P2PE Instruction Manual

This document contains requirements and guidance for merchants participating in Zettle's PCI P2PE (Payment Card Industry - Point to Point Encryption) solution. It includes important topics such as how to receive, handle and secure your card reader in a compliant manner.

The main point of the PCI P2PE standard is that sensitive data such as card numbers and PIN codes are protected from the point of interaction (your customer and card reader) to the card's issuing bank. By participating in the solution you are not only relieved of many compliance burdens, but also using a payment provider that has been audited to the highest available standards of PCI.

When you as a business reach a certain payment volume, you will be required by the card brands and acquiring banks to undergo a PCI DSS (Data Security Standard) audit. These come in the form of very detailed and time-consuming self-assessment questionnaires. By using our P2PE solution, the audit is greatly reduced in scope and you can focus on your business rather than compliance and paperwork.

1. P2PE Solution Information and Solution Provider Contact Details

1.1 P2PE Solution Information	
Solution name:	Zettle by PayPal E2EE
Solution reference number per PCI SSC website:	TBD

1.2 Solution Provider Contact Information	
Company name:	Zettle by PayPal
Company address:	Regeringsgatan 65, 111 56 Stockholm, Sweden
Company URL:	www.zettle.com
Contact name:	Zettle Customer Service
Contact phone number:	UK: 020 3984 8464 Sweden: 010 888 7267 Denmark: 89-88-78-70 Norway: 21 93 72 02 Finland: 075 326 7785 Germany: +49 157 3599 1237 Italy: +39 06 80335 012 Spain: +34 911 98 86 38 France: 0971 07 07 03
Contact e-mail address:	help@zettle.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.
Depending on your geographical location, Zettle will ship its card reader from one of the following locations

- **Poland**: 4Values, % Zettle, ul. Parzniewska 4, 05-800 Pruszków
- **Sweden**: Postnord TPL, % Zettle, Bergvägen 1, 341 32 Ljungby, Sweden
- **United Kingdom**: Power Body Nutrition Ltd, % Zettle, Unit 11 Chessingham Park, Common Road, Dunnington, York, YO19 5SE
- **Norway**: Inselo Logistikk, % Zettle, Port 1 Inselo Mesanin, Gneisveien 18, 2020 Skedsmokorset
- **USA:** Ingram Micro, 3510 E Francis Street, Ontario, CA 91761.
- **USA**: Global Logistics Connections Inc, S. Reyes Avenue 18737, Compton CA 90220.

When receiving the card reader, you must verify that the shipment originated from one of these locations. This information is available in the tracking link you received when the card reader shipped. The logistics centers above may utilize a trusted courier such as DHL, Fedex or UPS. Such courier information will also be included in the information received by Zettle when the card reader ships. You must verify this information when receiving the shipment.

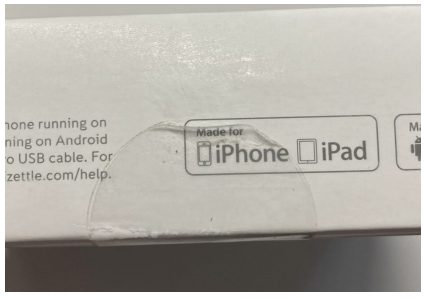
If the courier cannot identify themselves or the shipment does not originate from the above locations, you must not use the card reader but reach out to Zettle for a replacement, see section 1.2.

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

Use the following guidance when unpacking and verifying your card reader

- The postal packaging should be free from tapes, scratches or other discrepancies that might indicate that someone has opened, and then closed, the packaging.
- Once the card reader is out of the postal packaging, you must verify that the tamper seal is intact. This seal is circular and transparent, and placed so that the card reader's box cannot open without removing it and leaving marks. Please see images below for reference.
- There must be no tape or cuts in the card reader's box.
- When you have opened the card reader's box, make sure that the serial number on the back of the device is the same as communicated by Zettle in the email received when the card reader shipped.

Left image: OK.



Right image: Tampered.

If any of the above inspections fail, you must not use the card reader but reach out to Zettle for a replacement, see section 1.2. Save all packing slips, confirmation emails and other items related to 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

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.

