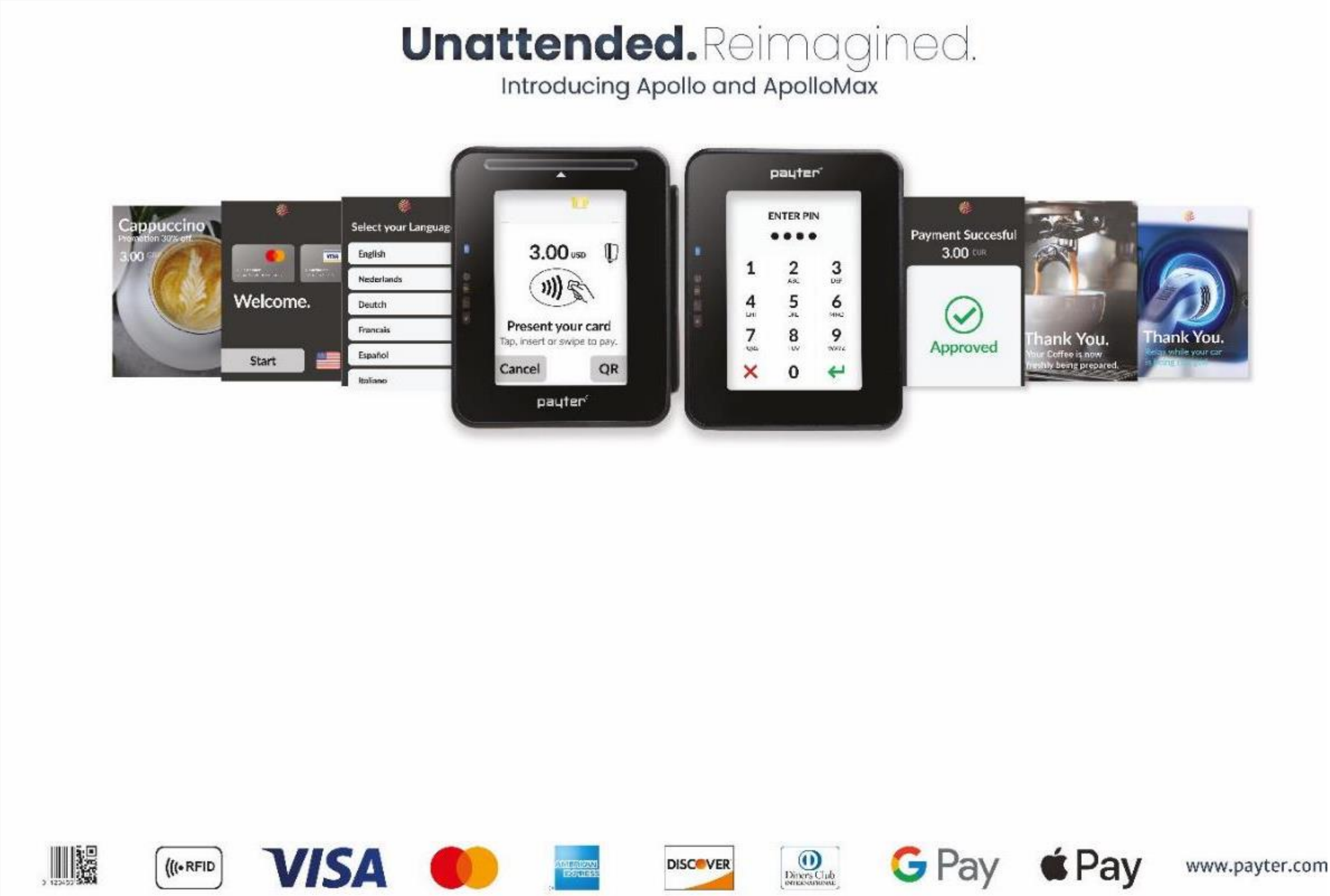
payter



Payter B.V.
Rozenlaan 115
3051 LP Rotterdam
The Netherlands

Apollo terminal series
User manual v1.3.3 (2023-10-03)

Copyright © 2023 PAYTER B.V.

Payter reserves the right to modify specifications stated in this manual.

Liability

Payter B.V. accepts no liability for claims arising from improper use other than that stated in this manual of from not obeying (safety) instructions and precautions in this manual. Although considerable care has been taken to ensure a correct and suitably comprehensive description of the product, this manual may nonetheless contain errors and inaccuracies.

Warranty

Payter B.V. warrants to the original purchaser that this product is free from defects in material or workmanship for the period of one year from the date of purchase. This warranty does not apply to damage incurred due to misuse, incorrect handling, unapproved repairs or unapproved alterations.

How to contact us

If you have any comments or queries concerning any aspect related to the product, do not hesitate to contact us:

Payter B.V.
Rozenlaan 115
3051 LP Rotterdam
t +31 (0)8 54 01 23 80

info@payter.nl

About this manual

This manual is intended for professionals responsible for the integration, installation, configuration or problem solving of the Apollo and/or ApolloMax terminal.

What you need to know

You will have a better understanding of how the terminal works if you are familiar with:

- Ethernet network technologies
- The MDB protocol

Reference documents

Professionals responsible for configuration or installation may also refer to:

- Response code and error list
- Payter session protocol document
- Payter Cloud Payments Service document

Professionals responsible for integration of the Apollo terminal into the host machine, may also refer to:

- Mechanical integration manual

You can find request these additional documents at through your account representative or via support@payter.nl

! To ensure proper operation, read this manual thoroughly before using the product and retain the information for future reference.

Terms and abbreviations

Abbreviation	Description
3G/4G	Third / Fourth Generation (i.e. a mobile communication system)
APN	Access Point Name
CCI	Coffee Credit Interface
DC	Direct Current
DHCP	Dynamic Host Control Protocol
DNS	Domain Name Server
EMV	Europay Mastercard Visa
EVA	European Vending Association
GPRS	General Packet Radio Service (i.e. a mobile communication system)
GSM	Global System for Mobile communication
HSPA	High Speed Packet Access (i.e. a mobile communication system)
IP	Internet Protocol
LAN	Local Area Network
MDB	Multidrop Bus (i.e. a communications bus standard for vending machines).
ms	Milliseconds
NAMA	National Automatic Merchandising Association
NFC	Near Field Communication
PSP	Payment Service Provider
QR	Quick Response
PVP	Payter Vending Protocol
RTP	Remote Terminal Protocol
SDK	Software Development Kit
SIM	Subscriber Identification Module
USB	Universal Serial Bus
VMC	Vending Machine Controller
PCI	Payment Card Industry Security Standards Council
SRED	Secure reading and exchange of data
DUKPT	Derived Unique Key per Transaction
AES	Advanced Encryption Standard
TDES	Triple - Data Encryption Standard
RSA	Rivest, Shamir, & Adleman Algorithm
SHA	Secure Hash Algorithm
HMAC	Hash-Based Message Authentication Code
CMAC	Cipher-Based Message Authentication Code

Table of Contents

1. Introduction

Thank you for choosing an Apollo series payment terminal for your host application. The Apollo terminals are designed for use in unattended points of sale, such as food and beverage vending machines, EV-Chargers, parking ticket machines and more.

The terminals support many payment schemes and can be used as a drop-in replacement for an existing host application, using industry standard interfaces such as multidrop bus (MDB) or potential free pulse contact. Also available are proprietary interface options (PSP and cloud API) that use Ethernet, USB or RS232 to connect the Apollo terminal to a host system.

An internet connection to the terminal, required for transaction processing, can be realized by connecting to a LAN network. If no LAN is available, an optional 4G modem can provide a high-quality internet connection, ensuring your transaction processing performance will not degrade because of a low internet speed.

The Apollo terminal series supports reliable remote management functionality for firmware updates and configuration changes.

! Please leave your terminal on and connected to the internet on a regular basis, in order to make sure that it can be managed properly at any time.

⚠ Failure to charge the batteries at notification by the MyPayter Terminal management System can result in tampering the terminal. A tampered terminal need to be returned to Payter for analysis, possible replacement of the batteries and key injection.

2. Safety

2.1 Safety symbols

In this manual, safety instructions and precautions are marked with a symbol. Always read and follow the safety instructions before reading on. This manual uses the following symbols:

⚠ **Warning!**

Risk of (serious) injury to the user or serious damage to the product if the user does not carefully follow the instructions.

△ **Caution!**

Risk of damage to the product if the user does not carefully follow the instructions.

❗ **Attention!**

A remark meant to point the user to a potential problem.

2.2 AC Adapter

⚠

- Use only power adapters that come with the terminal.
- Do not use the AC adapter if the cord is damaged.
- Do not disassemble the AC adapter. Only qualified technicians may service the adapter.
- The AC adapter is intended for indoor use only. Do not expose to rain or snow.
- Do not use the AC adapter in high-moisture environments.
- Never touch the AC adapter when your hands or feet are wet.
- Do not immerse the AC adapter or the terminal in fluid; these devices are not waterproof.

2.3 Terminal

⚠

- Do not place the terminal near electrical appliances or other devices that cause excessive voltage fluctuations or that emit electrical noise.
- Do not use where there is high heat, direct sunlight, humidity moisture, caustic chemicals or caustic oils.

2.4 Security

All Payter Point of Sale terminals are certified by the card schemes according to the latest standards and accredited through various acquirers to securely process transactions. The integrity of the payment terminals is crucial, because they process sensitive card data.
To ensure safe use, prevent fraud and compliance to related Scheme Rules, please follow all instructions as described in the chapters 9 Merchant Responsibilities Security, 10.5 Installation and User Guidance and 11 Operation and Maintenance.

3. The Apollo Terminal

The Apollo and ApolloMax are PIN Entry Devices (PED) for payment processing in unattended environments. The terminals have the ability to provide contact, contactless and magstripe transactions.

The terminals supports the following main features

- TFT LCD with capacitive touch
- Chip Card Reader
- Contactless Reader
- Magnetic Stripe Reader
- Ethernet
- USB
- Wifi, Blue Tooth
- MDB
- Optional 4G Modem

3.1 Package contents

The package contains the following items:

1. Cover plate
2. Terminal
3. Terminal Rubber gasket
4. Rear rubber gasket
5. Mounting frame
6. M4Screws, and bolts set

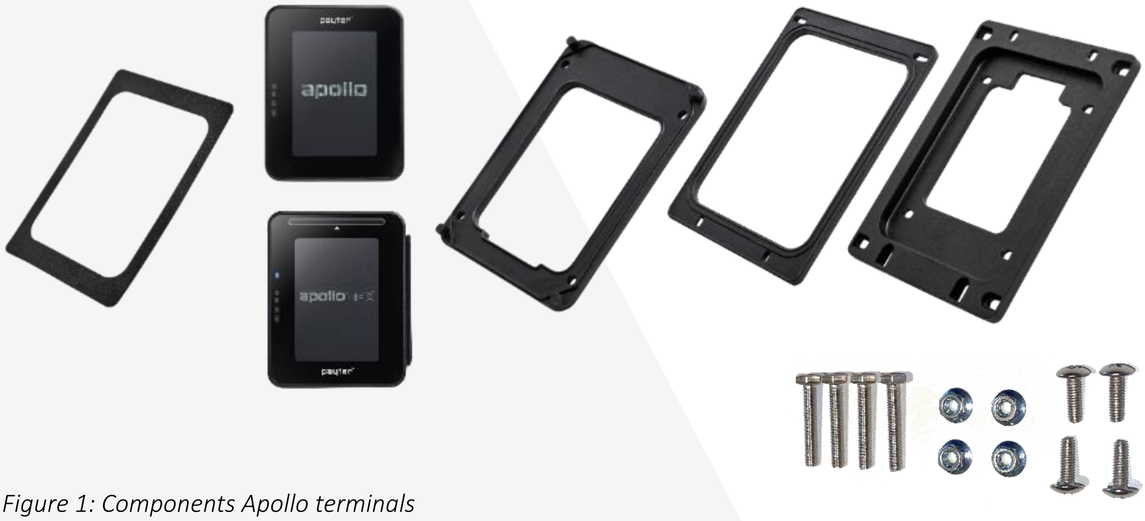
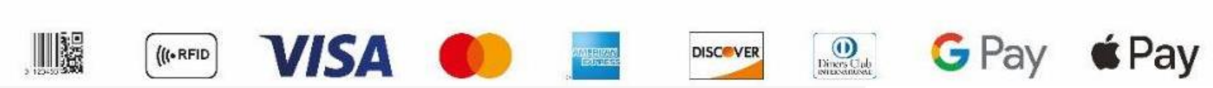


Figure 1: Components Apollo terminals

3.2 Supported cards schemes

The Apollo terminal support the following cards and card schemes.



