IDTECH®

Value through Innovation

VP3350

Integration Manual

80178501-001 Rev. S

28 July 2025

ID TECH

10721 Walker Street, Cypress, CA 90630-4720

Tel: (714) 761-6368 Fax (714) 761-8880

www.idtechproducts.com

ID TECH
10721 Walker Street
Cypress, CA 90630 USA

Warranty Disclaimer
The services and hardware are provided "as is" and "as available" and the use of the services and hardware are 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.

FCC warning 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.

The user manual for an intentional or unintentional radiator shall caution the user that changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Note: The grantee is not responsible for any changes or modifications not expressly approved by the party responsible for compliance. Such modifications could void the user's authority to operate the equipment.

Note: 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 or more of the following measures:

- Increase the distance between the equipment and the 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.

This device complies with FCC RF radiation exposure limits set forth for an uncontrolled environment.
The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter and must be installed to provide a separation distance of at least 20cm from all persons.

Innovation, Science and Economic Development Canada (ISED) statement

This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's licence-exempt RSS(s).

Operation is subject to the following two conditions:

1. This device may not cause interference, and
2. This device must accept any interference, including interference that may cause undesired operation of the device.

L'émetteur/récepteur exempt de licence contenu dans le présent appareil est conforme aux CNR d'Innovation, Sciences et Développement économique Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

1. l'appareil ne doit pas produire de brouillage, et
2. l'utilisateur de l'appareil doit accepter tout brouillage radioelectrique subi, meme si le brouillage est susceptible d'en compromettre le fonctionnement.

Cautions and Warnings

	Caution: Danger of Explosion if battery is incorrectly charged. Use only standard USB 5V power source. Device contains a lithium battery. Approved temperature range for storage: -20℃ to +60℃. Disposal: Contact your local recycling center.
	Warning: Avoid close proximity to radio transmitters, which may reduce the capabilities of the reader.

Caution: Exposure to Radio Frequency Radiation

To comply with the Canadian RF exposure compliance requirements, this device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter.

Attention: exposition au rayonnement radiofréquence

Pour se conformer aux exigences de conformité RF canadienne l'exposition, cet appareil et son antenne ne doivent pas être co-localisés ou fonctionnant en conjonction avec une autre antenne ou transmetteur.

Internal Rechargeable Battery Warning [1]

Danger: Do not attempt to replace the internal rechargeable lithium-ion battery. Replacing the original battery with an incompatible type may result in an increased risk of personal injury or property damage due to explosion, excessive heat, or other risks. Do not attempt to disassemble or modify the battery pack. Attempting to do so can cause a harmful explosion or battery fluid leakage.

When disposing of the battery, comply with all relevant local ordinances or regulations. Do not dispose of the battery pack in municipal waste. Dispose of used batteries according to the instructions.
The battery pack contains a small amount of harmful substances.

To avoid injury:

- Keep the battery pack away from open flames or other heat sources.
- Do not expose the batter pack to water, rain, or other corrosive liquids.
- Do not leave the battery in an environment with extremely low air pressure. It may result in an explosion or the leakage of flammable liquid or gas from the battery.

To extend battery life, we recommend charging the battery to at least 30% to 50% capacity each time and recharging it every three months to prevent over discharge.

[1] Note that the SRED VP3350 is a PCI SRED certified device; any attempt to replace the internal Lithium-Ion battery will result in a device tamper, rending the unit inoperable.

Revision History

Date	Rev	Changes	By
12/08/2022	A	Initial release.	CB
02/06/2023	B	Updated LED and Sound State Indicators table and footnote.	CB
02/16/2023	C	Updated mounting guidelines and diagrams.	CB
03/22/2023	D	Tag 9F33: Updated byte 2 bit 5 (feature not supported).	CB
05/24/2023	E	Added specifications section; moved environmental/storage specs and power consumption there. Added cable-related power requirements to VP3350 Connectors and Interfaces section. Added note to iOS Connectivity section about iOS SDK integration for apps.	CB
03/07/2024	G	Updated Major VP3350 Features, Contactless NFC Features and Brand Certifications, and Other Agency Approvals and Compliances. Updated Specifications section. Updated VP3350 Connectors and Interfaces. Added power management commands. Added charging capability commands.	CB
04/19/2024	H	Added Configuring a VP3350 with the ID TECH Universal SDK section.	CB
04/22/2024	J	Added Appendix A: VP3350 Demo Setup for Mobile Devices.	CB
06/27/2024	K	Added Set/Get BLE Chip Command (77-86). Miscellaneous updates.	CB
08/01/2024	L	Added Avoiding Device Tamper Issues section. Updated PMC state diagrams. Updated power-related command descriptions.	CB
10/01/2024	M	Updated LED state table. Added USB C PMC state diagram to Power management section. Updated Enter Low Power Mode (F0-03) command. Updated Set Low Power Consumption Configuration (F0-04) command. Added new Appendix A: LED 0 Behavior Status, renumbered previous appendix. Added new section: 24-Hour Device Reboot. Added new section: Checking Battery Levels.	CB
03/18/2025	N	Added Appendix C: Auto-Transaction Mode (AT). Misc improvements to descriptions throughout document. Updated PMC state diagrams Updated Low-Level Commands section.	CB
05/13/2025	P	Minor text updates.	CB
06/24/2025	R	Updated Decommissioning PCI-Certified Products section.	CB
07/28/2025	S	Added USB Specifications section.	CB

Table of Contents

1. Introduction

The VP3350 is ID TECH's latest PCI 6.X SRED-certified and non-SRED mobile reader. The VP3350 supports Magstripe, EMV contact, and contactless transactions using either USB-C, Lighting, and/or Bluetooth connections.

The VP3350's compact form factor makes it ideal for mobile applications requiring smart card reading, or for incorporating into a case or stand associated with a countertop POS terminal. As a mobile reader, VP3350 works in conjunction with Android and iOS phones and tablets using USB-C male, Lightning (iOS only), or Bluetooth (Model C only). The VP3350 is designed to be compatible with a wide range of third-party payment applications, and the ID TECH Universal SDK (described further below) is available for developing applications that communicate with VP3350.

Contact your acquirer, gateway, or POS partner for instructions on setting up and pairing the VP3350 to a compatible payment application and associated host device.

1.1. Major VP3350 Features

- Compliant with the latest security standard, PCI 6.x
- Accepts Magstripe, EMV, and NFC/Contactless in a small footprint
- Multiple communication options to host devices: Lightning, USB-C, and Bluetooth (BLE 5.0) interfaces
- Lightning and USB-C with MFi certification with compact and swivel connector design
- Side USB-C female connector supports battery charging as well as communication with Android or Windows host systems
- Rechargeable battery (Lightning and USB-C models), no external power necessary
- Supports pass-through charging
- Supports low power mode
- Supports direct and remote key Injection
- LED status indicator
- Field-upgradable firmware
- Supports Triple DES, AES128, and TransArmor with DUKPT key management
- Supports Retail MAC and HASH encryption algorithm
- Supports Apple Pay, Google Pay, Samsung Pay, and mobile loyalty programs like Apple VAS and Google SmartTap 2
- Support major International kernels such as eftpos, JCB, CUP, Interac and more
- Compact and ergonomic design to integrate with a variety of mobile devices
- Optional charging stand available to enable a countertop solution

Refer to the table below for the differences among the VP3350 models.

1.2. Contactless NFC Features and Brand Certifications

- ISO 14443 Type A&B
- ISO 18092
- CTLS L2 Payment Kernels:
    - MasterCard® MChip (Formerly PayPass)
    - Visa
    - Discover® DPAS
    - American Express® ExpressPay
    - Interac
    - Interac Transit
    - JCB
    - UPI and UPI Transit
    - eftpos
- MIFARE: native support
- FeliCa
- Apple Pay
- Apple VAS
- Samsung Pay NFC
- Android Pay
- Google Pay
- Google Smart Tap 2.1

1.3. Other Agency Approvals and Compliances

- CE (EN55032/EN55035, Class- B)
- FCC (Part 15, Class-B)
- RoHS (DIRECTIVE 2015/863/EU)
- REACH
- EMV Contact L1&L2
- EMV Contactless L1 and majority of Contactless 2
- TQM
- PCI PTS 6.X SRED
- AS/NZS 4268

2. Specifications

The sections below describe VP3350 environmental and power specifications.

2.1. Operation and Storage: Environmental Limits

Item	Specification	Note
Operating Temperature	0 °C to 55 °C or 32°F to 131°F	Non-condensing. Product operation temperature is limited to this range due to constraints of the Li-Battery specification.
Storage Temperature	-20 °C to 60 °C or -4°F to 140°F	Non-condensing. Product storage temperature is limited to this range due to constraints of the Li-Battery specification.
Operating Humidity	Up to 95%	Non-condensing.
Storage Humidity	Up to 95%	Non-condensing.

2.2. USB Specifications

USB C Female		
Power Supply Requirement	**Voltage (V)**	4.75 to 5.25
	Current (A)	3
	Power (W)	15
USB	**Version**	2.0
	Protocol	USB Standard
USB Speed (Full speed or High Speed)		Full speed
PD Support		Not supported
USB Role(Host or Device)		Device
OTG		Not supported
Pin Out		No

USB Power Delivery

Mode of Operation	Voltage	Max Current	Max Power
USB 1.x / USB 2.0	5 V	0.5 A	2.5 W
USB 3.X	5 V	0.9 A	4.5 W
USB-C (Standard)	5 V	3 A	15 W
USB-C (PD)	5 - 20 V	5 A	25W - 100W

2.3. Battery Life for Lightning and Bluetooth Models

The VP3350 Lighting and Bluetooth models come equipped with battery that can support transactions as below:

- Minimum 800 MSR transactions per battery charge (with 30 second interval)
- Minimum 500 contact transactions per battery charge (with 30 second interval)
- Minimum 400 contactless transactions per battery charge (with 30 second interval)
- Minimum 200 contactless + 200 contact + 100 MSR transactions per battery charge (with 30 second interval)

Maximum power draw is 500mA for VP3350 power consumption and internal battery charging.

3. VP3350 Connectors and Interfaces

The VP3350 is designed to work Windows, Android, and iOS via a physical USB-C, Lightning, and Bluetooth communication.

- All VP3350 models come equipped with USB-C female connector as the power source and communicate with Windows, mobile phones and tablets.
- VP3350 Model-B equipped with Lightning connector communicates with popular mobile iOS devices.
- VP3350 Model-C equipped with Bluetooth connection capability.
- VP3350 Model-F equipped with USB-C male connector allows for pass-through charging to the host device and communicate with Android or iOS mobile devices.

Part Number	IDMR-xLR93x	IDMR-xBT93x	IDMR-xUF93x	IDMR-xUR93
Picture				
Model (Device Tree)	B	C	D	F
USB-Female	○	○	○	○
USB-Male				○ (Rotatable)
Lighting-Male	○ (Rotatable)			
BLE 5.0		○		
Side Button		○		
Battery 400mAh	○	○		
Power Passthrough	○			○
MFi Certification	○			○
USB-KB Interface			○	
Female Application	Android/Windows	Android/Windows	Android/Windows	Android/Windows
Male Application	iOS			iOS/Android

When communicating over USB, the VP3350's default emulation mode is USB HID; rev D models of the reader can also emulate a USB HID-KB interface.

3.1. Pass-Through Charging Power Requirements

VP3350 readers require the following for pass-through charging:

- Mobile phones: 5V/1A
- Tablets: 5V/1.5A

Note that the VP3350's maximum power output is 7.5W (5V/1.5A).

3.2. Cabling Power Requirements

The following power requirements apply to all cabling permutations (for example, USB-C to USB-C vs. USB-A to USB-C).

- When using a USB-C to USB-C cable with power input, the VP3350 provides a maximum of 1.5A through the VP3350 male connector to a phone or tablet.
    - The Lightning version (IDMR-xLR93x) maximum is 1A.
    - The USB-C version (IDMR-xUR93x) maximum is 1.5A.
- When using a USB-A to USB-C cable with power input, the VP3350 provides a maximum of 0.5A through the VP3350 male connector to a phone or tablet. Note that the tablet will not show a charging symbol because it needs at least 1A for the charging symbol to appear.

4. Bluetooth Pairing Instructions (SRED-Only)

In addition to the following instructions, see the section on iOS Connectivity for more information on using an iPad or iPhone in conjunction with the VP3350.

1. Enable the Bluetooth device search function on the host device (smart phone or tablet).
2. Make sure the VP3350 is charged or connected to a power source via USB.
    a. When connected to a power source, the VP3350 automatically activates Bluetooth.
3. When not connected to a power source, press the VP3350's side button to manually activate Bluetooth.
4. Find a Bluetooth device named **IDTECH-VP3350-XXXXX** on the host smart phone or tablet and select **Pair**.
5. Enter the password for pairing. The default password is **123456**.
6. Follow the payment transaction instructions provided by a compatible payment application maker to complete a transaction.

The VP3350 will remain connected via Bluetooth to the host device indefinitely when powered via the USB cable. If the unit is operating on battery power, it will go to sleep after 20 seconds of idling to extend battery life. To perform a transaction again, press the side button to re-establish the Bluetooth connection.

