ID TECH Kiosk V Multi-Interface User Manual

FCC Regulatory Compliance
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:

- Reorient or relocate the receiving NFC antenna.
- Increase the separation 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 NFC 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.

IC Compliance Warning

Operation is subject to 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.

Cautions and Warnings

⚠️	**Caution:** The Kiosk V should be mounted 1-2 feet away from other Kiosk Vs. Can be adjusted based on lane setup.
⚡	**Warning:** Avoid close proximity to radio transmitters which may reduce the capability of the reader.
⚠️	**CAUTION:** Risk of Explosion if Battery is replaced by an Incorrect Type. Dispose of Used Batteries According to the Instructions.

Revision History

Rev	Date	Changes	By
A	08/10/2023	Initial Release	CB
B	03/29/2024	Added power adapter part numbers.	CB

Table of Contents

1. Overview

The ID TECH Kiosk V is a compact, one-piece EMV contactless reader with PCI PTS 6.X, designed to support contactless EMV transactions based on ISO 18092, ISO 14443 Type A/Type B/MiFare compatible cards, fobs, and tags, as well as NFC phones.

The Kiosk V supports multi-interface host communication using the protocol defined in the *NEO Interface Developers Guide*. This comprehensive guide describes all the firmware commands and other features available in NEO-series devices; it is the authoritative source for technical information of interest to systems integrators; contact your ID TECH representative to obtain a copy of this guide, which is available only on request.

1.1. Universal SDK

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

1.2. Encryption

Kiosk V supports industry-standard Triple DES or AES encryption, PCI PTS 6.1, and has DUKPT-based key management (per ANSI X.9-24). Encryption can be configured to occur with a data variant as desired. ID TECH operates a certified Key Injection Facility, capable of injecting your unit(s) with any required keys. Consult your ID TECH representative to learn about all available options involving key injection.

1.3. Kiosk V SRED Protocol Versus Non-SRED Protocol

Kiosk V Multi-Interface readers come in two models: SRED and non-SRED:
- Kiosk V SRED readers adhere to the NEO 2 group and AID design.
- Kiosk V non-SRED readers are backwards-compatible with Kiosk III and Kiosk IV readers (both of which use NEO 1.20 protocol).

Following those specifications, Kiosk V SRED readers use *NEO 2 IDG* commands, but Kiosk V Non-SRED readers use *NEO IDG* commands. Device integrators **should not** migrate configurations for a non-SRED Kiosk V reader from an SRED-designed reader (or vice-versa).

2. Features

Kiosk V MI Non-SRED readers support the following transaction types:

- ISO/IEC 14443 Type A and B
- ISO 18092
- Backwards-compatible to NEO 1 commands used in Kiosk III readers (non-SRED version only).
- Suitable for transit, kiosks, parking and various other unattended and attended verticals.
- Consumer Intuitive: Equipped with LEDs and sound to provide visual and audible cues to enable smooth and seamless transactions.
- Secure: Provides highly secure transactions whether financial, pre-paid, loyalty, or gift cards. Data is encrypted at the time of the transaction and never travels in clear-text form.
- Self-contained NFC antenna
- Contactless EMV L1 and L2 Certified
- Ruggedized product made for outdoor use
- USB, Bluetooth, UART/TTL, and RS-232 interfaces
- PCI PTS 6.1
- Supports TDES & AES
- Supports DUKPT key management
- Supports Remote Key Injection
- Supports remote FW updates
- Supports the latest Visa, Mastercard, American Express and Discover L2 Kernels
- Supports international certifications like: Interact, JCB
- Supports major transit kernel like Visa for transit, Interact Transit
- Supports Apple VAS & Google Smart Tap

2.1. Certifications and Approvals

- EMV CO Contactless L1 3.1a
- Visa 2.2C
- Visa Transit 2.2 C
- Master 3.1.4
- Amex 4.1
- Apple VAS
- Discover 2.0
- Interac 1.8
- Interac ABM 1.8
- Interact Transit 1.8
- Google SmartTap 2.1
- JCB 1.6
- Felica

- CE
- CE RED
- FCC
- IC
- REACH
- RoHS
- UL
- Mifare

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

3. Kiosk V Specifications

Hardware	
MTBF	500,000 hours based on Telcordia Technologies SR-332 modeled at 40° C.
Transmitter Frequency	13.56 MHz +/- 0.01%
Transmitter Modulation	ISO 14443-2 Type A Rise/Fall Time: 2-3 µsec. Rise, < 1 µsec fall ISO 14443-2 Type B Rise/Fall Time: < 2 µsec. each; 8% - 14% ASK ISO 18092 ISO 21481 (PCD & NFC)
Receiver Subcarrier Frequency	847.5 KHz
Receiver Subcarrier Data	ISO 14443-2 Type A: Modified Manchester ISO 14443-2 Type B: NRZ-L, BPSK ISO 18092 ISO 21481 (PCD & NFC)
Typical Read Range	0-4 cm (0 to 1.5 inches)
Physical	
Length	75 mm (2.95 inches)
Width	60 mm (2.36 inches)
Depth	11.2 mm (0.44 inches)
Environmental	
Operating Temperature	-30° C to 70° C (-22° F to 158° F), max change of 10° C per hour
Storage Temperature	-30° C to 85° C (-22° F to 185° F) [non-condensing]
IK Rating	IK 06
IP Rating	IP 65

3.1. Power Consumption
Note the following information about Kiosk V power consumption.

3.1.1. Working Mode

Working Mode	Contactless Transaction Mode		<400mA/5V
	Idle Mode		<200mA/5V
	Multi-Port	USB Suspend Mode	< 2.5mA/5V
		RS232/UART Sleep Mode	< 2.5mA/5V
		RS232/UART Stop Mode	< 2.5mA/5V

3.1.2. Power saving Mode of multiport
- USB port:
  - Suspend Mode: Power consumption in suspend mode is <2.5mA/5V. Kiosk V units can wake up to normal mode within <500ms.
- RS232/UART port:
  - Sleep mode:
    Power consumption in sleep mode is <2.5mA/5V. Kiosk V units can wake up to normal mode within <500ms.
  - Stop mode:
    Power consumption in stop mode is <2.5mA/5V. Kiosk V units can wake up to normal mode within <500ms.