3.3 Apollo terminal

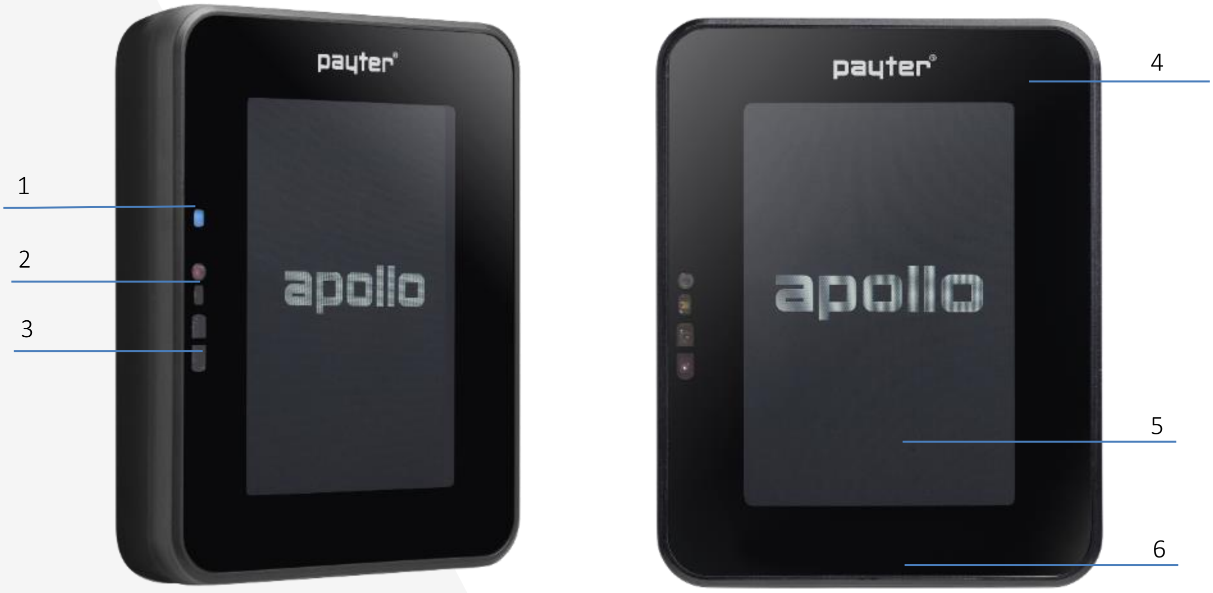


Figure 2: Front of the Apollo terminal

No.	Item	Description
1	LEDs (4)	Multi colour status LEDs
2	Camera and Locator light	Enabling QR-Code reading
3	Proximity sensor	
4	WiFi & Bluetooth Module	
5	3,5 Inch touch screen	
6	Speaker	

3.4 ApolloMax terminal

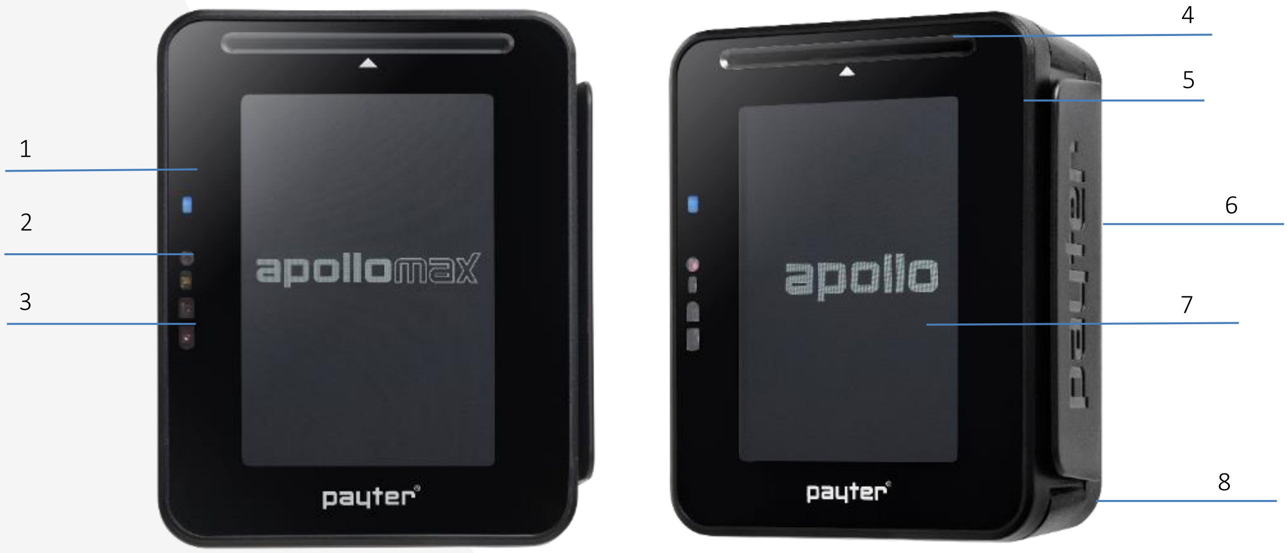


Figure 3: Front of the ApolloMax terminal

No.	Item	Description
1	LEDs (4)	Multi colour status LEDs
2	Camera and Locator light	Enabling QR-Code reading
3	Proximity sensor	
4	Chip Card Reader	
5	WiFi & Bluetooth Module	
6	Magnetic Stripe reader	
7	3,5 Inch touch screen	
8	Speaker	

3.5 Connections

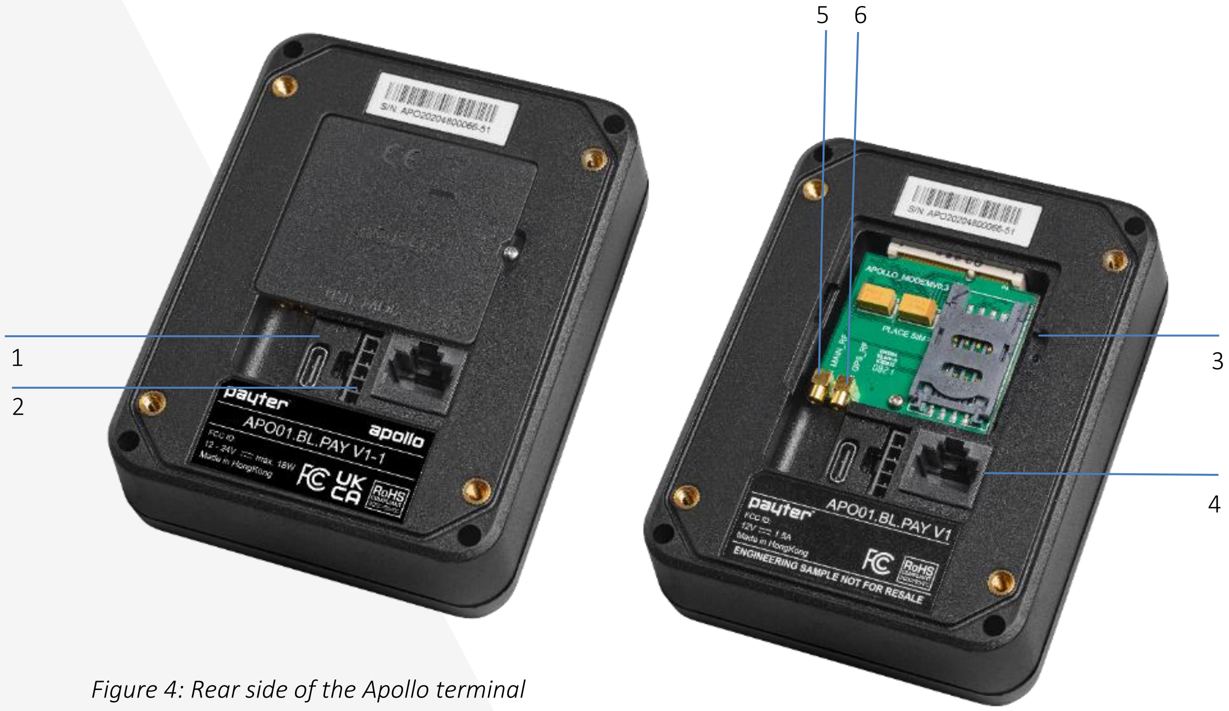


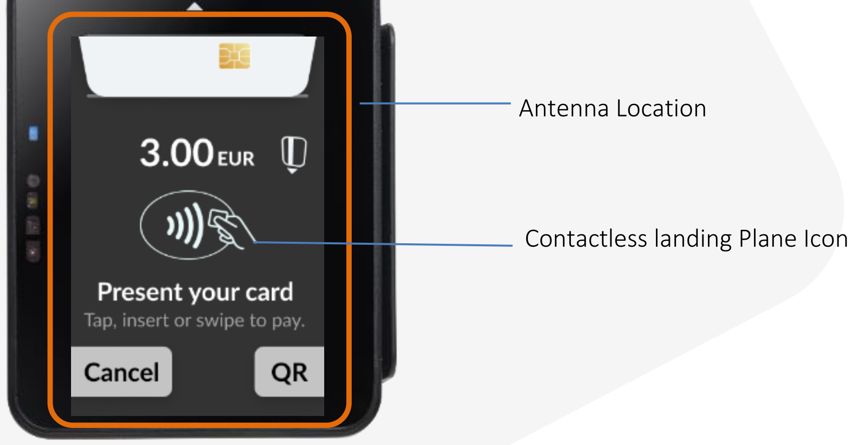
Figure 4: Rear side of the Apollo terminal

No.	Item	Description
1	USB-C port	Host and Slave Connector
2	Micro Fit MDB connector	Port to connect with the internet through the LAN.
3	4G/ GPS modem	Modem with GPS functionality (optional)
4	RJ 45 LAN Connector	Port for USB-C cable to interface with the terminal from the host machine.
5	Antenna connectors	MMCX Connector for 4G Antenna
6	GSSN Connector	Connector for GSSN (GPS) antenna

3.6 Contactless Card Reader

The Apollo and ApolloMax have a contactless reader that supports all contactless EMV cards including ApplePay, Google Pay, ISO14443 Type A & B (T=CL), Mifare Classic, Desfire cards as well as the ISO18092: NFC Protocol.

Cards and phones are best read when positioned over the center of the contactless icon.

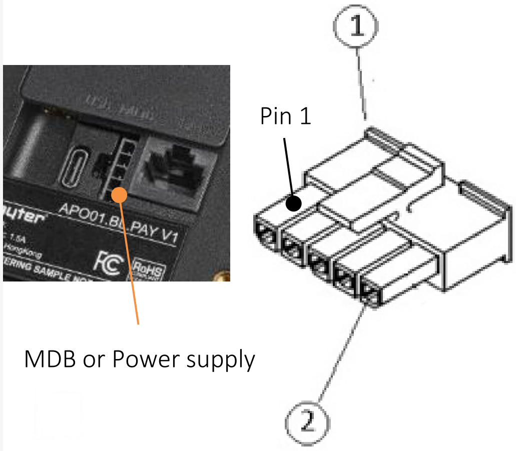


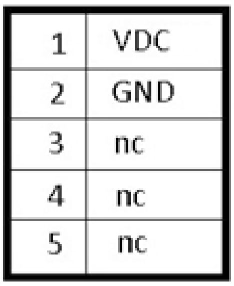
3.7 Power connection

The terminals require an external power supply for operation, using two options through the Micro fit connector:

- Provided 220V power supply
- MDB or similar bus

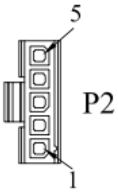
Please find below the specification for connecting the terminal:

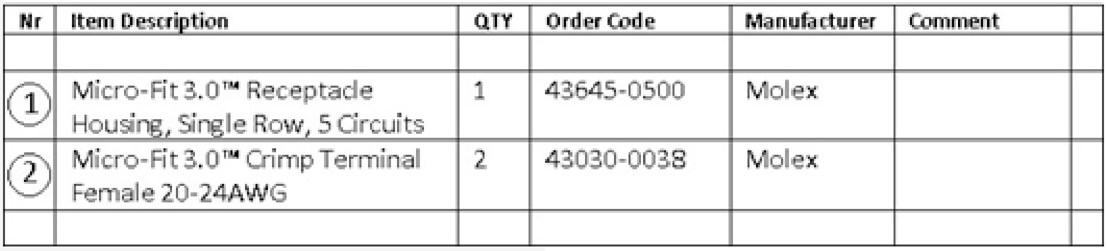




1	VDC
2	GND
3	nc
4	nc
5	nc

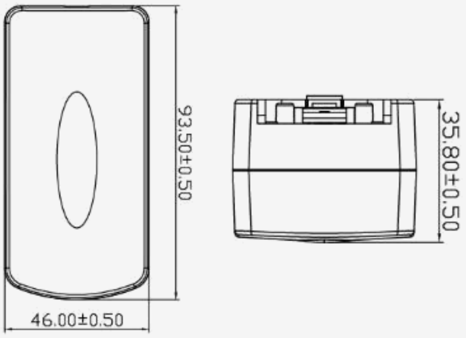
VDC = 12..24V
P = 18W max.





