



Integration Guide – VTAP100 access control reader assembly with Wiegand interface

VTAP100-PAC-W-OEM

Revised September 2025 v1.02

DOT ORIGIN

If you need help to set up or use your VTAP100-PAC-W, beyond what is contained in this Integration Guide, then please contact our support team.

Email: vtap-support@dotorigin.com

Download the latest documentation and firmware from <https://vtapnfc.com>

Telephone UK and Europe: +44 (0) 1428 685861

Telephone North America and Latin America: +1 (562) 262-9642

If you have any feedback on setting up or using your VTAP100-PAC-W or this documentation, then please contact our support team. The product is constantly being reviewed and improved and we value feedback about your experience.

Copyright 2025 Dot Origin Ltd. All rights reserved.

No part of this Integration Guide may be published or reproduced without the written permission of Dot Origin Ltd except for personal use. This Integration Guide relates to correct use of the VTAP100-PAC-W only. No liability can be accepted under any circumstances relating to the operation of the user's own PC, network or infrastructure.

Dot Origin Ltd

Unit 7, Coopers Place Business Park, Combe Lane, Wormley

Godalming GU8 5SZ United Kingdom

+44 (0) 1428 685861

Contents

1 Using this guide	1
2 How the VTAP100 works	2
2.1 Default operation	3
2.2 Start reading your own passes	3
2.3 Check status in BOOT.TXT	7
2.4 Send pass payload over a Wiegand interface	9
2.4.1 Send only part of pass payload over Wiegand	10
2.4.2 Format of pass data sent over Wiegand	10
3 Mechanical installation	12
3.1 Power	12
3.2 Environment	13
3.3 Mounting points	14
3.4 Optional RS-232 connection	16
3.5 Wiegand wiring (for model VTAP100-PAC-W only)	18
4 Module integration instructions – FCC/ISED	27
4.1 Applicable FCC/ISED rules	27
4.2 Specific operational use conditions	27
4.3 RF exposure considerations	27
4.4 Antennas	28
4.5 Label and compliance information	28
4.6 Information on test modes	28
4.7 Additional testing requirements	28
4.8 Maintaining Apple VAS(ECP1) or ECP2/Access compliance	29
5 Find your hardware version	30
6 Disposal	31
A VTAP100-PAC-W-OEM engineering drawing	A-1

Safety instructions



WARNING: INTENDED USE

The VTAPI00-PAC-W equipment is intended for use by suitably qualified integrators, who will integrate the VTAPI00-PAC-W-OEM (PCBs) into their own hardware, without any changes or modifications to the VTAPI00-PAC-W-OEM device. (An optional enclosure can be supplied.) Components mounted on the VTAPI00-PAC-W PCBs are not user-serviceable and an assembly of two boards should never be separated. Product safety has been tested to comply with IEC 62368-1.



WARNING: ESD PRECAUTIONS

We recommend careful handling and storage of Electrostatic Sensitive Devices (ESDs) during installation. The VTAPI00-PAC-W-OEM PCBs should always be protected by static shielding bags for shipping or storage.



WARNING: POWER SUPPLY

Use either a MicroUSB to USB cable, **or** the optional captive cable, if any, to connect the VTAPI00-PAC-W-OEM PCBs to a PC for power during configuration. In normal operation the VTAPI00-PAC-W model will be powered by connecting it to an access controller, via the Wiegand connector.

EMC emissions and immunity certifications are only valid when using the VTAPI00-PAC-W-OEM reader board with the optional captive cable.

**WARNING: FCC 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.

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

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 cm between the radiator and a human body.

If the identification number is not visible when the module is installed inside another device, then the outside of the device into which the module is installed must also display a label referring to the enclosed module, Contains FCC ID: 2A282-VTAP100G2 or Contains FCC ID: 2A282-VTAP100, in accordance with enclosed module ID.

Co-location of this module with other transmitters that operate simultaneously are required to be evaluated using the multi-transmitter procedures.

The host integrator must follow the integration instructions provided in this document and ensure that the composite-system end product complies with the requirements by a technical assessment or evaluation to the rules and to KDB Publication 996369.

The host integrator installing this module into their product must ensure that the final composite product complies with the requirements by a technical assessment or

evaluation to the rules, including the transmitter operation and should refer to guidance in KDB 996369.



WARNING: ISED COMPLIANCE

This device contains licence-exempt transmitter(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 any interference that may cause undesired operation of the device.

This equipment complies with ISED radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 cm between the radiator and a human body.

L'émetteur 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;
- (2) L'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Cet équipement est conforme aux limites d'exposition aux rayonnements de la ISED établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec une distance minimale de 20 cm entre le radiateur et un corps humain.

If the identification number is not visible when the module is installed inside another device, then the outside of the device into which the module is installed must also display a label referring to the enclosed module, Contains IC: 30458-VTAPI00G2.

Si le numéro d'identification n'est pas visible lorsque le module est installé à l'intérieur d'un autre appareil, alors l'extérieur de l'appareil dans lequel le module est installé doit également afficher une étiquette faisant référence au module fourni, Contient IC : 30458-VTAPI00G2.

1 Using this guide

This guide is for first-time users of the VTAPI00-PAC-W-OEM reader board assembly.



Figure 1-1 VTAP PAC W OEM reader assembly

It contains the information you need to connect your VTAPI00-PAC-W-OEM hardware. Beyond initial default operation, all information about configuration can be found in the Configuration Guide.

If you need help beyond what is contained in the guides please contact **vtap-support@dotorigin.com**.

2 How the VTAP100 works

With the VTAP100-PAC-W-OEM connected, simply tap your smartphone against the VTAP. Your mobile NFC pass will be read and data sent to the connected equipment. The VTAP100-PAC-W model is designed to be connected to an access controller, over Wiegand, for transferring data or commands.

Of course, the data can only be read if your phone contains a mobile NFC pass, which has been issued in connection with the Merchant ID(s)/Collector ID(s) and ECC key(s) that are known to the VTAP. The unit comes with default values, so that you can test **Default operation on factory settings** before you begin customising any settings.

When the VTAP100-PAC-W-OEM is connected to a computer via USB cable, it appears as a generic mass storage device (like a memory stick). To configure your VTAP, you simply edit or create text files. These will be read automatically, and control the operation of the VTAP reader. The VTAP100-PAC-W must be configured over USB from a PC, before it will send pass data over the Wiegand interface. After being configured it does not need to be connected to a PC. Consult the VTAP Configuration Guide for more detail.

By default the VTAP is fully upgradable in the field. However, the VTAP can be locked in software or hardware, before deploying the unit, so that operation is no longer easily changed.