3.2. 24-Hour Device Reboot
Per PCI Requirements, this device reboots every 24 hours. Please contact your device integrator if you need to check the reboot time for your unit.

3.3. KIOSK V Connectors and Interfaces
The KIOSK V is designed to work Windows, Android, and iOS via a physical USB-C, and Bluetooth communication.
- USB-C communicates with popular Android mobile phones and tablets.
- Bluetooth connection supports both Android and iOS.

When communicating over USB, the KIOSK V's default emulation mode is USB HID.

4. Bluetooth Pairing Instructions

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 KIOSK V.

1. Enable the Bluetooth device search function on the host smart phone or tablet.
2. Make sure the KIOSK V is charged or connected to a power source via USB.
   a. When connected to a power source, the KIOSK V automatically activates Bluetooth.
3. Find a Bluetooth device named **IDTECH-BLE-XXXXX** on the host smart phone or tablet and select **Pair**.
4. Enter the password for pairing. The default password is **123456**.
5. Follow the payment transaction instructions provided by a compatible payment application maker to complete a transaction.

The KIOSK V will remain connected via Bluetooth to the host device indefinitely when powered via the USB cable.

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 KIOSK V](#) below for more information.

4.1. iOS Connectivity: BLE and KIOSK V

The KIOSK V 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 KIOSK V.

It is critical to note that if the KIOSK V 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 KIOSK V has a default friendly name of **IDTECH-BLE-XXXX**. This is the default name the ID TECH Universal SDK uses to connect to the first KIOSK V 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 KIOSK V, you do not need to obtain the SDK.

5. KIOSK V LED and Sound State Indicators

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

Device State	LED1	LED2	LED3	LED4	Beeper[1]
Device FW, certificates, or keys self-test failed.	○ off	○ off	○ off	● blink	Beeps
Device Tampered	○ off	○ off	○ off	● blink	Beeps
Device Deactivated	○ off	○ off	○ off	● blink	Beeps
Device Activated[2]	○ off	○ off	○ off	● on	Off
Device Key Missing[3]	● blink	● blink	● blink	● blink	Off
Ready for Transaction	● blink	○ off	○ off	○ off	Off
Bluetooth Connected	○ off	○ off	○ off	● on	Beeps Once
Bluetooth Connection Failed / Bluetooth Disconnected	○ off	○ off	○ off	● on	Beeps Twice
Transaction Started[4]	● on	○ off	○ off	○ off	Off
Transaction Successful[5]	● on	● on	● on	● on	Beeps Once
Transaction Failed	○ off	○ off	○ off	○ off	Beeps Twice
Bootloader Mode	○ off	○ off	○ off	● on	Off

---

[1] Note that "beeps" indicates constant beeping unless the description includes a specific number of beeps (such as "twice").

[2] The device has loaded certificates successfully and is activated.

[3] The device only has LCL-KEK; the required key is not injected.

[4] The transaction has started and the device is waiting to read a card.

[5] LEDs remain on for 1000ms.

5.1. Tamper and Failed Self-Check Indicators

The KIOSK V 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
LED	LED4 blink Red
Buzzer	Alarm tone

6. ID TECH Universal SDK

By virtue of its EMV L2 kernel, KIOSK V 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 KIOSK V 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 KIOSK V comparatively easy while greatly facilitating debugging and event handling.

To obtain the Universal SDK free of charge, visit ID TECH's KIOSK V 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 KIOSK V'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 KIOSK V, request the *NEO Interface Developers Guide* (IDG), P/N 80139403-001. This document includes not only low level (firmware) commands but error codes, response codes, and information on various default settings.

7. Kiosk V Installation

This section provides information on how to install the Kiosk V on a kiosk.

7.1. Parts List

Verify that you have the following hardware for the installation of the Kiosk V:
- **Kiosk V**
- **USB Cable:** A standard USB-C cable could be used for both data communication and power

ID TECH also offers these USB-C cables for purchase:
- **80185227-001** (USB-C to USB-A)
- **80185226-001** (USB-C to UART/TTL)
- **80185224-001** (USB-C to RS232; Note: Requires a power supply)

ID TECH also offers the following power adapters for purchase:
- **AC0005R-28:** Adapter; AC 100-240V;DC 5V/2A;50/60HZ;US Plug
- **AC0005R-31:** Adapter; AC 100-240V;DC 5V/2A;50/60HZ;UK Plug
- **AC0005R-32:** Adapter; AC 100-240V;DC 5V/2A;50/60HZ;EU Plug

7.2. Mounting the Kiosk V

To optimize performance, install Kiosk V readers away from or in front of any metal surfaces or materials that have metallic content, which can interfere with the RF field.
- Kiosk V readers perform optimally when mounted away from metal surfaces.
- ID TECH offers solutions to enhance Kiosk V performance, such as spacers, available for versatile installations.

The default suggested installation uses the drilling template provided below on a non-metallic surface.

For installation on metallic surfaces, ID TECH offers three options:
1. Install the Kiosk V directly on a metallic surface using ID TECH's drilling template guide.
2. Install the Kiosk V with a plastic spacer between the metallic surface and Kiosk V to enhance RF performance (see Installing the Optional Spacer for mounting steps).
3. Install the Kiosk V using a flush installation embedded into the metallic surface for an integrated flush design and enhance RF performance.

Please contact your ID TECH sales rep for additional help with mounting options and customizations.

