



PAYMENT APPLICATION INSTRUCTION MANUAL

for Verifone Vx520 terminal and Verifone PP1000SE V3 PIN pad
with 2.2.1 application version

TABLE OF CONTENTS

1.	Verifone Vx520 terminal	4
1.1	Description of terminal.....	4
1.1.1	Technical data.....	4
1.1.2	Description and functions of terminal buttons	4
1.2	Operation of terminal and PIN pad	4
1.2.1	Preparing a set of devices for work.....	5
	Replacing the paper roll.....	7
2.	Activation of application, main screen, icons.....	7
2.1	Activating the payment application	7
2.2	Description of application indicators (icons).....	8
3.	Transactions.....	8
3.1	Standard transaction procedure	8
3.1.1	Starting - selecting the transaction type.....	9
3.1.2	Entering the amount	10
3.1.3	Entering the card and the payment methods	11
3.1.4	Questions about additional services – DCC and cash withdrawal.....	16
3.1.5	Card holder authentication methods (PIN, signature, lack of authentication)	16
3.2	Types of transactions	18
3.2.1	Sales	18
3.2.2	Cash Back (Sales and cash withdrawal).....	20
3.2.3	Cancellation	22
3.2.4	Copy of the Client's printout.....	23
3.2.5	Preauthorisation	25
3.2.6	Completion of preauthorisation.....	27
3.2.7	Prepaid GSM.....	29
3.2.8	Return	30
3.3	Dynamic currency conversion – DCC	33
4.	Administration functions.....	34
4.1	Settlement	34
4.1.1	Call of Settlement	35
4.1.2	Settlement printouts	35
4.2	Reports.....	36

4.2.1	Summary.....	37
4.2.2	Detailed.....	37
4.2.3	GSM top-up report.....	37
4.2.4	Generation of report.....	37
4.3	Update of application.....	38
4.4	Display of version.....	40
4.5	Change of password.....	40
4.6	Diagnostics.....	41
4.6.1	Call of Diagnostics and Diagnostics procedure.....	41
4.6.2	Diagnostics printouts.....	44
4.7	Demo mode.....	44
5.	Additional functions.....	46
5.1	Printout of the data of terminal and point of sale.....	46
5.2	Automatic return to main screen and screen saver.....	46
5.3	Time synchronisation with host.....	46

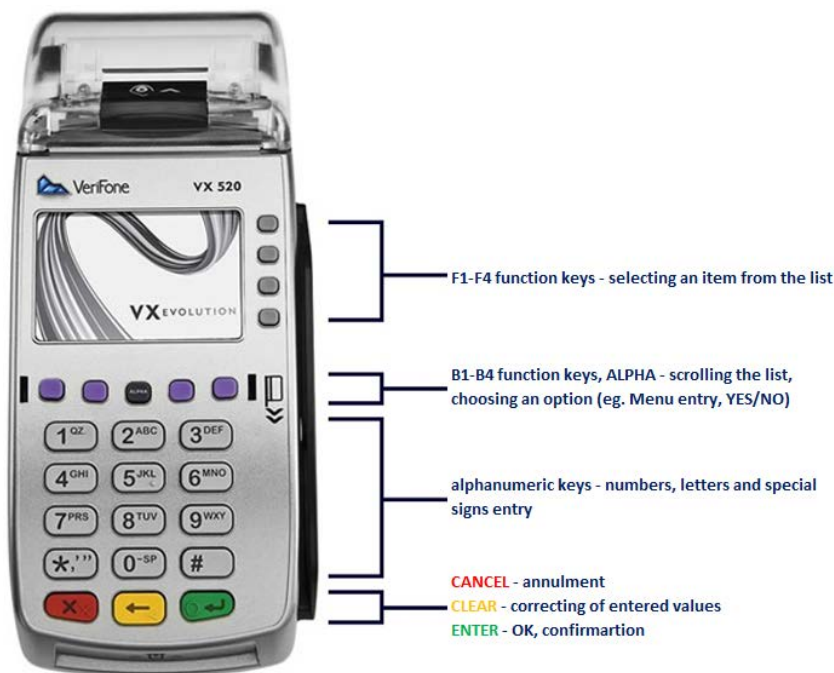
1. Verifone Vx520 terminal

1.1 Description of terminal

1.1.1 Technical data

Display	128x64 pixel backlit LCD screen
Card readers	magnetic strip reader electronic card reader
Printer	thermal, standard paper rolls 58 mm x 25 m
Dimensions (LxWxH)	203 mm x 78 mm x 84 mm
Temperature range	usage 0°C - 50°C storage -20°C - 60°C
Power	input: AC - 100-240V, 50/60Hz output: DC - 5V, 1A

1.1.2 Description and functions of terminal buttons



1.2 Operation of terminal and PIN pad



First, be sure to read the installation, operation and storage instruction manual delivered by the manufacturer of the devices. The usage against the manufacturer's guidance may cause malfunction of the devices and the payment application and result in warranty loss.

1. Terminal Verifone Vx520



2. Pinpad VerifonePP1000 SE v3



1.2.1 Preparing a set of devices for work

In order to ensure the proper function the set of devices should be appropriately prepared for work and controlled by the authorised person.

First, connect peripheral devices, e.g. PIN pad, bar code reader etc. to the terminal, finally, connect the set to the power source.



Never unscrew the bolts or interfere with the devices in other way, this may result in breakdown and consequently incapability of the set to use.

1.2.1.1 Connecting the PIN pad to the terminal

The connection of the PIN pad is necessary to ensure the correct function of the payment application.



The PP1000SE V3 PIN pad is equipped with the proximity card reader for the transactions performed with the proximity cards and for the mobile transactions.

If the connection of the terminal with the PIN pad during the transaction is not possible (e.g. due to damage to the sockets in the devices, damage to the cable connecting the PIN pad or due to breakdown of the PIN pad), **the contactless transactions are not available**

After the appropriate connection and activation the terminal establishes communication with the PIN pad.

If the PIN pad is detected, the contactless icon, meaning the availability of the contactless transactions, appears on the terminal screen. During normal use when idle (i.e. when no transaction is carried out):

- the “Planet Pay” wording is displayed on the PIN pad
- the first diode (located on the left hand side) on the PIN pad flashes every 5 seconds

- the PP1000SE V3 PIN pad has no its own power source – it draws current after the connection to the RS-232 socket in the terminal. This means that after the disconnection of the power source from the terminal the power of the PIN pad is also disconnected.