2.1 Default operation

Before anyone changes the configuration from its default, you can confirm that the unit is working.

These steps use a USB connection to demonstrate that the hardware can detect and interact with an OriginPass demo mobile NFC pass, which is ready to work with the default configuration of your VTAPI00-PAC-W.

1. If you don't already have one, obtain an OriginPass from Dot Origin by visiting <https://originpass.com/VTAP/> and add it to your NFC Wallet. (You will require a username and password – contact vtap-support@dotorigin.com to get these.)
2. Connect the VTAPI00-PAC-W to your PC, using a USB cable.
3. Open a text editor, such as Windows Notepad.
4. When you tap the OriginPass on the VTAPI00-PAC-W:
 - Pass contents will be displayed in the open text editor, through keyboard/barcode emulation.
 - The feedback LEDs on the VTAPI00-PAC-W PCBs will flash green.
 - Your smartphone may signal with a buzz or beep.

Note: Some Android phones will only interact if their screen is on, although it does not need to be unlocked. You may need to enable NFC in the settings for the smartphone.

Note: If the pass detected does not match the key and ID on the VTAP reader, or is moved away too quickly to be read, the pass contents displayed may be an 8 digit random hex string, such as '08E22AC1', different on each presentation. OriginPass contents will be a consistent string, such as '3~ffymeK9f_mziYtA6~53999301628695~Valued'. Any separator, such as '~' or '|', will depend on your keyboard language settings. (See VTAP Commands Reference Guide for option to ignore random UUIDs if needed.)

Note: If local security settings prevent or limit the use of removable storage devices, or the connection of additional keyboards, an administrator may need to alter those permissions.

2.2 Start reading your own passes

To read any mobile NFC pass, you will need to provide your pass reading parameters in the `config.txt` file. This means a collector ID or merchant ID and ECC keys. These allow you to read and decrypt pass data that is held by your users, on their smartphones. (There is a VTAP Application Note which explains more about ECC key pairs and how to generate your own keys.)

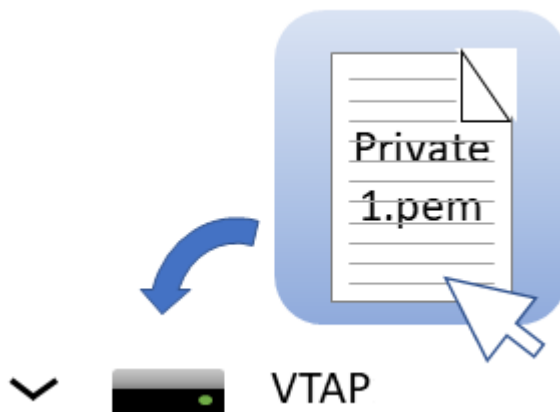
This first time, you will need to connect the VTAPI00-PAC-W to your PC, using a USB cable. (If needed, you can make changes remotely in future over a virtual COM port or serial port, see VTAP Serial Integration Guide.)

Step 1: Upload private key file(s) to your VTAPI00-PAC-W

1. Ensure these are ECC private key(s). Each is stored in a file with the name `private#.pem`, following the `.pem` format, where # is replaced with a number from 1 to 6, matching the key slot you will save it in. (The demo passes are accessed using the key in KeySlot 6, so don't overwrite this one unless you are finished with Dot Origin demo passes.)

Note: A VTAP reader cannot use more than 6 private key files.

2. Load your keys by copying these files onto your VTAPI00-PAC-W, which shows up in the file system of your PC as a mass storage device.



Note: When you reboot the VTAPI00-PAC-W your key will have been stored in hardware, and will no longer be listed as a file on the device. You can confirm key file(s) have been loaded when you **Check status in Boot.txt**. If the key file does not disappear and there is an error in `Boot.txt`, check your `.pem` file as it is likely it did not adhere to the standard – perhaps it was not an ECC key?

Step 2: Declare Merchant ID(s)/Collector ID(s) in the `config.txt` file

1. Open the file `config.txt` in a text editor (such as Windows Notepad). It already contains parameters for accessing the demo passes, prefixed `VAS1` and `ST1`, both relying on KeySlot 6. You can overwrite these, or keep them in addition to your own pass reading parameters.
2. Add your pass reading parameters in the `config.txt` file to access up to 6 Apple VAS and up to 6 Google Smart Tap IDs, and identify the keys to be used in each case.

Note: Although the VTAP100-PAC-W supports multiple IDs, Apple expect most users will only use one. Multiple collector IDs are not supported by Android, which means you cannot request more than one Collector ID from Google. Only one should be live at any one time. Multiple IDs is an advanced feature that should be used with care. The VAS# and ST# numbers define the order in which IDs will be requested from Apple or Android phones respectively. The lowest numbered ID will be requested first, then continuing in ascending numeric order. (There is a VTAP Application Note on Multiple Passes which explains more.)

Put each parameter on a new line. Order of parameters does not matter to the VTAP100-PAC-W, but could help other people who need to edit the file. Start any comment lines in the `config.txt` file, that the VTAP100-PAC-W should ignore, with a semicolon. Each parameter should only appear once – if it accidentally appears more than once then only the last instance will take effect.

Example: Settings in `config.txt` to interact with both Apple VAS and Google Smart Tap mobile passes

```
!VTAPconfig

VAS1MerchantID=<your merchant ID>
VAS1KeySlot=1
; This says use the key added as file 'private1.pem' to read and
; decrypt any pass connected to your merchant ID on an Apple iPhone

ST1CollectorID=<your collector ID>
ST1KeySlot=2
ST1KeyVersion=1
; This says use the key added as file 'private2.pem' at key version 1
; to read and decrypt any pass connected to your collector ID
; on an Android phone
```

3. Save the amended `config.txt` file and these changes will take effect immediately. (A small number of changes to the `config.txt` file require a reboot to take effect, for instance to the status of the virtual COM port, but these are highlighted in later sections).

Note: If a `VAS#KeySlot` parameter is omitted, or set to 0, then all available keys will be automatically tried to choose the right key. If the data received by the VTAPI00-PAC-W cannot be decrypted, the Apple iPhone will register a pass read, but the data will not be output.

Note: If an `ST#KeySlot` parameter is omitted, or set to 0, then authentication will be omitted and decryption will not be performed. In this case, Google Smart Tap data will be received and sent on by the VTAPI00-PAC-W, only if the pass does not require authentication by the terminal.