Kiosk V Part# IDVK-5XX:
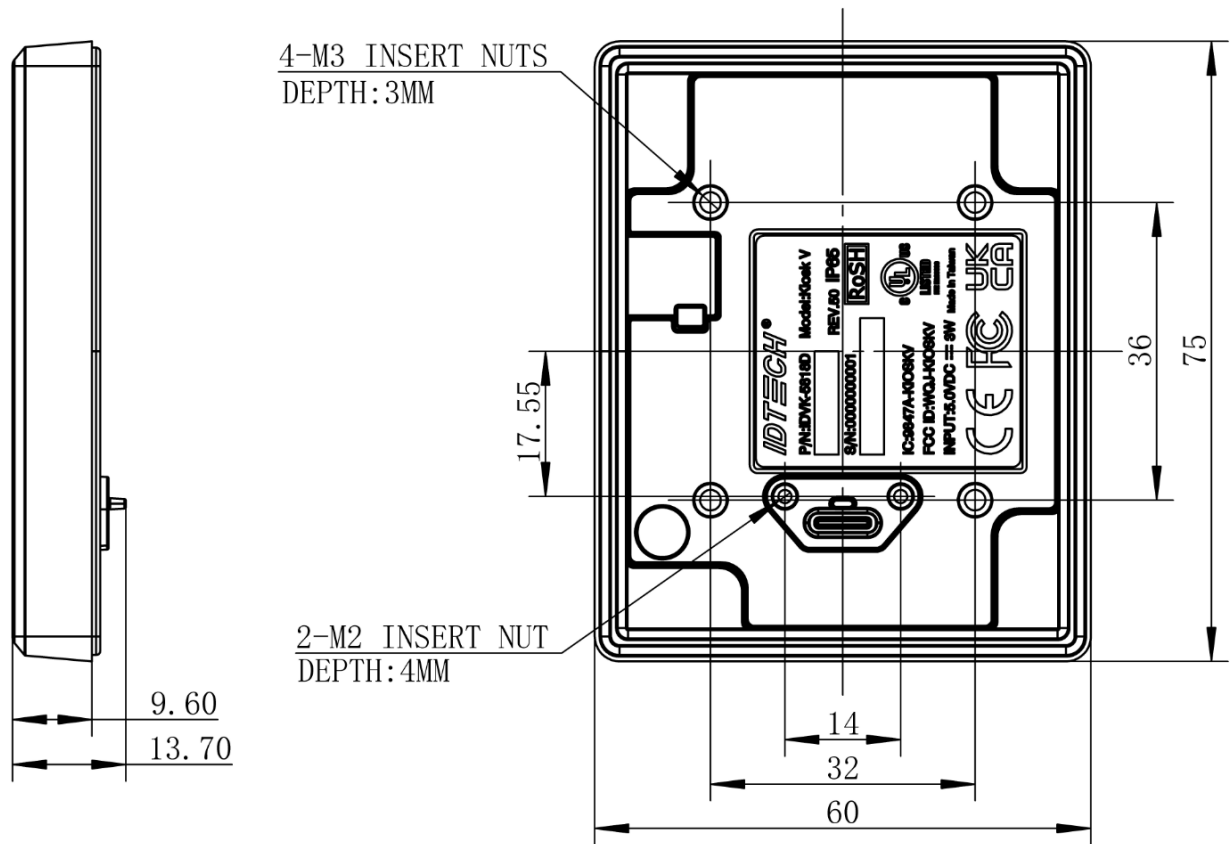
> **Note:** The Kiosk V is post-compatible with Kiosk III and Kiosk IV dimensions. Posts are 36mm apart in the lengthwise direction and 32mm apart widthwise. See drawing below.

Use the following instructions to mount the Kiosk V on the exterior of a kiosk structure:
Using the Drill Template below, locate and mark the (4) 3.25mm (0.138 inch) mounting holes.
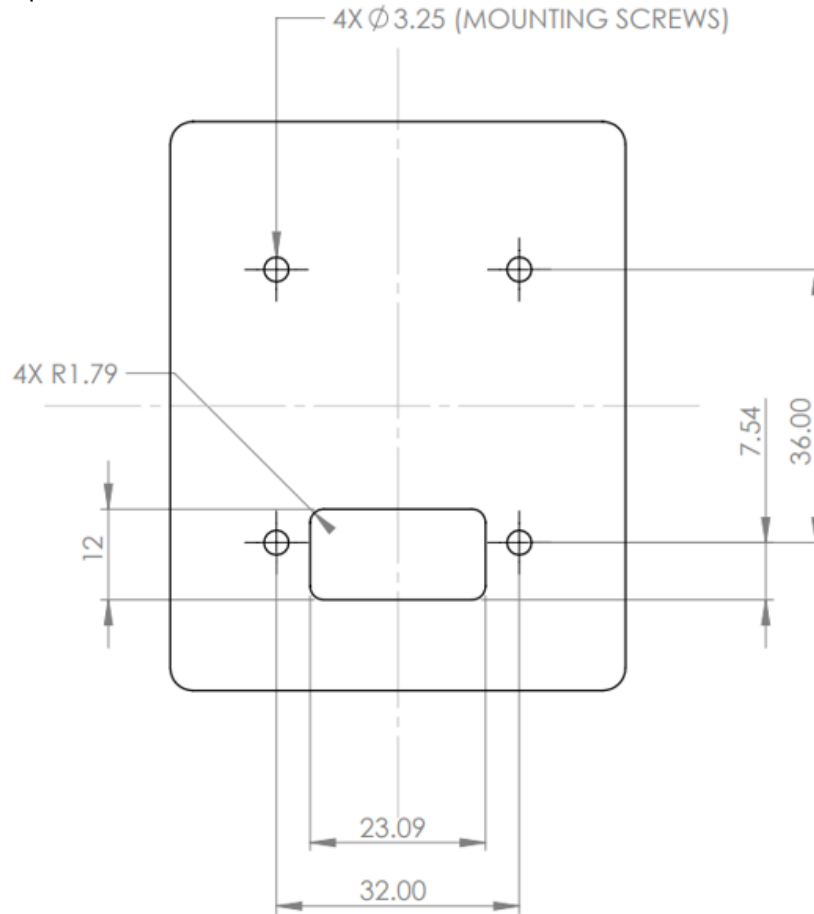
Dimensions are in mm; tolerance ±0.15mm.