Nr	Item Description	QTY	Order Code	Manufacturer	Comment	
1	Micro-Fit 3.0™ Receptacle Housing, Single Row, 5 Circuits	1	43645-0500	Molex		
2	Micro-Fit 3.0™ Crimp Terminal Female 20-24AWG	2	43030-0038	Molex		

3.8 Dimensions Power supply



3.9 Accessories

The following accessories are available for integration and connection.

MDB/Power Cable

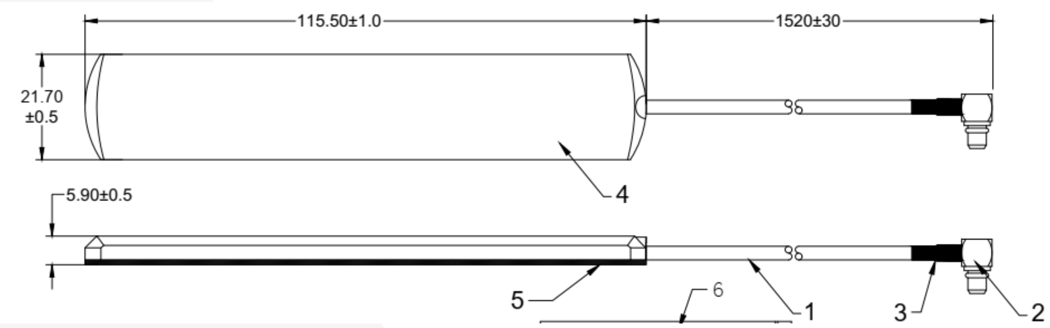
Stick on GSM Antenna

LAN Cable 10 meter

Molex Adapter cable

MMCX to SMA Adapter

3.10 Dimensions Antenna



3.11 Installation

Only use cables and mounting materials provided with the terminal, proper function of the terminals is not guaranteed when 3rd party accessories are used with the exception of the LAN cable.

- Always place the rubber gasket provided with the terminals
- Do not install the ApolloMax in a position where it is exposed to direct rain or hostile weather.
- to avoid reflections and guarantee readability, do not expose the display to direct sunlight

When supporting pin entry

- for the security of the card-holder, make sure that PIN privacy is guaranteed:
- locating the display outside the field of vision of cameras, mirrors and so on, and away from stairs
- check all local regulations and requirements for PIN privacy

⚠ Metal environments will influence the performance of the contactless operating field. Please ensure that the Apollo terminals are not completely enclosed in a metal environment otherwise the operating distance will be reduced. An offset of 5 mm along the sides and rear of the terminal will provide enough distance. If you have any questions with regards to the mechanical integration, please contact the Payter support desk.

3.12 Placing the antenna

1. Place antenna externally for better signal strength. (Recommended)
2. If signal strength is strong inside the machine (2+ bars) internal installation could be considered..
3. Make sure the antenna is not completely surrounded by metal or mounted on metal. (reception loss)
4. Use caution when fastening the external antenna cable to MMCX connector on the terminal, too much force can damage the connection.

You get the Most Consistent & Reliable Results by placing the antenna on top of the machine.
An optional External Mount Dome Antenna can be provided to help with Performance & Security

Things to consider…

- Radio waves move in a straight line between our antenna and the antenna on the cell tower
- They do not go around obstacles, they go through them if they can
- Glass and wood are no problem but steel and concrete pose a real challenge
- Consider heating ducts, plumbing and other such obstacles

4. Modes of operation

4.1 Machine Interface

The Apollo terminal family support several different interfaces to connect to your machine. Choosing an interface will largely depend on the interface that is supported by your machine, and the preferred method of powering the terminal. Table 1 gives a summary of available options.

Interface Mode	Description	Remarks
MDB	The Multi Drop Bus is an industry standard interface for vending machines. If your machine supports an MDB - Cashless Device, then this will require little effort to reach a working solution, provided that the MDB standard is correctly implemented in your machine. An advantage of MDB is that the interface also supplies power to the terminal, requiring no additional power supply.	
PSP	This message based protocol provides basic functionality for machine to payment terminal communication, over an RS232 or TCP/IP connection.	
Cloud	This API provides methods to manage payment sessions on Payter terminals, in this mode of operation the terminal is slaved to the Payter Cloud API.	
Potential Free Pulse Contact	A configurable potential free pulse contact is available to signal your application that a payment transaction was successfully processed. In addition, an input port is available to enable/disable the terminal, if for example the machine is out of order. Although a Potential free pulse contact interface is widely used, there is no standardization, and requires attention to electrical details before it can be used.	Require Accessory

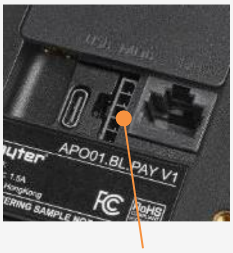
Table 5.1 – Available Host Machine interface modes.

For detailed and in depth information about the various interfaces, please check the Payter website for documentation or ask your Payter account representative.

4.2 MDB mode

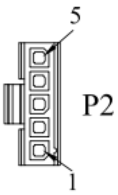
MDB stands for multidrop bus. Since the 1980, the multidrop computer bus has been used by vending machine controllers to communicate with the vending machine's components, such as a currency detector. It is now an open standard of the National Automatic Merchandising Association (NAMA).

The Apollo series terminals are classified as MDB Cashless Devices and support levels 1 to 3 of the MDB specification v4.2, including the always idle mode. For a detailed description of the MDB interface, see the MDB v4.2 specification documentation.



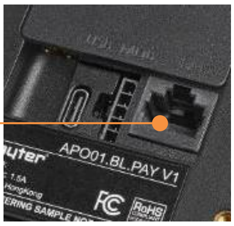
MDB or Power supply

1	VDC
2	GND
3	Master_TX
4	Master_RX
5	ISO GND



5. Internet connection

An internet connection to an Apollo series terminal is required, for configuration of the terminal and online verification of payments, remote management functionality and telemetry.



The following options are available to connect to the internet:

– LAN connection using the onboard RJ45 connector LAN port
  - o Ethernet (100BASE-TX, 10base-10) network port
– Mobile internet connection using an optional 4G/GSSN modem.

⚠ During the booting process, the terminal will check the connection to all configured payment hosts. If a payment host cannot be reached, an error will be displayed revealing the host that cannot be reached. This problem must be resolved before you continue.

5.1 Firewall network settings for the Payter Payment Terminal

When the terminal is connected through the LAN Cable or WiFi, it will require open ports in the Firewall. Below you will find a schedule with the required network settings.

⚠ Please ensure the firewall accepts URL's not just IP addresses.

Application	URL	Port	Internet protocol
Payter Terminal Management System	curo-api.payter.nl	3185	TCP
Gateway NMI/ CreditCall	https://live.cardeasexml.com	443	TCP / IP
Cloud Host	https://cps-rtp.mypayter.com	3185	TCP
Google NTP server 1	time1.google.com	UDP	123
Google NTP server 2	time2.google.com	UDP	123
Google NTP server 3	time3.google.com	UDP	123
Google NTP server 4	time4.google.com	UDP	123
MQTT Broker	mqtt.mypayter.com	TCP	8883
Storage bucket	update.mypayter.com	TCP	443
Shellhub	shellhub.infra.mypayter.com	TCP	443
Gateway Monet+ host	193.33.23.54	TCP	37696

The latest list can be found at ww.payter.com

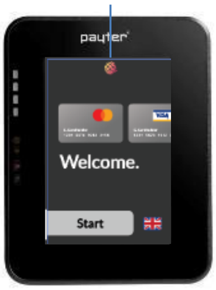
6. User Interface

6.1 Customisation

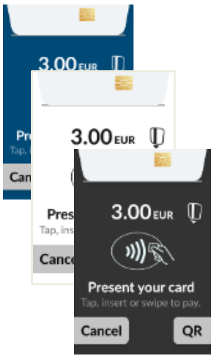
The following parts of the user Interface can be customized to reflect your company brand:

Idle screens prior to the start of transaction, i.e. with product placement

Small Logo in display



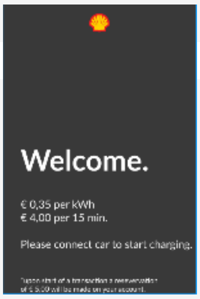
Background colour



Thank you message

6.2 Example Payment flow

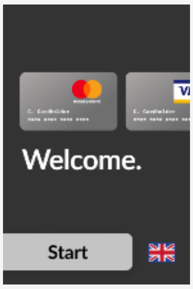
Idle screens Rotating

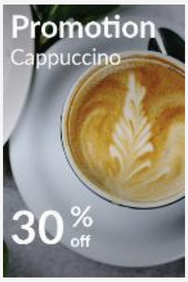

Welcome.

€ 0,35 per kWh
€ 4,00 per 15 min.

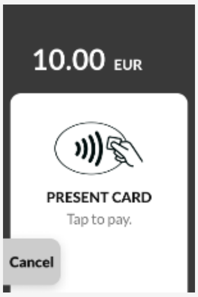
Please connect car to start charging.

Upon start of a transaction a reservation of € 5.00 will be made on your account.


Welcome.

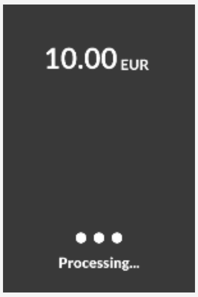


Scanning for card


10.00 EUR

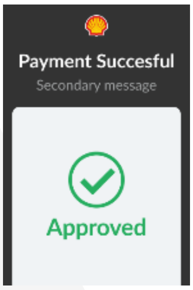
PRESENT CARD
Tap to pay.

Authorising

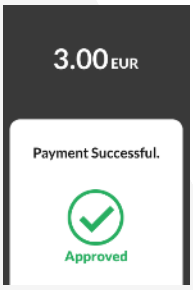

10.00 EUR

Processing...

Transaction Result


Payment Succesful
Secondary message

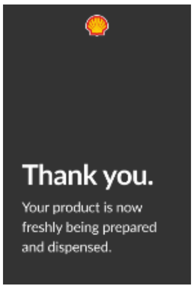
Approved


3.00 EUR

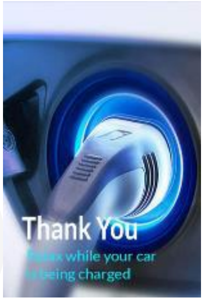
Payment Successful.

Approved

Thank message


Thank you.

Your product is now freshly being prepared and dispensed.

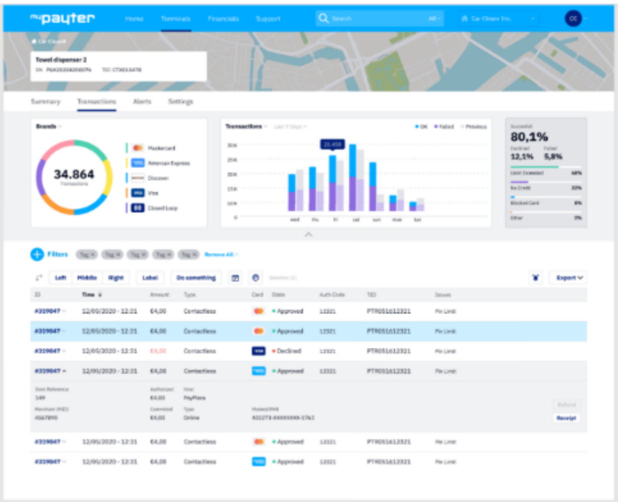


Customised

7. Configuration

The Apollo terminals are continuous connected to the Payter Terminal Management System (TMS). The configuration of the terminals, including Key loading can only be done through the MyPayter TMS portal.
The MyPayter portal allows:

- Efficient and timely deployment of keys, configuration updates and payment device firmware
- Remote management of large quantities of Payter Terminals
- Future proof system in which changes in functionality can be applied easily, safely, and quickly, while reducing the Cost of Ownership.
- Continued EMV compliance



The MyPayter Portal provides detailed insight into your transactions and the ability to create customized reports. Thanks to the real-time connection with the terminals, you'll have an instant overview of which terminals are on-line.

7.1 Access

You will receive an email invitation to set a password for your account. The 'Set Password' button will lead you to our Reset password site. We have generated a unique secure code for you, in case the code is not automatically populated, please copy this code from the invitation email.

8. Mechanical Integration

8.1 Front mounting

The Apollo series terminals can be directly mounted on the front panel of a machine.
The mounting footprint of Figure 5 is applicable for both the Apollo and the ApolloMax terminal.

Front Mounting should **NOT** be used for outdoor environments, as this makes the terminal more vulnerable to extreme weather conditions (Cold-heat), vandalism and wear and tear.