2.3 Check status in BOOT.TXT

Inspecting `BOOT.TXT` will give you essential information about your VTAPI00-PAC-W set up, at time of last reboot, which might be helpful when troubleshooting.

```
VTAPI00
Boot time: 2001/01/01 00:00:00
Firmware: V2.2.5.0
Storage: Dataflash
Status: 0
Hardware: 5.01
Expansion: VTAPI00C-V1-a2
VCP enabled
NCI: 0471125005-8C00
Serial number: 563230-798AEC17D053C05ADE6F6C36C79A6B12
VTAP label: CC123456
API level: 4
AppKeys used: 123-----
```

Figure 2-1 Example VTAPI00 v5 BOOT.TXT file

You are most likely to need:

- 'Serial number' ('ATCA' on VTAPI00 v4a or earlier) – the hardware serial number for your VTAPI00-PAC-W.
- 'VTAP label' (if set) – the assigned serial number for your VTAPI00-PAC-W, which matches that on its label. This will not show if not set.
- 'Firmware' – the VTAPI00-PAC-W core firmware version in use. You will find the latest firmware versions at <https://www.vtapnfc.com/download/>
- 'Hardware' – the VTAPI00-PAC-W hardware version in use.
- 'API level' – indicates which serial or OSDP API commands are supported.
- 'KeySlots used:' – Indicates the ECC private keys loaded on the VTAP reader, to access VAS or Smart Tap passes. Helps you check whether you have uploaded the necessary ECC private keys, which can be unclear as the files are deleted when they are uploaded. These two examples show how to read this information:
 - 'KeySlots used:-----' shows that no keys have been uploaded.
 - 'KeySlots used: 12--56' shows that key files 1 and 2 have been successfully uploaded, in addition to the defaults 5 and 6.
- 'AppKeys used:' Indicates the application keys (if any) uploaded to the VTAP reader for any other applications, such as keys loaded to use with DESFire applications.
- 'VCP enabled', if included – indicates that the virtual COM port has been enabled.
- 'Status' – should be 0 if operating normally, anything else indicates an error state.

- 'Expansion:' shows the name of the expansion board connected to the VTAP, for example: 'VTAP100W' for a Wiegand expansion board, 'VTAP100C' for a VTAP PRO BW expansion board, 'VTAP100E' for a VTAP PRO POE expansion board.
- 'Boot time' – The time at boot, which defaults to 1970/00/00 00:00:00 if power is removed to reboot.
- 'SE:' – Where there is a secure element (if any) for key storage, such as in VTAP25 readers, this will take the form:
`SE: v7.2.0,Active,----56,1-----`
 This includes:
 - the SE050 app version,
 - Active/Inactive to show whether the secure element is being used,
 - slot numbers for EC keys which are stored in the secure element,
 - then slot numbers for application keys which are stored in the secure element.

If the configuration has been locked the `BOOT.TXT` file will end with the words LOCKED S/W or LOCKED H/W.

2.4 Send pass payload over a Wiegand interface

The Wiegand interface allows a mobile NFC pass payload to be passed straight to an access controller from your VTAP reader, like data from any other card reader.

To enable the Wiegand interface you will need to make changes to the `config.txt` file.

Example: Changes to `config.txt` to enable the Wiegand interface

```
!VTAPconfig

WiegandMode=1      ; Enable Wiegand interface
PassWiegandBits=56 ; See note below, this must match bit length expected
                   ;   by controller and data must contain this number
                   ;   of bits, =56 is default if omitted
```

Here `WiegandMode=1` enables data transmission over the Wiegand interface.

`WiegandSource` controls which types of data (pass reads, card/tag reads, serial commands) will be sent to the Wiegand interface. The default value is `A1`, which allows sending of all NFC pass and card/tag data. Refer to the VTAP Commands Reference Guide for other options, if data sources need to be restricted for your application.

Additional settings are needed if you want to **Send only part of pass payload**, which are discussed in the following section. And there are a number of settings which will allow you to adjust the **Format of pass data** before it is sent over the Wiegand interface, discussed later in this section.

Note: `PassWiegandBits` should be set to match the bit length expected by the controller and the pass payload must contain sufficient data to provide this number of bits.

`PassWiegandBits` defaults to 56, so the expected form of the pass payload is 14 hex digits, unless `PassWiegandBits` is set to another value in your configuration.

2.4.1 Send only part of pass payload over Wiegand

`WiegandPassMode` allows you to extract only a part of each mobile NFC pass payload to send over the Wiegand interface. Setting `WiegandPassMode=1` enables all of the other `WiegandPass...` settings, to extract a short character sequence from the pass payload. This can then be interpreted as a decimal or hexadecimal number and sent over the Wiegand interface as a bit sequence. These settings let you fetch the specific section of the pass payload needed by your access control system, as in this example:

**Example: Changes to `config.txt`
to extract part of the full pass payload
for Wiegand interface [VTAP100-PAC-W only]**

```
!VTAPconfig

WiegandMode=1           ; Enable Wiegand interface
WiegandPassMode=1       ; Choose to extract only
                        ; a part of the pass payload
WiegandPassSeparator=|   ; Set the separator character the VTAP should
                        ; use to separate the payload into sections
WiegandPassSection=2     ; Section number to read based on that
                        ; WiegandPassSeparator
PassWiegandBits=32
```

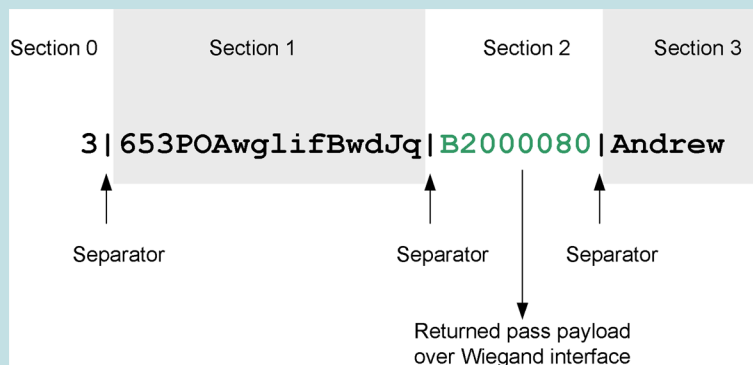


Figure 2-2 Separator |, Section 2 for Wiegand data (on VTAP100-PAC-W only)

Full pass payload:

3|653POAwglifBwdJq|B2000080|Andrew

Pass payload sent over the Wiegand interface:

B2000080

Refer to the VTAP Commands Reference Guide for all the possible `WiegandPass...` settings and options to extract even smaller parts of the pass payload.