Note: Verify the orientation of the Kiosk V before marking and drilling the holes. The **rectangle** hole should be located towards the bottom of the mounting location to ensure that the Kiosk V is oriented correctly with the LEDs at the top.

1. Using the Drill Template, locate and mark the 9.95mm*15.77mm (0.392inch*0.621inch) rectangle hole (used for connecting the USB-type C cable to the Kiosk V).
2. Align the four M3 screws with the mounting holes and attach the Kiosk V to the outside surface.
3. Use the four screws to secure the Kiosk V to the outside surface of the kiosk. Make sure to tighten the screws securely so that the Kiosk V does not move on the outside surface of the kiosk.
4. Route the end of the USB-Type C cable through the rectangle hole into the kiosk and tighten the two M2 screws in the over mode of the USB-Type C cable to ensure the cable is locked reliably.

7.3. Connecting to Power

The Kiosk V can be powered via the USB port or UART/TTL connectors. Note that the USB-C to RS-232 connector requires a power supply.

7.4. Communication via USB

The PID is 4690 (hex).

7.5. Connecting to the Data Port

The Kiosk V connects via USB-C.

7.6. Using the Kiosk V to Make a Purchase

The section below describes how to use the Kiosk V to make purchases.

7.6.1. Presenting Cards or NFC Phones

The Kiosk V supports Open Loop and Close Loop payments using Contactless/NFC/ technology. Present the card/phone in close proximity to the front portion of the Kiosk V. Present the card/phone so that maximum surface area is parallel to the Kiosk V as shown here:

The Kiosk V should beep, and the four green LEDs should illuminate in sequence, then all will illuminate together, briefly (750 msec), to indicate a successful test.

This tests the Kiosk V's ability to read the Contactless test card. The reader produces no reaction in the case of an unsuccessful test. If you use a test card and the Kiosk V, a dummy transaction can be tested. The transaction will not be authorized and will come back with a response but will at least test for end-to-end connectivity. ID TECH's Universal SDK Demo App (uDemo) is available free of charge for this test.

7.7. Installation Suggestions

- The Kiosk V is susceptible to RF and electromagnetic interference***. Do not mount the unit within 3 or 4 feet of large electric motors, computer UPS systems, microwave transmitters (Wi-Fi routers), anti-theft devices, radio transmitters, communications equipment and so on.***
- ***Close proximity of metal to the RF-emitting end of the NFC antenna can greatly reduce the NFC antenna's range.***
- Tie all cables neatly with nylon cable-ties and route them so that they are inaccessible and invisible to customers. Label the cable ends, host, ID TECH and power, to simplify connection testing or component replacement.
- Test the Kiosk V installation using a test card to perform an end-to-end transaction (the same as an actual purchase on the Kiosk). The kiosk display panel (if it exists) should display "Requesting Authorization." Even if the transaction is declined (as it should be with a test card), it will prove connectivity all the way through the system. If possible, the store manager or some other responsible party should test each Kiosk V on a regular basis (perhaps at the start of each day or at least once per week) with a test card to ensure continued operation and functionality. If the kiosk is rebooted on a regular basis (such as every night), it is important to test the contactless reader as soon as possible afterwards to ensure continued communication to the kiosk host.

8. RF Interference

Q. Why do I need to know about RF interference?
A. Contactless payment uses radio frequency technology to send card data to a contactless terminal reader.

Q. How can RF interference affect contactless payment?
A. RF interference can cause data errors. If RF interference is present, contactless payment devices may operate intermittently or inconsistently.

Q. Where does RF interference come from?
A. Radio frequency interference (RFI) can originate from a wide number of sources at the point-of-sale (POS). Some examples of sources of RF energy and RF interference include:
AM/FM radio, TV transmitters, 2-way radios, pagers, mobile telephones, power lines, transformers, medical equipment, microwaves, and electromechanical switches.

Q. What should I do if I suspect RF interference exists in my environment?
A. Begin by inspecting your environment for possible sources of RF interference.

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

Q. What RF levels will impact RF operations?
A. Factors that can cause RF interference vary case-by-case. There are no set rules defining a single RF level that will cause RFI. RFI depends on the sensitivity of the equipment under consideration, or how low an interpreting signal can be in the presence of the equipment and cause problems. Equipment can be particularly sensitive to very low signal levels of one frequency and yet be quite immune to high signal levels of another frequency - so frequency is an important factor. Some electronic system components are internally shielded and have a very high immunity to interference; but generally, most equipment has not been so engineered.

8.1. Updating Kiosk V Firmware

ID TECH strongly recommends updating firmware via the Universal SDK. Consult the Universal SDK Guide for your desired platform (included in the ZIP file downloaded from the Kiosk V product page) for integration details.

8.1.1. Universal SDK Demo App

The Universal SDK comes with a rich, fully featured demo app that allows users to run the Kiosk V in USB mode. Visit the Knowledge Base and go to the Kiosk V product page 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.