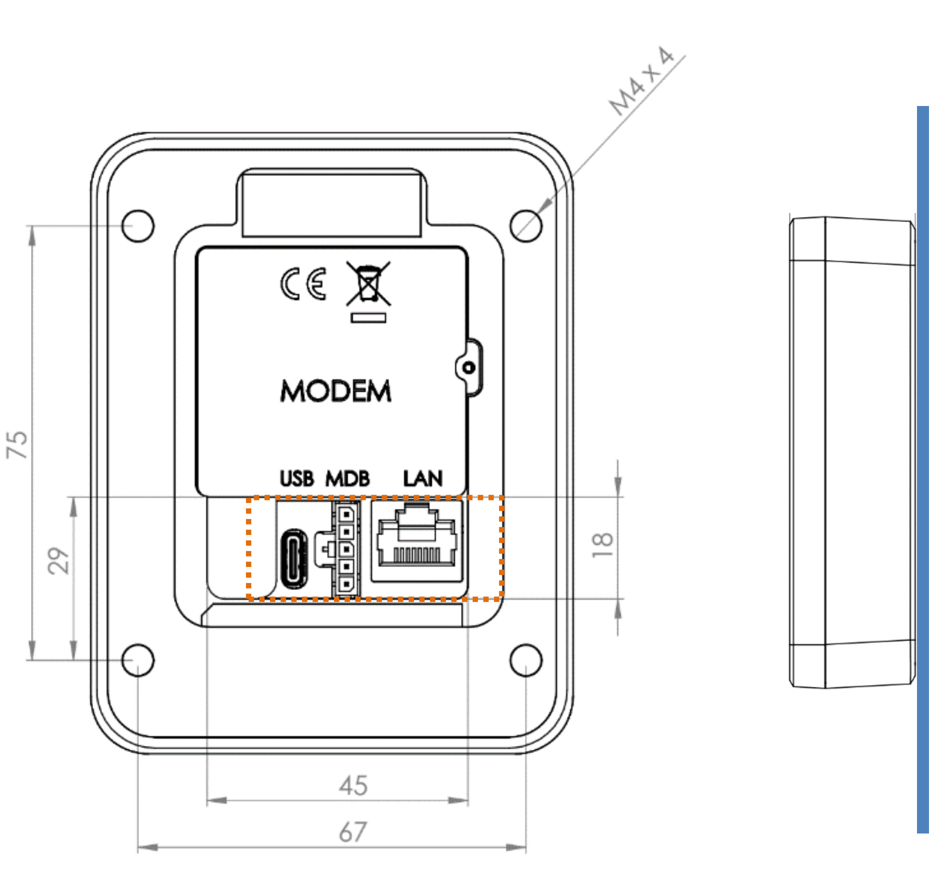


Figure 5: Mounting footprint with dimensions in millimeters (left) and side view (right)

Make sure that there is an opening in your machine large enough to accommodate the placement of the MDB/power cable and antenna cable or the LAN cable indicated by the orange rectangular in below figure.

8.2 EVA mounting

The majority of the vending machines have a provision for installing payment terminals. The dimensions of the Apollo series terminals are based on the European Vending Association (EVA) standard.

8.2.1 Device opening

Mounting an Apollo series terminal requires a device opening that complies with the EVA EPS – standard door model measurements (see Figure 6).

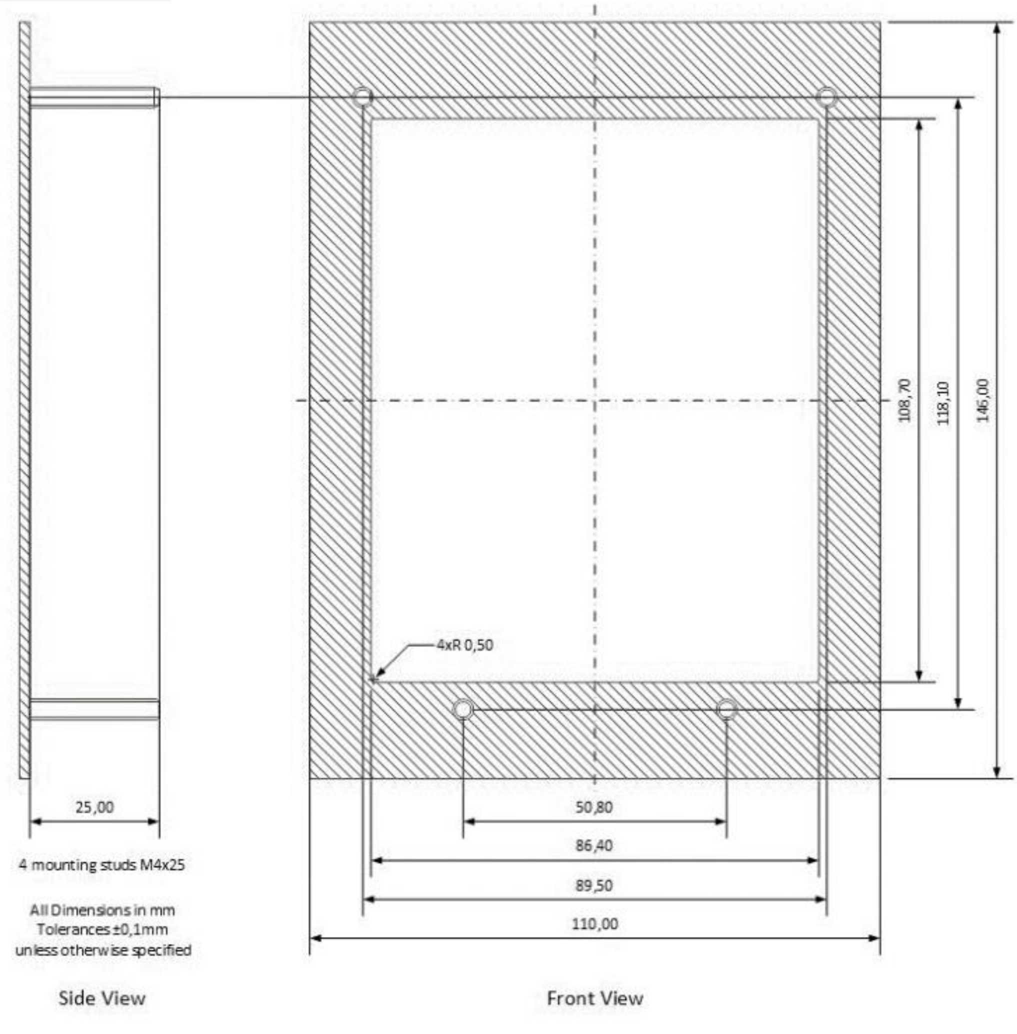


Figure 6: Dimensions of opening and weld studs (in millimeters)

When mounting the terminal:

- Use the supplied mounting frame if no weld studs are available.
- Drill mounting holes with a diameter of 4 millimeter at the positions of the indicated weld studs, to allow mounting of the frame.
- Recommended torque setting of 0.8- 1.0 Nm (mounting) or finger tight.

8.2.2 EVA mounting option 1: studs in machine

If the vending machine has pre-installed studs (see Figure 6):

1. Position the mounting frame at the rear of the opening.
2. Secure the terminal and frame with the four M4 nuts supplied with the terminal.

! For a clean and neat finish of the front, do not forget to place the cover plate at the front of the machine. The cover plate is secured with double-sided adhesive tape for a strong connection.

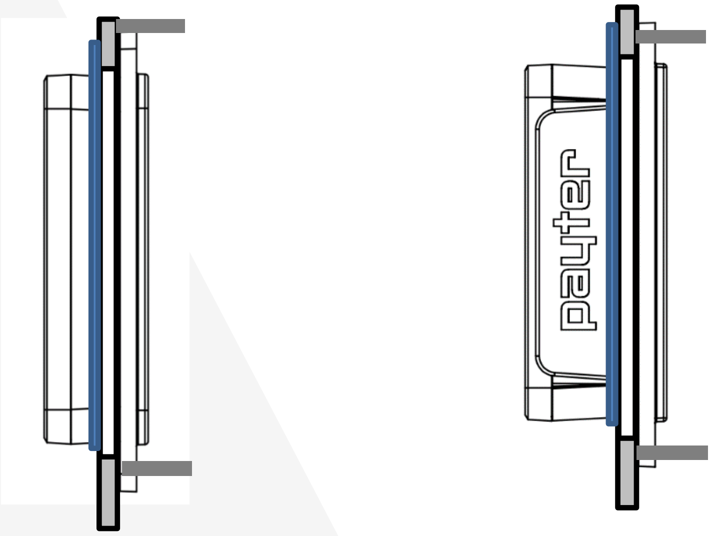


Figure 7: Section view of mounted Apollo terminal (left) and ApolloMax terminal (right)

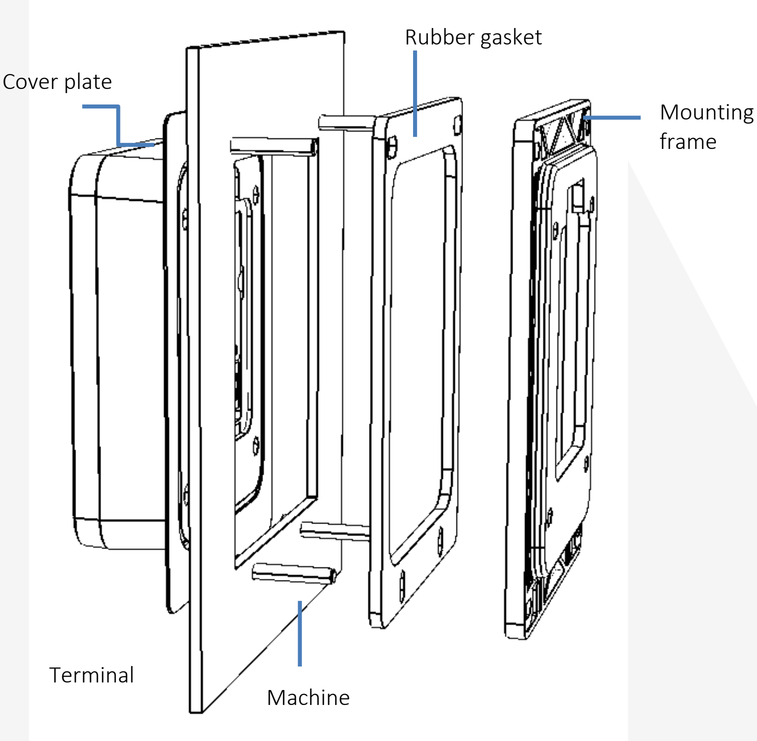


Figure 8: ISO view mounting option 1

8.2.3 EVA mounting option 2: no studs in machine

If the machine does not come with pre-installed studs:

1. Position the supplied mounting frame on the front of the vending machine.
2. Drill mounting holes with a diameter of 4 millimetres at the indicated well stud positions.
3. Secure the mounting frame by placing the four M4 bolts supplied with the terminal.

For a clean and neat finish of the front, don't forget to place the cover plate on the mounting frame to cover the bolts. The cover plate is secured with double-sided adhesive for a strong connection.