2.4.2 Format of pass data sent over Wiegand

Wiegand data is usually a short bit pattern, rather than a sequence of characters. So there are several optional settings, to use in `config.txt`, which allow you to change the output

format for any data read, in terms of bit length, parity bits and identification of pass type, for data transferred over a Wiegand connection:

- `PassWiegandBits=56` lets you specify the number of bits (1 to 255) to output over the Wiegand interface, from the start of the filtered pass payload. If omitted it defaults to 56. (`TagWiegandBits` does the same for card/tag data.)
- `PassFormat=d` is a setting to interpret ASCII pass payload characters as either hex (h) or decimal (d), when converting the pass payload to a Wiegand bit sequence.
(For cards and tags containing a sequence of ASCII characters, you may want `TagWiegandASCIIFormat` set to hex (h), decimal (d) or the default ASCII (a), along with `TagReadFormat=a`.)
- `PassWiegandParity=1` adds a single 'parity bit' equivalent to pass payload. This makes it possible to use mobile pass data formats that include parity bits. Parity bit equivalents can be used if the parity bit(s) are not being tested for validity. `PassWiegandParity=2` adds calculated odd and even parity bits to the data. Either can be used if `PassFormat=d` or `PassFormat=h`. Again, the default `=0` turns this feature off.
(Use `TagWiegandParity` to do the same operation for card and tag data, used with `TagReadFormat=a` and `TagWiegandASCIIFormat=d` or `=h` to interpret the tag byte data as an ASCII string representing a decimal or hex number, and to convert this to the corresponding Wiegand bit sequence by adding extra parity bits, which might be expected by the controller.)
- `WiegandPassTypeID=1` inserts an additional leading byte of pass type identifier (01 for Apple VAS, or 02 for Google ST) in the Wiegand output. This makes it possible to distinguish between cards/tags and mobile wallet passes. This setting overrides `PassWiegandBits` and results in a Wiegand bit length of 64 bits. The default `=0` turns this feature off.

For more information about the Wiegand interface refer to the VTAP Application Notes on Access Control.

3 Mechanical installation

The VTAPI00 reader board assembly for integration comprises two PCBs with an integral antenna in the lower board. Power is connected to the main board, through a cutaway in the expansion board on top.

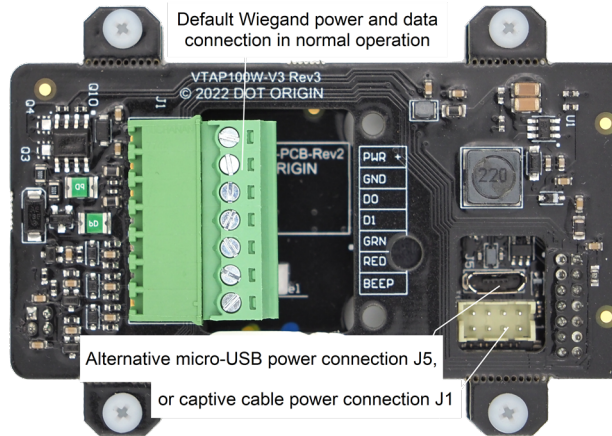


Figure 3-1 VTAPI00-PAC-W-OEM connection options for power



WARNING: Observe all Safety instructions when installing the VTAPI00 PCBs.

3.1 Power

For configuration – Connect the PCB assembly to a PC using **either** a MicroUSB to USB cable **or** a captive cable, as supplied with boxed models.

During normal operation the VTAPI00-PAC-W model will be powered by connecting it to an access controller, using the Wiegand connector. If the VTAPI00 is being powered through its Wiegand connection, you can still make an additional USB data connection to a PC, provided that the PC is already powered. (This avoids the risk that the USB data connection is driven to too high a voltage.)

The VTAPI00-PAC-W-OEM is rated at 5V DC (typ. 110mA, max 150mA) for power over USB. When powered over Wiegand it is rated at 8V-16V DC @ 30 to 100mA.



WARNING: Do not power the VTAPI00-PAC-W-OEM reader assembly if the NFC antenna is damaged. Components can reach higher operating temperatures than normal when an antenna is not attached, which could damage the VTAP reader and cause injury if handled.

3.2 Environment

The VTAPI00-PAC-W-OEM assembly must be stored and operated under the following conditions:

- Ambient temperature -25 to +70°C (-13 to 158°F)
- Humidity 0 to 95% RH non-condensing
- Pressure 86-106kPa

CAUTION: Always ensure sufficient clearance between the VTAP antenna and other RF transmitters, to avoid electromagnetic interference between equipment. Clearance required varies between antennas, depending on antenna size, power and sensitivity.

3.3 Mounting points

The PCB has 2.7mm diameter mounting holes, suitable for an M2.5 screw, spaced 50mm apart for fixing the unit. These will come with screws in place to hold the two boards of the assembly firmly together, but can be replaced with longer screws to connect the assembly into your housing.

CAUTION: Replace only one screw at a time, to keep the boards in contact at all times, if you need to replace the screws which hold the boards of an assembly together. Separating the boards of an assembly will invalidate your warranty.

Use 4 M2.5 nuts and bolts to mount the board securely.

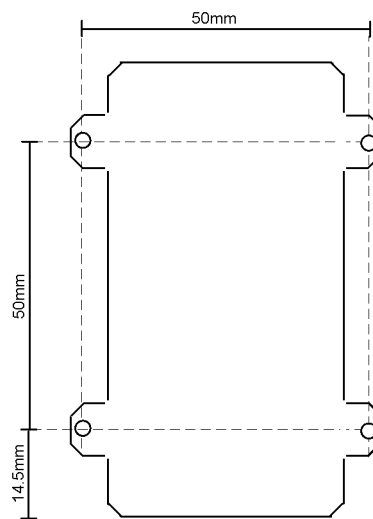


Figure 3-2 VTAP100 assembly mounting holes

The NFC antenna, which is in the lower PCB of the assembly, should not be mounted more than 10mm deep within your enclosure (measuring from the antenna surface to the enclosure surface), so that a user's smartphone will be able to come close enough to the antenna for reliable reading.

The antenna position should be clearly marked and easily accessed, so that users can position their smartphone appropriately. Be aware that antennas are positioned differently in different makes of smartphone. Apple iPhones often have antennas near the top and Android phones are more likely to have an antenna in the middle.

There is an engineering drawing you may find useful at Annex A.

CAUTION: Mounting a VTAP board near metal can reduce performance of the VTAP100-PAC-W, because metal can distort the NFC field. Never allow a metal surface between the VTAP100-PAC-W and the user's phone or card. If you have to mount the VTAP100-PAC-W near metal, you should ensure the separation is:

- at least 6mm and insert a ferrite sheet (suitable for 13.56MHz) between the VTAP100-PAC-W and any metal surface behind the reader, or
- at least 25mm separation between the VTAP PCB and any metal (in all directions).