8.2. Using the Demo Application

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

1. Plug the Kiosk V into the host device with a supported communication cable (not included).
2. Double-click the **UniversalSDKDemo.exe** file and allow a few seconds for the main window to appear (see illustration below).
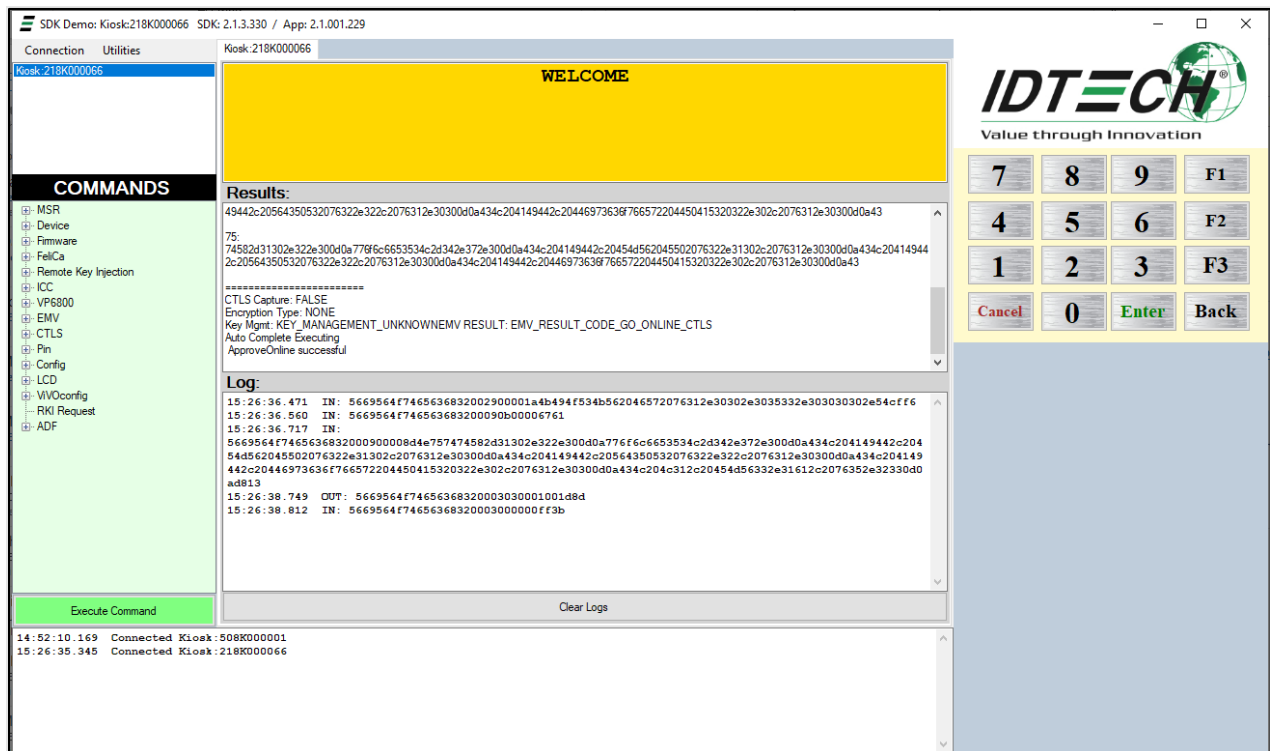
The Universal SDK Demo app displays KIOSK V's available commands in a command tree, as shown above. Single-click on a command to populate the center panel of the window with optional settings relevant to the command (for example, **Amount** and **Start EMV Additional Tags** above). In some cases, text 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 at the bottom of the window). The command executes in real time and a data trace appears automatically in the center and/or right-hand panels. Use the **Clear Logs** button to clear both panels.

9. Kiosk V Low-Level Commands

The following are commonly used commands for the Kiosk V. For a full list of available commands, contact your ID TECH representative for the *NEO Interface Developer's Guide* (for non-SRED Kiosk V readers) or the *NEO 2 Interface Developer's Guide* (for SRED versions of the Kiosk V reader).

> The protocol that Kiosk V devices use depends on whether the reader is an SRED unit or a non-SRED unit:
> - For SRED units, refer to the commands listed in the NEO 2 Interface Developer's Guide.
> - For non-SRED units, refer to commands listed in the NEO Interface Developer's Guide.

9.1. 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.

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* or *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* or *NEO 2 IDGs* (available from your ID TECH representative) for the full **Activate Transaction (02-40)** description.

9.2. Set CA Public Key (D0-03)

The **Set CA Public Key** command adds a new key to the reader.

Command Frame

Byte 0-9	Byte 10	Byte 11	Byte 12	Byte 13	Byte 14 – 18	Byte 19	Bytes 19-n	Byte n+1	Byte n+2
Header Tag & Protocol Version	Cmd	Sub Cmd	Length (MSB)	Length (LSB)	RID (5 bytes)	Key Index (1 byte)	Key Data	CRC (LSB)	CRC (MSB)
ViVOtech2\0	D0h	03h	varies	varies	varies	varies	See below	Varies	Varies

Key Data (all binary)

Byte	Name	Length (bytes)	Description
0	Hash Algorithm	1	The only algorithm supported is SHA-1. The value is set to 01h
1	Public Key Algorithm	1	The encryption algorithm in which this key is used. Currently support only one type: RSA. The value is set to 01h
3-22	Checksum/Hash	20	Checksum which is calculated using SHA-1 over the following fields: **RID** & **KeyIndex** & **Modulus** & **Exponent** where the exponent is either one byte or 3 bytes (although we store it in a 4-byte field)
23-26	Public Key Exponent	4	The real length of the exponent is either one byte or 3 bytes. It can have two values: 3, or 65537.
27-28	Modulus Length	2	Indicates the length of the next field, MSB followed by LSB.
29-n	Modulus	Variable	This is the modulus field of the public key. Its length is specified in the field above.