CONNECTING THE PIN PAD CABLE TO THE RS-232 SOCKET IN THE TERMINAL

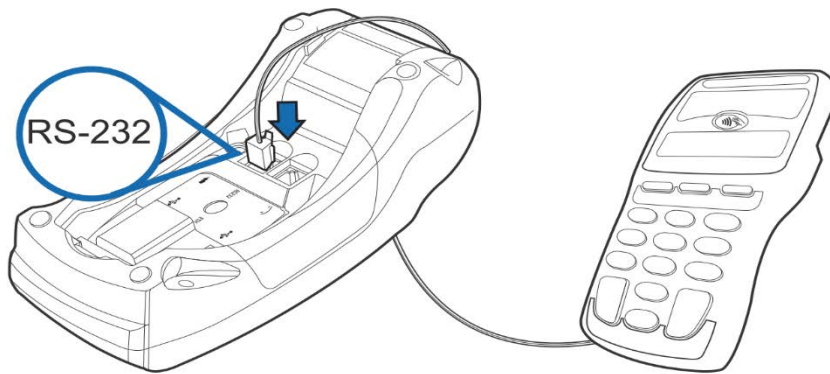


FIGURE 1 CONNECTING THE PIN PAD TO THE TERMINAL

1.2.1.2 Connecting the terminal to the power source

TURNING ON: The deactivated terminal can be turned on by connecting it to the power source.

TURNING OFF: The activated terminal can be turned off by disconnecting it from the power source.

In order to connect the terminal to the power source:

CONNECTING THE TERMINAL TO THE POWER SOURCE:

1. Take off the lower terminal cover
2. Insert the round end of the PSU to the power socket in the terminal
3. Connect the PSU plug to the electrical socket

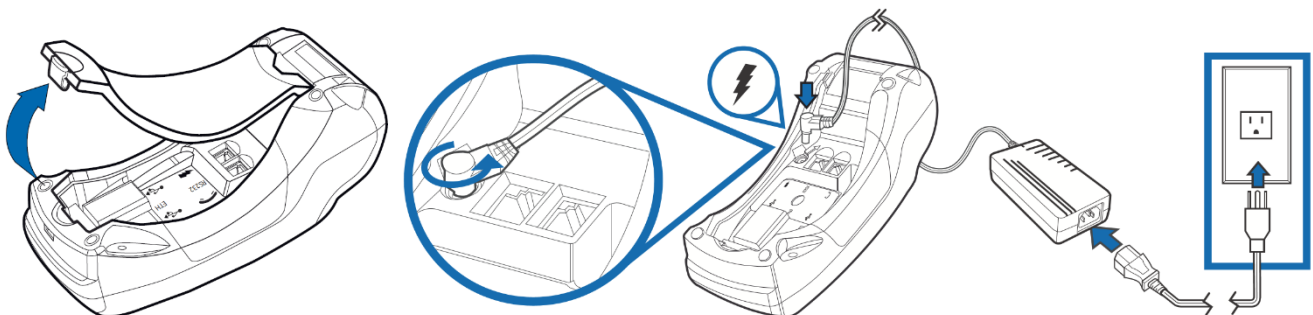


FIGURE 2 CONNECTING THE TERMINAL TO THE POWER SOURCE

The payment application is activated automatically when the device is turned on.

Replacing the paper roll

Use standard paper for thermal printers in rolls with a width of 58 mm and length of 25 m.

In order to replace the paper roll:

1. Pull gently the printer cover upwards, then backwards
2. Remove the remains of the previous roll and paper from the printer chamber
3. Unwind the new paper roll approx. 10 cm and place it in the printer chamber
4. Close the printer cover and tear off a protruding piece of paper

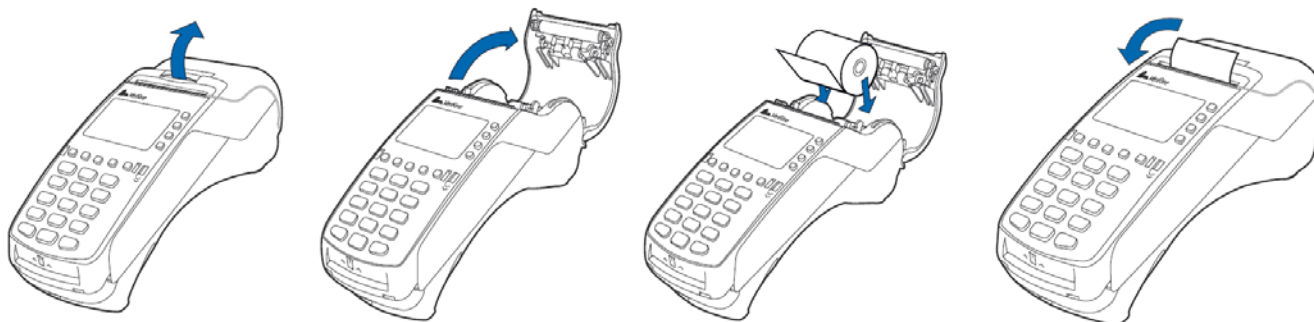


FIGURE 3 REPLACING THE PAPER ROLL

2. Activation of application, main screen, icons

2.1 Activating the payment application

The payment application is activated on the terminal automatically when the device is turned on [see: [Connecting the terminal to the power source](#)]. After the activation the main screen displays the following:

- Icons: CTLS, GPRS coverage/Ethernet connection
- Sales network name (in this case: Planet Pay; depends on the configuration)
- Default transaction amount entry field
- ADMIN and MORE menu buttons
- Time set currently on the terminal



Depending on the settings the view of the main screen in various locations may vary. In the standard setup the main screen includes the Sales transaction amount entry field.

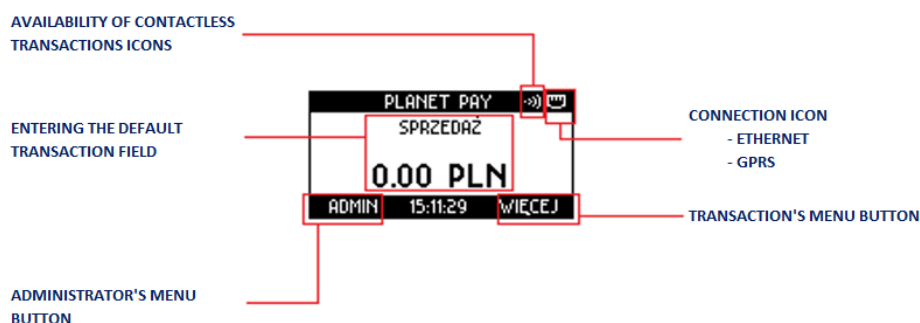


FIGURE 4 APPLICATION'S MAIN SCREEN

2.2 Description of application indicators (icons)

During normal application operation two icons informing about the connection condition and PIN pad status/contactless transaction availability is always visible on the main screen. The meaning of the individual icons is described below.

Connection icons – dependent on the type of a medium which is used by the terminal to communicate with the hosts

- **GPRS coverage** (for terminals connecting through GPRS)



	100% - full coverage		75%
	50%		25%
	0% - no connection, SIM card present		GPRS unavailable / no SIM card

2-1 GPRS coverage icons

- **Ethernet connection** (for terminals connecting through Ethernet)

	terminal connected to the network		terminal not connected to the network
---	-----------------------------------	---	---------------------------------------

- **Contactless (CTLS) icons** – contactless transaction availability/information about PIN pad status

	PIN pad detected, contactless transactions available
	PIN pad not detected, contactless transactions unavailable

2-1 CTLS icons

3. Transactions

3.1 Standard transaction procedure

The subsequent characteristic phases can be distinguished for the most common transactions. Each of them is described in detail below.