Always choose a plastic mounting bracket, where needed. And if a VTAP reader is mounted behind an acrylic window in an otherwise metal enclosure, always ensure the window is large enough not to distort the emerging field, which is larger than the reader itself.

Testing should be performed in the proposed mounting location, as other devices and structures in close proximity could affect pass reading performance.

3.4 Optional RS-232 connection

The PCB has a special connector J1 (an 8 pin, 2mm pitch header connector) which can be used to attach a captive cable with a matching crimp housing.

The standard connector fitted to the PCB is a Hirose DF11-8DP-2DSA male header plug with shroud. The matching crimp housing is the Hirose DF11-8DS-2C.

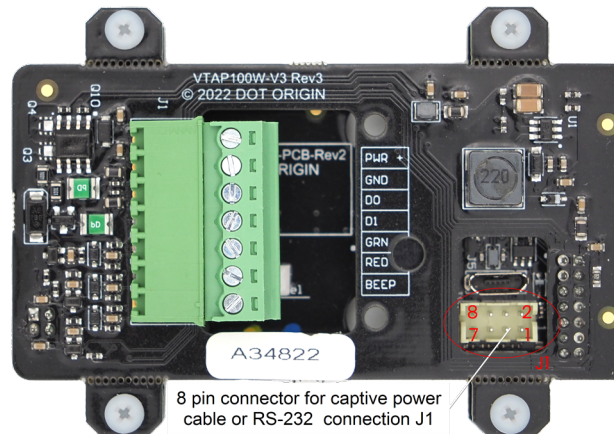


Figure 3-3 VTAP100-PAC-W-OEM captive power cable or RS-232 J1 connection

The connector J1 includes both USB and RS-232 signals, as follows:

Pin	Function
1	GND
2	USB D+
3	+5V supply
4	USB D-
5	RS232 RXD (input)
6	Reserved (sense input)
7	RS232 TXD (output)
8	Reserved (sense GND)

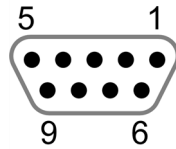


Figure 3-4 Typical RS-232 cable

A typical RS-232 cable has the following DB9 female connector pinout:

Pin	Function
2	TXD
3	RXD
5	GND
9	+5V supply (if any)

A PC or terminal RS-232 connector is usually DTE (data terminating equipment), typically a male DB9 with transmit (TXD) on pin 3 and receive (RXD) on pin 2. The appropriate connecting cable is then a DCE (data communications equipment) female DB9. TXD and RXD pins are swapped between the DCE and DTE devices, so that the transmit pin on one connects to the receive pin on the other.

The VTAPI00 requires a 5V power supply, but not all RS-232 devices have 5V on pin 9. Your options are:

- If your RS-232 connector provides 5V power on pin 9, disconnect the USB cable before making the serial connection, then power will be provided by J1 (pins 1 and 3) and the serial cable/host.
- If your RS-232 connector does not provide 5V power on pin 9, retain a USB connection in addition to the serial connection.

Some serial cables have a separate DC 5.5/2.1mm barrel connector to supply power. In these cables, typically, the centre pin is +5V and the outer barrel is GND.

3.5 Wiegand wiring (for model VTAPI00-PAC-W only)

Use the Wiegand connector supplied to make a Wiegand wiring connection to a configured VTAPI00 Wiegand reader from your access controller, like any other reader.

Use 24-26AWG shielded multi-core, overall screened, cable for the connection between VTAPI00 Wiegand reader and controller (for example Belden CR9538).

Note: Screened cable should always be used to connect VTAPI00 readers to door controllers, to avoid interference from other equipment. The cable screen must be connected electrically to GND at both the VTAPI00 reader and controller ends of the cable, using the bare wire 'drain' conductor.



CAUTION: If the VTAPI00 is being powered through its Wiegand connection, you can still make an additional USB data connection to a PC, provided that the PC is already powered before the connection is made. (This avoids the risk of damage to the USB interface on the PC, if the PC is not powered.)

Follow an appropriate figure and table to make the right connections in your access controller:

HID EH400

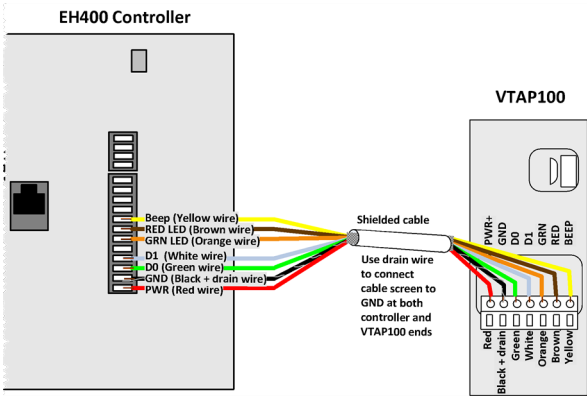


Figure 3-5 Connection between VTAP100-PAC-W v4a or v5 and HID EH400 access controller

HID EH400 Controller Signal Name	Wire colour (typical)	VTAP100 Signal Name (v4a or v5 hardware)
Beep	Yellow	BEEP
RED LED	Brown	RED
GRN LED	Orange	GRN
D1	White	D1
D0	Green	D0
GND	Black	GND
PWR	Red	PWR+

HID V2000

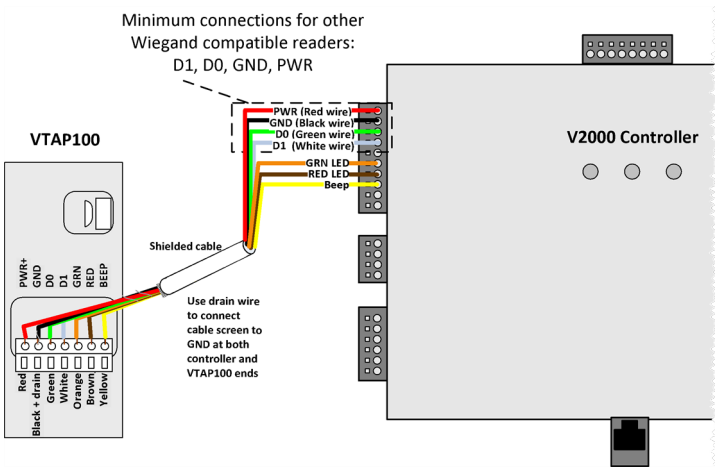


Figure 3-6 Connection between VTAP100-PAC-W v4a or v5 and HID V2000 access controller