When connecting to an iOS device, please install a compatible payment application and follow the instructions provided by that application's maker. See iOS Connectivity: BLE and VP3350 below for more information.

5. Battery Charging Instructions

VP3350 Lighting and Bluetooth readers are powered by a lithium-ion polymer battery and are delivered in a partially-charged state. Be sure to fully charge the VP3350 before using it for the first time.

Note: Make sure to allow two to three hours for the initial charge.

Use a standard USB to USB-C cable to charge the unit. An LED battery indicator displays the current battery charging status [2].

Warning: When using a "fast charger" with a VP3350 reader, only use a USB-C to USB-C cable.

5.1. Tamper and Failed Self-Check Indicators

The VP3350 displays the following indicators when it has been tampered or has any of the other following internal issues, such as an expired certificate, missing key, or similar fault discovered during a self-check.

Indicator	Tampered Status	Other Issue Status
Front Four LEDs	All LEDs blink red	All LEDs blink red
Buzzer	Alarm tone	Alarm tone

5.2. Avoiding Device Tamper Issues

All ID TECH PCI-certified devices integrate tamper switches and disable the card reader when it has been compromised. The section below describes best practices when handling PCI-secure devices to help prevent triggering the tamper switches.

Note that following these guidelines does not guarantee a device will not tamper if inadvertently mishandled or breached. User-induced tamper events will incur repair fees, key injection fees, and shipping both to and from ID TECH, regardless of warranty status.

[2] Use the **Get Battery Level (F0-02)** command to retrieve the reader's battery level.

5.2.1 Device Handling Best Practices

- Do not excessively shake the reader.
- Do not drop the reader.
- Do not strike the reader.
- Do not attempt to twist or cause any torsion to the reader.
- Do not expose the reader to extreme heat or cold.
- Do not intentionally subject the reader to electrical shocks.
- Do not submerge the reader in liquids of any type for extended time.
- Do not attempt to open the reader.
- Do not provide power to the reader until all connectors are plugged into the unit.
- Check the device manual to ensure the reader receives the correct power voltage. Providing power to wires and connectors before plugging them into the device may cause power spikes that can trigger a tamper event.
- When working with or installing the reader, minimize exposure to static electricity.

5.2.2 ID TECH Support

In the event the reader does tamper when under warranty, report the tampered device to ID TECH to troubleshoot and, if needed, be returned to ID TECH for analysis. Contact ID TECH support at support@idtechproducts.com for assistance.

5.3. VP3350 LED and Sound State Indicators

The VP3350 uses the following LEDs and sounds to indicate various statuses, including power management, Bluetooth, transactions, and security.

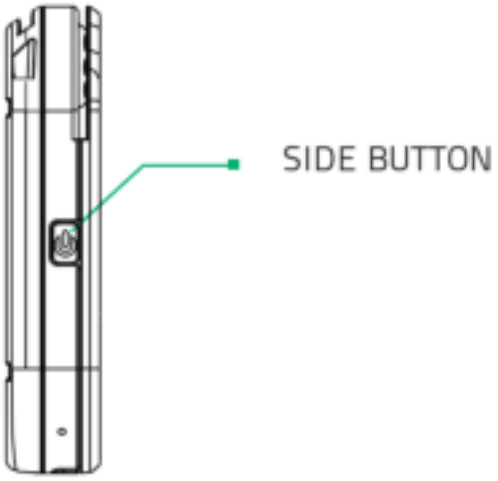
Device State	LED 1	LED 2	LED 3	LED 4	Sound
Power Off / Low-Power Consumption Mode	off	off	off	off	None
Unit On in Run Mode	blink	off	off	off	None
Unit On in Run Mode and Battery Low	blink	off	off	off	None
Unit On in Standby Mode*	short blink	off	off	off	None
Unit On in Standby Mode and Battery Low*	short blink	off	off	off	None
Bluetooth Connection Established	blink once	blink once	blink once	blink once	One Beep
Bluetooth Connection Disconnected	blink once	blink once	blink once	blink once	Two Beeps
Bluetooth Connected in Run Mode	blink	off	blink	off	None
Bluetooth Connected in Run Mode and Battery Low	blink	off	blink	off	None
Bluetooth Connected in Standby Mode	short blink	off	short blink	off	None
Bluetooth Connected in Standby Mode and Battery Low	short blink	off	short blink	off	None
Battery Charging Full**	on	on	on	on	None
Transaction Activated (Ready for Payment CT/CTLS/MSR)	on	off	off	off	None
Contactless Transaction Successful	blink once	blink once	blink once	blink once	One Long Beep
Contactless Transaction Failed	blink twice	blink twice	blink twice	blink twice	Two Short Beeps
Contactless Try Again	off	off	off	off	Three Short Beeps
Contactless Transaction Processing	fast blink	off	off	off	None
MSR Transaction Successful	blink once	blink once	blink once	blink once	One Long Beep
MSR Transaction Failed	off	off	off	off	Two Short Beeps
Device Tampered	blink	blink	blink	blink	Unit Beeps

*Note: VP3350 Model C only.

**Use the Get Battery Level (F0-02) command to retrieve battery level. When charging, the reader displays three green LEDs to indicate 75% charge, two green LEDs to indicate 50% charge, and one red LED to indicate a charge under 25%. Users may also press the reader's side button to view charge status.

5.3.1 Checking Battery Levels

Pressing the side button (below) on the VP3350 displays the reader's current battery level on the four front LEDs.



Pressing the side button shows the reader's battery level as described below:

Device State	LED 1	LED 2	LED 3	LED 4
Battery 0 to 25%	blink once	off	off	off
Battery 25 to 50%	blink once	blink once	off	off
Battery 50 to 75%	blink once	blink once	blink once	off
Battery 75 to 100%	blink once	blink once	blink once	blink once

5.4. 24-Hour Device Reboot

Per PCI Requirements, this device reboots every 24 hours. Note the following information about required device reboots:

- **Clock Setting:** The reader's internal clock is based on UTC time. By default, the 24-hour reboot time is set to 12:00 AM UTC time, which translates to 5:00 PM PST (UTC-7). Device integrators may adjust the 24-hour reboot time via the **Set/Get 24-Hour Self-Check Time (25-07)** command with hex data in the format of **hhmm** (two digits representing the hour followed by two digits representing minutes; for example, **hhmm = 1830** represents 6:30 PM UTC time).

- **Boot Up Beep Configuration:** By default, the reader beeps one time when it boots up. This behavior is controlled by Tag DFED5A, Byte 3 Bit 1. Setting this bit to 1 mutes the beep sound during a reboot. Because the beep is controlled at bit level, you must know the current value of Tag DFED5A to make the change. For example, use the **Get Configuration (03-02)** command to retrieve the Tag DFED5A value in group 0 and change its Byte 3 Bit 1 value to **1**. DFED5A's value is **00 00 C0 00 00 00 00 00**, send the **Set Configuration (04-00)** command with hex data **00 00 C2 00 00 00 00 00** to disable the bootup beep.

5.5. iOS Connectivity: BLE and VP3350

Note: Applications for iOS must integrate ID TECH's iOS SDK. The .ZIP file for the SDK, available on the ID TECH Knowledge Base, includes the *Apple iOS SDK Guide* and information on connecting ID TECH devices via BLE.

The VP3350 uses Bluetooth 5.0, also known as Bluetooth BLE (Bluetooth Low Energy). Unlike previous versions of Bluetooth, BLE does not require users to first pair their devices through the Bluetooth Settings in Apple iOS. If a payment application provider has enabled BLE scanning in their application, Apple iOS scans and locates all BLE devices in range to automatically connect with the VP3350.

It is critical to note that if the VP3350 is paired via the iOS Settings page, it will display as a connected device but not function with a payment app.

Unlike other operating systems that can detect or specify a BLE device by its MAC address, Apple does NOT allow users to specify a BLE device by MAC address for security reasons. Instead, after a device is selected by its "friendly" name (see the next paragraph), the Apple iOS calculates a unique identifier to allow that device to make further connections directly.

The VP3350 has a default friendly name of **IDTECH-VP3350-XXXXX**[3]. This is the default name the ID TECH Universal SDK uses to connect to the first VP3350 it encounters if no other friendly name is set in the SDK, or when the iOS-generated device identifier is not provided. See links given near the end of this document for information about the Universal SDK.

Note: The Universal SDK is primarily of interest to developers. If an application provider or POS software partner has already provided software to use with the VP3350, you do not need to obtain the SDK.

[3] Note that the last five digits (here denoted as XXXXX) are the same as the last five digits of the reader's serial number.

6. VP3350 Mounting and EMV Contactless Logo Requirements

Note that if the VP3350 is mounted behind any kind of casing or cover, that assembly MUST follow EMV requirements regarding contactless logo size and position. See EMVco Contactless Symbol Reproduction Requirements for details.

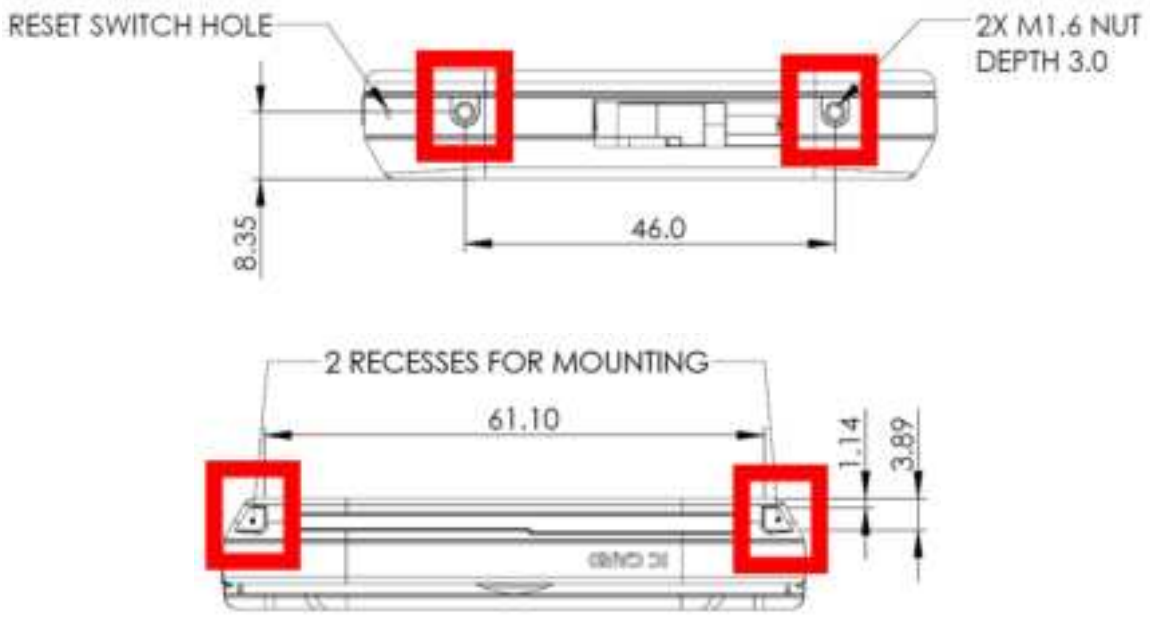
6.1. Contactless Mounting

To optimize performance, install VP3350 readers away from or in front of any metal surfaces or materials that have metallic content, which can interfere with the RF field. VP3350 readers perform optimally when mounted away from metal surfaces.

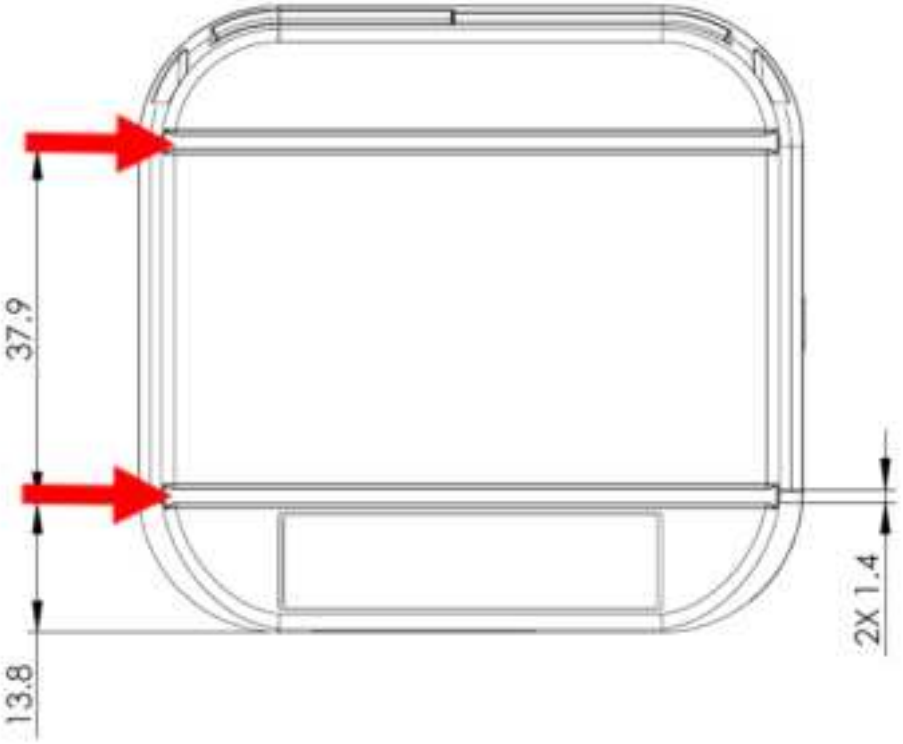
6.2. VP3350 Side Button Requirements and Mounting

When mounting the VP3350 to a surface or with another device (such as a tablet), use the following guidelines:

- For the Bluetooth version of the VP3350, make sure to keep the side button accessible.
- The USB-C male and USB-C female versions of the VP3350 do not require an exposed side button as those models do not have internal batteries.
- If desired, use the two screw holes on the bottom side of unit and two recesses on the top side of unit highlighted below for mounting:



- Likewise, the VP3350 has slots on the back for alignment, shown below:



7. ID TECH Universal SDK

By virtue of its EMV L2 kernel, VP3350 is designed to be compatible with a wide range of third-party payment applications. ID TECH offers a Universal SDK (available for iOS, Android, or Windows) to enable rapid application development using VP3350 as the target device. The languages supported include Objective C (on iOS), Java (on Android), and C# (on Windows). The Universal SDK includes rich, powerful libraries that make sending commands to the VP3350 comparatively easy while greatly facilitating debugging and event handling.

