Paygate P2PE v3.0 Solution with CCV Deutschland GmbH Hardware Terminals

VERSION: 3.0

DATE: 09.2023

1. P2PE Solution Information and Solution Provider Contact Details

1.1 P2PE Solution Information

Solution name:	paygate
Solution reference number per PCI SSC website:	2023-00999.007

1.2 Solution Provider Contact Information

Company name:	Computop Paygate GmbH
Company address:	Schwarzenbergstrasse 4, 96050 Bamberg, Germany
Company URL:	www.computop.com
Contact name:	Stephan Kueck
Contact phone number:	+49 951 9800960
Contact e-mail address:	info@computop.com

P2PE and PCI DSS

Merchants using this P2PE solution may be required to validate PCI DSS compliance and should be aware of their applicable PCI DSS requirements. Merchants should contact their acquirer or payment brands to determine their PCI DSS validation requirements.

2. Confirm Devices were not tampered with and confirm the identity of any third-party personnel

2.1 Instructions for ensuring POI devices originate from trusted sites/locations only.

Each P2PE device will be shipped by Computop's field Service.

Computop has two field service suppliers.

Field service - Europe:

CCV Deutschland GmbH
Gewerbering 1
84072 Au in der Hallertau
phone: +49-951-9800939
e-mail: helpdesk@computop.de

Only packages from these addresses are trusted senders for this solution.

The Merchant must ensure that only packages from them are used for operation and processing.

2.2 Instructions for confirming POI device and packaging were not tampered with, and for establishing secure, confirmed communications with the solution provider.

Devices will be set up and packet in P2PE certified area by Computop's field service.

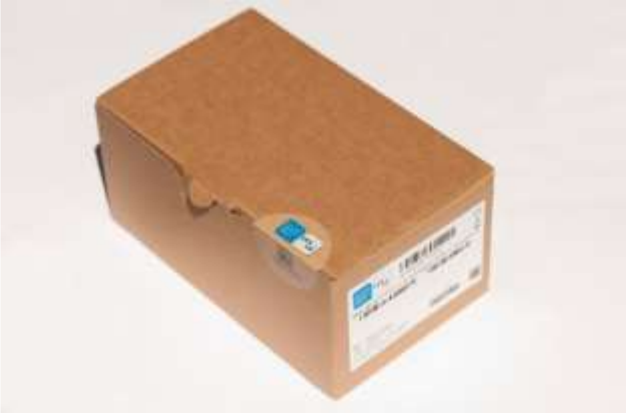
Before shipment package will be secured by a special package seal. After leaving the storage P2PE merchant will be informed about the dispatch of the package.

Once merchant gets the package he must check if everything is ok with the carton and especially with safety seal.

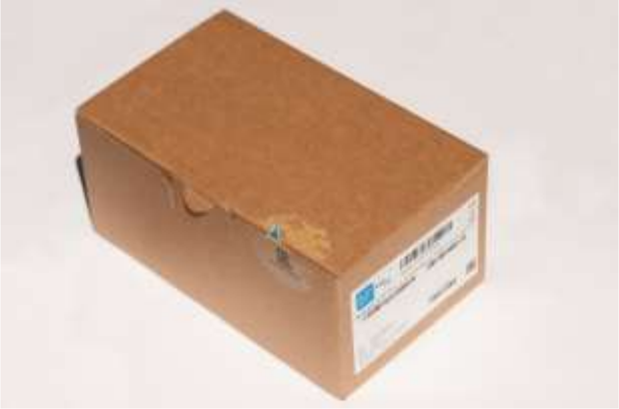
If everything is fine Merchant can unpack the device and can use it if seal on the device itself is fine as well. *(Please see section 9.2 for this as well)*

If not, he has to inform Computop by contact details displayed in *section 9.1*. In that case Merchant is not allowed to use the device and has to wait for instructions because the terminal can be tampered.

Example unbroken seal:



Example broken seal:



Physically secure POI devices in your possession, including devices:

- Awaiting deployment
- Undergoing repair or otherwise not in use
- Waiting transport between sites/locations

2.3 Instructions to confirm the business need for, and identities of, any third-party personnel claiming to be support or repair personnel, prior to granting those personnel access to POI devices.

The Merchant may only allow third parties to provide support or similar services on the P2PE device if they have been authorized to do so.

This must be proven by an authorization between the solution provider and the third party.

Otherwise, access to the terminal must be denied by the Merchant. Furthermore, the Merchant is obliged to inform the solution provider about the situation and the possible manipulation attempt.

3. Approved POI Devices, Applications/Software, and the Merchant Inventory

3.1 POI Device Details

The following information lists the details of the PCI-approved POI devices approved for use in this P2PE solution.

All POI device information can be verified by visiting:
https://www.pcisecuritystandards.org/approved_companies_providers/approved_pin_transaction_security.php

See also Section 9.2, “Instructions for how to confirm hardware, firmware, and application versions on POI devices.”

PCI PTS approval #:	POI device vendor:	POI device model name and number:	Hardware version #(s):	Firmware version #(s):
4-30210	PAX Computer Technology (Shenzhen) Co Ltd	Q80 (Base Next)	Q80-xxx-ax4-1xxx Q80-xxx-ax4-0xxx	14.00.xx xxxx, 14.01.xx xxxx
4-30272	PAX Computer Technology (Shenzhen) Co Ltd	Q30 (CCV Pad Next)	Q30-xxx-Rx5-0xxx (w/ CTLS) Q30-xxx-0x5-0xxx (w/o CTLS) Q30-xxx-Rx5-1xxx (w/ CTLS) Q30-xxx-0x5-1xxx (w/o CTLS)	15.00.xx xxxx
4-30159	PAX Computer Technology (Shenzhen) Co Ltd	S920, S920 L (CCV Mobile Premium)	S920-xxx-xx4-0xxx S920-xxx-xx4-1xxx S920-xxx-xx4-2xxx S920-xxx-xx4-Axxx S920-xxx-xx4-3xxx S920-xxx-xx4-Jxxx	Prolin OS: 14.00.xx, Prolin Boot: 2.0.x, Prolin OS: 14.01.xx xxxx, Prolin OS: 14.03.xx xxxx, Prolin Boot: 3.x.xx.xxxx
4-30224	PAX Computer Technology (Shenzhen) Co Ltd	S300 (CCV Pad)	S300-xxx-0x4-0xxx (w/o CTLS) S300-xxx-3x4-0xxx (with CTLS)	14.01.xx xxxx
4-40094	PAX Computer Technology (Shenzhen) Co Ltd	S300 (CCV Pad)*	S300-abo-dx3-0xxx (where a=0, M b=0, G, C, T, W, E c=0, L, A and D=0, 3)	SRED (CTLS): Prolin 21.3xx.xxx.xxx.1xx (Boot 1.0.0 PED 001), 3.02.xx

4-30134	PAX Computer Technology (Shenzhen) Co Ltd	D200 Fly (CCV Fly)*	D200-xxx-xx3-1xxx	SRED (CTLS): 13.02.xx, 13.03.xx
4-40215	PAX Computer Technology (Shenzhen) Co Ltd	A920	A920-xxx-0x5-0xxx, A920-xxx-Rx5-0xxx A920-xxx-0x5-1xxx A920-xxx-Rx5-1xxx A920-xxx-0x5-2xxx A920-xxx-Rx5-2xxx A920-xxx-Rx5-3xxx	25.00.xxxx, 25.01.xxxx, 25.03.xxxx
4-40269	PAX Computer Technology (Shenzhen) Co Ltd	A77	A77-xxx-Rx5-2xxx	25.02.xxxx

**Discontinued. Remaining stocks will continue to be operated. Product is no longer sold.*

3.2 POI Software/Application Details

The following information lists the details of all software/applications (both P2PE applications and P2PE non-payment software) on POI devices used in this P2PE solution.