- Starting - selecting the transaction type
- Entering the amount
- Downloading the card data
- Authenticating the card holder - the Client
- Connecting with the Authorisation Centre
- Displaying the result of the transaction and printing the confirmation

Independently, each of the transaction types available in the payment application, taking into account the operations and characteristics for each of them, is described in the further part of the instruction manual.

3.1.1 Starting - selecting the transaction type

3.1.1.1 Starting the transaction on the main screen (default transaction)

The application allows setting a so-called default transaction, i.e. the most common transaction, on the main screen. **This enables the amount to be entered immediately without selecting the transaction from the list.** The type of the default transaction can be different depending on the settings used by the Provider.

The Sales transaction is the standard default transaction.

If the default transaction is set, its name and the amount entry field is visible on the main screen. If the default transaction is not set, only the "WITAMY" (eng. "WELCOME") message is visible on the main screen.

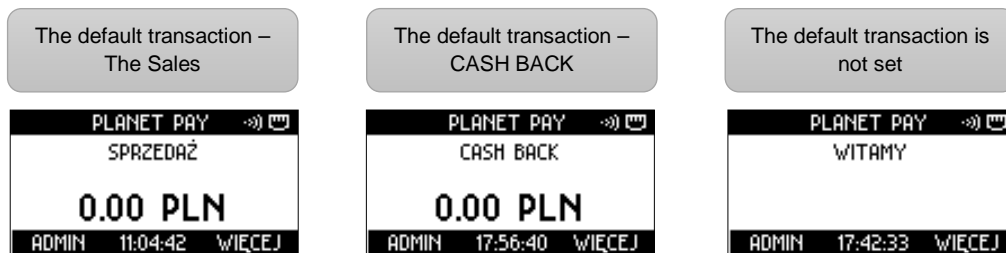


FIGURE 5 STARTING THE TRANSACTION – THE DEFAULT TRANSACTION

3.1.1.2 Selecting the transaction from the menu list

The list of transactions that can be carried out on the terminal is available in the transaction menu under the MORE button.

This list can be different depending on e.g. the sales network or point-of-sale profile.

In order to select the type of transaction from the list:

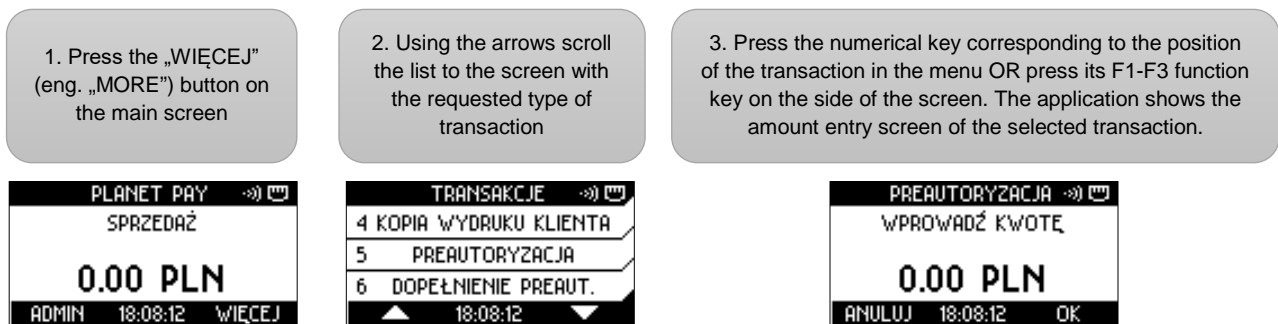


FIGURE 6 STARTING THE TRANSACTION – SELECTING FROM THE MENU LIST

In case of mistake in selection, in order to end (cancel) the transaction, press the red CANCEL key, the application returns to the main screen.

When the type of transaction is confirmed, the application switches to the amount entry screen.

3.1.2 Entering the amount

The amount is entered on the terminal by means of 0-9 alphanumerical keys. The entered characters appear on the screen one by one from the right hand side which means that in order to enter the amount of PLN 12.34, the 1-2-3-4 keys should be pressed in turn.

The transaction amount can be entered on the main screen of the application, if the default transaction is set, or on the screen with the “Wprowadź kwotę” (eng. “Enter the amount”) message which is displayed after the start of the transaction selected from the MORE menu.



The amount can be edited –the incorrectly entered characters can be removed – by pressing the yellow CLEAR key

- press the CLEAR key once to remove the last entered character
- press the CLEAR key and hold it to remove all entered characters

1. Enter the amount by means of the 0-9 alphanumerical keys	2. In case of mistake press the yellow CLEAR key. The last character is removed.	3. Enter the other figures of the amount and confirm with the green ENTER (OK) key.	4. The application will display the card insertion screen

FIGURE 7 ENTERING AND CORRECTING THE TRANSACTION AMOUNT



The amount cannot be edited when it is confirmed and the card insertion screen is displayed.

If the confirmed amount is incorrect, press the red CANCEL key and start the new transaction.

When the transaction amount is confirmed, the application switches to the card insertion screen.

3.1.2.1 Transaction limits

Depending on the Provider’s settings the minimum and maximum transaction amounts (i.e. the amounts that can be confirmed) can be different for the various points of sale.

The standard minimum amount is PLN 1.00, the maximum amount - PLN 20 000.00. In attempt to confirm the amount outside this range the application informs about the error and shows the correct expected limits of the transaction amount.

Similarly, the application behaves in attempt to confirm the cash withdrawal in the amount exceeding the specific limits (typically PLN 1.00-500.00).

The exemplary messages are presented below.



FIGURE 8 TRANSACTION LIMITS – ERROR MESSAGES

3.1.3 Entering the card and the payment methods

The payment application installed on the terminal allows making payments with all the types of cards currently available on the market – i.e. microprocessor and proximity cards as well cards with magnet strip.

The application supports also the mobile payments – made by means of a mobile phone on which a specially configured application (e.g. BLIK, AndroidPay etc.) is installed.

The individual card insertion methods are described below.

3.1.3.1 Electronic (microprocessor, chip) cards

The Vx520 terminal is equipped with the microprocessor card reader for reading the data from the card chip.

After the start of the transaction, confirmation of the amount and display of the card insertion request, insert the cards into the reader in the terminal (microprocessor upward) in a manner shown in figure below.

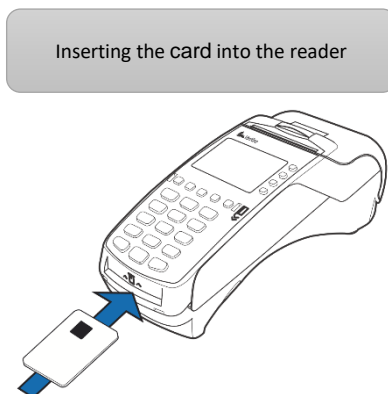


FIGURE 9 INSERTING THE ELECTRONIC CARD

In the basic procedure, after the insertion of the card, the application informs about the data processing, then, depending on the type of the card and transaction, displays the PIN entry request, or starts connecting with the Authorisation Centre.