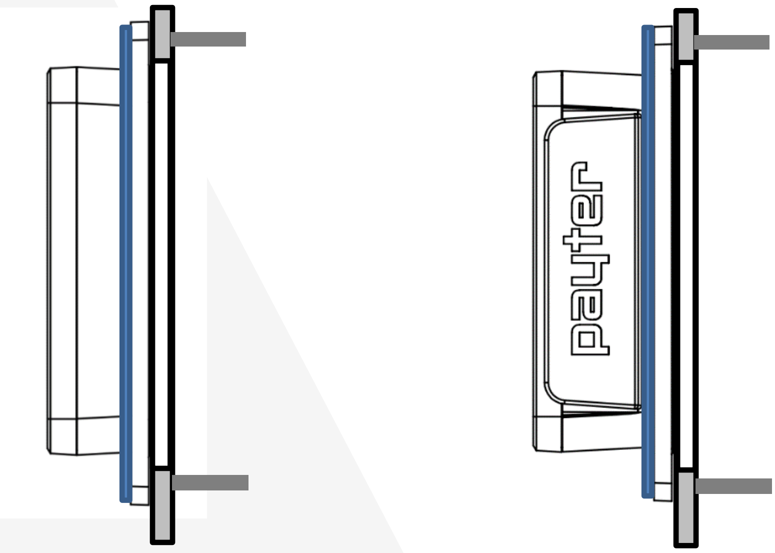


Figure 9: Section view of mounted Apollo terminal (left) and ApolloMax terminal (right)

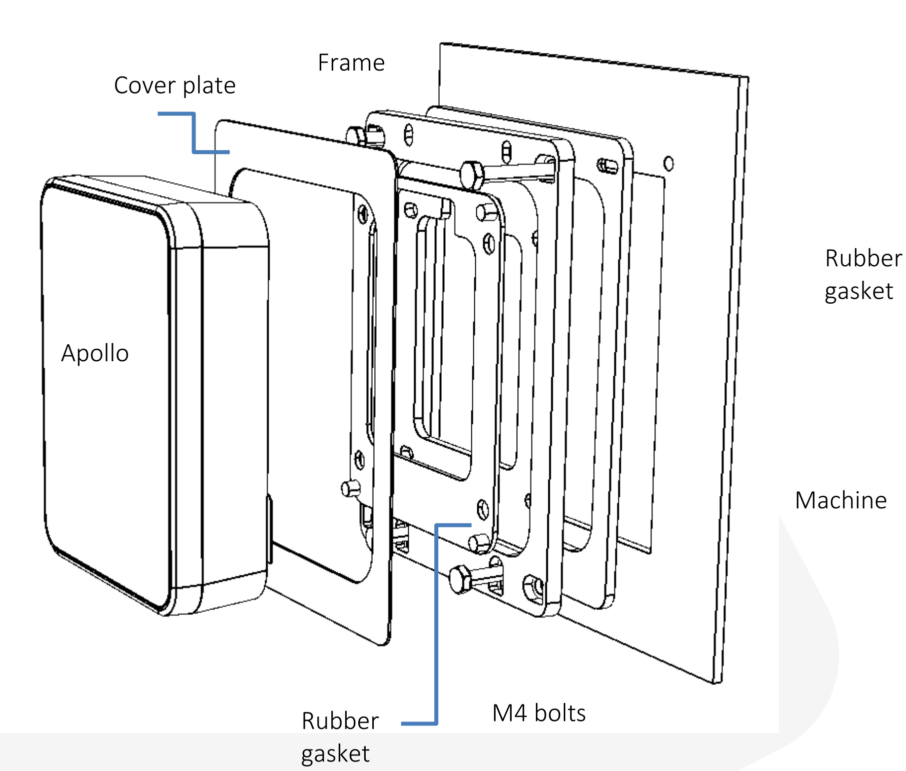


Figure 10: ISO view mounting option 2

8.3 Dimensions Apollo terminal

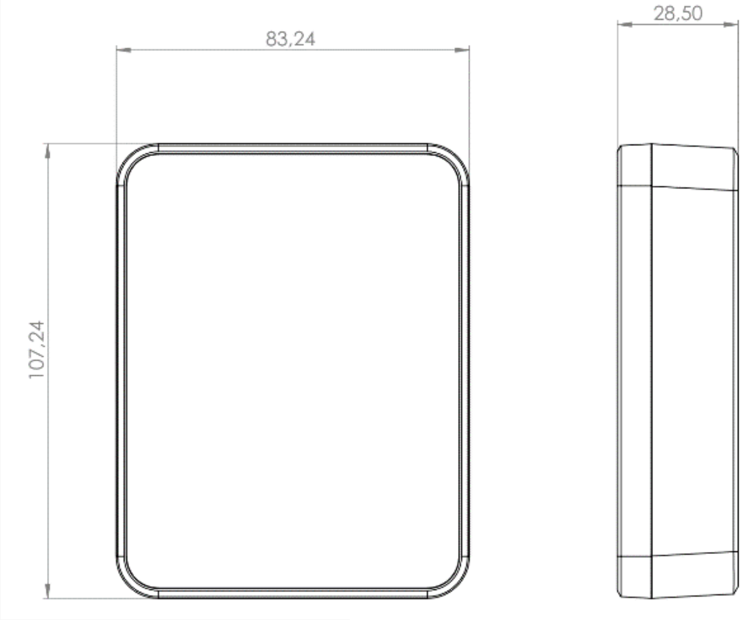


Figure 11: Dimension Apollo terminal without frame

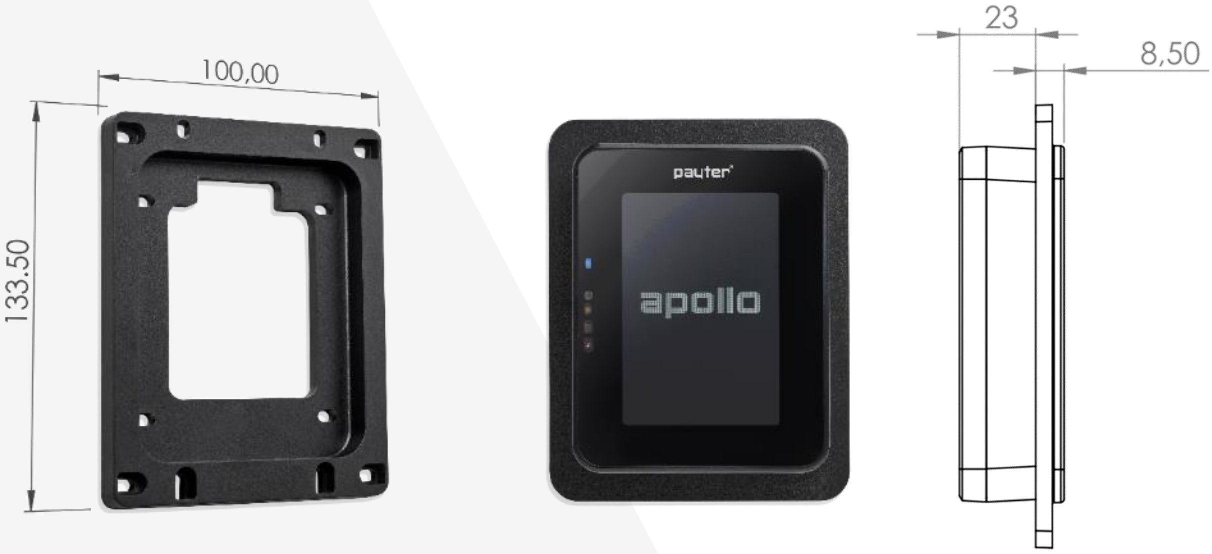


Figure 12: Dimension Apollo terminal with frame

8.4 Dimensions ApolloMax terminal

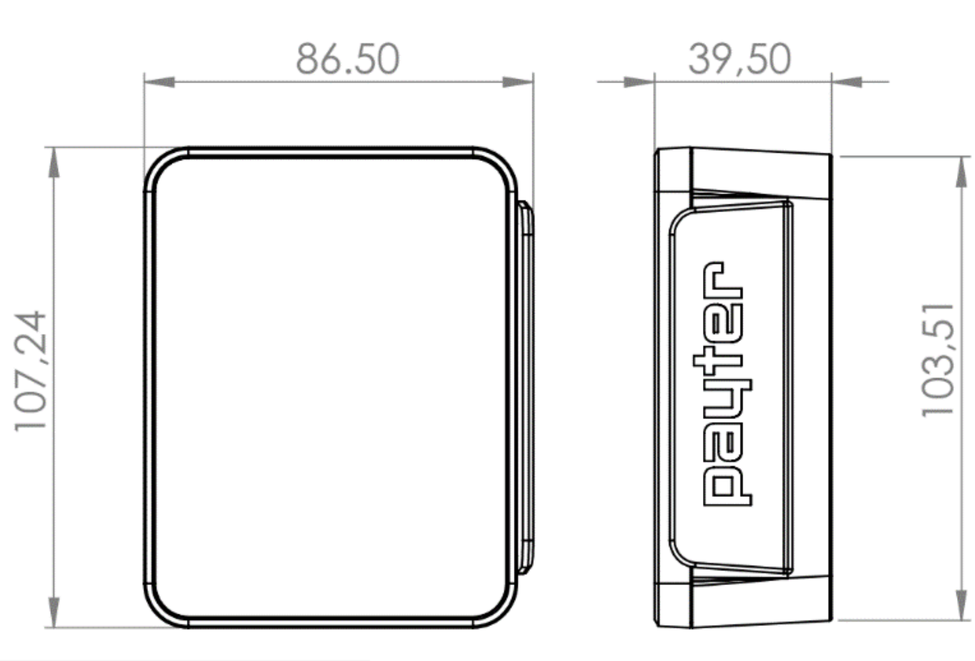


Figure 13: Dimensions ApolloMax terminal without frame

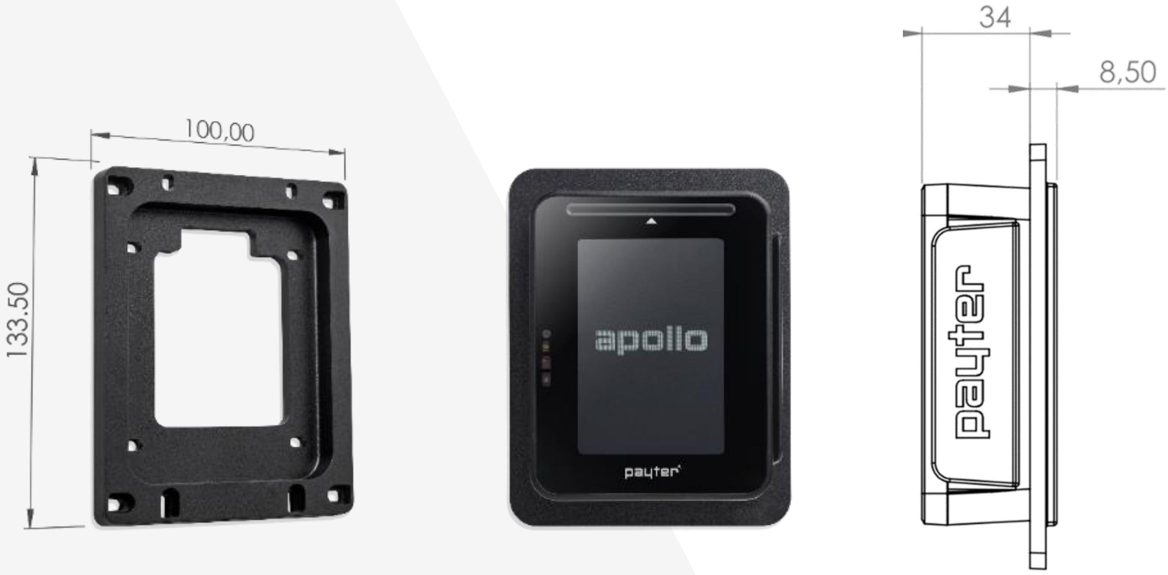


Figure 14: Dimensioins ApolloMax terminal with frame

9. Merchant Responsibilities Security

All Payter Point of Sale terminals are certified by the card schemes according to the latest standards and accredited through various acquirers to securely process transactions. The integrity of the payment terminals is crucial, because they process sensitive card data. Regularly inspect your payment terminal to ensure it is secure. This chapter describes the general responsibilities of the Merchant to assist you in ensuring safe use, prevent fraud and compliance to related Scheme Rules;

⚠ In case of any doubts, do not use the terminal and contact Payter via the regular escalation channels.

9.1 Receipt and Storage

Since the terminal will be processing payment transactions and funds you must verify that the terminal you received is the correct one, and hasn't been tampered with. On receipt of the Terminals please follow the following instructions

- Being available to accept delivery of the Payment Terminal at the designated address on the confirmed day of delivery. The risk of loss, theft, damage or destruction of the Payment Terminal passes to the Merchant when the Payment Terminal is offered for delivery at the Merchant designated location as specified in the order form or the RMA request form.
- Verify whether the shipment is complete and according to order.
- Verify whether the serial numbers of the Terminals are listed and match the serial number of the Terminals in the MyPayter Portal.
- Inspect the packaging and Terminals for visible damage to the housing
- Do not use a damaged Terminal, report any damage per described in section Faulty, lost, stolen, or damaged/tampered Terminals.
    - Create and maintain an inventory of the Terminals
    - Store the Terminals in a secure location prior to deployment and control access to them.

9.2 Deployment

Before deployment please perform the following:

- Install and configure Payment Terminals on site in accordance with the applicable installation and configuration instructions provided for the Payment Terminal. The applicable manual can be retrieved through your distributor.
- Check for visible damage to the housing
- Do not use the Terminal if it is damaged or covered with a non-standard sticker, report any damage/tampering per section 6. For reference images, please check the Payter website, section security policies: ApolloMAX Security Policy , Apollo Security Policy
    - Charge and or connect the Terminal to the Internet.
    - Verify the Payter logo shows up after turning on the terminal.
    - Do not use the Terminal if the logo does not appear, report per section 6.
- Check whether an internet connection is established
- Verify whether the terminal(s) connect to the MyPayter portal; can be verified with the coordinator
- if applicable check whether the amounts are set correctly in the terminal
- After extended storage a test transaction is recommended
- When distributing the Terminals in your organisation update the inventory (list of Terminals) created upon receipt (section 2) with Terminal locations and personnel authorised to operate the Terminals
- Ensure proper training and instruction of all personnel operating the Terminals, enforcing compliance to the responsibilities laid out in this document.