All applications with access to clear-text account data must be reviewed according to Domain 2 and are included in the P2PE solution listing. These applications may also be optionally included in the PCI P2PE list of Validated P2PE Applications list at vendor or solution provider discretion.

Application Vendor, Name, and Version #	POI Device Vendor	POI Device Model Name(s) and Number:	POI Device Hardware & Firmware Version #	Is Application PCI Listed? (Y/N)	Does Application Have Access to Clear-text Account Data (Y/N)
APAS PIN Pad 0023.09.02	PAX Computer Technology (Shenzhen) Co Ltd	Q80 (Base Next)	Q80-xxx-ax4-1xxx Q80-xxx-ax4-0xxx 14.00.xx xxxx, 14.01.xx xxxx	N	N
APAS PIN Pad 0024.31.02	PAX Computer Technology (Shenzhen) Co Ltd	Q80 (Base Next)	Q80-xxx-ax4-1xxx Q80-xxx-ax4-0xxx 14.00.xx xxxx, 14.01.xx xxxx	N	N
APAS PIN Pad	PAX Computer Technology	Q80 (Base Next)	Q80-xxx-ax4-1xxx Q80-xxx-ax4-0xxx	N	N

3.2 POI Software/Application Details

0025.15.01	(Shenzhen) Co Ltd		14.00.xx xxxx, 14.01.xx xxxx		
APAS PIN Pad 0023.09.02	PAX Computer Technology (Shenzhen) Co Ltd	Q30 (Pad Next)	Q30-xxx-Rx5-0xxx (w/ CTLS) Q30-xxx-0x5-0xxx (w/o CTLS) Q30-xxx-Rx5-1xxx (w/ CTLS) Q30-xxx-0x5-1xxx (w/o CTLS)15.00.xx xxxx	N	N
APAS PIN Pad 0024.20.01	PAX Computer Technology (Shenzhen) Co Ltd	Q30 (Pad Next)	Q30-xxx-Rx5-0xxx (w/ CTLS) Q30-xxx-0x5-0xxx (w/o CTLS) Q30-xxx-Rx5-1xxx (w/ CTLS) Q30-xxx-0x5-1xxx (w/o CTLS)15.00.xx xxxx	N	N
APAS PIN Pad 0025.15.01	PAX Computer Technology (Shenzhen) Co Ltd	Q30 (Pad Next)	Q30-xxx-Rx5-0xxx (w/ CTLS) Q30-xxx-0x5-0xxx (w/o CTLS) Q30-xxx-Rx5-1xxx (w/ CTLS) Q30-xxx-0x5-1xxx (w/o CTLS)15.00.xx xxxx	N	N
APAS PIN Pad 0021.15.01	PAX Computer Technology (Shenzhen) Co Ltd	S920, S920 L (CCV Mobile Premium)	S920-xxx-xx4-0xxx S920-xxx-xx4-1xxx S920-xxx-xx4-2xxx S920-xxx-xx4-Axxx S920-xxx-xx4-3xxx S920-xxx-xx4-Jxxx Prolin OS: 14.00.xx, Prolin Boot: 2.0.x, Prolin OS: 14.01.xx xxxx, Prolin OS: 14.03.xx xxxx, Prolin Boot: 3.x.xx.xxxx	N	N
APAS PIN Pad 0023.24.01	PAX Computer Technology (Shenzhen) Co Ltd	S920, S920 L (CCV Mobile Premium)	S920-xxx-xx4-0xxx S920-xxx-xx4-1xxx S920-xxx-xx4-2xxx	N	N

3.2 POI Software/Application Details					
			S920-xxx-xx4-Axxx S920-xxx-xx4-3xxx S920-xxx-xx4-Jxxx Prolin OS: 14.00.xx, Prolin Boot: 2.0.x, Prolin OS: 14.01.xx xxxx, Prolin OS: 14.03.xx xxxx, Prolin Boot: 3.x.xx.xxxx		
APAS PIN Pad 0025.15.01	PAX Computer Technology (Shenzhen) Co Ltd	S920, S920 L (CCV Mobile Premium)	S920-xxx-xx4-0xxx S920-xxx-xx4-1xxx S920-xxx-xx4-2xxx S920-xxx-xx4-Axxx S920-xxx-xx4-3xxx S920-xxx-xx4-Jxxx Prolin OS: 14.00.xx, Prolin Boot: 2.0.x, Prolin OS: 14.01.xx xxxx, Prolin OS: 14.03.xx xxxx, Prolin Boot: 3.x.xx.xxxx	N	N
APAS PIN Pad 0019.07.02	PAX Computer Technology (Shenzhen) Co Ltd	S300 (CCV Pad)	S300-xxx-0x4-0xxx (w/o CTLS), S300-xxx-3x4-0xxx (with CTLS) 14.01.xx xxxx	N	N
APAS PIN Pad 0021.14.01	PAX Computer Technology (Shenzhen) Co Ltd	S300 (CCV Pad)	S300-xxx-0x4-0xxx (w/o CTLS), S300-xxx-3x4-0xxx (with CTLS) 14.01.xx xxxx	N	N
APAS PIN Pad 0024.31.02	PAX Computer Technology (Shenzhen) Co Ltd	S300 (CCV Pad)	S300-xxx-0x4-0xxx (w/o CTLS), S300-xxx-3x4-0xxx (with CTLS) 14.01.xx xxxx	N	N
APAS PIN Pad 0025.15.01	PAX Computer Technology (Shenzhen) Co Ltd	S300 (CCV Pad)	S300-xxx-0x4-0xxx (w/o CTLS), S300-xxx-3x4-0xxx (with CTLS) 14.01.xx xxxx	N	N
APAS PIN Pad 0019.07.02	PAX Computer Technology (Shenzhen) Co Ltd	S300 (CCV Pad)*	S300-abo-dx3-0xxx SRED (CTLS): Prolin 21.3xx.xxx.xxx.1xx (Boot 1.0.0 PED 001), 3.02.xx	N	N