To obtain the Universal SDK free of charge, visit ID TECH's VP3350 product page and select the version of the SDK that applies to your desired host platform (Android, iOS, Linux, MacOS, or Windows).

Normally, development of applications that take advantage of VP3350's capabilities can be done in a high-level language like C# or Java (using convenience objects and data structures defined in the Universal SDK), obviating the need to send byte commands directly. Nevertheless, it is possible to communicate with the device at a low level if necessary. For a command reference for VP3350, contact your ID TECH representative to request the *NEO 2 Interface Developers Guide* (IDG), P/N 80139403-002. This document includes not only low level (firmware) commands but error codes, response codes, and information on various default settings.

7.1. Updating VP3350 Firmware

ID TECH strongly recommends updating firmware via the Universal SDK. Contact ID TECH support for your reader's firmware, then consult the Universal SDK Guide for your desired platform (included in the firmware update ZIP file) for integration details.

7.2. Using the Correct Firmware Files

Due to the multiple models of VP3350 readers, make sure to select the correct firmware update files. Contact your ID TECH support representative to receive a .ZIP archive with the necessary firmware for your reader.

7.3. Configuring a VP3350 with the ID TECH Universal SDK

The ID TECH Universal SDK exposes a variety of methods for obtaining low-level access to features of the kernel like AIDs and CAPKs, allowing users to override or update various features as needed.

Note: ID TECH's Universal SDK provides source code for two apps. One of the apps represents the project created using the Tutorial in the documentation and can be found here. The other demo app is more elaborate and used for general device testing and configuration. In the sections below, references to the "demo app" apply to the latter project, not the Tutorial project. The source code for the demo app can be found here, and the compiled executable of the demo app can be found here.

ID TECH readers can support at least 23 major kernel configurations (**1C** through **23C**). Refer to this document for more information about available configurations.

Many terminal capability settings are considered "minor" settings that can be tailored to fit a scenario. Some are considered "major" settings that can't be changed without producing a runtime error. For more information on Terminal Settings and kernel configurations (and the settings that can be changed without producing an error), consult Which Terminal Settings Am I Allowed to Change? on the ID TECH Knowledge Base.

7.3.1 Setting AIDs

The card reader needs to know which application identifiers (AIDs) you intend to support. Configure this using code similar to the following example:

```
RETURN_CODE rt;
      byte[] name = Common.getByteArray("a0000000031010");
      byte[] aid =
Common.getByteArray("9f01065649534130305f5701005f2a0208409f0902009
65f3601029f1b0400003a98df25039f3704df28039f0802dfee150101df1305000
0000000df14050000000000df15050000000000df180100df170400002710df190
100");

// Tell the reader the name and value of the AID you wish to
support: rt =
IDT_NEO2.SharedController.emv_setApplicationData(name, aid);

      if (rt == RETURN_CODE.RETURN_CODE_DO_SUCCESS)
            {
                  tbOutput.AppendText("Default AID Successful\r\n");
            }
      else
            {
                  tbOutput.AppenText("Default AID failed Error Code:
                  " +
                        "0x" + String.Format("{0:X}", (ushort)rt) +
                        ":" + IDTechSDK.errorCode.getErrorString(rt)
                        + "\r\n");
            }
```

As with Terminal Configuration, setting the default AIDs is something you will likely do only one time, not on a per-transaction basis.

7.3.2 Setting CAPKs

You will also want to set the reader's supported Certificate Authority Public Key values (each card brand has one or more CAPKs for doing offline data authentication). The example below shows sample code for setting a CAPK:

```
      byte[] capk =
Common.getByteArray("a000000003500101b769775668cacb5d22a647d1d9931
41edab7237b000100018000d11197590057b84196c2f4d11a8f3c05408f422a35d
702f90106ea5b019bb28ae607aa9cdebcd0d81a38d48c7ebb0062d287369ec0c42
124246ac30d80cd602ab7238d51084ded4698162c59d25eac1e66255b4db235252
6ef0982c3b8ad3d1cce85b01db5788e75e09f44be7361366def9d1e1317b05e5d0
ff5290f88a0db47");

      RETURN_CODE rt = IDT_NEO2.SharedController.emv_setCAPK(capk);
```

This again is something probably configured only one time, not on a per-transaction basis.

Note: If EMV transactions are failing because of inability to perform ODA/CDA (as indicated in the first byte of TVR data, Tag 95), make sure your CAPKs are up to date.

7.4. Performing Transactions

The section below walks through the steps required for performing transactions.

7.4.1 Start Transaction

The Start Transaction command, issued via the method **emv_startTransaction()**, does the following:

When a card is already seated:

- Initiates a **Power On** sequence with the ICC reader
- If an ICC cannot be detected (no **ATR:Answer To Reset**), a fallback condition occurs and the reader requests a swipe.
- If the reader receives an ATR, it establishes timeout for the receipt of an **Authenticate Transaction** command and transmits **Application Data** parameters to the card, and the EMV transaction starts.

When a card is not seated:

- The MSR Swipe and the Contactless antenna is enabled, along with monitoring for a card to be inserted.

When a Swipe is executed first:

- If a non-ICC card is swiped, the swipe data is returned and the transaction is over.
- If an ICC card is swiped, the swipe is rejected and the kernel prompts to use the ICC (insert the card).

When executing **emv_startTransaction()**, TLV data should, at a minimum, contain the following tags:

- **9F02:** Amount
- **9F03:** Other amount
- **9C:** Transaction type

In addition, you can optionally include a DFEE1A Tag to request which Tags to include in the final response callback. The DFEE1A Tag is a proprietary ID TECH Tag that wraps other Tags. For

example, to request that the output from the Authenticate Transaction stage includes Tags 9F36, 9F37, and 95, specify **DFEE1A059F369F3795** as part of the TLV byte array (the **05** after **DFEE1A** is the total length of the included Tags 9F36, 9F37, and 95). Note that this will override the default set of default Tags returned (see the discussion under Obtaining Extra Tags, further below).

Another optional Tag is DFEF1F, which causes the transaction to enter the the Authenticate Transaction phase automatically (without a call to **emv_authenticateTransaction()**) after finishing Start Transaction. To use this Tag, supply two bytes of data: a first byte (with **1** to signal auto-authenticate or **0** to signal no auto- authenticate) and a second byte that, if set to a value of **1**, will force the transaction to go online (the default is **0**). The complete TLV might look something like **DFEF1F020100**, where **02** is the length.

After issuing the Start Transaction command, the reader interacts with the card to determine the correct AID to use and carry out other low-level EMV operations. It calls the application back a minimum of two times (one time with **ACK** and one time with **TransactionData**), but there are typically additional status callbacks. Inspect the **DeviceState** object (the second argument to the callback) to determine if the reader is responding with device data, an EMV callback, or transaction data (the sample demo app that comes with the Universal SDK shows code for this).

Check the callback type when the reader returns an **EMVCallback**, and if it is **EMV_CALLBACK_TYPE_LCD**, have the terminal display the appropriate message on the device LCD or POS screen (the sample demo app contains code showing how to do this). If the transaction requires a customer action before proceeding, the payment app should prompt the customer as necessary (using the terminal UI) and collect any needed info. See the demo app's **processEMVCallback()** method for an example of how to handle **EMVCallback** messages.

When the reader responds with a **DeviceState** of **TransactionData** and an EMV result of **EMV_RESULT_CODE_AUTHENTICATE_TRANSACTION**, the transaction can go to the next step. At this stage, the reader responds only to three commands: **Authenticate EMV L2 Transaction**, **Cancel EMV L2 Transaction**, or **Retrieve EMV L2 Transaction Data**; these three commands correspond to the SDK methods **emv_authenticateTransaction()**, **emv_cancelTransaction()**,and **emv_retrieveTransactionResult()**. The reader will block, at this point, while your app decides which method to call, and eventually time out if no action is taken. Use this opportunity to inspect the available transaction data to determine whether to invoke any extra logic that might be appropriate to the transaction. For example, this might be when the app decides that the customer is eligible for a loyalty discount. If no special logic applies, simply proceed to the next step: Authenticate Transaction.

7.4.2 Authenticate Transaction

In this stage of the transaction, the card reader's EMV kernel attempts to apply cardholder verification methods, terminal risk management logic, and any other logic required under EMV processing rules, to determine whether the terminal needs to go online for authorization.

This stage allows the temporary interruption of program flow so an integration to (optionally) modify any existing Tags. For example, a common use of this stage is to determine (via business logic) if the cardholder is entitled to a discount, and if so, provide the discount by changing the previously submitted amount (Tag 9F02) to a lesser amount. Integrations can pass any Tags that need values changed passed as a TLV stream in this method's parameter list.

Often, this step of pausing the EMV transaction to evaluate collected card data is not necessary. An integrator can tell the reader to continue automatically (with no pausing) by passing Tag DFEF1F with a value of **0100** (or **0101** if force-online is requested) when executing the **emv_startTransaction()** method. This can be done on a per-transaction basis. But also note the SDK has an "**autoAuthenticate**" option **ON** by default. If **autoAuthenticate** is set to **ON** before the EMV transaction begins, the authenticate transaction step always occurs without pausing. The main class has a method to set this boolean: **emv_autoAuthenticate(bool authenticate)**.

The app should monitor the **DeviceState** via the second argument of the **MessageCallBack** method (the method that was registered with the device at the time the app was loaded). Direct inspection of the **DeviceState** shows if the callback is being called with device data, with a state of **EMVCallback** (requiring a change of UI message, or perhaps interaction with the user), or with transaction data.

The final callback has a **DeviceState** (second argument) of **TransactionData** and come with a standard EMV result code. Consult the most recent Universal SDK documentation for the latest list.

If the result code at the end of the Authenticate Transaction stage is **EMV_RESULT_CODE_GO_ONLINE**, the terminal app should go online to obtain final authorization. Note that going online is the responsibility of the payment app, not the reader. The EMV kernel has no knowledge of online endpoints, protocols, or APIs.

At the conclusion of Authenticate Transaction, the application should consider the transaction finished if the cryptogram received from the card was of type **TC** (approved) or **AAC** (declined). Otherwise, if the cryptogram was **ARQC**, the application should go online for authorization, then call **emv_completeTransaction()**.

Note: To determine what kind of cryptogram was received in Tag 9F26, inspect the top nibble of the CID in **9F27**. A hex value of **00** indicates **AAC**; **40** indicates **TC**; **80** indicates **ARQC**.

7.4.3 Complete Transaction

After going online for authorization, you must call **emv_completeTransaction()**. You must call this method even if you were unable to go online but still wish to proceed with the transaction (for example, if the network was down or the gateway failed to respond).

You must provide the **emv_completeTransaction()** method with the parameters that tell it if you were able to successfully reach the approver. These parameters should be provided in **Tag 8A**. Typical values here are **0x3030** for approval, **0x3032** for referral, **0x3035** for decline, and **0x5A33** for "unable to go online." Issuer Authentication Data (Tag 91) and Issuer Scripts (Tags 71 or 72) are not always present, but if they were returned by the online approver, they should be passed to this method. Consult the SDK documentation for the method signature and calling conventions; also consult the sample demo app code for an actual example of how to use this method.

When the transaction is complete, the reader will invoke your **MessageCallBack** method with a **DeviceState** of **TransactionData**. The sample demo app code shows how to pull TLV (Tag) data out of the **IDTTransactionData** object provided in the fourth argument to the callback. Typically, this Tag data includes TVR and TSI data in Tags 95 and 9B, respectively.

Tags from the reader may contain masked and encrypted data. ID TECH encrypts some (but not all) Tag data, using criteria described in *ID TECH Encrypted Data Output*. The SDK has methods that parse a TLV stream as necessary when the card data is returned, so manual parsing of the raw TLV data should not be required.