Zettle by PayPal does not have any maintenance or repair staff visiting merchant locations. Do not give physical or logical access to your card reader if someone claims to be from Zettle by PayPal.

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):
4-30206	Datecs Ltd	Card Reader One ("Card Reader One")	03.00.xx.xx, 03.00.1xx.xx	3.0.xx.xx
4-30288	Datecs Ltd	Card Reader One V1 ("Card Reader Two")	03.00.1x.xx, 03.00.2x.xx, 03.00.3x.xx, 03.00.4x.xx	3.0.xx.xx
4-30426	Datecs Ltd	Terminal ("Terminal")	31.10.x0.xx, 31.10.x1.xx, 32.10.x0.xx, 32.10.x1.xx,	SP: 3.0.xx.xx, Android: 1.0.xx.xx

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)
Zettle PA 1.1.xx.xx	Datecs Ltd	Card Reader One (“Card Reader One”)	See 3.1	Yes	Yes
Zettle PA 1.1.xx.xx	Datecs Ltd	Card Reader One V1 (“Card Reader Two”)	See 3.1	Yes	Yes
Zettle PA 1.1.xx.xx	Datecs Ltd	Terminal	See 3.1	Yes	Yes

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 Zettle by PayPal via the contact information in Section 1.2 above.
- Sample inventory table below is for illustrative purposes only. The actual inventory should be captured and maintained by the merchant in an external document.

Zettle card readers are not personalized, as is traditional with many other brands of card readers. It is therefore important that you as a merchant are in control of who has access to them. Preferably, this is done by having authorized staff checking in and out the card readers out of secure storage at the start and end of each working day. A safe or lock box with restricted access are good alternatives. The log must at minimum contain:

- Serial number
- Date and time of check in/out
- The status of the card reader (operative, malfunction, in shipment, etc)
- Who had access to the device
- Location (if you have several)

Store the logs digitally or inside the secure storage container. You may be required to present these logs when doing your PCI DSS self-assessment.

When starting or ending each day, pay close attention to the serial number of the device to make sure it is as expected. If it has been substituted, stop using it immediately and reach out to Zettle, see section 1.2.

When employees that have had access to card readers leave or change positions, you must promptly revoke their access to the secure container.

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.
-

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

Card Reader One and Card Reader Two

Download the Zettle app from your preferred app store and create an account if you do not have one already. Once you are logged into the app, go into “Settings” and then “Card Reader”. Power on your card reader by pressing the button at the top of the device. Make sure Bluetooth is enabled on your phone or tablet. The app will automatically detect the card reader and present it in the graphical user interface. Make sure that the last three digits of the serial number (found on the back of the card reader) are presented in the app before pressing it to connect.

When the card reader connects, compare the numbers presented in the app and the card reader’s display. If they match, press the card reader’s bottom right button to confirm the pairing.

The card reader only communicates via Bluetooth, so there is no need to connect the USB cable other than for charging it.

Terminal

Since the card reader is integrated, there is no need for pairing. Open up the Zettle app on the Terminal and sign in with your Zettle account. The Terminal has a SIM card, but you can connect it to your wifi for a quicker experience.

Configuration

Once you have signed in with your account and established connectivity to the card reader, it will automatically configure itself according to your merchant account. This process takes a few seconds and will display “Please Wait” on the card reader. Do not close the app or power off the card reader during this stage. Once completed, the card reader will display “Hello” or similar message, depending on your localization.

Merchants cannot configure Zettle card readers in any way outside of the business settings available in your Zettle portal or app. These are settings that influence certain aspects of a payment (tipping, down-payments, repeat payments etc) but never the security or compliance or the card reader.

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

Zettle’s card readers are certified for **attended** usage. This means that while the card reader is in use during normal business, it must be supervised by an authorized employee. At no point should it be left unattended.

Do not place the card reader’s buttons in view of any cameras or easy-access windows. It is recommended to use a shield or similar to prevent customers and employees from observing input on the card reader.