Response Frame

Byte 0-9	Byte 10	Byte 11	Byte 12	Byte 13	Byte 14	Byte 15
Header Tag & Protocol Version	Cmd	status	Length (MSB)	Length (LSB)	CRC (LSB)	CRC (MSB)
ViVOtech2\0	D0h	See Key Manager status codes	00h	00h	Calculated	Calculated

9.3. 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:

```
56 50 33 36 30 30 20 46 57 20 76 31 2E 30 30 2E 54 0D 0A 4E 45 4F 20
32 2E 30 20 76 31 2E 30 30 0D 0A 43 4C 20 41 49 44 2C 20 50 50 53 45
20 4D 6F 64 75 6C 65 2C 20 76 31 2E 32 0D 0A 43 4C 20 41 49 44 2C 20
56 69 73 61 20 56 43 50 53 20 32 2E 32 2C 20 76 31 2E 30 0D 0A 43 4C
20 41 49 44 2C 20 41 6D 65 78 20 45 78 70 72 65 73 73 50 61 79 20 33
2E 31 2C 20 76 31 2E 32 0D 0A 43 4C 20 41 49 44 2C 20 4D 61 73 74 65
72 43 61 72 64 20 50 61 79 50 61 73 73 20 4D 2F 43 68 69 70 20 33 2E
31 2C 20 76 31 2E 33 0D 0A 43 4C 20 41 49 44 2C 20 44 69 73 63 6F 76
65 72 20 44 50 41 53 20 31 2E 30 20 5A 69 70 20 33 2E 31 2E 32 2C 20
76 31 2E 31 0D 0A 43 4C 20 41 49 44 2C 20 43 55 50 20 71 55 49 43 53
20 31 2E 30 2E 32 2C 20 76 31 2E 31 0D 0A 43 4C 20 41 49 44 2C 20 49
6E 74 65 72 61 63 20 31 2E 35 2C 20 76 32 2E 30 30 0D 0A 43 4C 20 41
49 44 2C 20 4A 43 42 20 31 2E 34 2C 20 76 31 2E 30 0D 0A 43 4C 20 41
49 44 2C 20 41 70 70 6C 65 50 61 79 20 56 41 53 20 31 2E 30 2E 31 30
2C 20 76 31 2E 32 0D 0A 43 4C 20 41 49 44 2C 20 53 6D 61 72 74 54 61
70 20 32 2E 31 2C 20 76 31 2E 32 0D 0A 43 4C 20 4C 31 2C 20 45 4D 56
32 2E 36 62 2C 20 76 35 2E 30 32 0D 0A 43 54 20 4C 32 2C 20 45 4D 56
20 43 6F 6D 6D 6F 6E 20 4C 32 20 56 31 2E 31 30 2E 30 33 37 0D 0A 43
54 20 4C 31 2C 20 45 4D 56 34 2E 33 61 2C 20 76 32 2E 30 30 0D 0A
```

ASCII translation of the data field:
```
VP3600 FW v1.00.T<CR><LF>
NEO 2.0 v1.00<CR><LF>
CL AID, PPSE Module, v1.2<CR><LF>
CL AID, Visa VCPS 2.2, v1.0<CR><LF>
CL AID, Amex ExpressPay 3.1, v1.2<CR><LF>
CL AID, MasterCard PayPass M/Chip 3.1, v1.3<CR><LF>
CL AID, Discover DPAS 1.0 Zip 3.1.2, v1.1<CR><LF>
CL AID, CUP qUICS 1.0.2, v1.1<CR><LF>
CL AID, Interac 1.5, v2.00<CR><LF>
CL AID, JCB 1.4, v1.0<CR><LF>
CL AID, ApplePay VAS 1.0.10, v1.2
CL AID, SmartTap 2.1, v1.2<CR><LF>
CL L1, EMV2.6b, v5.02<CR><LF>
CT L2, EMV Common L2 V1.10.037<CR><LF>
CT L1, EMV4.3a, v2.00<CR><LF>
```

9.4. 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.

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		

10. Periodic Inspection Instructions

The KIOSK V is an unattended 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.

11. Decommissioning PCI-Certified Devices

All PCI-certified devices require proper decommissioning prior to device disposal in order 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.

12. Troubleshooting

Kiosk V readers are reliable and easy to troubleshoot. The components that may require troubleshooting include the power supply, the reader itself, and the serial cable. **If you are unable to resolve the problem, contact** support@idtechproducts.com **(sending an e-mail to this address will automatically open a support ticket).**

| Symptom	Possible Cause	Remedy
General Issues		
Reader does not appear to be powered on (no LEDs are lit). Note that when the unit is expecting a transaction, the first LED (on the left) will illuminate continuously. Otherwise, in the idle state, it will blink.	• Reader not powered on or incorrect voltage. • Improper use of internal power supply provided by the kiosk.	• Check cable connections. • Verify that power is on and correct voltage and current are present. • Make sure that the correct pins are utilized. • Make sure that the power provided is within the specified range of the Kiosk V reader. • Make sure that the correct polarity is observed. • For more information, refer to the Input Voltage under the Electrical specification section. • Replace the Kiosk V.
Reading Cards/Phones		
First LED is lit, but beeper is not audible when card/fob presented.	• Card/fob/phone not properly presented. • RF interference. • Unsupported card used. • Wrong firmware (contact your local support representative).	• Present card/fob/phone closer to the NFC antenna, and ensure it is parallel to the face of the reader. • Verify that the card/fob/phone is valid/current. • Verify that metal is not interfering with the NFC antenna. • Test with "ViVOcard Contactless Test Card" • part number 241-0015-03 Rev A. • Try a different card/fob. • Check to see if card/fob is damaged. • Verify that correct firmware is loaded on reader (local support representative only). • Power cable plug is fully inserted. • Replace the Kiosk V.
Some cards/fobs read, but not all.	• Possible bad card/fob. • Unsupported card used. • Wrong firmware (contact your local support representative).	• Check to see if card/fob is damaged. • Verify that correct firmware is loaded on reader (local support representative only). • Present the card in a different orientation.
Communication to Kiosk		
No data is received, or data is garbled.	• Faulty or incorrect cable connections.	• Check that the cable connection is secure and in the correct port on the Kiosk V.
Load Firmware		
Firmware loading software indicate "Load firmware failed"	Device is not well connected to PC	• Check the cable connection
Firmware loading software indicates "Send Command failed"	Bootloader firmware in device is destroyed	• contact your local support representative to reload manufacture firmware

13. Appendix A: Installing the Optional Spacer

ID TECH offers an optional spacer (P/N: 80185232-001) for integrations on metal surfaces. Note that the line art below uses a metal plate for the mounting point; your integration may differ.