HID V2000 Controller Signal Name	Wire colour (typical)	VTAP100 Signal Name (v4a or v5 hardware)
Beep	Yellow	BEEP
RED LED	Brown	RED
GRN LED	Orange	GRN
D1	White	D1
D0	Green	D0
GND	Black	GND
PWR	Red	PWR+

Axis A1001

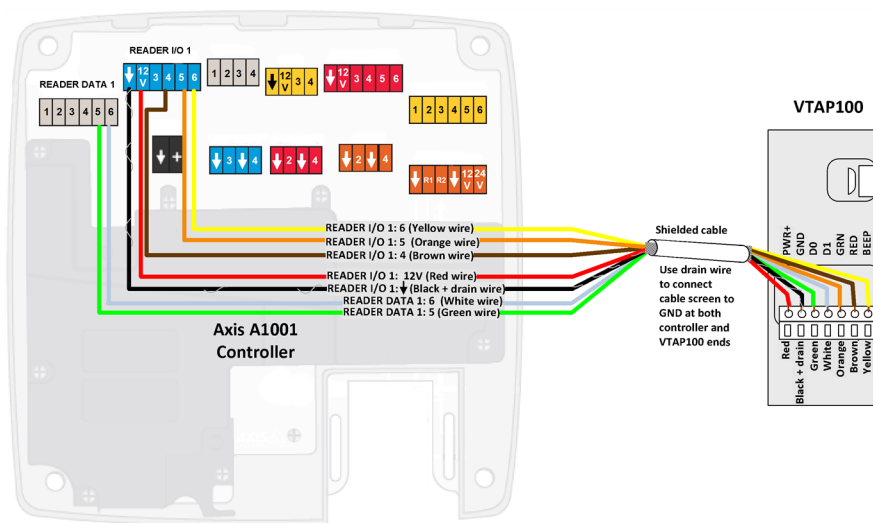


Figure 3-7 Connection between VTAP100-PAC-W v4a or v5 and Axis A1001 access controller

Axis A1001 Controller Signal Name	Wire colour (typical)	VTAP100 Signal Name (v4a or v5 hardware)
READER I/O 1: 6	Yellow	BEEP
READER I/O 1: 4	Brown	RED
READER I/O 1: 5	Orange	GRN
READER DATA 1: 6	White	D1
READER DATA 1: 5	Green	D0
READER I/O 1: ↓	Black	GND
READER I/O 1: 12V	Red	PWR+

Axis A1601

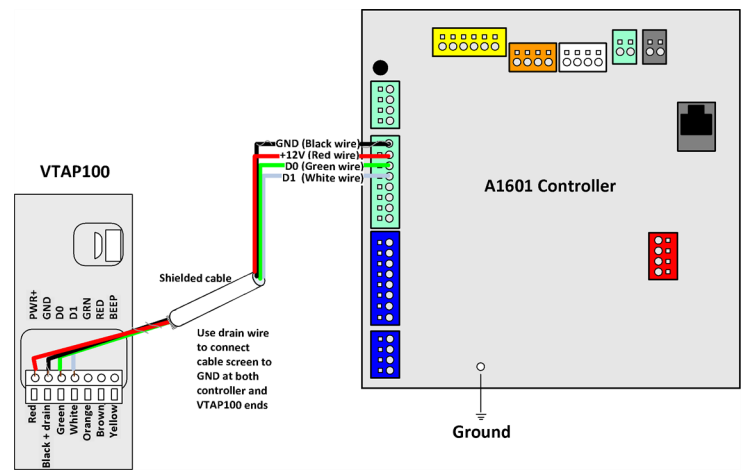


Figure 3-8 Connection between VTAP100-PAC-W v4a or v5 and Axis A1601 access controller

Axis A1601 Controller Signal Name	Wire colour (typical)	VTAP100 Signal Name (v4a or v5 hardware)
D1	White	D1
D0	Green	D0
GND	Black	GND
+12V	Red	PWR+

Nortech CRC400

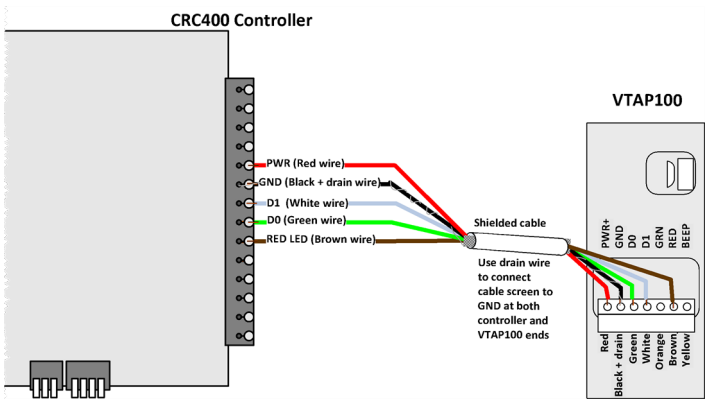


Figure 3-9 Connection between VTAP100-PAC-W v4a or v5 and Nortech CRC400 access controller

Nortech CRC400 Controller Signal Name	Wire colour (typical)	VTAP100 Signal Name (v4a or v5 hardware)
LED	Brown	RED
Data/D1	White	D1
Data/D0	Green	D0
0 Volts	Black	GND
+VE	Red	PWR+

Nortech Dataquest

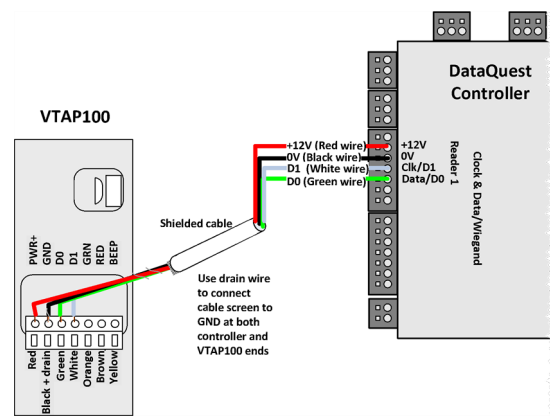


Figure 3–10 Connection between VTAP100–PAC–W v4a or v5 and Nortech Dataquest access controller

Nortech Dataquest Controller Signal Name	Wire colour (typical)	VTAP100 Signal Name (v4a or v5 hardware)
Clk/D1	White	D1
Data/D0	Green	D0
0V	Black	GND
+12V	Red	PWR+