The payment card microprocessor is provided with applications for the various transactions performed with the card.

- **Selecting the application on the card**

The certain cards may be provided with more than one application (the applications on a single card may be related to several various Client's accounts, e.g. with the debit account and credit account). In such a case:

read the list of the options displayed on the terminal for the Client and make the selection according to his/her decision.

The majority of the cards are related to the single Client's account which means that most of the cards are provided with one application for making the payment on the terminal. In such cases: after the insertion of the card this application is selected and used automatically, in a manner invisible for the user – the application selection screens are not visible on the terminal.



The name of the used application and its identifier as well as the masked number of the payment card are shown on every transaction confirmation (printed after the completion of the transaction) above the account number. The exemplary data are marked on the printout below.

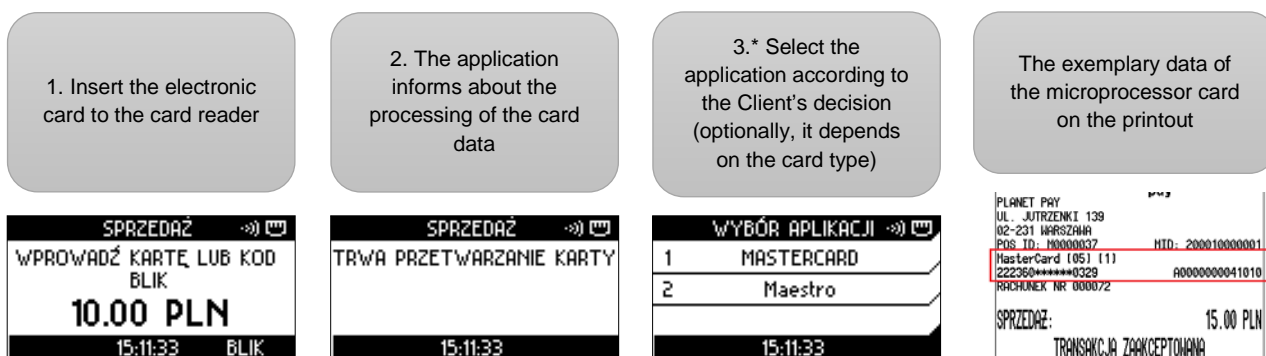


FIGURE 10 READING THE DATA OF THE CARD



The card should be left in the reader until the completion of the transaction. The transaction may be rejected if the card is removed before the confirmations are printed out.



For the electronic cards in order to accelerate the transaction the card can be also inserted into the reader **BEFORE** the confirmation of the amount - in this case after the confirmation of the amount the application immediately starts processing the card data and the card insertion request screen is omitted.

When the data of the card are read, the application continues the transaction – depending on the settings and the type of the selected transaction:

- displays the questions about additional services or
- displays the request for entering the PIN or
- starts connecting with the Authorisation Centre

3.1.3.2 Payments with contactless cards

The majority of the currently issued microprocessor cards allows making the contactless payments. Such cards are marked by the contactless symbol.

The contactless card reader is located below the display of the PP1000SE V3 PIN pad. The data of the contactless card are read when the card is put against the PIN pad screen after the confirmation of the completion of the transaction amount and after the display of the transaction amount, contactless symbol and card insertion request on the PIN pad screen.



The correct read of the data of the contactless card is signalled by the activation of all four diodes located above the PIN pad display and by the emission of the long continuous acoustic signal.

The incorrect read is signalled by the activation of all the diodes and the short double acoustic signal.

When the contactless card is read correctly, depending on the amount and the type of the card, the application:

- connects with the Authorisation Centre or
- connects with the Authorisation Centre and display the PIN entry request

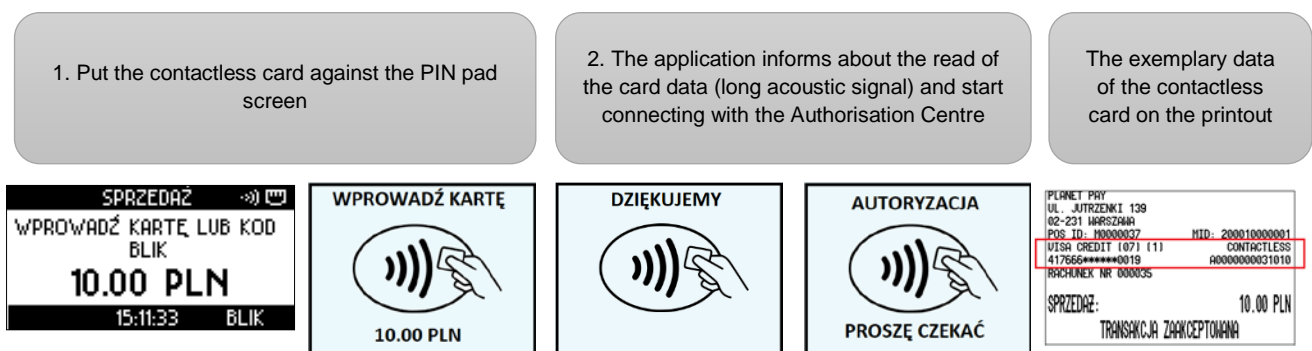


FIGURE 11 INSERTING AND READING THE CONTACTLESS CARD



The contactless icon displayed on the terminal screen in the upper right hand corner informs about the availability of contactless transactions. Before the start of the contactless transaction make sure that the PIN pad is detected and the contactless transaction is available (see also: [Description of application indicators \(icons\)](#))

The DCC service is always unavailable (see: [Dynamic currency conversion – DCC](#)) for the contactless transactions

3.1.3.3 Payments with magnetic strip cards

All the payment cards issued currently allow making transactions by using the magnetic strip located on the reverse (backside) of the card.

The magnetic card reader of the terminal is located on the right hand side of the device and marked by the magnetic card symbol.

In order to read the data of the magnetic card pull the card (up or down) with the strip facing the left hand side (the terminal) as it is shown in figure below.

Reading the data of the magnetic card

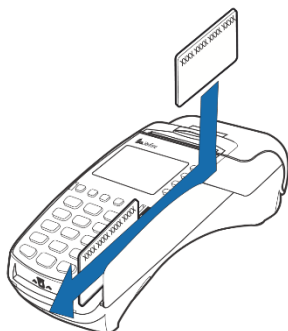


FIGURE 12 INSERTING THE MAGNETIC STRIP CARD

When the magnetic card is read correctly, depending on the settings and the type of the card, the application:

- displays questions about additional services
- connects with the Authorisation Centre in order to obtain the authorisation or
- displays the PIN entry request

After the confirmations of the transaction with the use of the magnetic strip there are no application identifier field or contactless transaction field.