9.3 Transactions and reconciliation

Payter or Distributor does not have access to the Customer's Merchant Account and that it is therefore the Customer's responsibility to reconcile the payments being made into the Customer's Merchant Account with the Transactions processed by the Payment Terminal and PSP Service. In the event that the Customer identifies a discrepancy they must notify Payter as soon as reasonably practical. Payter and the PSP will treat any such notification as a high priority problem.

Payter recommends to check your account and the MyPayter portal for transactions, connectivity of the Terminal and error messages.

9.4 Usage and Management

Merchant must in operating and using the Payment Terminal:

- Ensure that the Payment Terminal is kept and operated in a suitable environment (please check manual), used only for the purposes for which it is designed, and operated in a proper manner;
- Make no alteration to the Payment Terminal and not remove any component(s) from the Payment Terminal without the prior written consent of Payter;
- Not, without the prior written consent of Payter, allow any third party to use the Payment Terminal or submit Transactions via the Payment Terminal on behalf of a third party. The Payment Terminal may only be used by Merchant to submit Transactions to the PSP in its own name and for the business it registered for in the Merchant registration Process;
- Comply with the relevant usage manuals for the Payment Terminals, including in particular when applicable:
    - The manual of the particular type of Payment Terminal;
    - The Installation guide for Payment Terminals to ensure IP connectivity for the Payment Terminals to enable their proper functioning;

9.5 Battery and storage

The Apollo terminals are equipped with Li-Ion batteries to ensure the integrity of the payment terminals even when not powered. To ensure the security during the full life time of the terminals, these batteries need to be recharged at regular intervals (once every three (3) months) to avoid fall back to the back-up battery. When a terminal has not connected to the MyPayter terminal management portal for an extended period of time, the Merchant will receive an alerts through the terminal management system to charge the terminal.

Please note: Failure to charge the batteries at notification drastically reduce the shelf life of a terminal and can result in tampering the terminal. A tampered terminal need to be returned to Payter for analysis, possible replacement of the batteries and key injection.

9.6 Security

For security reasons, Merchants and staff are advised to check Payment Terminal regularly for:

- Visible damage to the housing
- Do not use the Terminal if it is damaged or covered with a non-standard sticker. For reference images, please check the Payter website, section Security policies, : ApolloMAX Security Policy , Apollo Security Policy P6X User manual PTR-40-10-ML-C-0003-03.
- Unusual cables connected anywhere on the terminal
- Verify the Payter logo shows up after turning on the terminal.
- Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot terminals.
- Do not install, replace, or return Terminals without verification.
- Be aware of suspicious behaviour around Terminals (for example, attempts by unknown persons to unplug or open the terminals).

- Report suspicious behaviour and indications of terminal tampering or substitution to appropriate personnel (for example, to a manager or security officer).

Merchants should use their terminal inventory to ensure that the location of all Terminals is known and to confirm that no Terminals have been lost, stolen or substituted. Payter recommends enforcing procedures to perform visual Terminal integrity inspections on a weekly basis as well as before and after storage of the Terminals.

In case of any doubts, do not use the terminal and contact Payter via the regular escalation channels.

- Follow the Scheme Rules in operating the Payment Terminals to submit point of Sale Transactions.

For as far as applicable comply with PCI DSS security requirements imposed by the Card Schemes in handling and using Payment Terminals and on the acquirers' request fill out Self-Assessment Questionnaires ('SAQs') prescribed by the Scheme Owners under applicable PCI DSS regulations to confirm such compliance.

9.7 Faulty, lost, stolen, or damaged/tampered Terminals

In the event of loss, theft, damage, tampering or destruction of a Payment Terminal, Merchant must inform Payter or distributor immediately, and in no event later than 24 hours after discovery of the incident, by sending an email to support@payter.com . The notification must provide a complete description of the details of the incident, summarize all efforts undertaken and planned to investigate the incident and secure the information and terminals at issue, and identify appropriate contacts at Merchant who will be reasonably available to Payter.

In the event of a hardware failure, please contact Payters' or the local distributor to obtain a Return Material Authorization (RMA) number.

Merchant must ensure a central contact point manned by trained representatives of Merchant is made available for all end users of Payment Terminals to assist in performing the above tasks which such end users cannot perform themselves without assistance.

Only such designated trained key representatives of Merchant may contact Payter or Distributor to receive support with respect to the Payment Terminals and the Services of Payter. For requesting support with respect to Payment Terminals such representative must use the current contact details to submit the support request by email or trouble ticketing tool, following the relevant procedures.

10. PCI Security

This chapter describes how to operate the Apollo payment terminal in a secure manner. The terminal is approved to PCI-PTS V6.0, this document describes how to use the device in a manner compliant to the requirements set out in PCI-PTS V6.0.

Using the terminal in a way that deviates from this document will invalidate the PCI PTS approval of the device.

10.1 Model Name and Appearance

Apollo

ApolloMax

10.2 Product Type

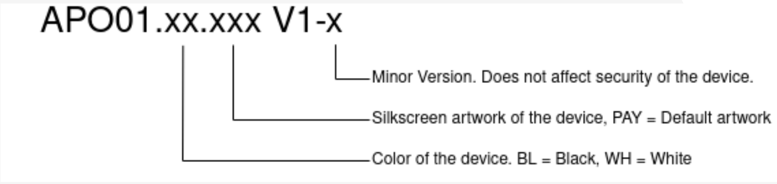
The Apollo is a PIN Entry Device (PED) for payment processing in an unattended environment. It provides the ability to conduct contactless transactions.
The PCI approval is only valid when using the device as described in this document.

10.3 Identification

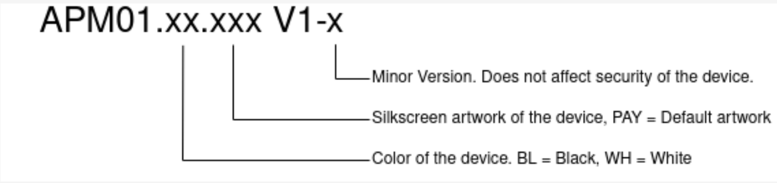
10.3.1 Hardware

This document applies to any hardware version as per below.

Apollo

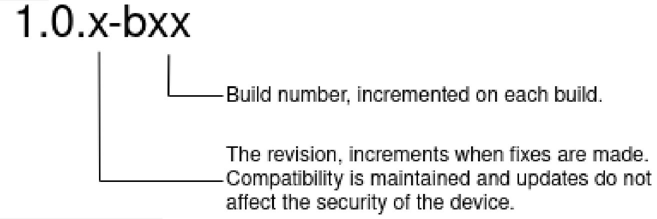

APO01.xx.xxx V1-x
Minor Version. Does not affect security of the device.
Silkscreen artwork of the device, PAY = Default artwork
Color of the device. BL = Black, WH = White

ApolloMax


APM01.xx.xxx V1-x
Minor Version. Does not affect security of the device.
Silkscreen artwork of the device, PAY = Default artwork
Color of the device. BL = Black, WH = White

10.3.2 Firmware

This document applies to any firmware version as per below.



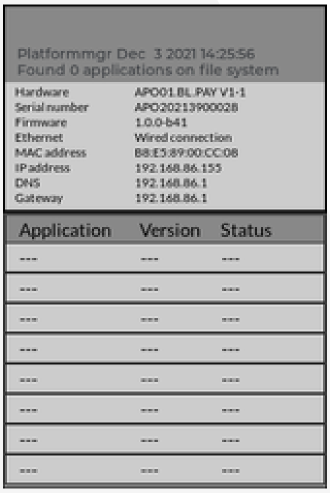
1.0.x-bxx

Build number, incremented on each build.

The revision, increments when fixes are made. Compatibility is maintained and updates do not affect the security of the device.

10.4 Location of Identifiers

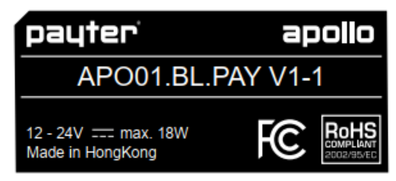
The hardware and firmware identifiers are presented during the boot process.

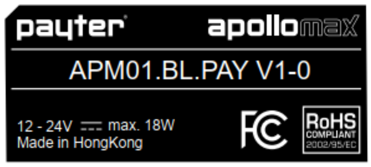


```
Platformmgr Dec  3 2021 14:25:56
Found 0 applications on file system
Hardware          APO01.BL.PAY V1-1
Serial number     APO20213900028
Firmware          1.0.0-b41
Ethernet          Wired connection
MAC address       B8:E5:89:00:CC:08
IP address        192.168.86.155
DNS               192.168.86.1
Gateway           192.168.86.1
```

Application	Version	Status
---	---	---
---	---	---
---	---	---
---	---	---
---	---	---
---	---	---
---	---	---
---	---	---

The hardware identifier is also printed on a label on the back of the device.





The identification label shall not be torn off or altered in any way.

10.5 Installation and User Guidance

10.5.1 Initial Inspection

When the merchant first receives the Apollo terminal, they must check for signs of tampering. This is described in the documentation for the Apollo terminal. It is strongly advised to carry out the same checks when the terminal is in use.
The merchant should inspect the Apollo terminal to ensure that:

- There is no sign of unusual cables connected anywhere on the device.
- Where applicable, the device is still firmly secured in its intended installation location.
- The device is not showing any warning / error messages.
- There is no visible damage to the device.
- The device serial number matches the inventory.

10.5.2 Installation

Installation instructions including the following information are provided in digital format [5].

- Equipment checklist
- Power cable connection information
- Main characteristics of the terminal

- Safety and Security recommendations
- Troubleshooting information

10.6 Environmental Conditions

The recommended operating conditions of the terminal are:

- Operating Temperatures : -20^0 C to 55^0 C
- Operating Humidity: 10-90% RH Non-condensing
- Power Supply: 12-24 VDC
-

The security of the device is not compromised by subjecting the device to conditions outside these limits.
The terminal will detect a security violation if the internal temperature exceeds the range -40^0 C to 100^0 C. All operational keys will be deleted from the device and it will no longer be functional.

10.7 Communications and Security Protocols

The device is approved for use with USB, cellular, Ethernet and WiFi; and the approved security protocol is TLS 1.2

The device supports Wi-Fi with WPA/WPA2; WEP and open WiFi networks are not supported. The device will refuse to connect to these networks even if they show up in network scans.

The security protocols should be used in accordance with the Application Developer Guidance [1].

10.8 Configuration Settings

The terminal enforces all settings necessary to meet the PCI requirements. Payter manages a remote key loading facility which ensures all security critical settings are deployed securely.

There are no configuration changes that need to be done by the user in order to meet the security requirement defined in this document. There are no security sensitive default values that need to be changed before operating the device.

Application developers need to follow the Application Developer Guidance [1] to ensure the applications are developed in a secure manner.

11. Operation and Maintenance

11.1 Periodic Inspection

To ensure the device has not been tampered with, the merchant should inspect the Apollo terminal on a bi-monthly basis to ensure that:

- There is no sign of unusual cables connected anywhere on the device
- The device is still firmly secured in its intended installation location
- The device is not showing any warning / error messages
- There is no visible damage to the device
- The device serial number matches the inventory

11.2 Self-Test

The terminal contains a self-test cycle and will restart every 24 hours to perform this self-test. The device will perform the following tests:

- Authentication of all firmware
- Authentication of all application software
- Tests of cryptographic functions

11.3 Passwords and Certificates

All applications have to be signed by Payter following a review of the application, optionally an Acquirer can be issued its own application signing certificate but it is the acquirer's responsibility to ensure a secure environment to generate the required RSA key pair and associated certificate signing request. Signing must then be performed as per [1] and [2].

11.4 Tamper Response

The device contains mechanisms to detect physical tampering. Any penetration of the device will trigger a tamper detection alarm and the device will delete all its operational key material. The device will immediately restart into an inactive mode and will display a security violation.

11.5 Privacy Shield

The Apollo is designed to be used in an unattended environment, integrated into a larger solution. To avoid disclosing the PIN code from intended or unintended observation the card holder needs to be made aware that they must prevent others from viewing the PIN during PIN entry. The payment application must display a message to notify the card holder to protect his PIN during entry. Such as: "Keep your PIN safe; block the keypad with a free hand or block the view using your body."
Care must be taken with respect to any video recording equipment that may have a view of the device, such as CCTV or similar equipment that may be installed at the deployment location. The terminal should be placed such that the entered PIN is not visible from any such equipment. Refer to Apollo / ApolloMax Mechanical Integration Guide for details about installation requirements.

11.6 Patching and Updating

The terminal makes use of the Payter central software repository and can as such retrieve any updates it may require. Payter will take the initiative in informing customers if any updates are required.