7.4.4 TLV Data

EMV transactions produce TLV data. At any stage in a transaction, you can use the **emv_unencryptedTags** field of your **IDTTransactionData** object (which has an instance name of **cardData** in the SDK sample code) to obtain unencrypted Tags, or the **emv_encryptedTags** field to obtain encrypted Tags. These fields point to **byte[]** arrays that you then need to process further to obtain actual TLVs. For example, a routine like the following converts the byte arrays to a Dictionary from which you can obtain text versions of the TLVs:

```
private string tlvToValues(byte[] tlv) {

      string text = "";
      Dictionary<string, string> dict =
            Common.processTLVUnencrypted(tlv);
      foreach (KeyValuePair<string, string> kvp in dict)
            text += kvp.Key + ": " + kvp.Value + "\r\n";
      return text;
}
```

7.4.5 Default Tags

Each stage of the transaction produces specific TLV data. The default TLVs obtained at each stage vary somewhat by product, but the transaction typically returns the following:

Start Transaction:

- 4F
- 50
- 57
- 5A
- 5F20
- 5F24
- 5F25
- 5F2D
- 5F34
- 84
- 9F20
- DFEE12
- DFEE23

Authenticate Transaction:

- 95
- 9B
- 9F02
- 9F03
- 9F10
- 9F13
- 9F26
- 9F27
- 9F34
- 9F36
- 9F37
- 9F4D
- 9F4F

Complete Transaction

- 95
- 99
- 9B
- 9F02
- 9F03
- 9F10
- 9F13
- 9F26
- 9F27
- 9F34
- 9F36

- 9F37
- 9F4D
- 9F4F
- 9F5B

Note that almost all of these are EMVCo-defined standard Tags. ID TECH proprietary Tags (typically three bytes in length, starting with DFEE or DFEF) sometimes also appear. For example, DFEE12 contains the transaction's KSN (Key Serial Number).

For a complete listing of ID TECH proprietary Tags and their meanings, see the *ID TECH TLV Tag Reference Guide*.

7.4.6 Encrypted Tags

Some TLVs contain encrypted data if your device has been key-injected and has encryption turned on. Generally speaking, any Tags containing track data (56, 57, 9F6B), PAN data (5A), or any other data considered sensitive are encrypted according to the rules described in *ID TECH Encrypted Data Output*.

By default, the following Tags (if present in your data) will be encrypted, assuming you are using a device that has been key-injected, with encryption enabled:

- 5A
- 56
- 57
- 9F1F
- 9F20
- 9F6B
- FFEE13
- FFEE14
- DF812A
- DF812B
- DF31
- DF32

7.4.7 Obtaining Extra Tags

Including a **DFEE1A** Tag in your original call to **emv_startTransaction()** notifies the card reader to produce extra Tags (see Start Transaction above). To obtain extra Tags, first include a **DFEE1A** TLV in your call to **emv_startTransaction(), emv_authenticateTransaction()**, or **emv_completeTransaction()** (or any combination of the three). Then, after each phase has finished, call **emv_retrieveTransactionResult()** to retrieve the requested TLVs.

Note: You must call **retrieveTransactionResult()** within **15 seconds** after the transaction is over. For security reasons, this data does not persist in memory for an extended period of time after the transaction completes.

Important: When specifying additional Tags in **emv_startTransaction()**, the request only returns the specified Tags. The request for additional Tags overrides the default set of EMV Tags.

Also note that Tags **57** and **5A** are available after **emv_startTransaction()** by default but are not included by default after **emv_authenticateTransaction()**, or **emv_completeTransaction()**. As a rule, collect the desired TLVs immediately after each transaction phase.

7.5. Contactless EMV Transactions

Most ID TECH readers, including the VP3350, have contactless EMV capability, allowing transactions to be initiated via RFID. The following section provides a very brief overview on performing contactless transactions with the Universal SDK.

7.5.1 Contactless Configuration

As with contact EMV, contactless EMV requires that you first configure the reader with terminal settings, CAPKs, and AIDs before doing any transactions. Contactless EMV configurations do not share settings with contact EMV configuration items; instead, integrators must set up contactless configurations separately. Use the Universal SDK's **ctls_setApplicationData()** and **ctls_setCAPK()** methods to load each AID and CAPK the payment app needs to support. Note that this setup is only required one time; the settings persist across device reboots.

Terminal settings are more complicated in contactless EMV than in contact EMV; contactless EMV requires multiple EMV kernels—one kernel per card brand with different terminal settings for different card brands. In contactless readers, groups of TLVs specify terminal settings Predefined Groups exist (with Group numbers, such as 00, 80, 90, A0, B0, and C0), containing configurable TLVs that allow a set of behaviors to be mapped to a particular card or set of cards.

ID TECH has predefined a number of Groups populated or set by default with the **Set Configuration Defaults (04-09)** command. In the Universal SDK, run the **Set Configuration Defaults (04-09)** command using the **device_sendVivoCommandP2()** method, with **04** as the command argument and **09** as the subcommand argument. After running this command, all Groups are initialized for all card brands with common defaults.

Integrators may need to override certain defaults. For example, integrators outside of the U.S. might need to set the currency code (Tag 5F2A) to something other than **0840**. In the Universal SDK, run the **Set Configuration Group (04-03)** command. To override terminal settings using an API command, provide the TLVs to override along with a specified Group number to the **ctls_setConfigurationGroup((byte[] tlv)** method. The first TLV in the byte array should be the Group number (specified using Tag DFEE2D in NEO 2 and NEO 3); then at least one TLV should follow, containing configuration information. For example, in a NEO 3 device, you could set Group 90 to have a Currency Code of **0978** (for Euros) by supplying the following TLV data (as a byte array):

```
0DF EE 2D 01 90 9F 1A 02 08 40 5F 2A 02 09 78 5F 36 01 02 9F
35 01 15 9F 66 04 30 80 C0 00 DF EE 34 06 00 00 00 01 00 00
DF 81 26 06 00 00 00 00 60 00 9F 1B 04 00 00 1F 40 DF 5B 01
05 9F 33 03 E0 08 40 DF EC 2E 01 61 9F 40 05 80 00 00 00 00
9F 02 06 00 00 00 00 05 00
```

Note that the first Tag is **DFEE2D**, which has **90** as the data value (meaning all of the downstream TLVs should be applied to Group 90). Even though the intention is to only change Tag 5F2A to **0978** (highlighted in yellow), we supply all the TLVs for this group to make sure no values are dropped and no values get accidentally picked up from Group 0 (any TLVs that don't exist in your Group but that do exist in the default Group 00 will get picked up from Group 00 unless you explicitly override the default value explicitly).

Important: When editing Group 00 (the default group, which cannot be deleted), you can replace individual Tags without affecting other Tags. However, for all other Groups, the **ctls_setConfigurationGroup(byte[] tlv)** method overwrites all data and installs only the TLVs that were passed in as a byte array. The best practice to follow, even if you are only modifying one TLV, is to read all TLVs from the Group in question using **ctls_getConfigurationGroup(int group, ref byte[] tlv)** and then modify the desired Tags, then replace all TLVs. Also remember that any Tags you fail to supply to a custom group, if they already exist in Group 00 will inherit values from Group 00 by default.

7.5.2 Starting a Contactless Transaction

Contactless transactions start in any NEO 3 device with an **Activate Transaction Command (02-40)**, or the SDK method **device_startTransaction (double amount, double amtOther, int exponent, int type, int timeout, byte[] Tags, bool forceOnline)**. You can use the same callback routine that you defined for contact EMV (see Performing Transactions above). When your callback is called, you can inspect the **IDTechSDK.IDTTransactionData** instance (in the final argument of the callback) to determine what kind of transaction occurred, and many other types of info (see SDK documentation included with the ID TECH SDK for an exhaustive list of properties).

When issuing **device_startTransaction()**, you can tell the device to accept contactless presentations only, or you can tell it to accept all three types of presentations (MSR, contact, and contactless). To specify the types of desired presentations, use Tag **DFEF37** (as shown below); specify fallback support using **DFEF3C**.

DFEF37	01	Define the type of interface to activate with (02-40). Interface Select: **Bit 0:** MSR **Bit 1:** Contactless **Bit 2:** Contact	DF EF 37 01 07 07 = 0000 0111 This activates transactions for all 3 interfaces.

DFEF3C	03	Fallback support and Timeout value for waiting for the next command (mainly to support EMV workflow) **Byte 1:** Fallback support **Byte 2~3:** Timeout for next command (Unit: Sec)	DF EF 3C 03 01 00 60 Fallback supported and the timeout is set to 60 seconds before the transaction times out.

7.5.3 Example raw command (NEO 3 firmware instructions):

```
5669564F7465636832000240000221E9C01009F02060000000001009F0306000000
000000DFEF370107DFEF3C0301006018D1

5669564F746563683200026300004BB4
```

If the command parse is successful and the ICC transaction starts, the response contains the first command and the status code is 0x63.

To send this command via the SDK, use the **device_sendVivoCommandP2()** method with a command of **02**, a subcommand of **40**, and Tag data (as byte array) of **9C01009F02060000000001009F03060000000000000DFEF370107DFEF3C03010060**.

Note: Unlike contact EMV, a contactless transaction runs straight through to completion, without interruption, in one step. The response contains one cryptogram, in Tag 9F26, at the end, rather than two cryptograms (corresponding to the two Gen AC events of contact EMV). A contactless transaction occurs in one swift step lasting about 500 milliseconds. There is no **device_completeTransaction()** method because completion is automatic. If the transaction occurs without error, all the necessary TLVs (including clearing-record TLVs) are in the returned data.

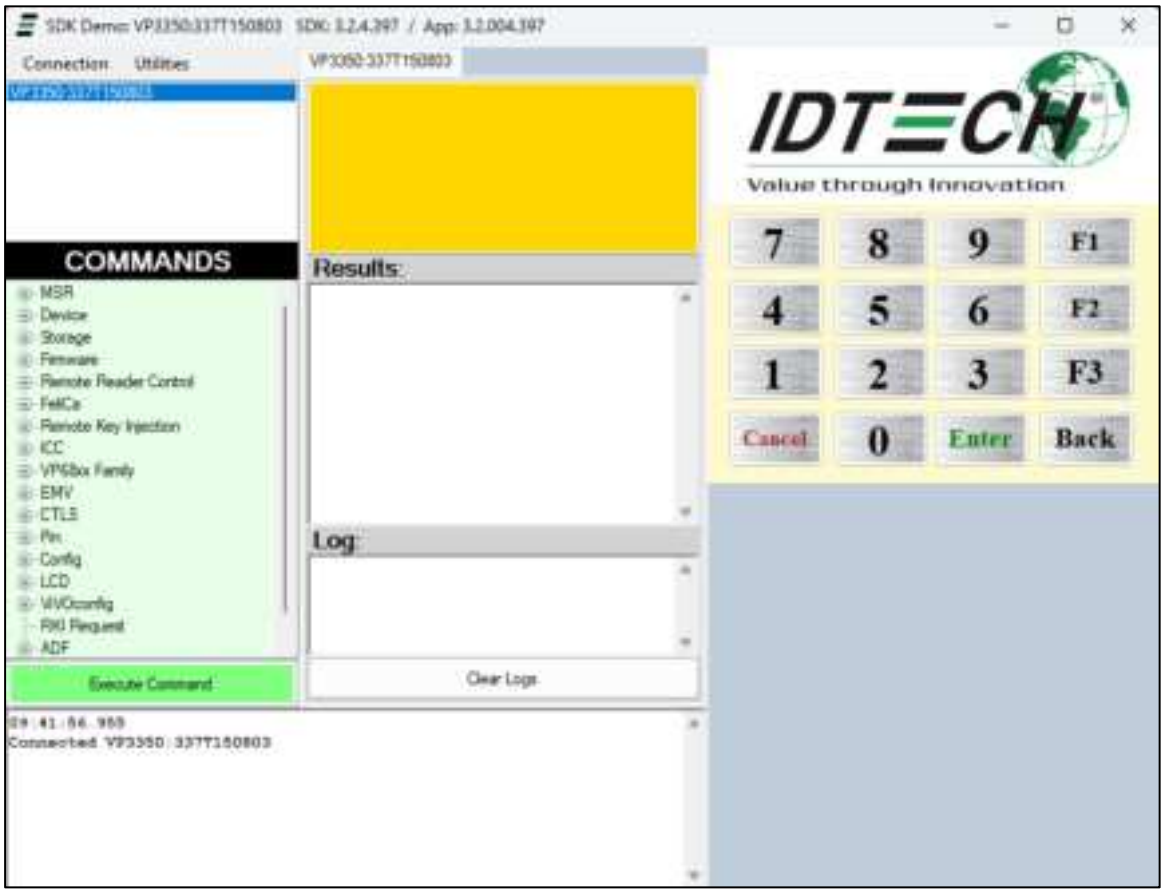
8. Universal SDK Demo App

The Universal SDK comes with a rich, fully featured demo app that allows users to run the VP3350 in USB mode. Visit the Universal Library for Visual Studio to download the Universal SDK Demo app as a standalone executable, separate from the SDK; the full SDK is not required to use the demo. Be sure to check out the Universal Demo QuickStart Guide for more detailed instructions about using the Universal SDK Demo app.

8.1. Using the Demo Application

Follow the steps below to run the Universal SDK Demo app on Windows:

1. Plug the VP3350 into the host device with a standard USB cable.
2. Open the **SDK Demo** application and allow a few seconds for the main window to appear (see illustration below).