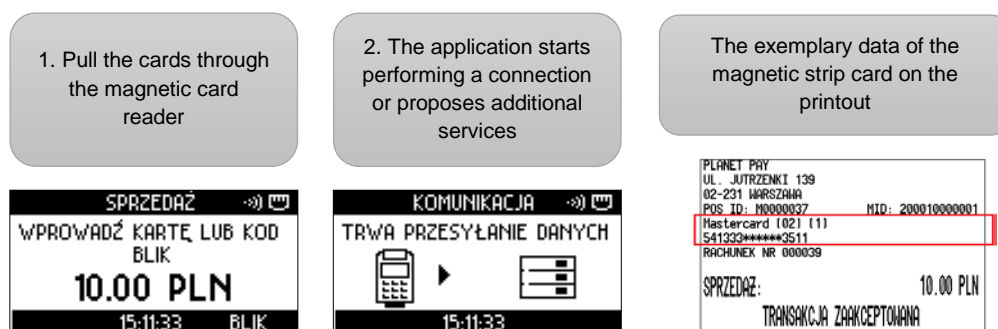


FIGURE 13 READING THE MAGNETIC STRIP CARD

3.1.3.4 BLIK mobile payment

The application allows making payments with the use of BLIK codes. The BLIK transaction can be performed at the Client's request and it is done without the physical participation of the payment card.

When the transaction amount is confirmed the application displays the card entry screen on which the BLIK button is located in the lower right hand corner. In order to conduct the transaction with the use of the BLIK code, press the function key corresponding to the button on the terminal screen (violet B3 and B4 keys on the right hand side of the ALPHA key).

Then, the Client should enter the BLIK code on the PIN pad keyboard and confirm by using the ENTER key.



The 6- or 9-digit code can be entered. In addition, the 9-digit code requires the Client to enter the PIN.

The 6-digit code does not require the additional PIN confirmation.

When the BLIK code is entered by the Client and confirmed, the application connects with the Authorisation Centre, displays the result of the transaction and prints out the confirmation.

The procedure of the BLIK payment transaction is described below.

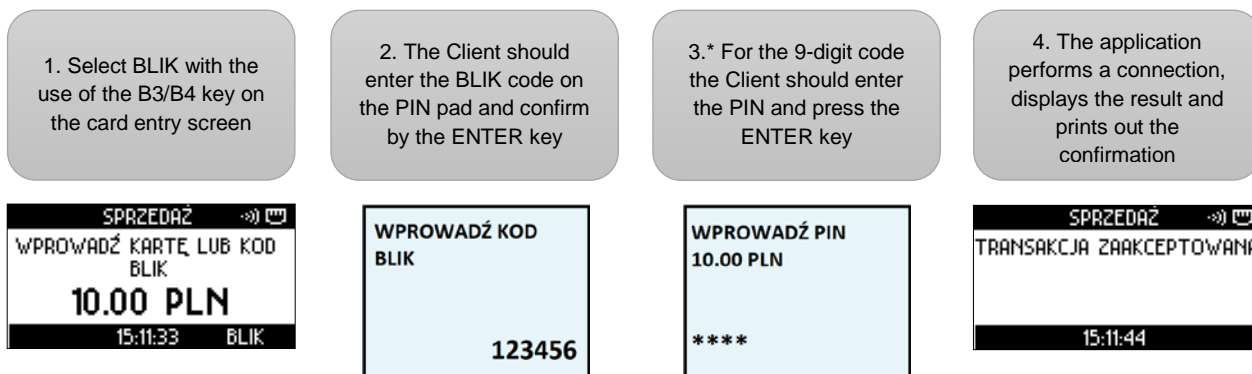


FIGURE 14 BLIK MOBILE PAYMENT

The masked BLIK code used for the authentication of the transaction and the REFERENCE CODE field (not present for other transactions) are included on the printout of the BLIK payment transaction above the account number.

The exemplary confirmation printout of the BLIK payment transaction

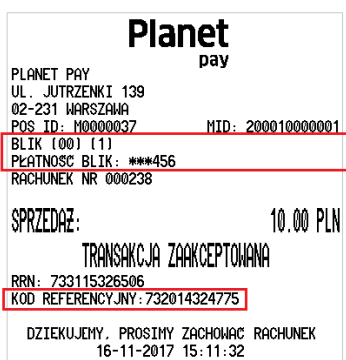


FIGURE 15 BLIK MOBILE PAYMENT – THE CONFIRMATION PRINTOUT

3.1.3.5 Mobile contactless payments

The payment application on the terminal allows making mobile contactless payments by using mobile phones / smartphones with installed software for mobile payments.

The procedure of the mobile phone payment transaction is similar to the standard contactless transaction but instead of the card the Client puts the mobile phone against the proximity reader on the PIN pad and he/she is requested to enter the PIN or the transaction is continued without the PIN.

The confirmation printouts of the mobile phone payment transactions have the same fields as the confirmation printouts of the standard contactless transactions (see: [Proximity \(contactless\) cards](#))

3.1.4 Questions about additional services – DCC and cash withdrawal

Depending on the Provider's settings, when the card is inserted and read, the questions about the additional services - dynamic currency conversion (DCC) and/or cash withdrawal - can appear on the terminal display. In such a case, inform the Client about these questions and continue the transaction according to his/her decision.

Detailed information about the additional services is included in the chapters: [Dynamic currency conversion – DCC](#) and [Additional question about cash withdrawal during Sales transaction – description and procedure](#).

3.1.5 Card holder authentication methods (PIN, signature, lack of authentication)

The card holder authentication is the confirmation made by the Client that he/she has the right to dispose of the card and the funds accumulated on the account to which the card is assigned.



The authentication method depends on the type of the card used, the method of its read, the amount and the type of the transaction. E.g. some transactions require the confirmation of the correctness of the Client's signature (Return) despite the fact that he/she usually confirms the transactions with the PIN.

The request for the authentication appears on the terminal and/or the PIN pad when the data of the card are read properly (see: [Inserting the card and payment methods](#)).

3.1.5.1 Transactions confirmed with the PIN code

The authentication of the transactions with the PIN code is most common for:

- the transactions with the use of the microprocessor card reader
- the contactless transactions in the amount over PLN 50.00 (including also the mobile phone payments)

The Client is always also asked to enter the PIN in case of the BLIK payment with the use of 9-digit code.

The PIN transactions performed with the magnetic strip cards are less frequent.

If the transaction requires the PIN confirmation, when the data of the card are entered and read properly, the instructions for the Seller and the Client appear on the terminal and on the PIN pad.



The Client should enter his/her PIN code on the keyboard of the PIN pad and confirm it by pressing ENTER (the green key).

In case of mistake in the entry of the characters, press the yellow CLEAR key to remove the entered character.

Press CANCEL (the red key) to abort – cancel the transaction.

The PIN code is confidential therefore the characters entered by Client are masked with asterisks.