11.7 Decommissioning

In order to permanently decommission a device all key material should be removed from the device. This can be accomplished by removing the 4 case screws on the back of the device and opening the case. Once assembled the device will boot into a tampered state.

12. Security measures

12.1 Software Development Guidance

The following outlines the functions certified under PCI PTS 6.0

- Key management system (Crypto API)
- SRED (EMV L1 API)
- PIN Entry (PIN API)
- Open Protocols (Apollo Proxy)

Only signed firmware can be loaded onto the terminal and it is not possible to run unauthorized functions.

12.2 Signing

The Apollo will only run applications that provide a signature created using a certificate that has been issued by the Payter Root certificate.

Applications are signed using RSA 4096 for signature verification and SHA256 calculating data integrity hashes.

During signing a file is generated that contains the SHA256 hash of all the files in the application. This file is then signed using RSA 4096 and a file containing the signature using the Cryptographic Message Syntax is generated. Both the file containing hashes as the signature file are packed into the application, these are verified by Apollo upon starting the application, see [2] for more details. The signing process must be performed offline and under dual control using split knowledge.

12.3 Account-data Protection

The device supports DUKPT 2009 (TDES) and DUKPT 2017 (TDES and AES) for account data protection, the device supports pass-through of clear-text account data for authenticated applications. The device does not support turning off the SRED functionality.

12.4 Algorithms Supported

The device supports the following cryptographic algorithms

- TDES (112 bits and 168 bits)
- AES (128 bits)
- RSA (Signature Verification and Key Exchange 4096 bits)
- HMAC SHA256
- CMAC AES 128

12.5 Key Management

The device supports DUKPT as its key management technique, the technique uses a unique key per transactions as specified in [3] and [4].

The use of the POI with different key management systems will invalidate any PCI approval of this POI.

12.6 Key Loading

Key loading cannot be performed directly on the device, all key loading activities are performed over the air via an online key loading facility that is cryptographically bound to the terminal.

12.7 Key Table

Key Name	Designator	Type	Size (Bits)	Form Factor Loaded / Stored to Device	Num Slots
Payter Root	PK_{ROOT}^{ROOT}	RSA Public	4096	Loaded: x509 Stored: x509	1
Terminal Intermediate	$PK_{TERMINAL\text{-}INT}^{ROOT}$	RSA Public	4096	Loaded: x509 Stored: x509	1
Terminal Certificate Key Pair	$KP_{TERMINAL}^{TERMINAL\text{-}INT}$	RSA Key Pair	4096	Loaded : NA Stored : OPTEE Key Object	1
Application Intermediate	$PK_{APP\text{-}INT}^{ROOT}$	RSA Public	4096	Loaded: x509 Stored: x509	1
Application Signing Key	$PK_{APP}^{APP\text{-}INT}$	RSA Public	4096	Loaded: x509 Stored: x509	1 per application
Crypto Domain - DUKPT					

DUKPT 2009 IPEK	DUKPT-IPEK-2009	2TDEA	112	Loaded : TR-31 Stored : N/A	1 per Crypto Domain
DUKPT 2017 IPEK	DUKPT-IPEK-2017	2TDEA 3TDEA AES	112 168 128	Loaded : TR-31 Stored : N/A	1 per Crypto Domain
DUKPT 2009 Future Keys	DUKPT-FK-2009	2TDEA	112	Loaded : NA Stored : OPTEE Object	21 per Crypto Domain
DUKPT 2017 Future Keys	DUKPT-FK-2017	2TDEA 3TDEA AES	112 168 128	Loaded : NA Stored : OPTEE Object	32 per Crypto Domain
DUKPT 2009 Active PIN Key	DUKPT-PIN-2009	2TDEA	112	Loaded : NA Stored : OPTEE Object	1 per Crypto Domain
DUKPT 2017 Active PIN Key	DUKPT-PIN-2017	2TDEA 3TDEA AES	112 168 128	Loaded : NA Stored : OPTEE Object	1 per Crypto Domain
DUKPT 2009 Active Data Enc Key	DUKPT-DATA-ENC-2009	2TDEA	112	Loaded : NA Stored : OPTEE Object	1 per Crypto Domain
DUKPT 2017 Active Data Enc Key	DUKPT-DATA-ENC-2017	2TDEA 3TDEA AES	112 168 128	Loaded : NA Stored : OPTEE Object	1 per Crypto Domain
DUKPT 2009 Active Data Dec Key	DUKPT-DATA-DEC-2009	2TDEA	112	Loaded : NA Stored : OPTEE Object	1 per Crypto Domain
DUKPT 2017 Active Data Dec Key	DUKPT-DATA-DEC-2017	2TDEA 3TDEA AES	112 168 128	Loaded : NA Stored : OPTEE Object	1 per Crypto Domain
DUKPT 2009 Active MAC Req Key	DUKPT-MAC-REQ-2009	2TDEA	112	Loaded : NA Stored : OPTEE Object	1 per Crypto Domain
DUKPT 2017 Active MAC Req Key	DUKPT-MAC-REQ-2017	2TDEA 3TDEA AES	112 168 128	Loaded : NA Stored : OPTEE Object	1 per Crypto Domain
DUKPT 2009 Active MAC Res Key	DUKPT-MAC-RES-2009	2TDEA	112	Loaded : NA Stored : OPTEE Object	1 per Crypto Domain
DUKPT 2017 Active MAC Res Key	DUKPT-MAC-RES-2017	2TDEA 3TDEA AES	112 168 128	Loaded : NA Stored : OPTEE Object	1 per Crypto Domain
Crypto Domain - Hash					
HMAC	HMAC	HMAC	256	Loaded : TR-31 Stored : OPTEE Object	1 per Crypto Domain
CMAC	CMAC	AES	128	Loaded : TR-31 Stored : OPTEE Object	1 per Crypto Domain

CONLON	CONLON	2TDEA	112	Loaded : TR-31 Stored: OPTEE Object	1 per Crypto Domain

12.8 References

1. Application Developer Guidance
2. Application Signing
3. ANS X9.24-1:2009, Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques
4. ANS X9.24 - 3: 2017, Retail Financial Services Symmetric Key Management Part 1: Unique Key Per Transaction
5. Apollo / ApolloMax Mechanical Integration Guide

13. Technical specifications

Contactless Interface	EMVCo. L1 v3.0 Certified ISO14443 Type A & B (T=CL) Mifare Classic protocol Desfire protocol ISO18092: Support NFC Protocol	Operating Distance	Depending on the card/token up to 10 cm from Reader
Contact Card Interface[*2]	EMV L1 v4.3 Certified	Compliances	CE, FCC, RoHS, WEEE , REACH EMVCo, PCI-PTS 6.x, TQM MasterCard, VISA, American Express, Discover, Diners
Magnetic Stripe Reader[*2]	3 Track	LED indicators	4 RGB LEDs
CPU	ARM Cortex A7 Core Operating at 528MHz with ARM TrustZone technology	Display	3.5” IPS LCD Display, 320x480 with Backlight 256K Color palette, Capacitive Touch screen interface
Memory	256 MB, DDR3-800 8GB eMMC, high-speed DDR	Barcode Reading	Integrated camera supporting QR code scanning
Peripheral ports	USB Type C, dual role port capable of powering expansion modules.	Audio	Internal speaker, Mono audio playback. Buzzer
Communication ports	RJ45 connector, Ethernet (100BASE-TX, 10base-10) network port IEEE802.11b/g/n W-LAN GSM/GPRS/LTE CAT 1 MODEM (optional) GNSS, (GPS) support with modem	Integrated Sensor	Ambient Light sensor Proximity Sensor
Expansion modules (optional)	Pulse I/O Expansion Module RS232 interface Extension Module	Dimensions	European Vending Association Compliant Frame Apollo 83.2 x 107.2 x 28.5 mm (LxWxH) ApolloMax 86.5 x 107.2 x 39.5 mm (LxWxH) ApolloPolar[*3] 91 x 121 x 42 mm
Environmental	Operating temperature -20 - 55°C Storage Temperature -20 - 70°C Humidity 10 – 90% RH Non-condensing Apollo IP 65 Front ApolloMax IP 50 Front Apollo Polar[3] IP 54 Vandal proof IK 09	Power Supply	110 – 230 VAC, Power Supply with 1.5m cable. MDB port 12–24VDC
Battery	Li-Ion rechargeable Coincell back-up	Color	Black, White

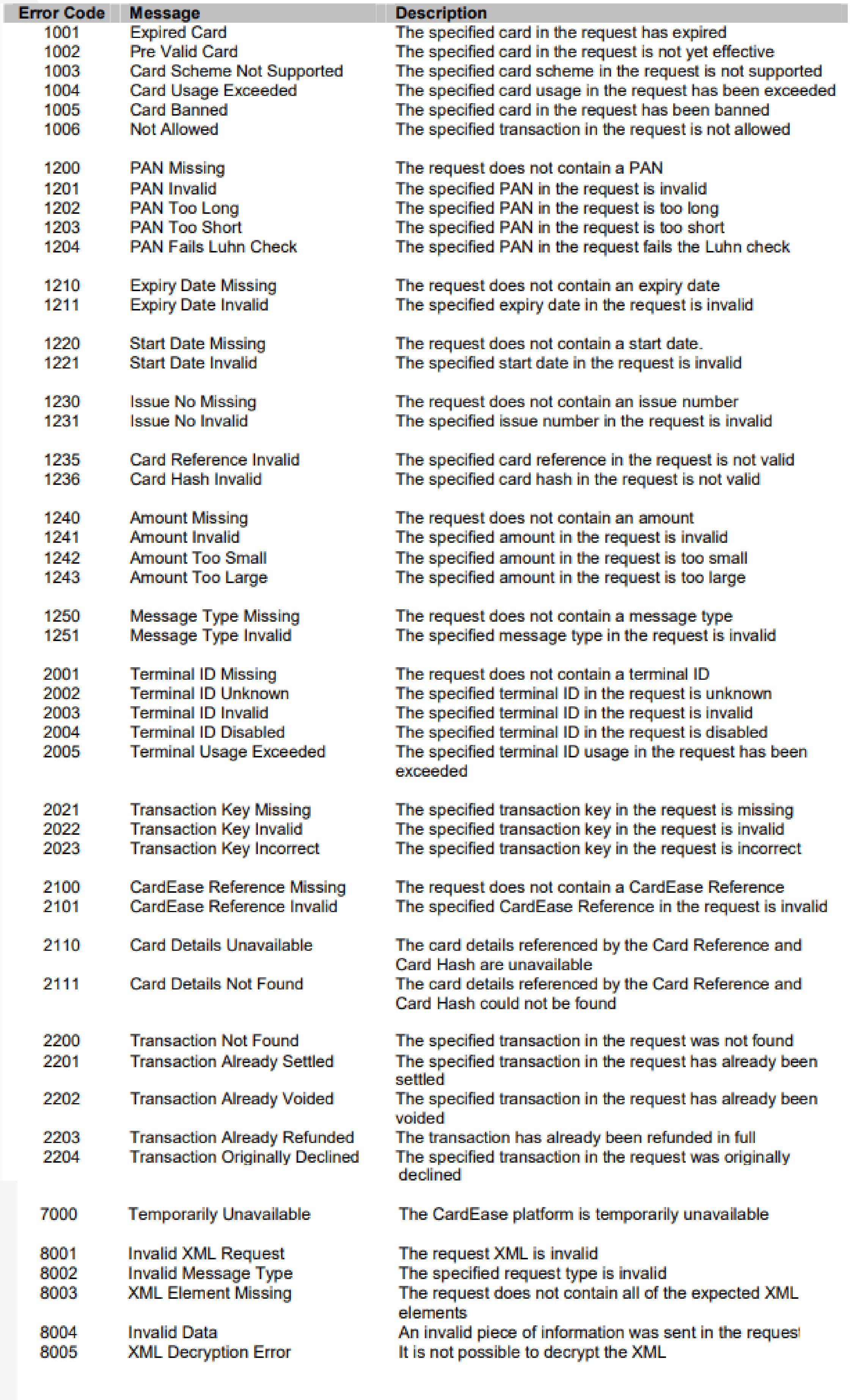
[2] Apollo Max only [3]Not yet released

14. Troubleshooting

14.1 HTTP Error codes

900	Informational (1××)	934	Conflict (409)
901	Continue (100)	935	Gone (410)
902	Switching Protocols (101)	936	Length Required (411)
903	Processing (102)	937	Precondition Failed (412)
904	Success (2××)	938	Payload Too Large (413)
905	OK (200)	939	Request-URI Too Long (414)
906	Created (201)	940	Unsupported Media Type (415)
907	Accepted (202)	941	Requested Range Not Satisfiable (416)
908	Non-authoritative Information (203)	942	Expectation Failed (417)
909	No Content (204)	943	I'm a teapot (418)
910	Reset Content (205)	944	Misdirected Request (421)
911	Partial Content (206)	945	Unprocessable Entity (422)
912	Multi-Status (207)	946	Locked (423)
913	Already Reported (208)	947	Failed Dependency (424)
914	IM Used (226)	948	Upgrade Required (426)
915	Redirection (3××)	949	Precondition Required (428)
916	Multiple Choices (300)	950	Too Many Requests (429)
917	Moved Permanently (301)	951	Request Header Fields Too Large (431)
918	Found (302)	952	Connection Closed Without Response (444)
919	See Other (303)	953	Unavailable For Legal Reasons (451)
920	Not Modified (304)	954	Client Closed Request (499)
921	Use Proxy (305)	955	Server Error (5××)
922	Temporary Redirect (307)	956	Internal Server Error (500)
923	Permanent Redirect (308)	957	Not Implemented (501)
924	Client Error (4××)	958	Bad Gateway (502)
925	Bad Request (400)	959	Service Unavailable (503)
926	Unauthorized (401)	960	Gateway Timeout (504)
927	Payment Required (402)	961	HTTP Version Not Supported (505)
928	Forbidden (403)	962	Variant Also Negotiates (506)
929	Not Found (404)	963	Insufficient Storage (507)
930	Method Not Allowed (405)	964	Loop Detected (508)
931	Not Acceptable (406)	965	Not Extended (510)
932	Proxy Authentication Required (407)	966	Network Authentication Required (511)
933	Request Timeout (408)	967	Network Connect Timeout Error (599)