The Universal SDK Demo app displays VP3350's available commands in a command tree, as shown above. Single-click on a command to populate the lower-right panel of the window with optional settings relevant to the command (for example, "Amount" and "Start EMV Additional Tags" above). In some cases, text fields appear, allowing users to enter custom values.

To execute a command, double-click it in the command tree or use the **Execute Command** button. The command executes in real time and a data trace appears automatically in the center panels. Use the **Clear Logs** button to clear both panels.

9. VP3350 Low-Level Commands

The following are commonly-used commands for the VP3350. For a full list of available commands, contact your ID TECH representative for the *NEO 2 Interface Developer's Guide* (available under NDA).

9.1. Get Main Firmware Version (09-03)

The **Get Main Firmware Version** command returns main firmware version TLV.

Command Frame

Byte 0-9	Byte 10	Byte 11	Byte 12	Byte 13	Byte 14	Byte 15
Header Tag & Protocol	Command	Sub-Command	Data Length (MSB)	Data Length (LSB)	CRC (LSB)	CRC (MSB)
ViVOtech2\0	09h	03	00h	00h		

Response Frame

Byte 0-9	Byte 10	Byte 11	Byte 12	Byte 13	Byte 14	Byte 15	Byte 0-9
Header Tag & Protocol	Command	Status Code	Data Length (MSB)	Data Length (LSB)	Data	CRC (MSB)	CRC (LSB)
ViVOtech2\0	09h	See Status Code Table			See below		

The Get Main Firmware Version sub-command returns a TLV string as follows:

- **Tag:** 0xDFEE62
- **Length:** Varies
- **Value:** Varies field representing the main firmware version.

The following example shows the command and response.

Command: Get Main Firmware Version: `56 69 56 4F 74 65 63 68 32 00 09 03 00 00 C0 CE`

Response: `56 69 56 4F 74 65 63 68 32 00 09 00 00 13 DF EE 62 0F 56 50 33 33 35 30 20 46 57 20 76 31 2E 30 31 7A 06`

9.2. Get Serial Number (12-01)

The **Get Serial Number** command instructs the ViVOpay reader to return the 15-digit serial number stored in its non-volatile memory. If a serial number has not been previously set in the reader, this command fails with a **Command Not Allowed** error status. If the command frame is not valid, the reader returns an error response frame.

Command Frame

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

The serial number will be returned tail-padded with **0x00** to a length of 15.

Example:

TX: 56 69 56 4F 74 65 63 68 32 00 12 01 00 00 18 A5

RX: 56 69 56 4F 74 65 63 68 32 00 12 00 00 0F **36 33 30 5A 30 30 30 30 30 31 00 00 00 00 00** 94 BC

Response 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	Status Code	Data Length (MSB)	Data Length (LSB)	Data	CRC (MSB)	CRC (LSB)
ViVOtech2\0	12h	See Status Code Table	00h	0Fh	15-digit Serial Number		

9.3. Get Hardware Information (09-14)

The **Get Hardware Information** command retrieves information about the reader's hardware.

Command Frame

Byte 0-9	Byte 10	Byte 11	Byte 12	Byte 13	Byte 14	Byte 15
Header Tag & Protocol	Command	Sub-Command	Data Length (MSB)	Data Length (LSB)	CRC (LSB)	CRC (MSB)
ViVOtech2\0	09h	14h	00h	00h		

Response Frame

Byte 0-9	Byte 10	Byte 11	Byte12	Byte 13	Byte 14 … Byte 13+n	Byte 14+n	Byte 15+n
Header Tag & Protocol	Command	Status Code	Data Length (MSB)	Data Length (LSB)	Data	CRC (MSB)	CRC (LSB)
ViVOtech2\0	09h	See Status Code Table			See below		

The format for hardware module version information returned is "human readable," consisting of fields that are separated by commas, and lines separated by carriage return and line feed characters:

```
<module type>,<module name><CRLF>
<chip version>
```

The following example shows the hardware version information subcommand and the information being returned (in ASCII format).

Command: Get Hardware Version Information: `56 69 56 4F 74 65 63 68 32 00 09 14 00 00 33 08`

Response: For example, a VP5300 returns
`5669564F7465636832000900001548572C205650333335300D0A4B38314620526576 34E170`
In ASCII: `HW, VP3350 <CR><LF> K81F Rev4`

9.4. Get Processor Type (09-02)

The **Get Processor Type** command returns a processor type TLV.

Command Frame

Byte 0-9	Byte 10	Byte 11	Byte 12	Byte 13	Byte 14	Byte 15
Header Tag & Protocol	Command	Sub-Command	Data Length (MSB)	Data Length (LSB)	CRC (LSB)	CRC (MSB)
ViVOtech2\0	09h	02	00h	00h		

Response Frame

Byte 0-9	Byte 10	Byte 11	Byte12	Byte 13	Byte 14 … Byte 13+n	Byte 14+n	Byte 15+n
Header Tag & Protocol	Command	Status Code	Data Length (MSB)	Data Length (LSB)	Data	CRC (MSB)	CRC (LSB)
ViVOtech2\0	09h	See Status Code Table			See below		

The **Get Processor Type** sub-command returns a TLV string as follows:

- **Tag:** 0xDFEE61
- **Length:** 0x02
- **Value:** a field representing the processor type.

The following types of processors may be identified in the **Value** field:

Processor Type (hex values)	Description
45 00	ARM7/ LPC21xx
4D 00	ARM Cortex-M4/ K21 Family
4E 00	ARM Cortex-M4/ K81 Family

The following example shows the command and response.

Command: Get Processor Type: `56 69 56 4F 74 65 63 68 32 00 09 02 00 00 F0 F9`

Response: `56 69 56 4F 74 65 63 68 32 00 09 00 00 06 DF EE 61 02 4E 00 7B 9C`

9.5. Get Module Version Information (09-20)

The **Get Module Version Information** command retrieves the reader's module information.

Command Frame

Byte 0-9	Byte 10	Byte 11	Byte 12	Byte 13	Byte 14	Byte 15
Header Tag & Protocol	Command	Sub-Command	Data Length (MSB)	Data Length (LSB)	CRC (LSB)	CRC (MSB)
ViVOtech2\0	09h	20h	00h	00h		

Response Frame

Byte 0-9	Byte 10	Byte 11	Byte12	Byte 13	Byte 14 … Byte 13+n	Byte 14+n	Byte 15+n
Header Tag & Protocol	Command	Status Code	Data Length (MSB)	Data Length (LSB)	Data	CRC (MSB)	CRC (LSB)
ViVOtech2\0	09h	See Status Code Table			See below		

If there is an error, the reader returns the appropriate status code with an empty data field (Data Length = 0000h).

The format for module version information returned is "human readable," consisting of fields separated by commas and lines separated by carriage return and line feed characters:

```
<module type>,<module name and spec. version>,[<implementation
version>],<CRLF>
```

The following example shows the module version information subcommand and the information being returned (in ASCII format).

Command: Get Module Version Information: 56 69 56 4F 74 65 63 68 32 00 09 20 00 00 56 11

Response:

```
5669564F7465636832000900022E56503333353020465720763l2E30310D0A4E7574
74582D31302E322E300D0A776F6C6653534C2D342E372E300D0A434C204149442C20
454D562045502076322E31302C2076312E30300D0A434C204149442C204D61737465
724361726420332E312E342C2076312E30300D0A434C204149442C20564350532076
322E322C2076312E30300D0A434C204149442C20416D6578204578707265737350 61
7920342E312C2076312E30300D0A434C204149442C204A43422076312E362C207631
2E30300D0A434C204149442C20446973636F766572204450415320322E302C207631
2E30300D0A434C204149442C20515549435320312E302E32205549435320332E302C
2076312E30300D0A434C204149442C20507572652076322E312E382C2076312E3030
0D0A434C204149442C20496E746572616320312E38612C2076312E30300D0A434C20
4149442C207153504152432032 2E302E312C2076312E30300D0A434C204149442C20
454654504F53207632332E30322E30322076312E30300D0A434C204149442C204350
4143452076312E312C2076312E30300D0A434C204149442C204170706C6550617920
56415320312E302E31302C2076312E320D0A434C204149442C20536D617274546170
20322E312C2076312E320D0A434C204C312C20454D56332E31612C2076352E32330D
0A4354204C322C20454D5620436F6D6D6F6E2047656E2033204C322056312E33302E
3033390D0A4354204C312C20454D56342E33632C2076322E30310D0A035D
```

ASCII translation of the data field:

```
ASCII: VP3350 FW v1.01
NuttX-10.2.0
wolfSSL-4.7.0
CL AID, EMV EP v2.10, v1.00
CL AID, MasterCard 3.1.4, v1.00
CL AID, VCPS v2.2, v1.00
CL AID, Amex ExpressPay 4.1, v1.00
CL AID, JCB v1.6, v1.00
CL AID, Discover DPAS 2.0, v1.00
CL AID, QUICS 1.0.2 UICS 3.0, v1.00
CL AID, Pure v2.1.8, v1.00
CL AID, Interac 1.8a, v1.00
CL AID, qSPARC 2.0.1, v1.00
CL AID, EFTPOS v23.02.02 v1.00
CL AID, CPACE v1.1, v1.00
CL AID, ApplePay VAS 1.0.10, v1.2
CL AID, SmartTap 2.1, v1.2
CL L1, EMV3.1a, v5.23
CT L2, EMV Common Gen 3 L2 V1.30.039
CT L1, EMV4.3c, v2.01
```

9.6. Activate Transaction Command (02-40)

The **Activate Transaction** command begins a contactless EMV or contactless MagStripe Card transaction.

Note: While an **Activate** command is in progress, readers only accept a **Cancel** or **Stop** command. Do not send other commands until **Activate Transaction** has completed, because the reader will interpret these as a **Cancel Transaction** command.

To control the behavior, use the DFEF37 and DFEF3C tags:

Tag	Length	Description	Example
DF EF 37	01	Define the type of interface to be activated with 02-40. Interface selection: • Bit 0: MSR • Bit 1: Contactless • Bit 2: Contact	DF EF 37 01 07 07 = 0000 0111 This activates transaction for all three interfaces.
DF EF 3C	03	Fallback support and Timeout value for waiting for the next command (mainly to support EMV workflow). Byte 1: Fallback support • 0x00: fallback not supported • 0x01: support fallback Byte 2~3: Timeout for next command (Unit: Sec) (Hex format) • 00 0A = 10s • 01 00 = 256s	DF EF 3C 03 01 00 60 Fallback is supported, and the timeout is set to 96 seconds before the transaction times out.

Example:
5669564f7465636832000240002 21e9c01009f02060000000001009f030600000000 0000**dfef370107dfef3c03010060**18d1

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	02h	40h			See Data Format below		

Activate Transaction Command Frame Data Format

Data Item	Length (bytes)	Description
Timeout	1	Time in seconds that the reader waits for a card to be presented before timing out and returning an Error response. The reader will continue to poll for this amount of time if no card is found. Note that if a card is found, the transaction may not complete within the timeout period. This field must be present in the **Activate** command. Format: Binary
TLV Data	varies	See Activate Command TLVs in the *NEO 2 IDG*.

Response Frame

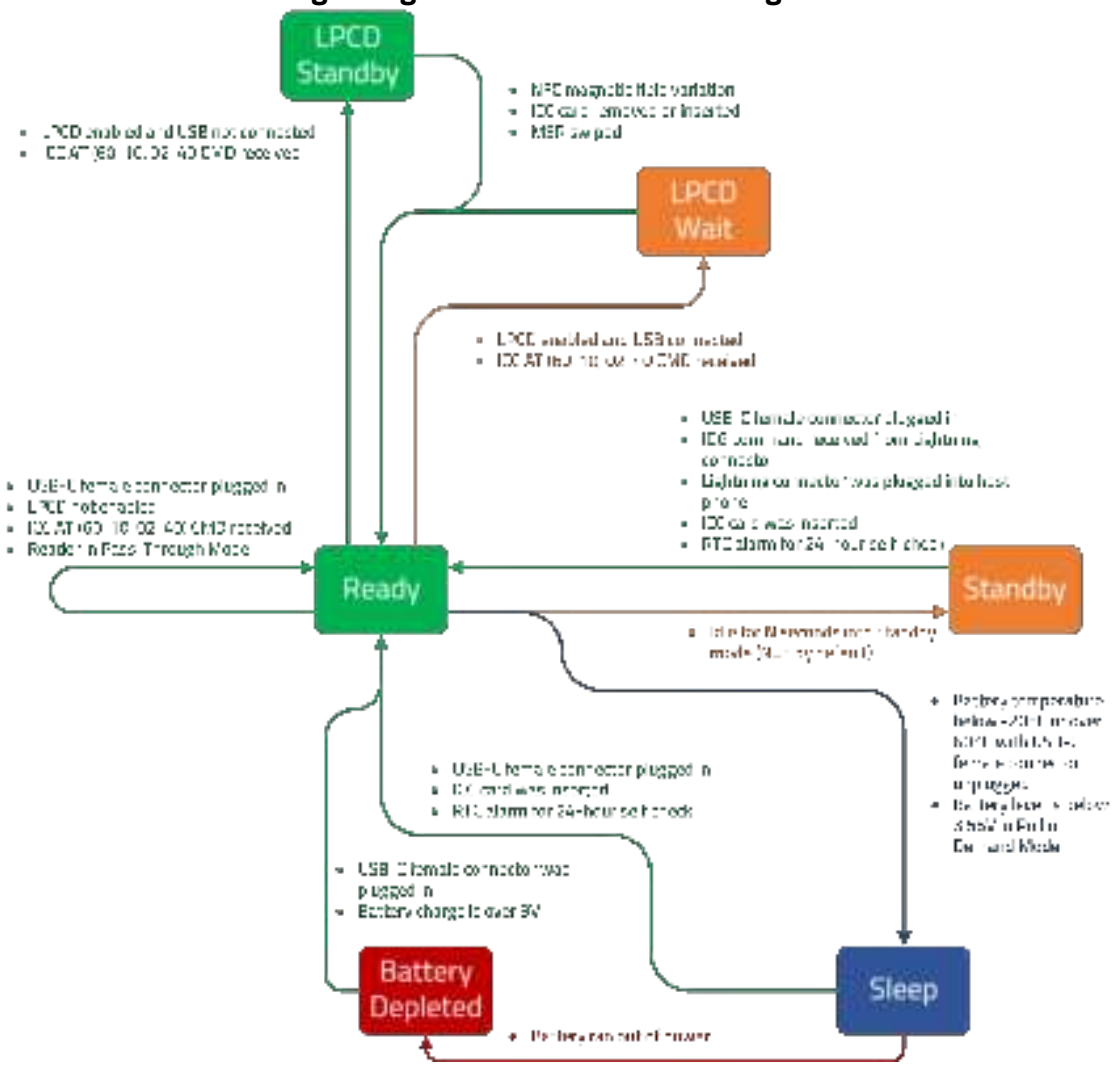
Byte 0-9	Byte 10	Byte 11	Byte 12	Byte 13	Byte 14 … Byte 14+n-1	Byte 14+n	Byte 15+n
Header Tag & Protocol Version	Command	Status Code	Data Length (MSB)	Data Length (LSB)	Data	CRC (MSB)	CRC (LSB)
ViVOtech2\0	02h	See Status Code Table			See Response Frame Data Format		