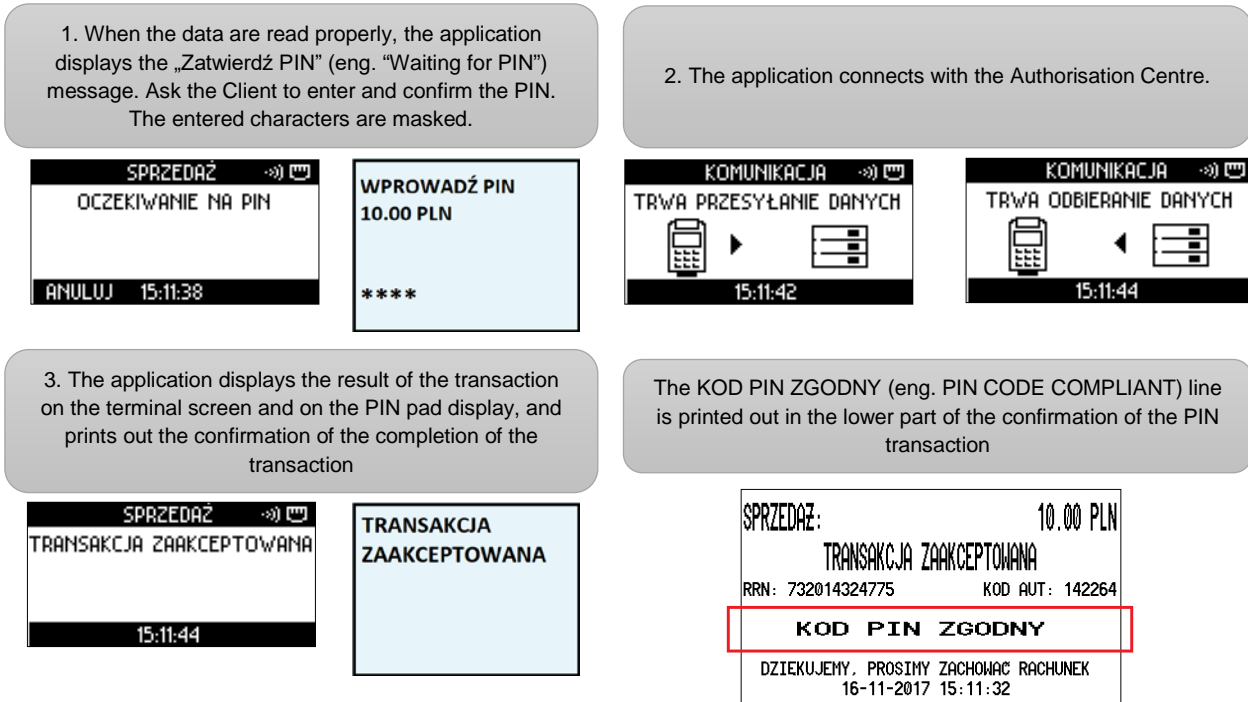


FIGURE 16 PIN AUTHENTICATION

3.1.5.2 Transaction confirmed with the signature

The request for the confirmation of the compliance of the Client's signature with the specimen located on the card reverse is required less frequently than the confirmation with the PIN code. Usually the Client is asked to put his/her signature during the transaction using the magnetic strip card.

The signature is always required for the Return transaction.

When the card is read properly, the application connects with the Authorisation Centre, then, displays the result of the transaction and prints out the Seller's confirmation with the place for the Client's signature.

If the Client's signatures on the confirmation and on the card reverse are compliant, confirm the compliance on the terminal by pressing ENTER (YES).

If the signatures are noncompliant, confirm NONCOMPLIANCE on the terminal by pressing CANCEL (NO) – the application prints out the cancellation of the transaction – a copy for the Seller, then, a copy for the Client.

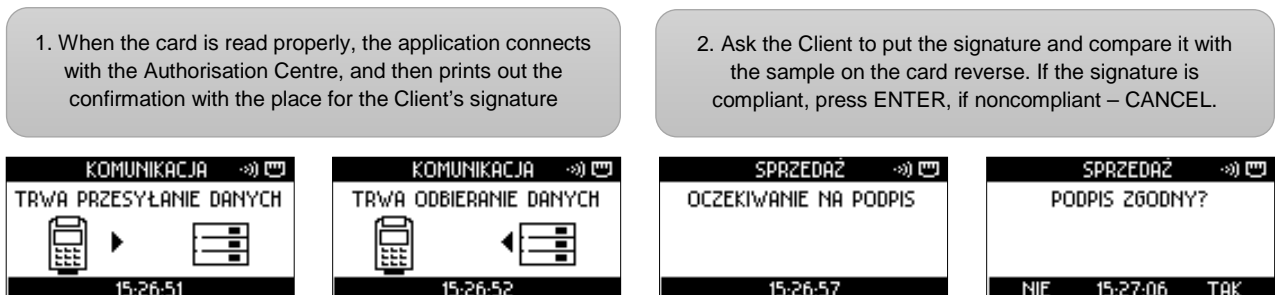


FIGURE 17 TRANSACTION CONFIRMED WITH THE SIGNATURE

If the signature is COMPLIANT, the application prints out the confirmation for the Client and returns to the main screen

If the signature is NONCOMPLIANT, the application CANCELS the transaction and prints out the confirmation. The printout of the copy for the Client is obligatory

Planet pay

PLANET PAY
UL. JUTRZENKI 139
02-231 WARSZAWA
POS ID: M0000037 MID: 200010000001
Mastercard (02) (11)
541333*****3511
RACHUNEK NR 000039

SPRZEDAZ: 4.00 PLN
TRANSAKCJA ZAOKREPTOWANA

RRN: 732014324791 KOD AUT: HOSTOK

PODPIS:
.....

DZIEKUJEMY. PROSIMY ZACHOWAC RACHUNEK
16-11-2017 15:26:46

Planet pay

PLANET PAY
UL. JUTRZENKI 139
02-231 WARSZAWA
POS ID: M0000037 MID: 200010000001
Mastercard (02) (11)
541333*****3511
RACHUNEK NR 000039 KOPIA KLIENTA

SPRZEDAZ: 4.00 PLN
TRANSAKCJA ZAOKREPTOWANA

RRN: 732014324791 KOD AUT: HOSTOK

DZIEKUJEMY. PROSIMY ZACHOWAC RACHUNEK
16-11-2017 15:26:46

Planet pay

PLANET PAY
UL. JUTRZENKI 139
02-231 WARSZAWA
POS ID: M0000037 MID: 200010000001
Mastercard (02) (11)
541333*****3511
RACHUNEK NR 000040

SPRZEDAZ: 5.00 PLN
TRANSAKCJA ZAOKREPTOWANA

RRN: 732014324793 KOD AUT: HOSTOK

PODPIS:
.....