3.2 POI Software/Application Details

APAS PIN Pad 0021.14.01	PAX Computer Technology (Shenzhen) Co Ltd	S300 (CCV Pad)*	S300-abo-dx3-0xxx SRED (CTLS): Prolin 21.3xx.xxx.xxx.1xx (Boot 1.0.0 PED 001), 3.02.xx	N	N
APAS PIN Pad 0024.31.02	PAX Computer Technology (Shenzhen) Co Ltd	S300 (CCV Pad)*	S300-abo-dx3-0xxx SRED (CTLS): Prolin 21.3xx.xxx.xxx.1xx (Boot 1.0.0 PED 001), 3.02.xx	N	N
APAS PIN Pad 0025.15.01	PAX Computer Technology (Shenzhen) Co Ltd	S300 (CCV Pad)*	S300-abo-dx3-0xxx SRED (CTLS): Prolin 21.3xx.xxx.xxx.1xx (Boot 1.0.0 PED 001), 3.02.xx	N	N
APAS PIN Pad 0019.10.05	PAX Computer Technology (Shenzhen) Co Ltd	D200 Fly (CCV Fly)*	D200-xxx-xx3-1xxx SRED (CTLS): 13.02.xx, 13.03.xx	N	N
APAS PIN Pad 0025.15.01	PAX Computer Technology (Shenzhen) Co Ltd	A920	A920-xxx-0x5-0xxx, A920-xxx-Rx5-0xxx A920-xxx-0x5-1xxx A920-xxx-Rx5-1xxx A920-xxx-0x5-2xxx A920-xxx-Rx5-2xxx A920-xxx-Rx5-3xxx 25.00.xxxx, 25.01.xxxx, 25.03.xxxx	N	N
APAS PIN Pad 0025.15.01	PAX Computer Technology (Shenzhen) Co Ltd	A77	A77-xxx-Rx5-2xxx 25.02.xxxx	N	N
SEC CCVCTP.v0016.xx.xx	PAX Computer Technology (Shenzhen) Co Ltd	Q80 (Base Next)	Q80-xxx-ax4-1xxx Q80-xxx-ax4-0xxx 14.00.xx xxxx, 14.01.xx xxxx	Y	Y
SEC CCVCTP.v0016.xx.xx	PAX Computer Technology (Shenzhen) Co Ltd	Q30 (Pad Next)	Q30-xxx-Rx5-0xxx (w/ CTLS) Q30-xxx-0x5-0xxx (w/o CTLS) Q30-xxx-Rx5-1xxx (w/ CTLS)	Y	Y

3.2 POI Software/Application Details

			Q30-xxx-0x5-1xxx (w/o CTLS)15.00.xx xxxx		
SEC CCVCTP.v0 016.xx.xx	PAX Computer Technology (Shenzhen) Co Ltd	S920, S920 L (CCV Mobile Premium)	S920-xxx-xx4-0xxx S920-xxx-xx4-1xxx S920-xxx-xx4-2xxx S920-xxx-xx4-Axxx S920-xxx-xx4-3xxx S920-xxx-xx4-Jxxx Prolin OS: 14.00.xx, Prolin Boot: 2.0.x, Prolin OS: 14.01.xx xxxx, Prolin OS: 14.03.xx xxxx, Prolin Boot: 3.x.xx.xxxx	Y	Y
SEC CCVCTP.v0 016.xx.xx	PAX Computer Technology (Shenzhen) Co Ltd	S300 (CCV Pad)	S300-xxx-0x4-0xxx (w/o CTLS), S300-xxx-3x4-0xxx (with CTLS) 14.01.xx xxxx	Y	Y
SEC CCVCTP.v0 016.xx.xx	PAX Computer Technology (Shenzhen) Co Ltd	S300 (CCV Pad)*	S300-abo-dx3-0xxx SRED (CTLS): Prolin 21.3xx.xxx.xxx.1xx (Boot 1.0.0 PED 001), 3.02.xx	Y	Y
SEC CCVCTP.v0 016.xx.xx	PAX Computer Technology (Shenzhen) Co Ltd	D200 Fly (CCV Fly)*	D200-xxx-xx3-1xxx SRED (CTLS): 13.02.xx, 13.03.xx	Y	Y
SEC CCVCTP.v0 017.xx.xx	PAX Computer Technology (Shenzhen) Co Ltd	A920	A920-xxx-0x5-0xxx, A920-xxx-Rx5-0xxx A920-xxx-0x5-1xxx A920-xxx-Rx5-1xxx A920-xxx-0x5-2xxx A920-xxx-Rx5-2xxx A920-xxx-Rx5-3xxx 25.00.xxxx, 25.01.xxxx, 25.03.xxxx	Y	Y
SEC CCVCTP.v0 017.xx.xx	PAX Computer Technology (Shenzhen) Co Ltd	A77	A77-xxx-Rx5-2xxx 25.02.xxxx	Y	Y

**Discontinued. Remaining stocks will continue to be operated. Product is no longer sold.*

3.3 POI Inventory & Monitoring

- All POI devices must be documented via inventory control and monitoring procedures, including device status (deployed, awaiting deployment, undergoing repair or otherwise not in use, or in transit).
- This inventory must be performed annually, at a minimum.
- Any variances in inventory, including missing or substituted POI devices, must be reported to *Computop Paygate GmbH* via the contact information in Section 9.1.
- Sample inventory table below is for illustrative purposes only. The actual inventory should be captured and maintained by the merchant in an external document.

As a user of our P2PE solution you must maintain a device tracking system to identify and locate all devices including where these devices are:

- Device vendor: CCV Deutschland GmbH
- Device model name and number: Base Next, Pad Next, CCV Mobile Premium, CCV Pad, CCV Fly, A920, A77
- Device location: Store xyz, 12345 Long St., Sometown, Someplace
- Device status:
  - Device deployed (The device is in use by you in your shop)
  - Awaiting deployment (The device is delivered to you, ready to use, but not yet deployed to production)
  - Undergoing repair or otherwise not in use (The device is down, being repaired at your site, prepared for shipment to the vendor, or retired)
  - In transit (The device is shipped back to the vendor for repair or replacement)
- Serial Number (SN, the SN is displayed in the startup screen of the terminal, see picture in *section 9.2*) or other unique identify, such as the terminal ID.
- You may also want to add the weight of each device to be able to meet requirements for regular monitoring more easily.

A sample inventory table is provided for your reference below.

Sample Inventory Table

Device Vendor	Device Model Name(s) and Number	Device Location	Device Status	Serial Number or Other Unique Identifier	Date of Inventory

4. POI Device Installation Instructions

Do not connect non-approved cardholder data capture devices.

The P2PE solution is approved to include specific PCI-approved POI devices. Only these devices denoted above in Table 3.1 are allowed for cardholder data capture.

If a merchant's PCI-approved POI device is connected to a data capture mechanism that is not PCI approved, (for example, if a PCI-approved SCR was connected to a keypad that was not PCI-approved):

- The use of such mechanisms to collect PCI payment-card data could mean that more PCI DSS requirements are now applicable for the merchant.
- Only P2PE approved capture mechanisms as designated on PCI's list of Validated P2PE Solutions and in the PIM can be used.

Do not change or attempt to change device configurations or settings.

Changing device configurations or settings may invalidate the PCI-approved P2PE solution in its entirety. Examples include, but are not limited to:

- Enabling any device interfaces or data-capture mechanisms that were disabled on the P2PE solution POI device.
- Altering security configurations or authentication controls on the POI device.
- Physically opening the POI device.
- Attempting to install unauthorized applications onto the POI device.

4.1 Installation and connection instructions

Please follow the instruction of the *Computop Quick Start Guide*. For Hardware information please use the *CCV Handbook*.

***Note:** Only PCI-approved POI devices listed in the PIM are allowed for use in the P2PE solution for account data capture.*

4.2 Guidance for selecting appropriate locations for deployed devices

As a user of our P2PE solution you must select appropriate locations for deployed devices. You must restrict public access to the device to only parts of the device and for the time that a person is expected to use to complete a transaction.