14.2 Creditcall/NMI Error codes



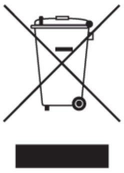
Error Code	Message	Description
1001	Expired Card	The specified card in the request has expired
1002	Pre Valid Card	The specified card in the request is not yet effective
1003	Card Scheme Not Supported	The specified card scheme in the request is not supported
1004	Card Usage Exceeded	The specified card usage in the request has been exceeded
1005	Card Banned	The specified card in the request has been banned
1006	Not Allowed	The specified transaction in the request is not allowed
1200	PAN Missing	The request does not contain a PAN
1201	PAN Invalid	The specified PAN in the request is invalid
1202	PAN Too Long	The specified PAN in the request is too long
1203	PAN Too Short	The specified PAN in the request is too short
1204	PAN Fails Luhn Check	The specified PAN in the request fails the Luhn check
1210	Expiry Date Missing	The request does not contain an expiry date
1211	Expiry Date Invalid	The specified expiry date in the request is invalid
1220	Start Date Missing	The request does not contain a start date.
1221	Start Date Invalid	The specified start date in the request is invalid
1230	Issue No Missing	The request does not contain an issue number
1231	Issue No Invalid	The specified issue number in the request is invalid
1235	Card Reference Invalid	The specified card reference in the request is not valid
1236	Card Hash Invalid	The specified card hash in the request is not valid
1240	Amount Missing	The request does not contain an amount
1241	Amount Invalid	The specified amount in the request is invalid
1242	Amount Too Small	The specified amount in the request is too small
1243	Amount Too Large	The specified amount in the request is too large
1250	Message Type Missing	The request does not contain a message type
1251	Message Type Invalid	The specified message type in the request is invalid
2001	Terminal ID Missing	The request does not contain a terminal ID
2002	Terminal ID Unknown	The specified terminal ID in the request is unknown
2003	Terminal ID Invalid	The specified terminal ID in the request is invalid
2004	Terminal ID Disabled	The specified terminal ID in the request is disabled
2005	Terminal Usage Exceeded	The specified terminal ID usage in the request has been exceeded
2021	Transaction Key Missing	The specified transaction key in the request is missing
2022	Transaction Key Invalid	The specified transaction key in the request is invalid
2023	Transaction Key Incorrect	The specified transaction key in the request is incorrect
2100	CardEase Reference Missing	The request does not contain a CardEase Reference
2101	CardEase Reference Invalid	The specified CardEase Reference in the request is invalid
2110	Card Details Unavailable	The card details referenced by the Card Reference and Card Hash are unavailable
2111	Card Details Not Found	The card details referenced by the Card Reference and Card Hash could not be found
2200	Transaction Not Found	The specified transaction in the request was not found
2201	Transaction Already Settled	The specified transaction in the request has already been settled
2202	Transaction Already Voided	The specified transaction in the request has already been voided
2203	Transaction Already Refunded	The transaction has already been refunded in full
2204	Transaction Originally Declined	The specified transaction in the request was originally declined
7000	Temporarily Unavailable	The CardEase platform is temporarily unavailable
8001	Invalid XML Request	The request XML is invalid
8002	Invalid Message Type	The specified request type is invalid
8003	XML Element Missing	The request does not contain all of the expected XML elements
8004	Invalid Data	An invalid piece of information was sent in the request
8005	XML Decryption Error	It is not possible to decrypt the XML

14.3 Issuer Decline Codes

Response	Description
01	Declined - Call Issuer
01A	Declined – Limits reached, PIN required
04	Declined - Pick Up Card
05	Declined - Do Not Honor
10	Declined - Partial Approval
12	Declined - Invalid Transaction
13	Declined - Card Amount Invalid
14	Declined - Card Number Invalid
15	Declined - No Such Issuer
19	Declined - Re-Enter
51	Declined - Insufficient Funds
54	Declined - Card Expired
55	Declined - Wrong PIN Entered by Card Holder
57	Declined - Service Not Allowed
61	Declined - Customer Exceeds Withdrawal Limit
62	Declined - Restricted SIC Code
63	Declined - Restricted
65	Declined - Customer Exceeds Activity Limit, PIN required
70	Declined - PIN data required Applies for Visa.
78	Declined - No Account
97	Declined - CVV MisMatch

15. End-of-life

This marking shown on the product or its literature, indicates that it should not be disposed with other household wastes at the end of its working life. To prevent possible harm to the environment or human health from uncontrolled waste disposal, separate this from other types of wastes and recycle it responsibly to promote the sustainable reuse of material resources. In doing so, recycle as many components as possible and dispose of hazardous materials in a professional manner. Any cryptographic components should be erased securely and completely.



16. Declaration of Conformity

Manufacturer Name: Payter B.V.
Manufacturer Address: Rozenlaan 115
3051LP Rotterdam
The Netherlands

Hereby declares that the products,

Product Name: Apollo, ApolloMax
Product Description: Contactless Payment Terminal
Product Model Number(s):APO01.XX.PAY V1-X, APM01.XX.PAY V1-X
Product Model Options: All

Is in conformity with the essential requirements of the Radio Equipment Directive (RED) 2014/53/EU,
in accordance with the listed Safety, EMC and Radio Spectrum standards:

Low Voltage Directive 2014/35/EU, covering requirements of RED art. 3.1(a)

- EN 62368-1:2014/AC:2015
- EN 60950-22:2006/AC:2008
- EN 62311:2008

EMC Directive 2014/30/EU, covering requirements of RED art. 3.1(b)

- EN 301 489-1 V1.9.2
- EN 301 489-3 V2.1.1
- EN 301 489-17 V1.3.1
- EN 301 489-19 V2.1.1
- EN 301 489-52 v1.1.0

Radio Spectrum Matters, covering requirements of RED art. 3.2

- EN 300 330 V2.1.1
- EN 300 328 V2.2.2
- EN 301 511 V12.5.1
- EN 301 908-1 V13.1.1
- EN 301 908-2 V13.1.1
- EN 301 908-13 V13.1.1
- EN 303 413 V1.1.1

17. FCC

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.

FCC ID: 2AHPPAPX01 - Terminal

Contains:
FCC ID: VPYLB1DX - WiFi, Bluetooth Module

Contains optionally:
FCC ID: N7NRC76B - LTE/GNSS modem

Note

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Caution

Changes or modifications made to this equipment not expressly approved by Payter BV may void the FCC authorization to operate this equipment.

This device does not contain any user serviceable parts, under no condition are modifications to this device allowed.

External Antenna

! External modem antennas should always be installed at least 20cm away from human body parts.

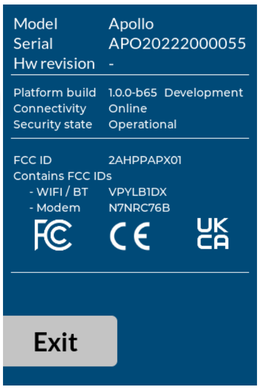
17.1 Radiofrequency radiation exposure Information:

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

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

17.2 Electronic Label

The electronic label is accessible from the main screen by tapping the screen at the top 5 times within 15 seconds.



Model	Apollo
Serial	APO20222000055
Hw revision	-
Platform build	1.0.0-b65 Development
Connectivity	Online
Security state	Operational
FCC ID	2AHPPAPX01
Contains FCC IDs	
- WIFI / BT	VPYLB1DX
- Modem	N7NRC76B

18. Family Letter

DECLARATION OF CONFORMITY (DoC)

Manufacturer Name:	Payter B.V.
Manufacturer Address:	Rozenlaan 115 3051LP Rotterdam The Netherlands

Hereby declares that the following products constitute a family. They share the same hardware and software platform; including but not limited to all EMV L1, L2 and payment application modules.

Product Descriptions:	Cashless Payment terminal
Product Model Number(s):	APO01.XX.XXX V1-X APM01.XX.XXX V1-X
Product Model Options:	All

Any changes to the last digits of the product reference (e.g. APO01.XX.XXX) reflect only minor variation which do not create any regression and do not affect even partially any of the tested items. Where X is a place holder for product features that do not impact the further functionality of the device, e.g. the presence of a modem, colour of device or custom branding options. All models share the same EMV L1 and kernel modules as listed below.

Contactless		
EMV CL L1	APO-PCD.1.0	16960 0320 300 30a 30a CETI
Mastercard	CL_PayPass 3.3.85	TLOA-PTER200301-200424(a)
Visa	CL_Visa V3.0.39	CDPYTR01826
Contact		
EMV CT L1	APO-IFM.1.0	17367 0521 430 43c 43c CETI
EMV CT L2	EMVLib Version 3.5.50	2-04848-1-1C-CETI-0721-4.3j 2-04848-1-1OS-CETI-0721-4.3j

19. REACH/RoHS-3 Certificate of Compliance

Restriction of the use of certain Hazardous Substances
Registration, Evaluation, Authorisation and restriction of Chemicals

Manufacturer Name:	Payter B.V.
Manufacturer Address:	Rozenlaan 115 3051LP Rotterdam The Netherlands

Hereby declares that the products,

Document status	Released	Product Descriptions:	Cashless Payment terminal
Date	June 2022	Product Model Number(s):	APO01.XX.XXX V1-X APM01.XX.XXX V1-X
Document ID	PTR-00-03-PP-P-0006-01	Product Model Options:	All

EC Directive 2015/863/EU restricts the use of the hazardous substances listed below in electrical and electronic equipment. The products listed conform to European Commission Directive 2015/863/EU as of the date hereof and does not intentionally contain more than the Maximum Limit.

Substance	Maximum Limit (ppm)
Cadmium (Cd):	< 100 ppm
Lead (Pb):	< 1000 ppm
Mercury (Hg):	< 1000 ppm
Hexavalent Chromium: (Cr VI)	< 1000 ppm
Polybrominated Biphenyls (PBB):	< 1000 ppm
Polybrominated Diphenyl Ethers (PBDE):	< 1000 ppm
Bis(2-Ethylhexyl) phthalate (DEHP):	< 1000 ppm
Benzyl butyl phthalate (BBP):	< 1000 ppm
Dibutyl phthalate (DBP):	< 1000 ppm
Diisobutyl phthalate (DIBP):	< 1000 ppm

Based on the information provided by our suppliers, and to the best of our knowledge, Payter B.V. designates that Payter B.V. listed products are RoHS Compliant and conform to the European Union Restrictions of the use of Hazardous Substances. This information is subject to change and if a change occurs which affects compliance then this Statement will be updated. Payter's information on SVHC's in articles is currently based on the European Chemicals Agency (ECHA) 'Guidance on requirements for substances in articles'. The REACH SVHC declaration statement is related to the substances on the most recent Candidate list. If this statement reports REACH Candidate List substance present in an article > 0.1%, unless specified otherwise, these substances do not pose any risk if the article is used as intended (including disposal). Additional information is not necessary to allow safe use of the article.

For these purposes, REACH/RoHS compliant means that:

1. Our suppliers have confirmed the compliance status of the relevant products to us.
2. We have implemented processes to confirm suppliers' statements and maintain relevant documents to support this.

To the best of our knowledge, none of our suppliers use these banned substances to manufacture their products. Our statements in this letter regarding RoHS compliance and lead content do not extend to, or apply to any product subjected to unintended contamination, misuse, neglect, accident, or improper installation. Product does not contain listed substances exceeding the threshold according to Regulatory List REACH-SVHC / EU REACH SVHC - 1907/2006/EC : 2020-01-16.