Kiosk V Reader

Optional Spacer

M3 Screws
(not included)

Gasket

Gasket

Mounting Point
(not included)
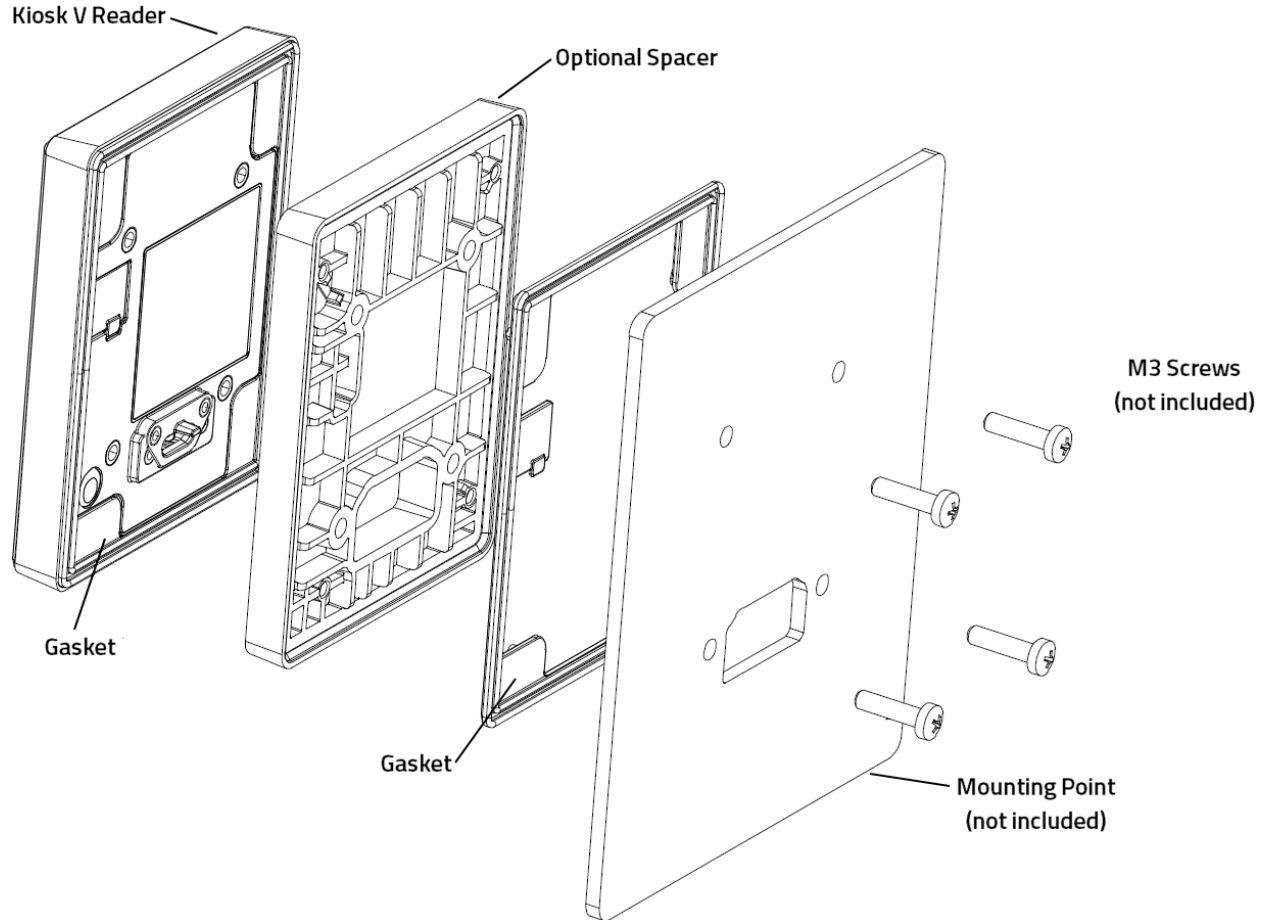
Follow the steps below to install the optional spacer.
1. Place the optional spacer and gasket module on the Kiosk V reader. Make sure to orient the spacer as illustrated below.
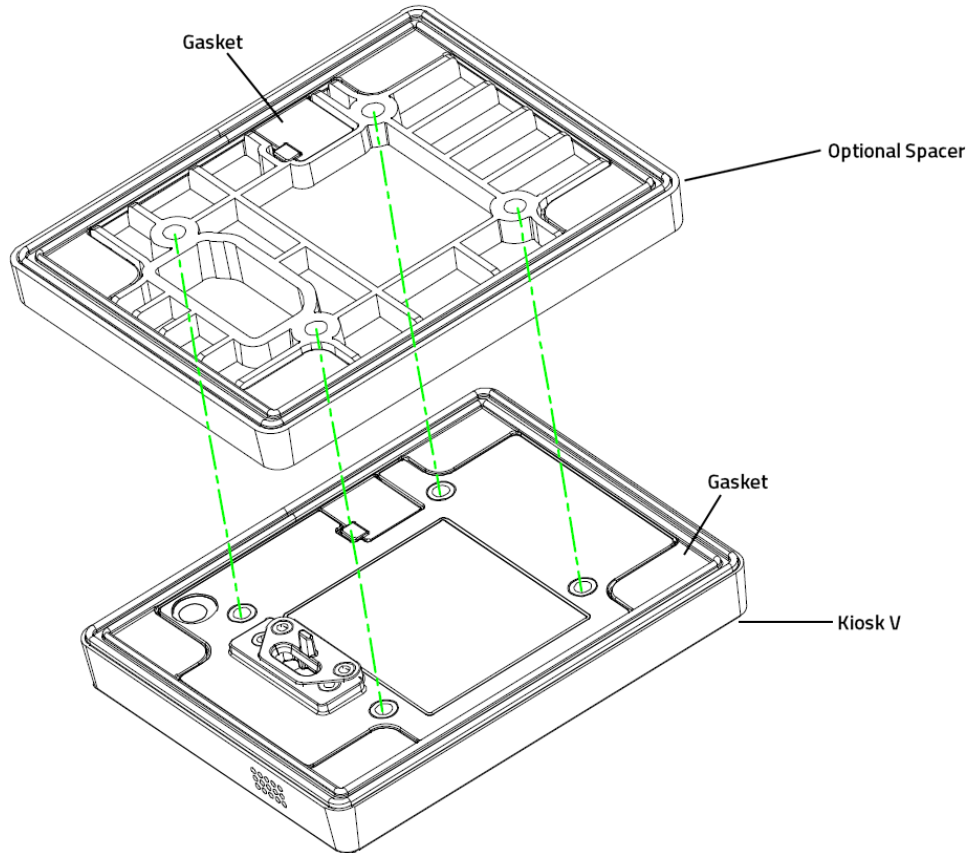
2. Place the second gasket module on the optional spacer; if the gasket and spacer have separated, assemble the gasket to the spacer according to the diagram below.

