ECDSA digital signature key pair) can be generated several different ways. Below is an example using the freely available OpenSSL package to generate a prime256v1 Elliptical Curve Cipher key pair (and to sign messages) as shown below.

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
```

Revision History

Version	Date	By	Comment
Rev. A	8/10/2018 8/15/2018	KT	Initial draft of public version. Disclaimers regarding firmware differences.
Rev. B	8/30/2018 8/31/2018	KT	Clarifications of various security-related items. Add updated Service Byte definitions.
Rev. C Rev. D	11/30/2018	KT	Include discussion of tag DFED3F for encryption of VAS data separate from financial data. Specify that tags with no defaults should exist, but should be empty.
Rev. E	12/21/2018	KT	Add info about UID in tag DFED44.
Rev. F	12/28/2018	KT	Change examples to use 04-03 instead of 04-00.