The device should always be placed in an area of the staff, for example, next to the cash register.

The customers must access the PIN Pad, the magnetic stripe and/or chip reader and the signature capture pen to complete a transaction.

Place the device in an area that deters compromise attempts - for example, appropriate ligthning, access paths, visible security measures, etc.

place devices so they can be observed/monitored by authorized personnel—for example, during daily store checks of the devices performed by store/security staff.

Authorized personnel should check the device on a daly base if it has indication of tampering or if the security labels are undamaged.

Mobile devices should always be carried by the staff. If devices have to be loaded or stored, this should be done in a lockable room or the devices should be secured - neraby the stuff - in such a way (e.g. kensigton lock or similar) that they cannot be stolen.

4.3 Guidance for physically securing deployed devices to prevent unauthorized removal or substitution

As a user of our P2PE solution you must physically secure deployed devices to prevent unauthorized removal or substitution.

Put the device in a holder or keep it under control of your employees all time to prevent unauthorized removal or substitution. The POI devices must be observed at all times.

POI devices not yet deployed or removed from service for repairs that are awating their shipment to the field service must be kept in a locked room.

In situations where the normally fixed devices are re-located temporarily, the following needs to be performed:

- The devices must be locked in a secure room when not in use
- An individual must be assigned the repoonsibility for the devices when they are in use.
- During their temporary deployment the devices must be observed at all times.

The devices need to be signed in and signed out of their storage location or their regular location to enable tracking of the device’s whereabouts.

5. POI Device Transit

5.1 Instructions for securing POI devices intended for, and during, transit

As a user of our P2PE solution you must store any POI device awaiting deployment or return shipment in a physically secure location. Keep the devices under lock and key, for example. Restrict the access to the devices to those persons who have a business need to access these devices.

Prior to returning a device to the field service, you must inform the field service that you are returning one or more devices. During this communication you will be provided with an RMA number to allow for tracking of the case. Contact details are displayed in *section 9.1*.

You must use secure and trackable transport method, such as bonded carrier or secure courier to transfer the terminals from one site to another or while returning to field service.

We recommend the use of DHL, UPS or FedEx.

You need to provide the tracking code of your courier service to the field service to allow tracking of the shipment.

Physically secure POI devices in your possession, including devices:

- Awaiting deployment
- Undergoing repair or otherwise not in use
- Waiting transport between sites/locations

5.2 Instructions for ensuring POI devices are shipped to, trusted sites/locations only

General:

All shipments must be made using a trackable method, such as a courier serivce.

Inbound shipments:

As a user of our P2PE solution you must only use devices received from the trusted sites. Trusted sites of the field service from which a device may be accepted for use are listed in *section 2.1* of this document.

In case you receive a device from an untrusted or unknown source location you have to verify the location the device was sent from. To verify a location please contact the field service with the contact details specified in *section 2.1*.

The field service uses e-mail to send shipping documents that can be used to validate device serial numbers. The documents used for validating device serial numbers are always sent via a separate communication channel and not with the device shipment. Tracking codes are also provided separately from the shipment via e-mail.

To detect unauthorized modification, substitution, or tampering of POI devices during transit, you need to verify the following after receipt of the device:

- Confirm that the tracking codes provided by the field services match the one of the shipment.

- Confirm that the tamper evident packing is not damaged or manipulated.
- Match the device serial number as displayed on the sticker at the bottom of the devices to the serial number documented by the sender (field service).

As a user of our P2PE solution you must not use the device unless and until the source location is verified as trusted.

Outbound shipments (return transport for repair, etc.)

All devices must be shipped to the location of the field service company as specified in *section 2.1*. This address will also be provided to you as part of the RMA process.

Tracking codes and the device serial numbers must be provided to the field service via e-mail in advance of the shipment.

6. POI Device Tamper & Modification Guidance

6.1 Instructions for physically inspecting POI devices and preventing skimming, including instructions and contact details for reporting any suspicious activity

Additional guidance for inspecting POI devices can be found in the document entitled *Skimming Prevention: Best Practices for Merchants,* available at www.pcisecuritystandards.org.

Inspections:

As a user of our P2PE solution you must perform periodic physical inspections of devices to detect tampering or modification. The following section describes how the physical inspection must be performed:

1. You must check all tamper detection mechanisms (see below for details)
2. You must verify that the device looks like it should look (see *section 9.2* for sample pictures)
3. You must check the device for missing or altered seals, missing screws, extraneous wiring, holes in the device, or the addition of labels or other covering material that could be used to mask damage from device tampering. (You should use the pictures in *section 2.1* for comparison)
4. You must weigh the device to verify that it has the same weight as it has when receipt. This is necessary to identify potential insertion of tapping mechanisms within device.

The physical inspection should be performed on regular basis. We recommend physical inspections on quarterly basis.

POI Devices in remote or unattended locations should be monitored via video surveillance or should be equipped with sensors to alert personnel in case of unauthorized modification or manipulation.

Tamper detection mechanisms:

- You must inspect the seal (sticker with label “sealed”) on the device (see picture in *section 2.2* of this document for comparison).
- *Section 9* shows pictures how the device should look like.
- If anything suspicious or signs of tampering or manipulation are detected, stop using the device immediately.
- Should any suspicious activity be identified, please contact the Field Service with the contact details specified in *section 2.1*. The field service will provide you with procedures to return and replace the device.

Provide the device serial number and/or the terminal ID to allow for easier identification and disabling of the device.

6.2 Instructions for responding to evidence of POI device tampering

As a user of our P2PE solution you must follow the response procedures described below:

Inspect the device packing upon receipt of the device. If the packaging shows signs of manipulation or tampering or if you suspect the device has been tamperd with while being deployed, stop using the device immediately. Contact the field service immediately to report the tampering. The field service will provide further instructions after reporting the tampering.

Contact data for reporting of compromises and for returning of devices is provided in *section 2.1* of this document.

6.3 Instructions for physically inspecting or support by third-parties

As a user of our P2PE solution you may only allow third parties to provide support or similar services on the P2PE device if they have been authorized to do so.

This must be proven by an authorization between the solution provider and the third party.

Otherwise, access to the terminal must be denied by the Merchant. Furthermore, the Merchant is obliged to inform the solution provider about the situation and the possible manipulation attempt.

7. Device Encryption Issues

7.1 Instructions for responding to POI device encryption failures

As a user of our P2PE solution you must follow the instructions below in the event of a device encryption failure:

- You must ensure that devices are not re-enabled for use before the P2PE-encryption has been restored and reenabled.
- In any case, the devices must be checked by field service.
- Contact the field service immediately. Contact details are available in *section 2.1*.
- At this time, the devices in use cannot be configured to send plain text data, no opt-out process exists.

The following troubleshooting process has been established for your convenience:

- Troubleshooting is only done at the field service.
- You must return the devices to the field service for troubleshooting. Contact the field service via e-mail to request a RMA ID.
- Follow the instructions of the field service.

8. POI Device Troubleshooting

8.1 Instructions for troubleshooting a POI device

For your convenience, all trouble shooting will be performed by the field service.

To initiate the trouble shooting process, please perform the following:

You must send the devices to the field service for troubleshooting. You must contact the field service via e-mail to request a RMA ID. Please follow the instructions of the field service and return it to them. You must send needed information via e-mail to field service prior to sending the device. It is not allowed to return devices without RMA ID.