Paxton Net2

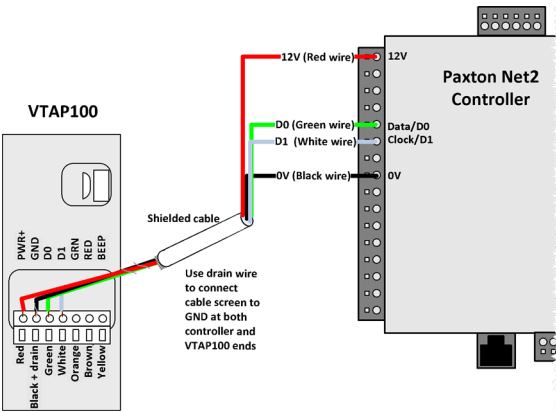


Figure 3-11 Connection between VTAP100-PAC-W v4a or v5 and Paxton Net2 access controller

Paxton Net2 Controller Signal Name	Wire colour (typical)	VTAP100 Signal Name (v4a or v5 hardware)
Clock/D1	White	D1
Data/D0	Green	D0
0V	Black	GND
12V	Red	PWR+

HID Mercury MR52-S3B

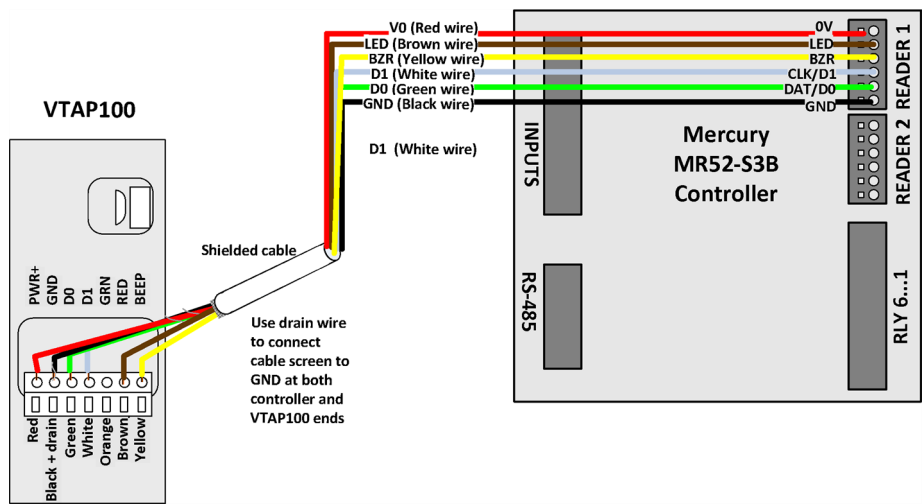


Figure 3-12 Connection between VTAP100-PAC-W v4a or v5 and HID Mercury access controller (MR52-S3B)

Connections are shown for Reader 1 on the controller, but Reader 2 connections are equivalent.

HID Mercury Controller Signal Name	Wire colour (typical)	VTAP100 Signal Name (v4a or v5 hardware)
D0/DAT/TR-	Green	D0
D1/CLK/TR+	White	D1
GND	Black	GND
V0	Red	PWR+
BZR	Yellow	BEEP
LED	Orange	RED (or GRN)

4 Module integration instructions – FCC/ISED

The VTAPI00–OEM reader board is the part of any OEM assembly which carries the NFC antenna. This has received FCC/ISED modular approval. In order to maintain this approval for your integration, you must follow the instructions in this section. If your equipment contains another RF transmitter, that works in conjunction with the VTAP reader, you may want to request an FCC Permissive Change approval based on the existing VTAPI00–OEM modular approval. Contact us early in the process if you need help with FCC/ISED testing and permissive change.

The VTAPI00–OEM reader board has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- (1) This device may not cause harmful interference.
- (2) This device must accept any interference received, including interference that may cause undesired operation

These instructions must be followed to maintain the FCC/ISED approval for the VTAPI00–OEM reader board, when it is integrated into a host system.

CAUTION: Changes or modifications made to the VTAPI00–OEM reader board, that have not been expressly approved by Dot Origin Ltd could void the user's authority to operate the equipment.

4.1 Applicable FCC/ISED rules

The VTAPI00–OEM reader board operates at 13.56MHz and is therefore subject to FCC/ISED rules for radio frequency devices.

4.2 Specific operational use conditions

The VTAPI00–OEM reader board must be stored and operated under the following conditions:

- Ambient temperature –25 to +70°C (–13 to 158°F)
- Humidity 0 to 95% RH non-condensing
- Pressure 86–106kPa

4.3 RF exposure considerations

This reader board complies with FCC/ISED RF radiation exposure limits set for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 cm between the radiator and a human body.

Screened cable should be used, wherever possible, to connect VTAPI00–OEM reader boards to other devices, to avoid interference from other equipment.

The end-user manual for the host equipment, that contains a VTAPI00-OEM reader board, must clearly indicate the operating conditions to be observed, so that the user remains in compliance with current FCC/ISED RF exposure guidelines.

4.4 Antennas

The VTAPI00-OEM reader board has been tested with its integrated loop antenna, printed on the PCB. There are no alternative antennas approved for use. If an external antenna is attached, the new arrangement would require a new FCC/ISED approval.

4.5 Label and compliance information

The integrator must attach a label to the new equipment, hosting the VTAPI00-OEM reader board.

For FCC approval: 'Contains FCC ID: 2A282-VTAPI00G2'

For ISED approval: 'Contains IC: 30458-VTAPI00G2'

4.6 Information on test modes

The following test modes are recommended to achieve states of maximum emission levels or susceptibility in the VTAPI00-OEM reader board:

1. VTAPI00-OEM reader board powered on. Communicating with PC over USB. Continuously reading tag.
2. VTAPI00-OEM reader board powered on and tag present, but not communicating with external device.

4.7 Additional testing requirements

The VTAPI00-OEM reader board is only FCC/ISED authorised for use in compliance with the specific FCC/ISED transmitter rules listed on the grant. The integrator is responsible for compliance to any other FCC/ISED rules that apply to the host, which are not covered by the modular transmitter grant of certification.

The final host product, with the VTAPI00-OEM reader board installed, will still require Part 15 Subpart B compliance testing, to evaluate transmission effects when the VTAPI00-OEM reader board and host equipment operate at the same time. Be aware that additional testing can be required on the final integrated system. We recommend integrators refer to further advice from the FCC OET Knowledge Base, such as **996369 D04** **Module Integration Guide v02**.

4.8 Maintaining Apple VAS(ECPI) or ECP2/Access compliance

There are some steps required in order to maintain Apple VAS(ECPI) and/or ECP2/Access compliance.