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

To prevent your card reader from being stolen or replaced, we first and foremost recommend that you keep it under constant supervision, and locked away (or on your person) while you are not at the sales desk. Another option is to purchase a stand from the Zettle web shop. The stands have hollow areas

where one can fit a chain to anchor it to the desk. There are also third party PIN pad stands available in a multitude of shapes and sizes.

As detailed in section 3.3, it is very important that you keep logs of all interactions of the card reader. Should you discover that the serial number has changed, do not use the card reader but store it securely. You must promptly report unauthorized removal or substitution to Zettle, see section 1.2.

5. POI Device Transit

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

When moving a card reader to a new location, you must package it carefully since the device is tamper resistant and designed to (cryptographically) break when subject to poking and prodding.

- If you are moving the card reader without personal supervision, you must seal the carefully packaged card reader in tamper-evident and authenticable ("TEA") tape or bag and make note of the authentication numbers. The numbers need to reach the receiver in an out-of-band channel, such as email or phone. The receiver then needs to verify the numbers upon reception.
- Only use trusted couriers with proper tracking functionality.
- If you are moving the card reader yourself, keep it on your person at all times until it reaches the destination.
- Store all documents produced during transit (tracking links, receipts, etc).

If your device is to be sent for repair or troubleshooting to Zettle, we will supply you with the necessary items and instructions in the support ticket.

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

The only authorized locations to send card readers to are listed in section 2.1. As noted in section 5.1, we will supply you with the necessary items and instructions for a compliant shipment in the support ticket.

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.

Routinely inspect your card reader, paying special attention to the following

- The NFC antenna section and the card reader slot look exactly like the pictures below.
- The screen should be on level or somewhat lower than the surrounding frame.
- The buttons should not have any kind of overlay material and require a firm press to activate (Reader Two).
- Inserting and ejecting a card should produce a mechanical click.
- There should not be much resistance when ejecting the card.
- The serial number on the back of the card reader must match what is shown in your Zettle app and your card reader inventory.
- There should not be any dongles attached to the card reader, nor any other unknown hardware around your sales desk.

Card Reader One and Card Reader Two

Terminal

6.2 Instructions for responding to evidence of POI device tampering

If any of the above inspections are unsatisfactory, or you suspect something else is off with your card reader, stop using it immediately and store it securely. Reach out to Zettle for a replacement, see section 1.2.

7. Device Encryption Issues

7.1 Instructions for responding to POI device encryption failures

There is no logical or physical way for Zettle card readers to disable encryption. Any security failure will show “Reader Damaged” on the screen and the device becomes unusable. Reach out to Zettle for a replacement, see section 1.2

8. POI Device Troubleshooting

8.1 Instructions for troubleshooting a POI device

Most issues can be resolved by the following checklist

- Reboot the device by holding down the power button for 3 seconds, then turn it back on again
- Go to “Settings”, “Card Readers” and install any updates that are pending

- (Card Reader Two) Update the Zettle app from your app store
- (Card Reader Two) If the Bluetooth pairing malfunctions, go into your phone's Bluetooth settings and forget the device. Go to "Settings", "Card Readers" and pair it again.

For more common troubleshooting topics, please visit
https://www.zettle.com/gb/help/articles/2966945-troubleshooting-zettle-reader-2 for Card Reader Two and
https://www.zettle.com/gb/help/articles/0231667-zettle-terminal-troubleshooting for Terminal

9. Additional Guidance

9.1 Instructions for troubleshooting a POI device

Our support staff can help you out if the above troubleshooting fails. See section 1.2 how to reach them.

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

In section 3.1 there is a link to the official PCI PTS listing containing the certified versions, please use that website as a reference when verifying that your card reader has the correct applications installed.

Card Reader One and Card Reader Two

Both "Payment Application" and "Firmware" versions can be found by connecting your card reader to the Zettle app. Go to "Settings" and "Card readers" to locate your device. Click it, and you will be presented with the "Software version" (Payment Application) and "Firmware version".

Terminal

Both "Payment Application" and "Firmware" versions can be found by opening the Zettle app. Go to "Settings" and "Card reader". Here you will be presented with the "Software version" (Payment Application) and "Firmware version".

The hardware version is visible on the barcode label on the back of both card readers.

These three numbers should align with those of the PCI PTS listing.