Contact details are listed in section 2.1 of this document.

By following the troubleshooting process, the field service ensures that:

- PAN and/or SAD is never output to the merchant environment,
- Collection of PAN and/or SAD only when needed to solve a specific problem
- Storage of such data only in specific, known locations with limited access
- Collection of only a limited amount of data needed to solve a specific problem
- Encryption of account data while stored

Secure deletion of such data immediately after use

9. Additional Guidance

9.1 Instructions for troubleshooting a POI device

For assistance with your P2PE solution device please have a view on the Computop quick start guide via

https://computop.com/fileadmin/user_upload/Landing-Pages/Pim/Computop_Quick_Start_Guide_POS_CCV_english.pdf

or get in contact with our helpdesk team via e-mail: *helpdesk@computop.de* or phone: *+49-951-9800939*

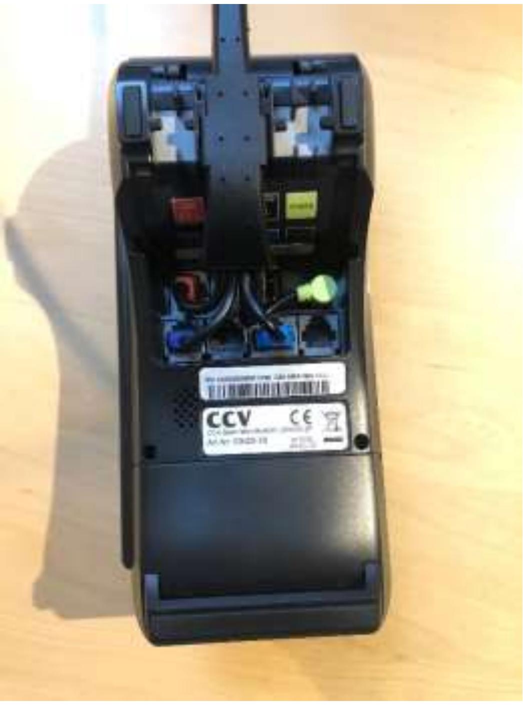
9.2 Instructions for how to confirm hardware, firmware, and application versions on POI devices

In the following reader label, security seal and the software version will be described for each type of solution device.

Device – Base Next

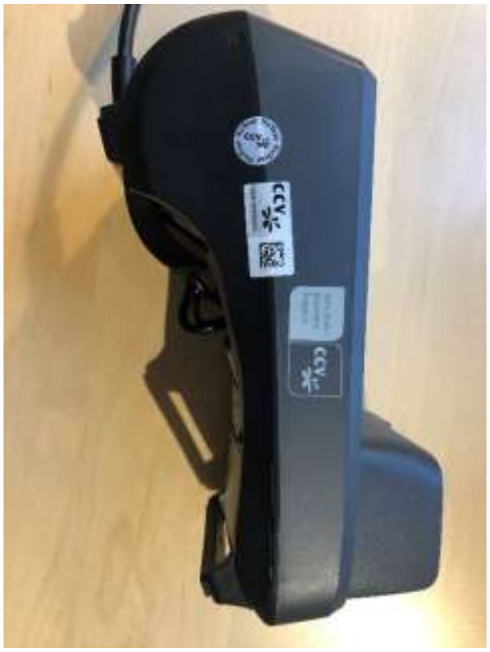
Reader label

Reader label with serial number (A030252980810160), product number (03025-29) and hardware version (Q80-MBA-R84-14LU) on back side



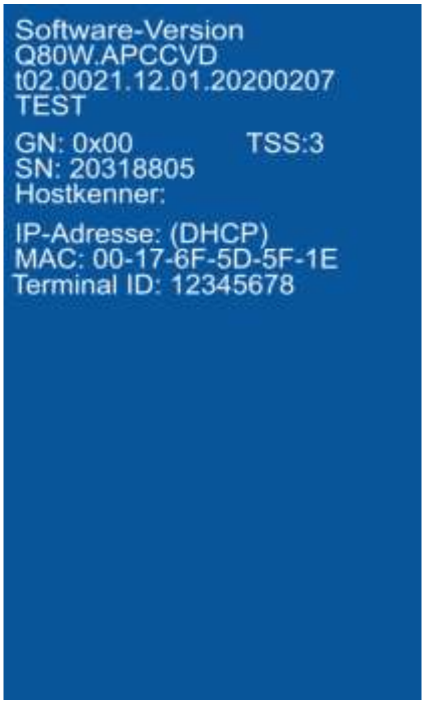
Security seal

Security seal on the device.



Software version

Example startup screen with serial number (20318805) and software version (Q80W.APCCVD t02.0021.12.01.20200207)

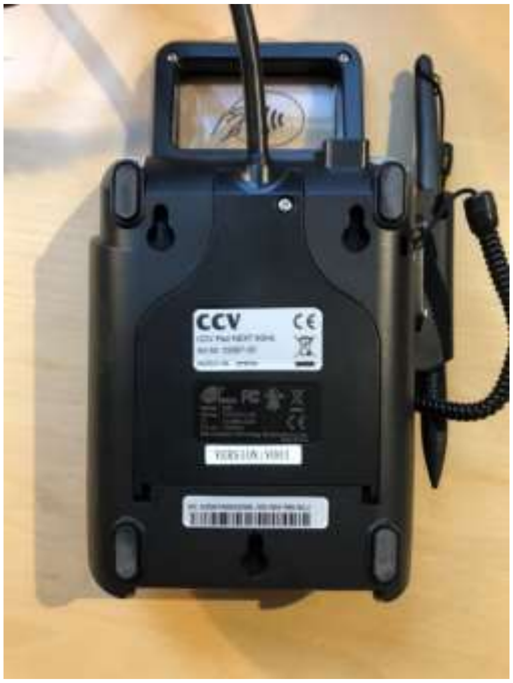


```
Software-Version
Q80W.APCCVD
t02.0021.12.01.20200207
TEST
GN: 0x00          TSS:3
SN: 20318805
Hostkenner:
IP-Adresse: (DHCP)
MAC: 00-17-6F-5D-5F-1E
Terminal ID: 12345678
```

Device – Pad Next

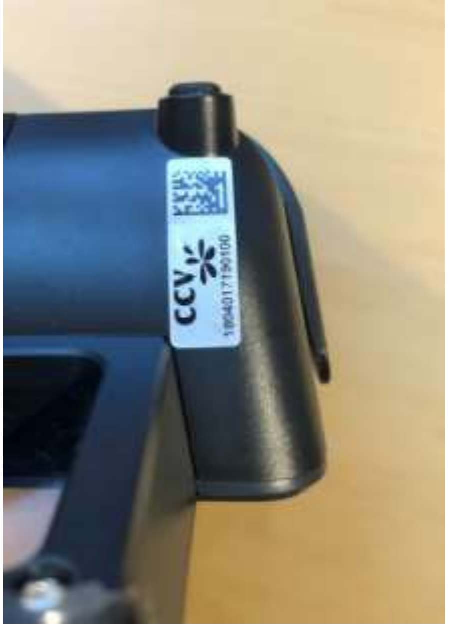
Reader label

Reader label with serial number (A033573080302585), product number (003357-30) and hardware version (Q30-0BW-R85-06LU) on back side