Note: The information above omits many command details, particularly TLV information. See the *NEO 2 Interface Developer's Guide* for the full **Activate Transaction (02-40)** description.

9.7. Power Management

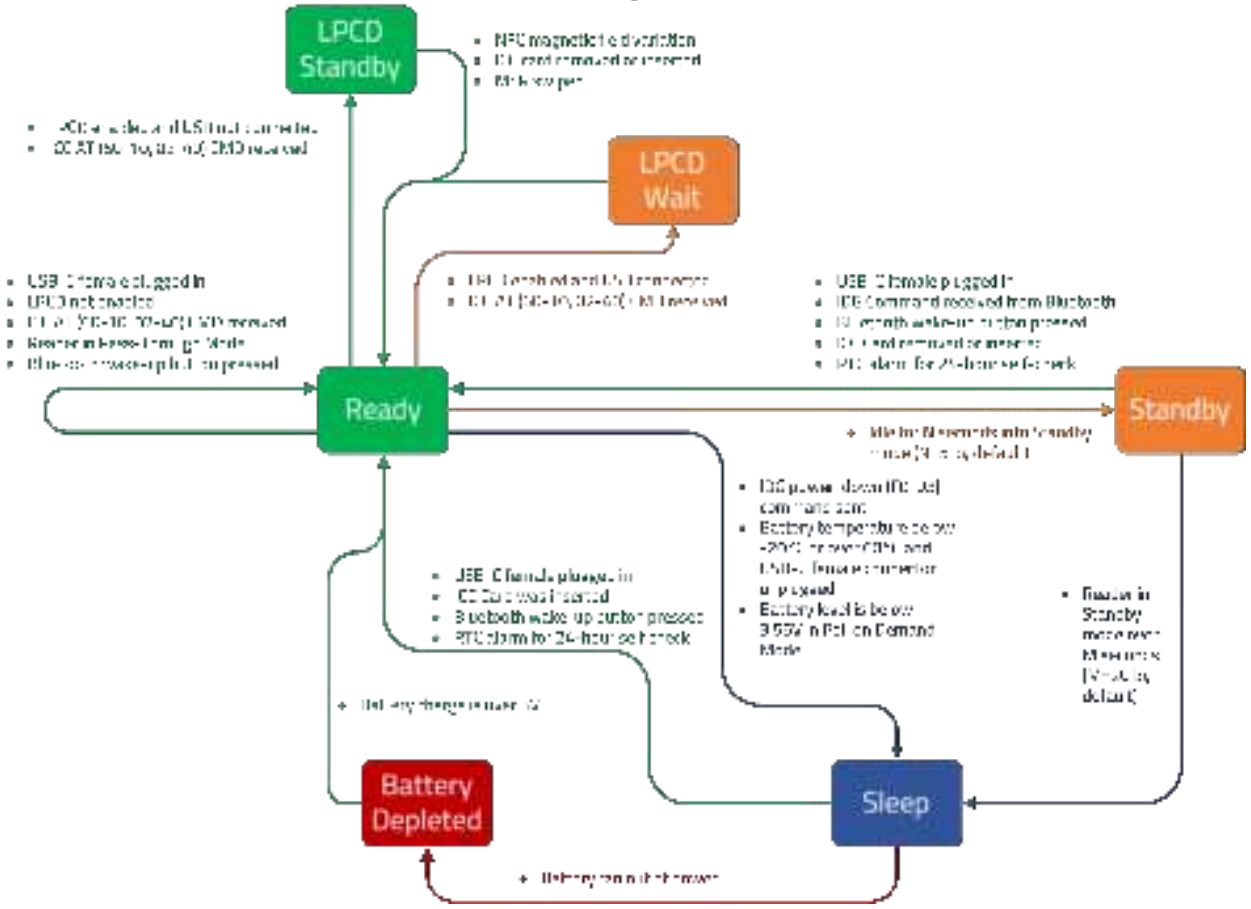
The diagrams and commands below describe power management for Lightning and Bluetooth VP3350 models.

9.7.1 VP3350 Lightning Connector PMC State Diagram



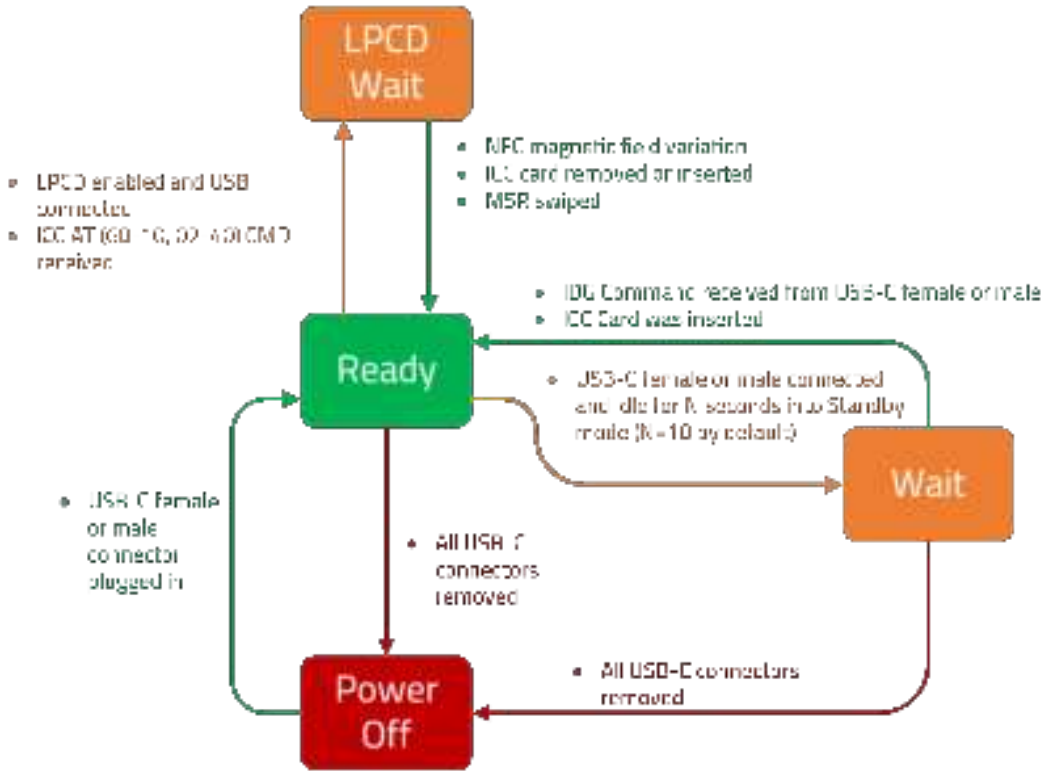
Note that pressing the reader's reset button will force the reader into a power off/battery depleted state and then restart the reader in the Ready state.

9.7.2 VP3350 Bluetooth PMC State Diagram



Note that pressing the reader's reset button will force the reader into a power off/battery depleted state and then restart the reader in the Ready state.

9.7.3 VP3350 USB-C PMC State Diagram



9.7.4 Enter Low Power Mode (F0-03)

The **Enter Low Power Mode** command places the reader in low power mode.

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	F0h	03h	0x00 0x02		See Command Data Table		

Command Data

Data Item	Length (bytes)	Description/Example
Low Power Mode	1	0x00: Standby Mode (resume from last instruction) 0x01: Sleep Mode (power on reset POR required)
MSR / NFC Option	1	0x00: OFF 0x01: ON (Swipe/Tap will wake from low power)

Use `00 01` to put the reader in **Sleep Mode**. It will awaken upon card insertion.

With `00 00`, the reader will wake up with card *insertion*, but not with contactless (NFC) presentation (the card-seated switch is always enabled; it cannot be disabled).

Wakeup from Sleep Mode involves a reboot (which takes several seconds). **Wakeup from Standby Mode** does not reboot the reader.

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	F0h	See status code table	00h	00h		

The reader will wake up automatically upon card insert, or when a command is issued.
On waking up (after being triggered by card insert), the reader will output `5669564F746563683200F10000008D1E`.

Note:

- VP3350 Model B supports the use of `F0 03 00 00` to enter Standby Mode with MSR and NFC options off.
- VP3350 Model C supports the use of `F0 03 00 00` and `F0 03 01 00` to enter standby and sleep mode, respectively, with MSR and NFC options off.

Model	Low Power Mode		MSR / NFC Option	
	0x00: Standby	0x01: Sleep	0x00: Off	**0x01: On**
VP3350 Model B	Supported	Not Supported	Supported	Supported
VP3350 Model C	Supported	Supported	Supported	Supported

9.7.5 Set Low Power Consumption Configuration (F0-04)

The **Set Low Power Consumption Configuration** command enables or disables some level Low Power Consumption functions and the waiting timer of the previous state.

Note: Low Speed Run and Wait is not supported in NEO3. Any attempt to set either of the two timers results in an error response.

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	F0h	04h			See Tables below		

Data Field	Length (bytes)	Description
The low power level ID	1	The range of low power ID is 1~4. The detailed supported level is defined by the PDS of the product.
low power timer	2	Time (**default 30s**) • 0000h = Does NOT support the level of low power consumption function (should be skipped). • 0001h ~ 0E10h (1~3600 Seconds) = Supports the level of low power consumption function. The value is defined by the previous state's timer "The low power level ID" level.

Default Settings for VP3350 readers:

Setting ID	1	2	3	4
	Low speed run	Wait	Standby	Sleep
VP3350 Model B	Not supported	Not supported	5s	Not supported
VP3350 Model C	Not supported	Not supported	5s	20s
VP3350 Model D	Not supported	0s	Not supported	Not supported
VP3350 Model F	Not supported	0s	Not supported	Not supported

IDLE (30s) -> LowSpeedRun (30s) -> Wait (30s) -> Standby (30s) -> Sleep

After sending the following commands:

- `01 00 1F`: Enable Low Speed Run state and the previous state (Idle) waiting timer is 31 seconds.
- `02 00 00`: Disable Wait.
- `03 00 21`: Enable Standby state and the previous state (Low Speed Run) waiting timer is 33 seconds.
- `04 00 22`: Enable Sleep state and the previous state (Standby) waiting timer is 34 seconds.

The reader changes to these values:

ID	Current Name	Timeout
1	Low speed run	31s
2	Wait	0
3	Standby	33s
4	Sleep	34s

IDLE (31s) -> LowSpeedRun (33s) -> Standby (34s) -> Sleep

Response 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	Status Code	Data Length (MSB)	Data Length (LSB)	Data	CRC (MSB)	CRC (LSB)
ViVOtech2\0	F0h	See status code table	00h	00h			

9.7.6 Get Low Power Consumption Configuration (F0-05)

The **Get Low Power Consumption** command retrieves reader's the low power consumption function configuration.

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	F0h	05h	00h	00h			

Response 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	Status Code	Data Length (MSB)	Data Length (LSB)	Data	CRC (MSB)	CRC (LSB)
ViVOtech2\0	F0h	See status code table	00h	09h	See Tables below		

Data Field	Length (bytes)	Description/Example
Modes number	1	Total number of supported low power modes. It will be 4.
1st lower power timer	2	
…		
4th lower power timer	2	

Note:

For example, if a VP3350 Model C reader's configuration is:

ID	Current Name	Timeout
1	Low speed run	0
2	Wait	0
3	Standby	5s
4	Sleep	20s

The data is: `04 00 00 00 00 00 05 00 14`

9.7.7 Get Battery Level (F0-02)

The **Get Battery Level** command retrieves the reader's battery level.