When you request an NFC entitlement and/or permission for an Apple Access deployment we recommend that you inform Apple that a Dot Origin VTAP OEM board or module has been used in your finished product. Apple are aware that our products are available both in finished form and as OEM modules.

- For VAS applications Apple reserves the right to review the final form factor of the reader, to ensure that satisfactory performance and user experience is maintained.
- For ECP2 applications it is essential that the new equipment hosting a VTAP reader board or module is tested and certified against Apple Access specifications. This includes ensuring that the read range meets their minimum distance requirements (40mm at various presentation angles, in Express and CDCVM modes) and that the reader is tested against all the different categories of iPhone and Apple Watch, as required by Apple. Apple may also require on-site functional testing as part of the end-to-end certification of an Apple Access deployment, which is usually conducted by the Credential Manager.

Some of these certification tests do require the user feedback from the VTAP reader for a successful read, either visually or by sound. The buzzer on a VTAP reader produces a long beep, sufficient to pass this test.

In both cases, our engineering team can advise and assist on certification issues, which could include taking a product through formal certification, if required.

5 Find your hardware version

If you need to report a problem with your VTAPI00-PAC-W or find the right reference diagram you will need to know your hardware version.

If you can connect your VTAPI00-PAC-W to a PC via USB, you can easily check the BOOT.TXT file.

If you navigate to the VTAPI00-PAC-W in the computer's file system. It will appear as an attached mass storage device and list the files contained, including the `BOOT.TXT` file.

Inspecting `BOOT.TXT` you will find a number next to the word `Hardware:` such as `v5`. This is the Hardware version in use.

Alternatively, over a serial connection to the VTAPI00-PAC-W, sending the `?b` command will return the `BOOT.TXT` information.

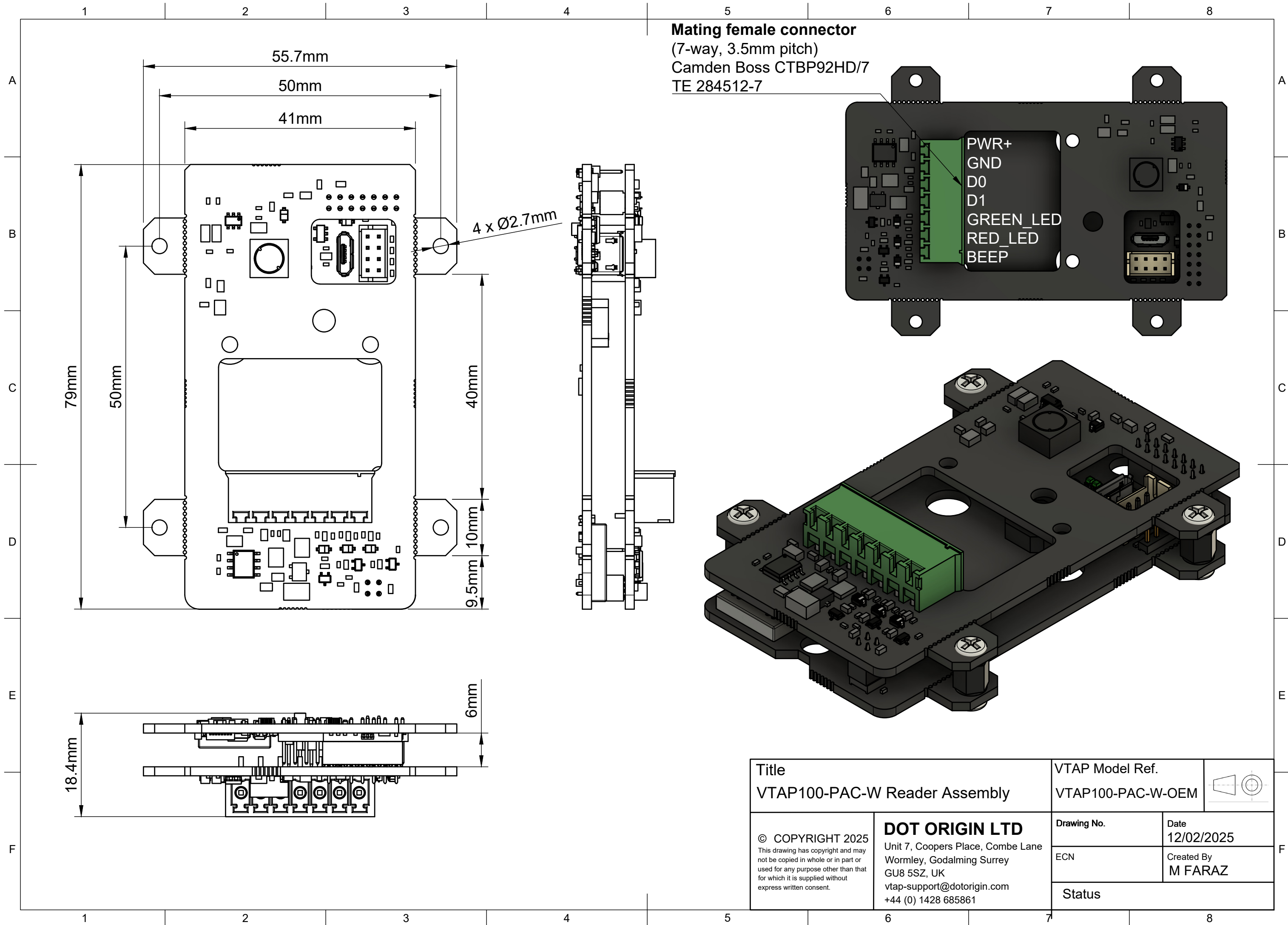
6 Disposal

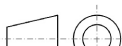
For safety and sustainability, it is the responsibility of the integrator to ensure that when equipment containing a VTAP100-PAC-W reaches the end of its life, it is recycled in accordance with WEEE Regulations within the EU.



VTAP100-PAC-W (PCB assembly) should not be disposed of in general waste. If you wish to discard electrical and electronic equipment (EEE), please contact your supplier for further information.





Title VTAP100-PAC-W Reader Assembly		VTAP Model Ref. VTAP100-PAC-W-OEM		
© COPYRIGHT 2025 This drawing has copyright and may not be copied in whole or in part or used for any purpose other than that for which it is supplied without express written consent.	DOT ORIGIN LTD Unit 7, Coopers Place, Combe Lane Wormley, Godalming Surrey GU8 5SZ, UK vtap-support@dotorigin.com +44 (0) 1428 685861	Drawing No.	Date 12/02/2025	
		ECN	Created By M FARAZ	
		Status		