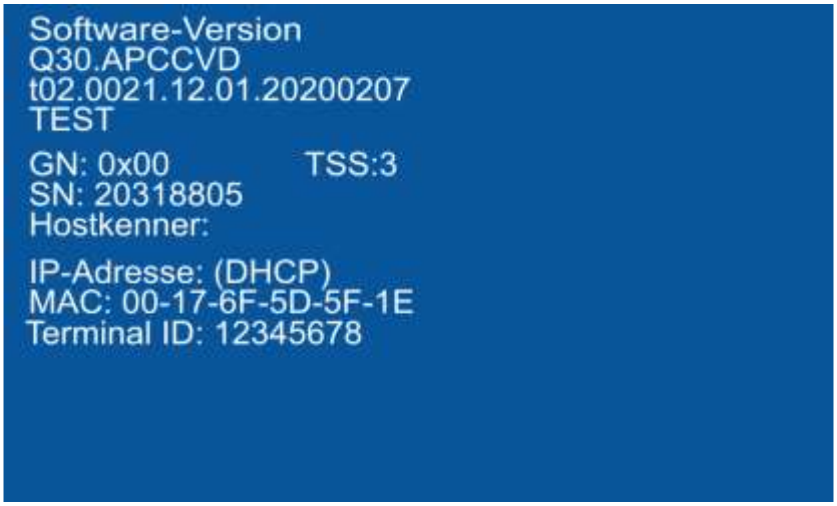
Security seal

Security seal on the device.



Software version

Example startup screen with serial number (20318805) and software version (Q30.APCCVD t02.0021.12.01.20200207)

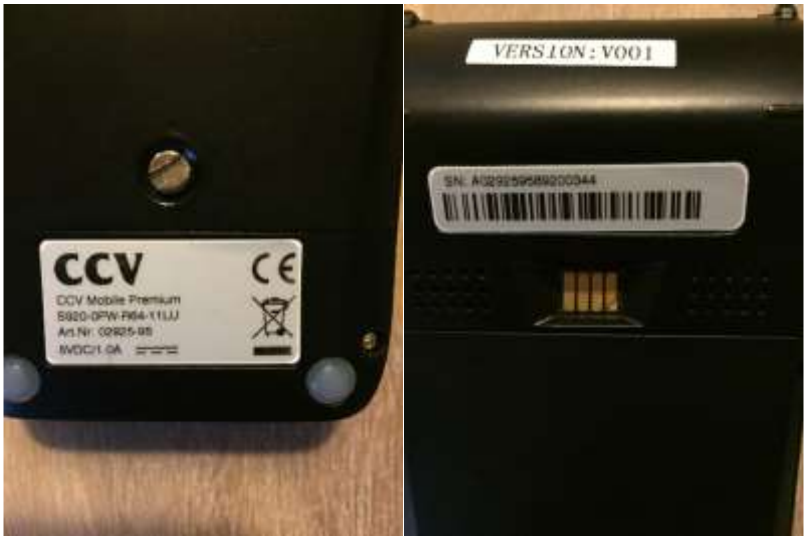


```
Software-Version
Q30.APCCVD
t02.0021.12.01.20200207
TEST
GN: 0x00           TSS:3
SN: 20318805
Hostkenner:
IP-Adresse: (DHCP)
MAC: 00-17-6F-5D-5F-1E
Terminal ID: 12345678
```

Device – CCV Mobile Premium

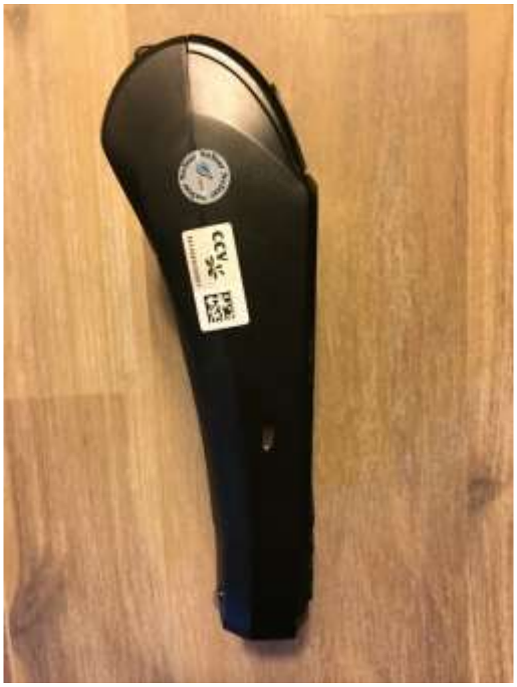
Reader label

Reader label with serial number (A029259589200344), product number (02925-95) and hardware version (S920-OPW-R63-11LU) on back side



Security seal

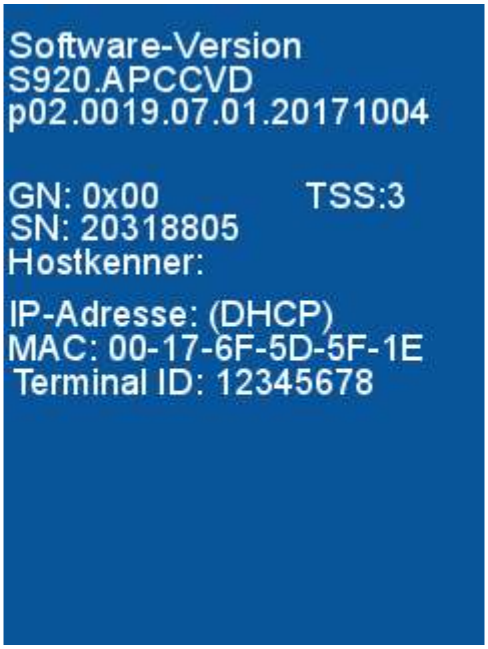
Security seal on the device.



E

Software version

Example startup screen with serial number (20318805) and software version (S920.APCCVD p02.0019.07.01.20171004)

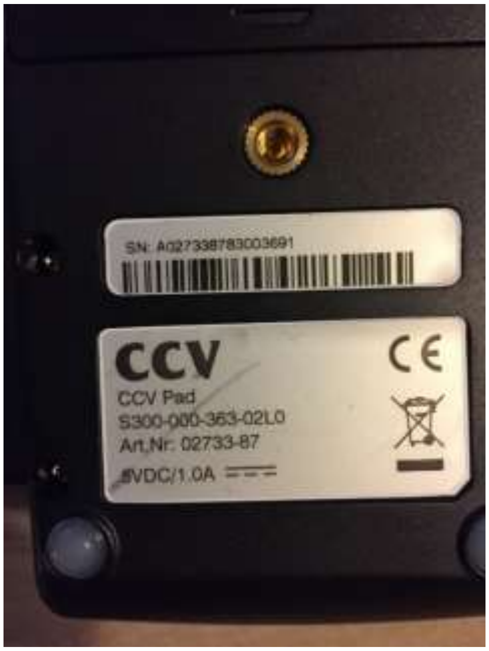


```
Software-Version
S920.APCCVD
p02.0019.07.01.20171004

GN: 0x00          TSS:3
SN: 20318805
Hostkenner:

IP-Adresse: (DHCP)
MAC: 00-17-6F-5D-5F-1E
 Terminal ID: 12345678
```