Command Frame

Byte 0-9	Byte 10	Byte 11	Byte 12	Byte 13	Byte 14	Byte 14	Byte 15
Header Tag & Protocol Version	Command	Sub-Command	Data Length (MSB)	Data Length (LSB)	See Below	CRC (LSB)	CRC (MSB)
ViVOtech2\0	F0h	02h					

Data Format

Item	Length (bytes)	Description
Get Li Battery Voltage Percentage	0	
Get Battery Voltage Value	1	0x00: Coin Battery Voltage Value 0x01: Li Battery Voltage Value

Response Frame

Byte 0-9	Byte 10	Byte 11	Byte 12	Byte 13	Byte 14	Byte 15	Byte 16
Header Tag & Protocol Version	Command	Status Code	Data Length (MSB)	Data Length (LSB)	Data	CRC (MSB)	CRC (LSB)
ViVOtech2\0	F0h	See status code table			See Below		

Response Data Format

Item	Length (bytes)	Description
Li Battery Percentage	1	0x05 ~ 0x64 (5% ~ 100%)
Coin Battery Voltage Value	2	Low byte is first, unit is mV
Li Battery Voltage Value	2	Low byte is first, unit is mV

9.7.8 Set USB Sleep Configuration (F0-06)

The Set USB Sleep Configuration command enables or disables the reader's USB Sleep Configuration.

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	F0h	06h	00h	01h	00h: OFF 01h: ON		

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	F0h	See status code table	00h	00h		

9.7.9 Get USB Sleep Configuration (F0-07)

The Get USB Sleep Configuration retrieves the reader's USB sleep configuration.

Note: When retrieving the **USB sleep configuration** value, the priority is as follows:

1. **F0-06** takes precedence over Device Tree settings.
2. Device Tree settings take precedence over any hardcoded value.
3. The USB sleep configuration hardcoded default value is OFF.

Ex: The **F0-06** operation is not active and there is NO Device Tree setting or a defective Device Tree setting: the USB sleep configuration value is OFF.
Ex: The **F0-06** operation is not active and valid there is a valid Device Tree setting: the USB sleep configuration value follows Device Tree settings.
Ex: The **F0-06** operation is active: the USB sleep configuration value follows the setting in **F0-06**.

Command Frame

Byte 0-9	Byte 10	Byte 11	Byte 12	Byte 13	Byte 14	Byte 15
Header Tag & Protocol Version	Command	Sub-Command	Data Length (MSB)	Data Length (LSB)	CRC (LSB)	CRC (MSB)
ViVOtech2\0	F0h	07h	00h	00h		

Response Frame

Byte 0-9	Byte 10	Byte 11	Byte 12	Byte 13	Byte 14	Byte 15	Byte 16
Header Tag & Protocol Version	Command	Status Code	Data Length (MSB)	Data Length (LSB)	Data	CRC (MSB)	CRC (LSB)
ViVOtech2\0	F0h	See status code table	00h	01h	USB Sleep Configuration		

Data:
00h: OFF
01h: ON

9.8. Charging Capability Configuration Commands

The section below describes commands for configuring VP3350 charging capabilities.

9.8.1 Set Charging Capability Configuration (F0-10)

IDTECH products facilitate passthrough charging via Lightning or USB-C male connectors. The **Set Charging Capability Configuration** command establishes the charging capability through the Lightning or USB-C male connector for device connection. This configured setting is permanently stored in the device's flash memory and becomes operational following either a re-plug of the female connector or a power cycle of the reader. Make sure the desired charging capability aligns with the power source of your connected device.

Command Frame

Byte 0-9	Byte 10	Byte 11	Byte 12	Byte 13	Byte 14 ... 13+n	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	F0h	10h	00	01	See below	Varies	Varies

Data Format

Data	Description
00h	Dynamic charging capability.
01h	Minimum charging capability.
02h	Maximum charging capability.

VP3350 Charging Capability		
Dynamic	Minimum	Maximum
Lightning: 0.5A ~ 1.5A @ 5V	**Lightning**: 0.5A @ 5V	**Lightning**: 1.5A @ 5V
USB-C: 0.5A ~ 1.5A @ 5V	**USB-C**: 0.5A @ 5V	**USB-C**: 1.5A @ 5V

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	F0h	See status code table	00h	00h	Varies	Varies

9.8.2 Get Charging Capability Configuration (F0-11)

The **Get Charging Capability Configuration** command retrieves the current charging capability configurations from flash memory.

Command Frame

Byte 0-9	Byte 10	Byte 11	Byte 12	Byte 13	Byte 14	Byte 15
Header Tag & Protocol Version	Command	Sub-Command	Data Length (MSB)	Data Length (LSB)	CRC (LSB)	CRC (MSB)
ViVOtech2\0	F0h	11h	00h	00h	Varies	Varies

Response Frame

Byte 0-9	Byte 10	Byte 11	Byte 12	Byte 13	Byte14… 13+n	Byte 14+n	Byte 15+n
Header Tag & Protocol Version	Command	Status Code	Data Length (MSB)	Data Length (LSB)	Data	CRC (MSB)	CRC (LSB)
ViVOtech2\0	F0h	See status code table	00h	01h	See F0 10 command data format	Varies	Varies

9.9. BLE Communication Commands

The section below describes BLE chip commands.

9.9.1 Set/Get BLE Chip Command (77-86)

The Set/Get BLE Chip Command retrieves or sets specific configurations or operational behaviors. To differentiate chips from various vendors, it is necessary to specify the chip type, sub-command, and parameter.

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)
ViVOpayV2\0	77h	86h		03h ~ var	See Data Table		

Data Table

Data Item	Length	Description
Chip type	1	0x00: Dialog DA14585 other: N/A
Sub command	1	Refer to the sub command table for specified chip types
Parameter length	1	var
Parameter data	var	

DA14585 sub command table

Command Code	Description
0x01	Retrieve BLE security level setting. If parameter length = 0 Get security setting (0:enable security; 1:disable security) If parameter length = 1 Set security setting (0: enable security; 1:disable security) **Note:** If the security level is disabled, pairing with the device does not require a passkey. **Note:** Security level setting is only supported on the VP3350-NSRED with default disabled security settings and is invalid for SRED devices.

Response 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	Status Code	Data Length (MSB)	Data Length (LSB)	Data	CRC (LSB)	CRC (MSB)
ViVOpayV2\0	77h	See status code table			Data		

Example 1:

Get security level:

Command:

```
56 69 56 4F 74 65 63 68 32 00 77 86 00 03 00 01 00 A2 87
```

Response:

```
56 69 56 4F 74 65 63 68 32 00 77 00 00 01 01 92 60
```

Example 2:

Set security level ON

Command:

```
56 69 56 4F 74 65 63 68 32 00 77 86 00 04 00 01 01 00 46 4D
```

Response**:**

```
56 69 56 4F 74 65 63 68 32 00 77 00 00 00 77 BF
```

10. Basic Card Reading Data Flow

The following examples describe the basic steps for setting a reader's terminal settings and activating a transaction.

10.1. Example: Reading a Card via Firmware Commands

Perform the following steps and commands to read a card with the VP3350 via NEO 2 protocol firmware commands.

1. Set the device's terminal settings:
    a. Run **Set Kernel Configuration (60-16)** to set the kernel configuration number, which acts as a filter to validate that the tags in the next step have the correct major parameters.
    b. Run **Set Terminal Configuration (60-06)** to set the TLV tags, which must have the correct major parameters set in step 1a.
2. Run **Contact Set Application Data (60-03)** to set the device's AID file. Note that, prior to device certification, devices require dummy AIDs to function.
3. Run **Activate Transaction (02-40)** and read the card.

10.2. Example: Reading a Card via Universal SDK Methods

Perform the following steps and commands to read a card with the VP3350 via USDK methods.

1. Set the device's terminal settings:
    a. Run **Set Kernel Configuration**:
    ```
    public RETURN_CODE
    emv_setTerminalMajorConfiguration(int configuration)
    ```
    b. Run **Set Terminal Configuration**:
    ```
    public RETURN_CODE emv_setTerminalData(byte[]
    tlv, string ident = "")
    ```
2. Run **Set Application Data**:
    ```
    public RETURN_CODE emv_setApplicationData(byte[] name, byte[]
    tlv, string ident = "")
    ```
3. Run **Activate Transaction**:
    ```
    public RETURN_CODE device_startTransaction(double amount, double
    amtOther, int exponent, int type, int timeout, byte[] tags, bool
    isFastEMV = false, string ident = "")
    ```
4. Read the card.

10.3. Example: Reading a Card via the USDK Demo App

1. Download and install the latest USDK Demo app from the ID TECH Knowledge Base (if you cannot access the link, please contact support).
2. Connect the VP3350 to your PC via USB or serial port.
3. Open the USDK Demo app from the Windows Start menu.
4. Select **EMV** > **Terminal Config** > **Set Kernel Config**, then input the Config Number (example 2).
5. Select **EMV** > **Terminal Config** > **Save Terminal Data** > **Pick Tag List** (example 2C) > **Execute.**
6. Select **EMV** > **AID** > **Load Default AID**.
7. Select **EMV** > **Activate Transaction**.

11. Application Development Considerations

When developing applications for the VP3350, make sure to consult the *ID TECH Universal SDK Guide* for your respective platform for best practices to follow. Download the *Universal SDK Guide* from the VP3350 product page as part of the ZIP file for your development platform.

ID TECH strongly recommends that integrators include a way for users to update their passwords.

11.1. Performing Key Injection on a VP3350 via Tablet

The VP3350 accepts key injection in two ways when integrated into a tablet:

- Via RKI with the tablet running an application that supports ID TECH RKI (for example, an ID TECH application or ISV application).
- Via the USB-C female port.

Note: When performing key injection via the USB-C female port, the tablet must be turned off. Using a Futurex machine requires the appropriate IDT-Futurex conversion box (ID TECH P/N: ID-80000001-012).

12. Periodic Inspection Instructions

The VP3350 is an attended device; contact an ID TECH representative with any questions for the device's daily use.

Users are also required to complete the following checks daily:

- Check the device overlay to make sure it is intact.
- Power on the device to check the beeper and the display message:
    - Make sure there is no beeping that indicates the tamper was triggered.
    - Read the firmware version to make sure the version number is correct.
- Check the device appearance to make sure there are no holes on the device or any suspicious objects around the ICC card slot.

13. Decommissioning PCI-Certified Devices

All PCI-certified devices require proper decommissioning prior to device disposal to ensure the protection of all sensitive financial card data. For instructions on decommissioning your device, see Decommissioning of PCI-Certified Devices on the ID TECH Knowledge Base.

14. Troubleshooting

The VP3350 is designed to be reliable and easy to troubleshoot. The components that may require troubleshooting include the power module (if applicable), the reader, and the serial cable.

Symptom	Probable Cause	Remedy
General Issues		
4 RED LEDs blink and the device beeps	Unit has been tampered	Contact IDTECH Support
4 Yellow blink and the device beeps	Unit was not activated	Contact IDTECH Support
4 Yellow LEDs are on	LCL-KEK is not loaded or was erased	Contact IDTECH Support
4 Green LEDs blink	DEK is not loaded or was erased	Contact IDTECH Support
No communication and all LEDs off	• Power off • Battery out of charge • Host device not connected	• Charge the battery • Press the device Reset button • Make sure to enter the correct paring password
Bluetooth paring failed	• Host device running Android 6.x or earlier • Mobile does not work in BLE security mode	• Make sure the host device is running Android 6.x or later
Reader does not appear to be powered on after pressing the side button (no LEDs are lit)	• Reader not powered on • Battery out of charge	• Connect the device to PC via a USB cable • Replace the device with another unit known to work to verify that the installed USB cable wiring works correctly
Some cards or fobs read, but not all	• Possible bad card or fob. • Unsupported card used. • Wrong firmware	• Check to see if the card or fob is damaged • Verify that the correct firmware is loaded on reader; contact your ID TECH representative
LEDs do not light and the beeper is not audible when presenting a card or fob	• Card, fob, or phone not properly presented • RF interference • Unsupported card used • Wrong firmware	• Present card, fob, or phone closer to the antenna and ensure it is parallel to the face of the reader • Verify that the card, fob, or phone is valid and current • Verify that metal is not interfering with the antenna • Test with *ViVOcard Contactless Test Card* part number 241-0015-03, Rev A • Try a different card, fob, or phone • Check to see if the card, fob, or phone is damaged • Verify that correct firmware is loaded on reader; contact your ID TECH representative • Power cable plug is fully inserted • Make sure device is not set to Passthrough mode • Replace the unit
Communication Issues		
No data received or data is garbled	Faulty or incorrect cable connections.	Check that the cable connection is secure and in the correct port on the device
Fail to start transaction, 0x0B returned	Device in Passthrough mode or transaction mode	• Need to exit Passthrough mode • Need to cancel transaction
Fail to start transaction, 0x60 returned	No terminal data or application data	Need to load terminal data or application data for Contact EMV transactions
Fail to start transaction, 0x04 returned	Missing Key	Please re-start VP3350 and monitor the LEDs to confirm whether to Load LCL key or Data Key

Symptom	Probable Cause	Remedy
Firmware loading software indicates "Open device failed"	Device is not fully connected to PC	• Check the cable connection • Check the device
Firmware loading software indicates "Load firmware failed"	Device is not fully connected to PC	Check the cable connections
Firmware loading software indicates "Send Command failed"	Bootloader firmware in device was destroyed	Contact your ID TECH representative to reload manufacture's firmware

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

14.1. Tamper Detection Codes

If a tamper event occurs, the VP3350 stores a tamper code in its security log. Check the security log with the **Get DRS Info (C7-3A)** command; see the *NEO 2 Interface Developer's Guide* for details.