DZIEKUJEMY. PROSIMY ZACHOWAC RACHUNEK
16-11-2017 15:27:19

Planet pay

PLANET PAY
UL. JUTRZENKI 139
02-231 WARSZAWA
POS ID: M0000037 MID: 200010000001
Mastercard (02) (11)
541333*****3511
RACHUNEK NR 000040

SPRZEDAZ: 5.00 PLN
TRANSAKCJA ZAOKREPTOWANA

RRN: 732014324793

DZIEKUJEMY. PROSIMY ZACHOWAC RACHUNEK
16-11-2017 15:27:19

Planet pay

PLANET PAY
UL. JUTRZENKI 139
02-231 WARSZAWA
POS ID: M0000037 MID: 200010000001
Mastercard (02) (11)
541333*****3511
RACHUNEK NR 000040 KOPIA KLIENTA

SPRZEDAZ: 5.00 PLN
TRANSAKCJA ZAOKREPTOWANA

RRN: 732014324793

DZIEKUJEMY. PROSIMY ZACHOWAC RACHUNEK
16-11-2017 15:27:19

FIGURE 18 TRANSACTION CONFIRMED WITH THE SIGNATURE - PRINTOUTS

3.1.5.3 Transactions without the additional authentication

The transactions without the additional authentication in the form of the PIN or signature concern the contactless and mobile transactions whose amounts amount is not higher than PLN 50.00.

When the card data are read, the application connects with the Authorisation Centre, then, displays the result and prints out the confirmation typical of the specific type of the transaction.

3.2 Types of transactions

The list of transactions that can be carried out on the terminal is available in the transaction menu under the MORE button.

This list can be different depending on e.g. the sales network or point-of-sale profile. Each type of transactions made available by the payment application is described below.

3.2.1 Sales

The Sales transaction is the most popular and most common transaction. It consists in deducting the specific amount from the Client's account in payment for the purchased goods or service.

The Sales transaction is usually set as the default transaction which means that the Sales amount entry field is displayed on the main screen what significantly accelerates the payment acceptance [see: [Starting the transaction on the main screen \(default transaction\)](#)].

In order to make the Sales transaction (the exemplary PIN card transaction procedure):

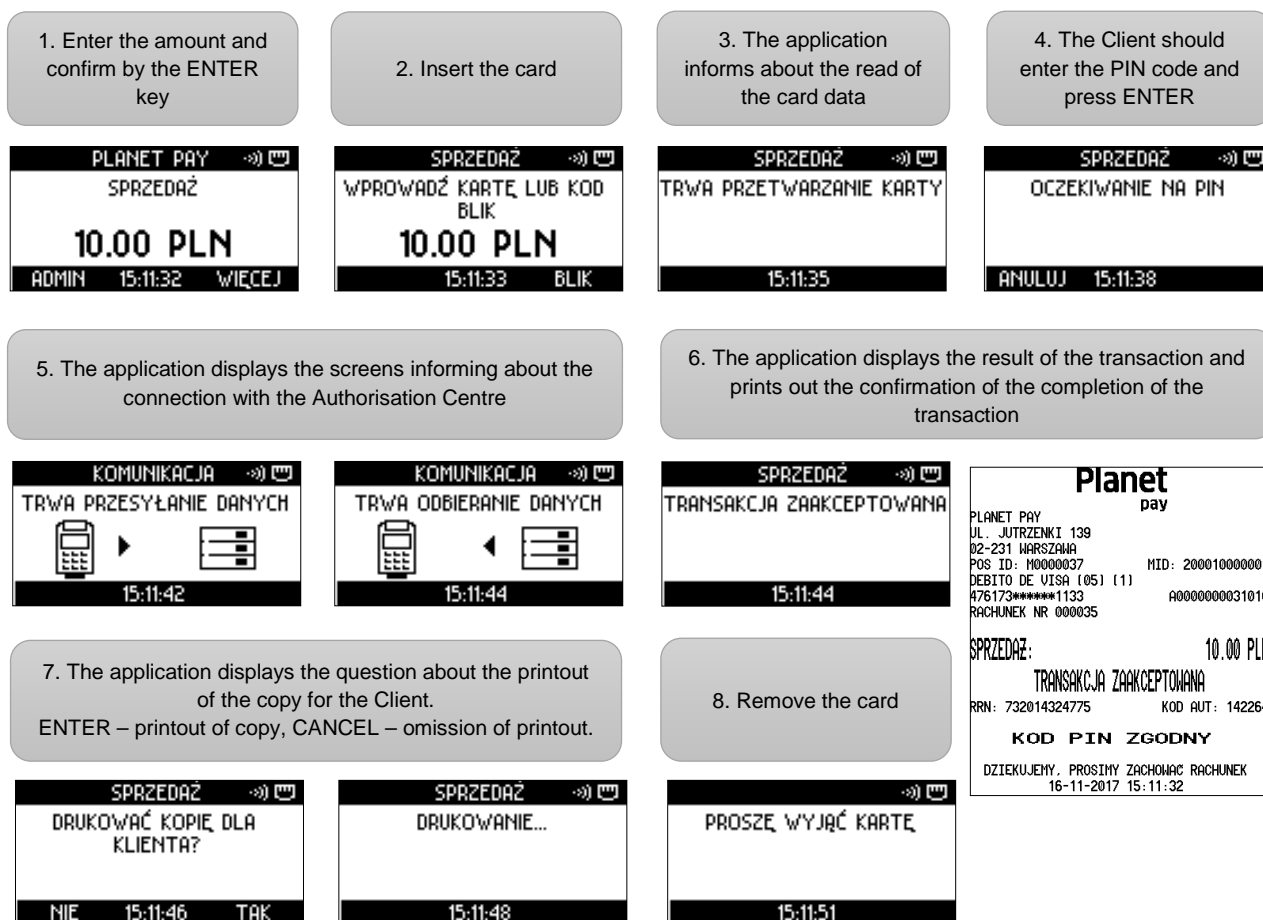


FIGURE 19 THE SALES TRANSACTION WITH PIN CARD –STANDARD PROCESS

Depending on the application settings, when the card is inserted, **the cash withdrawal proposition** can be also displayed on the terminal [see: [Promoted Cash Back – description and procedure](#)]. In such a case the transaction should be continued according to the Client’s decision.

The dynamic currency conversion (DCC) service is available for the Sales transaction. The DCC transaction is carried out in the Client card currency (if it is other than PLN). [see [Dynamic currency conversion – DCC](#)]

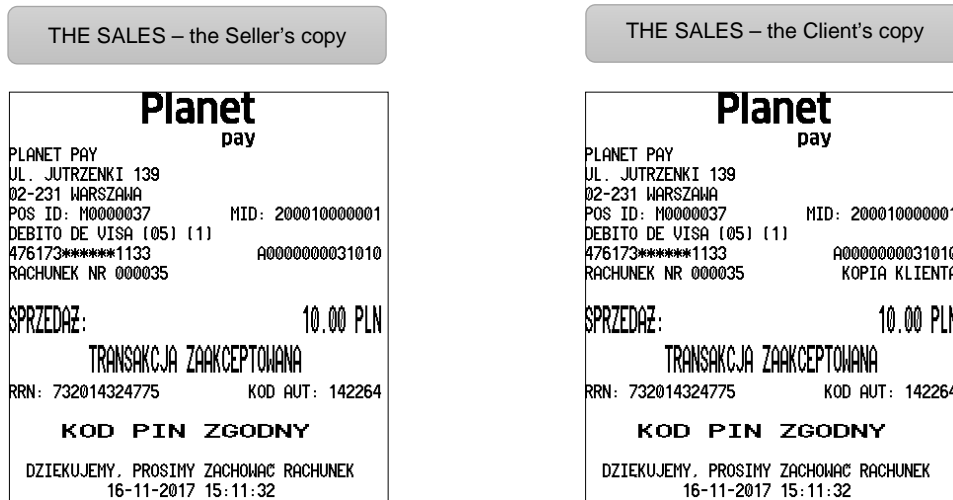


FIGURE 20 THE SALES - THE EXEMPLARY PRINTOUT

3.2.2 Cash Back (Sales and cash withdrawal)

The Cash Back (or Sales and cash withdrawal) transaction is the transaction consisting in making the Sales transaction and paying the Client a sum of money specified by him/her at the same time. The whole amount of the transaction is deducted from the Client's account.