Device – CCV Pad

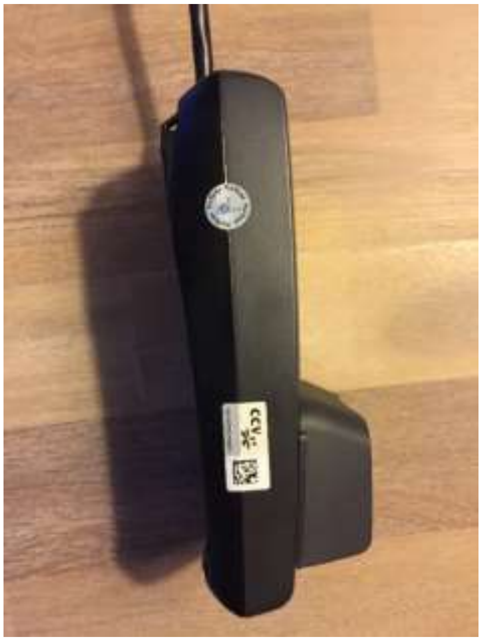
Reader label

Reader label with serial number (A027338783003691), product number (02733-87) and hardware version (S300-000-363-02L0) on back side



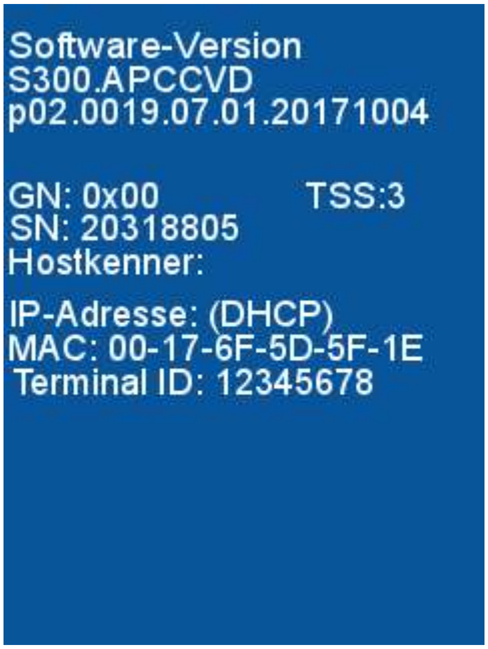
Security seal

Security seal on the device.



Software version

Example startup screen with serial number (20318805) and software version (S300.APCCVD p02.0019.07.01.20171004)

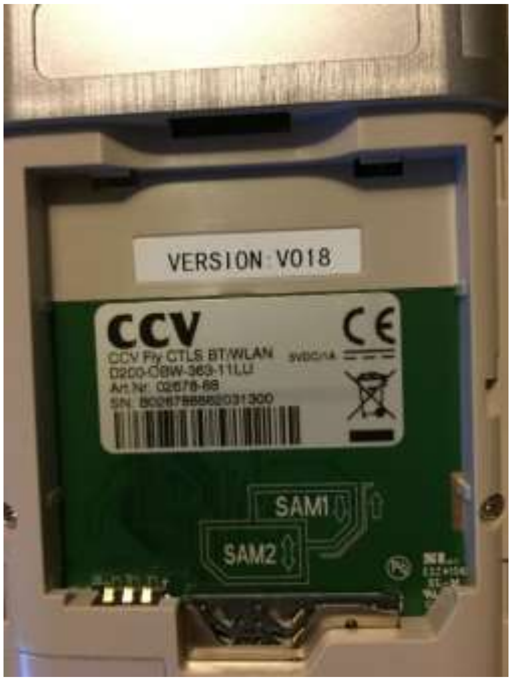


```
Software-Version
S300.APCCVD
p02.0019.07.01.20171004

GN: 0x00           TSS:3
SN: 20318805
Hostkenner:

IP-Adresse: (DHCP)
MAC: 00-17-6F-5D-5F-1E
 Terminal ID: 12345678
```

Device – CCV Fly

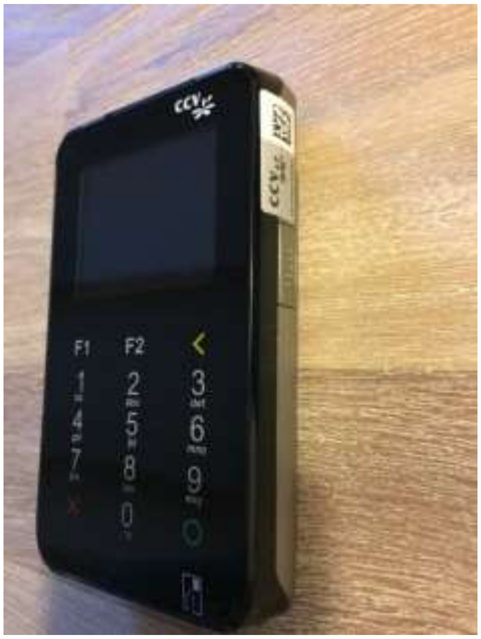
Reader label

Reader label with serial number (B026788882031300), product number (02678-88) and hardware version (D200-OBW-363-11LU) on back side



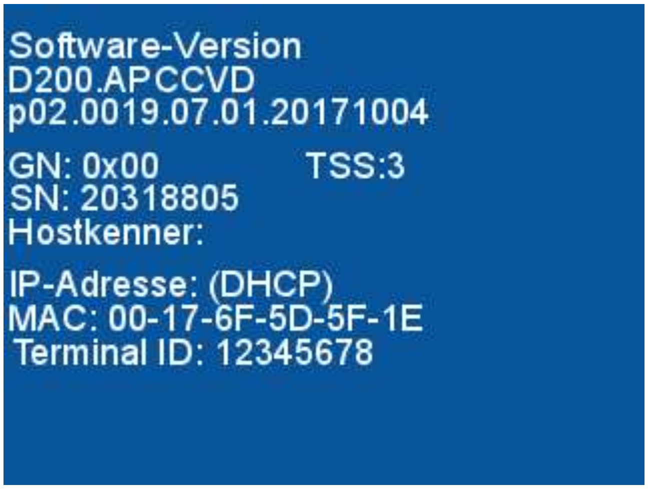
Security seal

Security seal device



Software version

Example startup screen with serial number (20318805) and software version (D200.APCCVD p02.0019.07.01.20171004)



Software-Version
D200.APCCVD
p02.0019.07.01.20171004

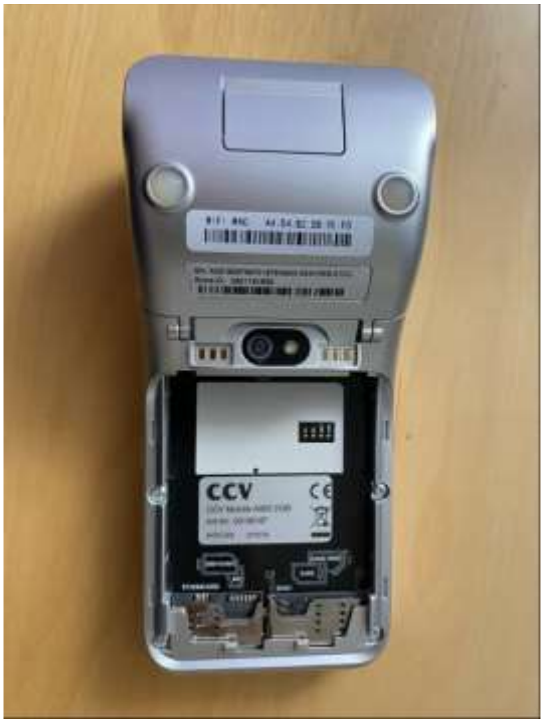
GN: 0x00 TSS:3
SN: 20318805
Hostkenner:

IP-Adresse: (DHCP)
MAC: 00-17-6F-5D-5F-1E
Terminal ID: 12345678

Device – A920

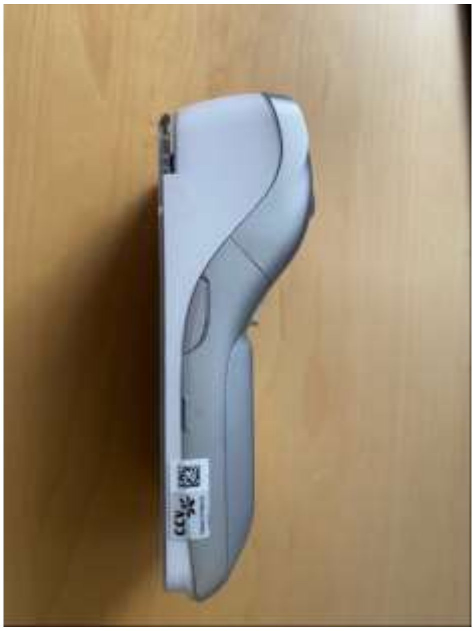
Reader label

Reader label with serial number (A031909789701978), product number (03190-97) and hardware version (A920-3AW-RE5-21EU) on back side



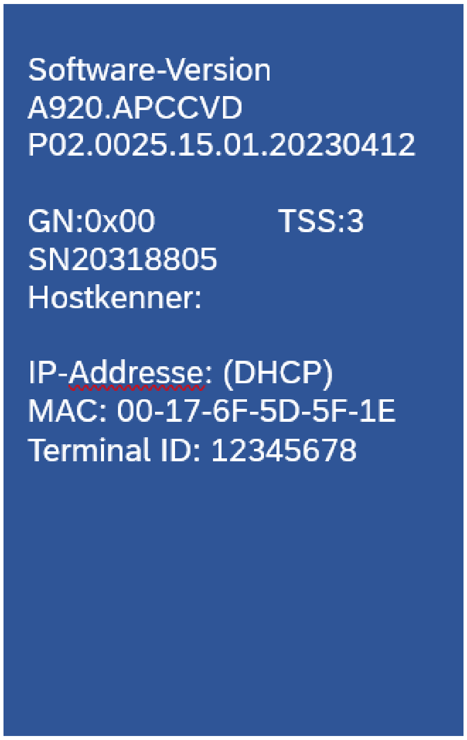
Security seal

Security seal on the device.



Software version

Example startup screen with serial number (20318805) and software version (A920.APCCVD p02.0025.15.01.20230412)

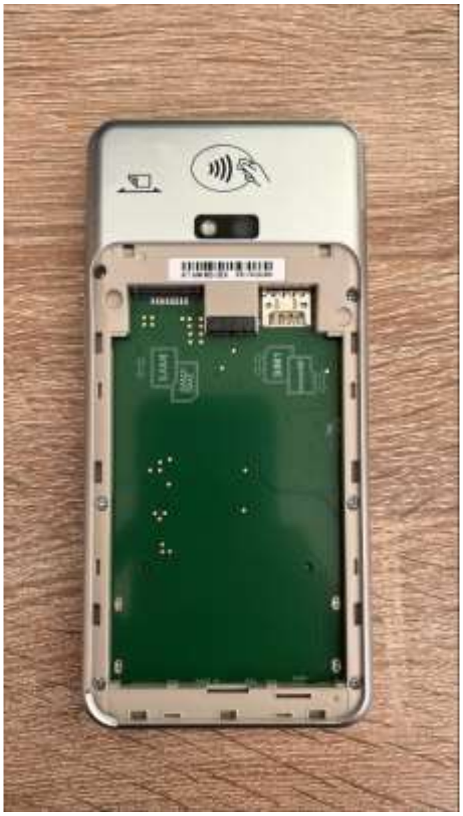


```
Software-Version
A920.APCCVD
P02.0025.15.01.20230412

GN:0x00           TSS:3
SN20318805
Hostkenner:

IP-Addresse: (DHCP)
MAC: 00-17-6F-5D-5F-1E
Terminal ID: 12345678
```

Device – A77

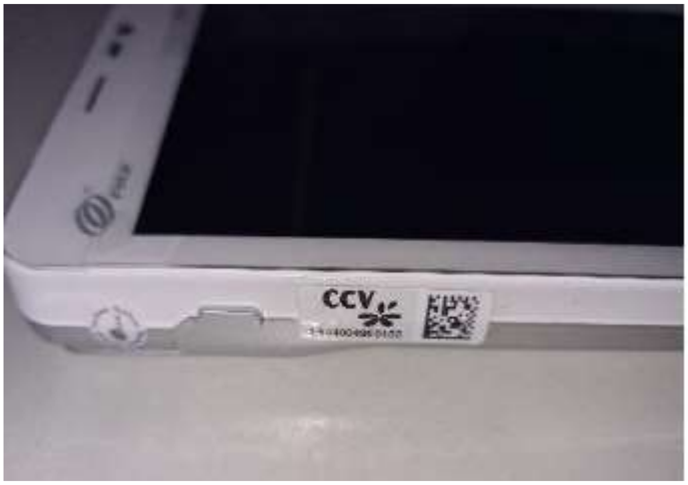
Reader label

Reader label with serial number (1760161898) and hardware version (A77-OAW-RE5-25EU) on back side



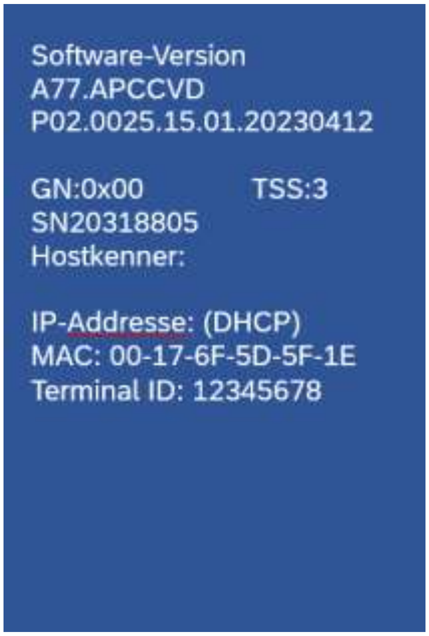
Security seal

Security seal on the device.



Software version

Example startup screen with serial number (20318805) and software version (S300.APCCVD p02.0019.07.01.20171004)



Software-Version
A77.APCCVD
P02.0025.15.01.20230412

GN:0x00 TSS:3
SN20318805
Hostkenner:

IP-Addresse: (DHCP)
MAC: 00-17-6F-5D-5F-1E
Terminal ID: 12345678