Tamper Event Type	Code
EVENT_TYPE_TAMPER_ACTIVE	0
EVENT_TYPE_TAMPER_DEACTIVE	1
EVENT_TYPE_TAMPER_GENERIC	2
EVENT_TYPE_TAMPER_ACK	3
EVENT_TYPE_TAMPER_TIMEOVRF	4
EVENT_TYPE_TAMPER_MONOTONICOVRF	5
EVENT_TYPE_TAMPER_VOLT	6
EVENT_TYPE_TAMPER_CLK	7
EVENT_TYPE_TAMPER_TEMP	8
EVENT_TYPE_TAMPER_FLASH	9
EVENT_TYPE_TAMPER_TST	10
EVENT_TYPE_TAMPER_PIN	11
EVENT_TYPE_TAMPER_BAT	12
EVENT_TYPE_TAMPER_ALL	255

15. For More Information

- To learn more about VP3350 and other ID TECH products, visit the ID TECH Knowledge Base.
- Visit us online at http://idtechproducts.com.
- Find more Tech Support resources at the ID TECH Tech Support home page.

16. Appendix A: LED 0 Behavior status

The following table describes the LED 0 status between the polling mode and the UI scheme.

Table 93: LED 0 Behavior status

LED 0 Behavior		Poll mode	
		Auto poll	Poll on demand
UI Scheme	ViVOtech	ON	ON
	Visa Wave	Flash every 1 sec.	Toggle
	EMEA	ON	Blink per setting in DFEE37

Tag	Length	Value	Description
DF EE 37	01	03	EMEA Language Line UI Scheme + in run mode, the LED blink duty is 0.5s/4.5s and in standby mode, the LED blink duty is 0.1s/5s. LED1 blinks in run mode and LED 3 blinks when BT is connected.
DF EE 37	01	13	EMEA Language Line UI Scheme + in run mode, the LED blink duty is 0.5s/1s, and in standby mode, the LED blink duty is 0.1s/1s. LED1 blinks in run and standby mode and LED3 blinks when BT is connected.
DF EE 37	01	23	EMEA Language Line UI Scheme + in run mode, the LED blink duty is 0.5s/2s, and in standby mode, the LED blink duty is 0.1s/2s. LED1 blinks in run and standby mode and LED3 blinks when BT is connected.
DF EE 37	01	33	EMEA Language Line UI Scheme + in run mode, the LED blink duty is 0.5s/3s, and in standby mode, the LED blink duty is 0.1s/3s. LED1 blinks in run and standby mode and LED3 blinks when BT is connected.
DF EE 37	01	43	EMEA Language Line UI Scheme + in run mode, the LED blink duty is 0.5s/4s, and in standby mode, the LED blink duty is 0.1s/4s. LED1 blinks in run and standby mode and LED3 blinks when BT is connected.
DF EE 37	01	53	EMEA Language Line UI Scheme + in run mode, the LED blink duty is 0.5s/5s, and in standby mode, the LED blink duty is 0.1s/5s. LED1 blinks in run and standby mode and LED3 blinks when BT is connected.
DF EE 37	01	63	EMEA Language Line UI Scheme + in run mode, the LED blink duty is 0.5s/1s, and in standby mode, the LED blink duty is 0.1s/1s. LED1 blinks in run mode and LED3 blinks when BT is connected.
DF EE 37	01	73	EMEA Language Line UI Scheme + in run mode, the LED blink duty is 0.5s/2s, and in standby mode, the LED blink duty is 0.1s/2s. LED1 blinks in run mode and LED3 blinks when BT is connected.
DF EE 37	01	83	EMEA Language Line UI Scheme + in run mode, the LED blink duty is 0.5s/3s, and in standby mode, the LED blink duty is 0.1s/3s. LED1 blinks in run mode and LED3 blinks when BT is connected.
DF EE 37	01	93	EMEA Language Line UI Scheme + in run mode, the LED blink duty is 0.5s/4s, and in standby mode, the LED blink duty is 0.1s/4s. LED1 blinks in run mode and LED3 blinks when BT is connected.

Tag	Length	Value	Description
DF EE 37	01	A3	EMEA Language Line UI Scheme + in run mode, the LED blink duty is 0.5s/5s, and in standby mode, the LED blink duty is 0.1s/5s. LED1 blinks in run mode and LED3 blinks when BT is connected.
DF EE 37	01	F3	EMEA Language Line UI Scheme + in run mode, the LED always on, and in standby mode, the LED blink duty is 0.1s/5s. The LED1 always on in run mode and LED3 always on in run and blink in standby.

17. Appendix B: VP3350 Demo Setup for Mobile Devices

This document provides instructions for setting up a VP3350 for demo purposes.

Before You Begin:

- Make sure there are no other ID TECH readers connected to your mobile device.
  - **iPhone:** Check for ID TECH devices under **Settings -> Bluetooth -> My Devices**. If any are present, select the blue information icon (ⓘ) and select **Forget This Device** at the bottom of the screen.
  - **Android:** Check for ID TECH devices under **Settings -> Connections -> Bluetooth -> Paired Devices**. If any are present, select the settings icon (⚙) for that device, then select **Unpair** on the next screen.
- Go to the Apple App Store or Google Play Store and install the ID TECH NEO 3 app.

Disclaimer: This procedure is for setting up VP3350 for demo purposes only. If a reader is configured for demo purposes, you must re-configure it for use in a production environment.

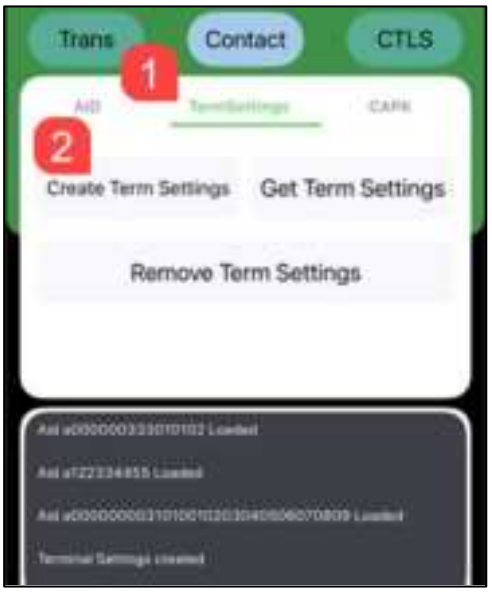
1. Plug the VP3350 into your mobile device (note that if your VP3350 is a Bluetooth model, make sure the reader is paired to your device).
2. Locate and open the ID TECH NEO 3 app. The message pane indicates there is a device connected.

3. Select the **Start** button. The message pane displays **Start Transaction info ERROR: ID-"RETURN_CODE(rawValue:61024)", message: Data not exist**. This error indicates the device has not yet been configured.

4. Select the **Clear** button to delete all messages in the bottom two panes.

5. Select the **Contact** button at the top of the screen. The default tab is **AID**. Select the **Load Default AIDs** to load the demo AIDs. The message pane below will display that the app has loaded many AIDs onto the reader.

6. Select the **TermSettings** tab, then select the **Create Term Settings** button. The message pane below will display **Terminal Settings created**.



7. Select the **CAPK** tab, then select **Load Default CAPK**. The message pane below will display that the app has loaded many CAPKs onto the reader. VP3350 is now configured for demo purposes.

- Select the **Trans** button and test the demo by selecting the **Start** button. The message pane below displays that a transaction command was accepted.

18. Appendix C: Auto Transaction Mode (AT)

VP3350 supports USB composite interfaces (such as USB-HID and USB-Keyboard). When a VP3350 enables AT mode after tapping, inserting or swiping a card, the transaction data can be output via USB-KB in ASCII format.

18.1. Configuration

VP3350 readers must have their transaction settings properly configured to successfully enable AT Mode, including:

- EMV Contact terminal configuration 4C or 5C and corresponding data (REQUIRED)
- EMV Contact AID (REQUIRED)
- Transaction Interface (Tag DFEF37) is recommended, wherein all MSR/CT/CTLS are enabled by default
- Other AT-dedicated Tags, as listed below

Tag	Length (Bytes)	Description
DFEC14	1	Enable/Disable tag DFEC15. Default is disabled.
DFEC15	Up to 117	Output customized data (ASCII HEX) in Tag DFEC15 when finished with CT/CTLS. Default is SN (10 bytes) when DFEC14 is enabled.
DFEC17	1	**1:** Output MSR data is in ASCII format and plaintext when encryption is enabled and the MSR card information is on the whitelist (Default). **0:** Output MSR data is in an enhanced format and encrypted when encryption is enabled and the MSR card information is not on the whitelist.
DFED0A	1	Enable/Disable DFEE25 output when ICC falls back to MSR. Default is 1: Enabled.
DFED20	Up to 16	Company Name. Set by the customer. The output data includes this Tag during a CTLS transaction. The Tag must appear within Tag DFEF5A for the output data to include it during a CT transaction. Default is none.
DFED21	Up to 3	Configuration Data. Set by the customer. The output data includes this Tag during a CTLS transaction. The Tag must appear within Tag DFEF5A for the output data to include it during a CT transaction. Default is none.
DFED22	Up to 32	Current Configuration Version. Set by the customer. The output data includes this Tag during a CTLS transaction. The Tag must appear within Tag DFEF5A for the output data to include it during a CT transaction. Default is none.
DFED4F	Up to 8	USB KB I/F prefix. Default is none.
DFED5A	8	Byte 4 bit 0: Indicate whether the reader should make a sound/beep upon CT-only completion. 1: Beep off.

		0: Beep on (Default). Byte 4 bit 1: Indicate whether the start sound/beep should occur before starting to send R-Frame or after finishing sending R-Frame until removing the card to stop the sound/beep. 1: Start beep after finishing sending R-Frame. 0: Start beep before starting to send R-Frame (Default).
DFEF59	6	Transaction amount. AT chooses this Tag instead of 9F02. Default is US$4.44 (00 00 00 00 04 44)
DFEF5A	Up to 127	Specify any EMV Tags in DFEF5A to output to the USB KB I/F when choosing CT only.
DFEF5B	Card	Mask Tag for Tag 5A PAN. If encryption is disabled, this Tag is not present. This Tag is always masked, but without "A1" before the length.
DFEF5C	Card	Mask Tag for Tag 56 Track 1. If encryption is disabled, this Tag is not present. This Tag is always masked, but without "A1" before the length.
DFEF5D	Card	Mask Tag for Tag 57 Track 2. If encryption is disabled, this Tag is not present. This Tag is always masked, but without "A1" before the length.
DFEF5E	Card	Mask Tag for Tag 9F6B Track 2 of the MCHIP. If encryption is disabled, this Tag is not present. This Tag is always masked, but without "A1" before the length.
DFEF5F	Card	Mask Tag for Tag DFEF17 Track 1. If encryption is disabled, this Tag is not present. This Tag is always masked, but without "A1" before the length.
DFEF60	Card	Mask Tag for Tag DFEF18 Track 2. If encryption is disabled, this Tag is not present. This Tag is always masked, but without "A1" before the length.
DFEF61	2	Details in Tag DFEF61 AT mode error code.
DFEF62	1	Enable/Disable MSR fall back to ICC. If this Tag is enabled and an MSR transaction encounters a service code of 2 or 6 in MSR tracks, the reader automatically falls back to an ICC transaction. 0: The outcome is MSR data (Default). 1: MSR falls back to CT in only service code of 2 or 6 in MSR tracks.
DFEF65	1	Enable/Disable DFEF61 error report. 1: Enabled (Default). 0: Disabled.
DFEF6E	Up to 8	USB KB I/F postfix. Default is 0D0D.
DFEF6F	1	Character delay time (US). 0x30: 1200 (Default) 0x31: 2 000 0x32: 5 000 0x33: 10 000 0x34: 20 000 0x35: 50 000 0x36: 0

DFEF7E	2~20	Error Code List for Fallback to MSR This Tag can hold 1 set of 2 bytes, up to a total of 10 sets of error codes. After a CT transaction encounters a CT error code (DFEE25), the error code is compared against the error code list (DFEF7E). If it matches, the reader forces a fallback from CT to MSR.

18.2. Enable AT Mode

The **Set Poll Mode** command (01-01) allows the host device to switch a VP3350 between Poll on Demand Mode (01) and AT Mode (02). The reader reboots when the command is successful.

Note: Transaction configuration commands are not allowed in AT Mode; to apply the proper configuration, set the VP3350 to Poll on Demand Mode.