Note: The gasket's four positioning pins must be fully inserted into the spacer's four holes, and the gasket must be tightly fitted to the spacer assembly's surface without any bumps.

Four Positioning Pins

Gasket

Optional Spacer assembled with Gasket Module

Optional Spacer
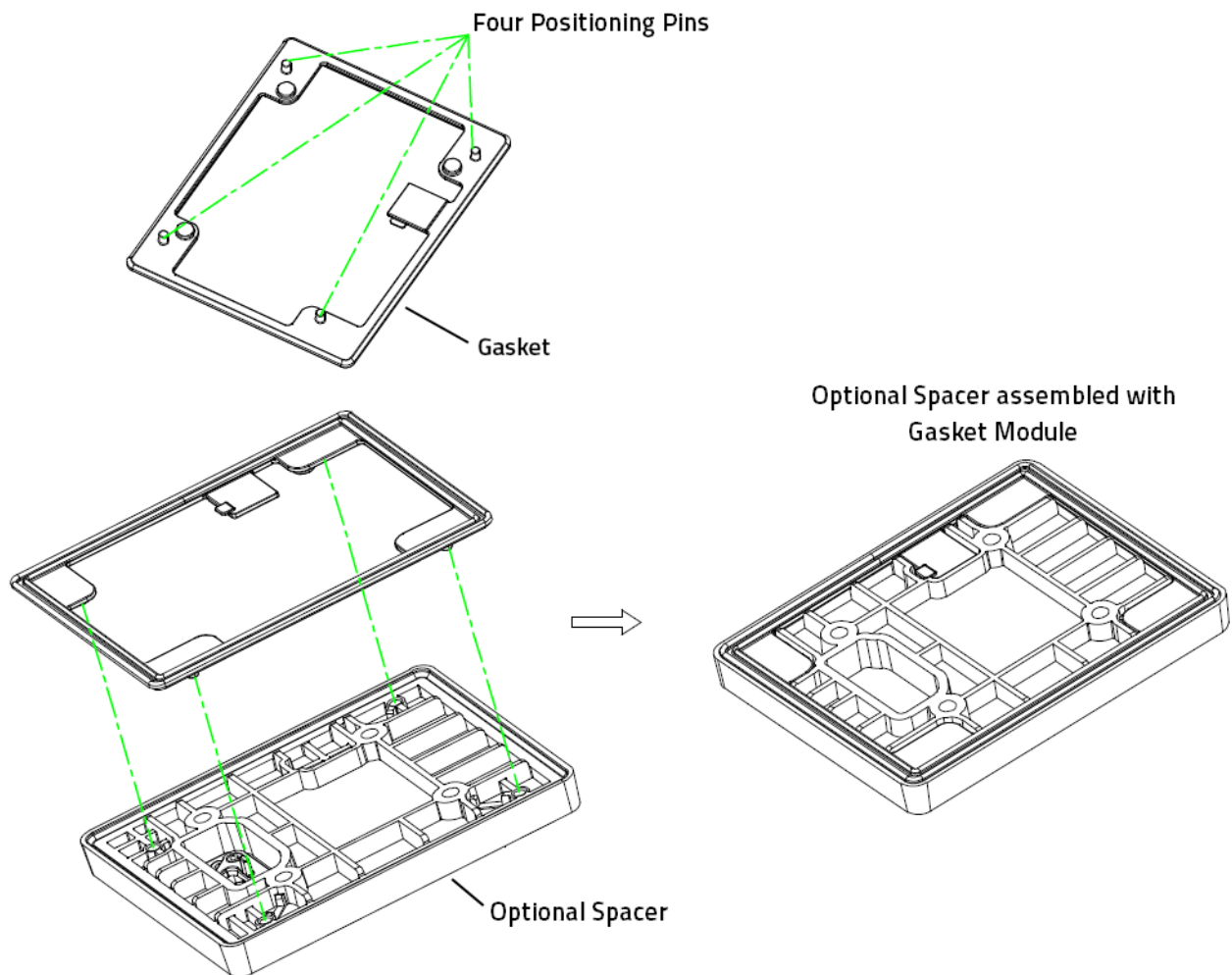
3. Insert and tighten the four M3 screws to mount the spacer assembly to the metal backing plate.

> **Note:** The screws used in your integration should be 9.5mm (the thickness of the spacer + 2.5mm) + X (where X = the thickness of your mounting point). The screws should be tightened to a **maximum** torque setting of 6 kgf.cm. Do not overtighten the screws.