In order to make the Cash Back transaction:

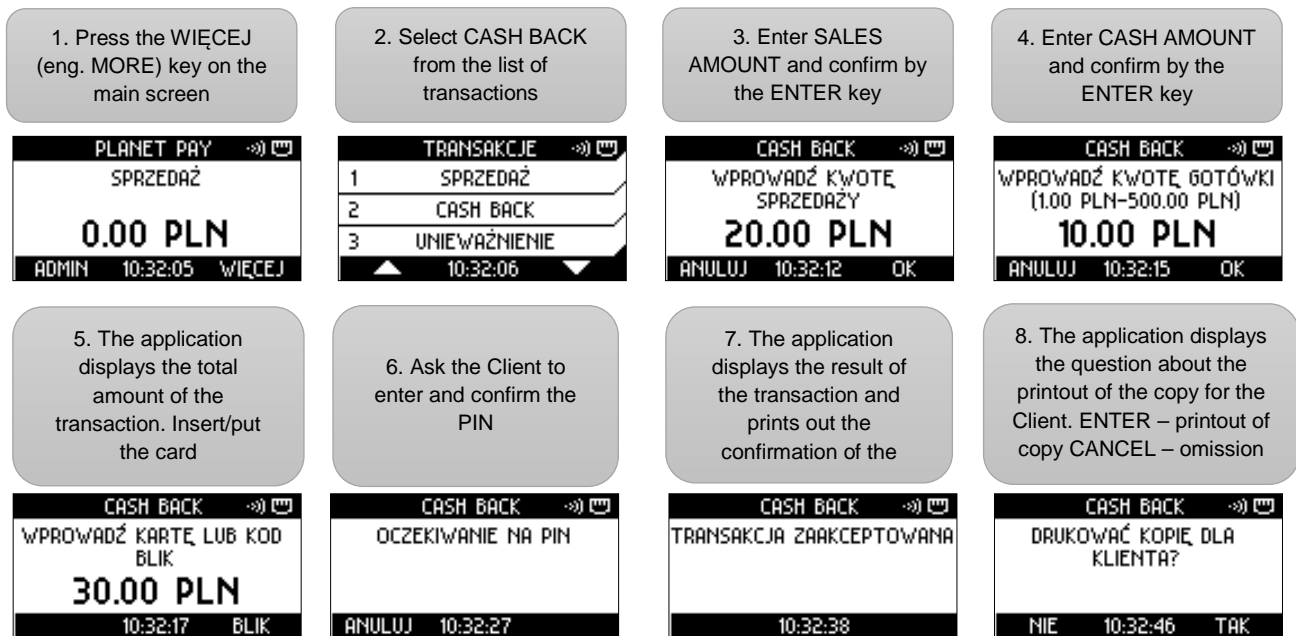


FIGURE 21 THE CASH BACK TRANSACTION - STANDARD PROCEDURE



The Cash Back transaction may be unavailable for certain cards – in such cases the transaction can be rejected OR the application proposes continuing the Sales transaction itself.

The maximum (and minimum) cash withdrawal amount can be different depending on the type of the card used during the transaction and the transaction limits resulting from the application settings (see: [Transaction limits](#))



The Cash Back and DCC transaction cannot be made at the same time [see: [Dynamic currency conversion – DCC](#)]

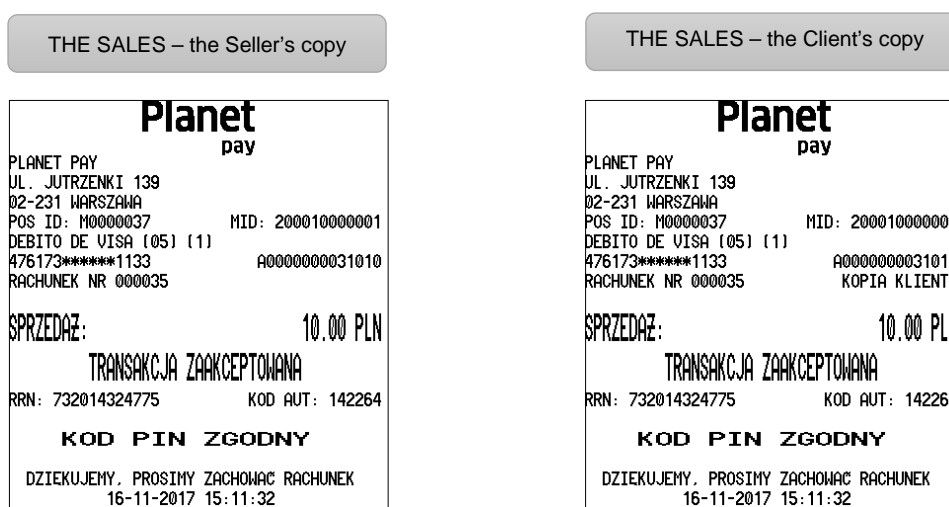


FIGURE 22 THE CASH BACK TRANSACTION - THE EXEMPLARY PRINTOUT

3.2.2.1 Additional question about cash withdrawal during Sales transaction – description and procedure

In certain cases the application may display the cash withdrawal proposition during the Sales transaction [see: [Sales](#)]. The additional question about the cash withdrawal appears when the chip or magnetic card is inserted into the reader.



FIGURE 23 ADDITIONAL QUESTION ABOUT CASH WITHDRAWAL

In this case **ask the Client if he/she wants to withdraw cash and continue the transaction according to his/her decision** (the application continues the Sales transaction if the Client resigns the cash withdrawal)

transaction or Cash Back - Sales and cash withdrawal transaction, if he/she confirms his/her willingness to withdraw cash).

The availability of the cash withdrawal during the Sales transaction depends on the application settings: if the cash withdrawal promotion is not activated - the Client does not receive the cash withdrawal proposition.

However, the Cash Back (Sales and cash withdrawal) transaction as the separate transaction can be visible in the transaction menu (also depending on the application settings).

3.2.3 Cancellation

The Cancellation consists in annulling (withdrawing) the accepted Sales or Cash Back transaction which is not yet sent to be settled (i.e. in practice – which is made the same day).

The Cancellation of the transactions other than the Sales or Cash Back transactions cannot be performed.



NOTE: When the Cash Back transaction is cancelled, remember to take cash from the Client, if it is paid earlier.

In order to perform the Cancellation:

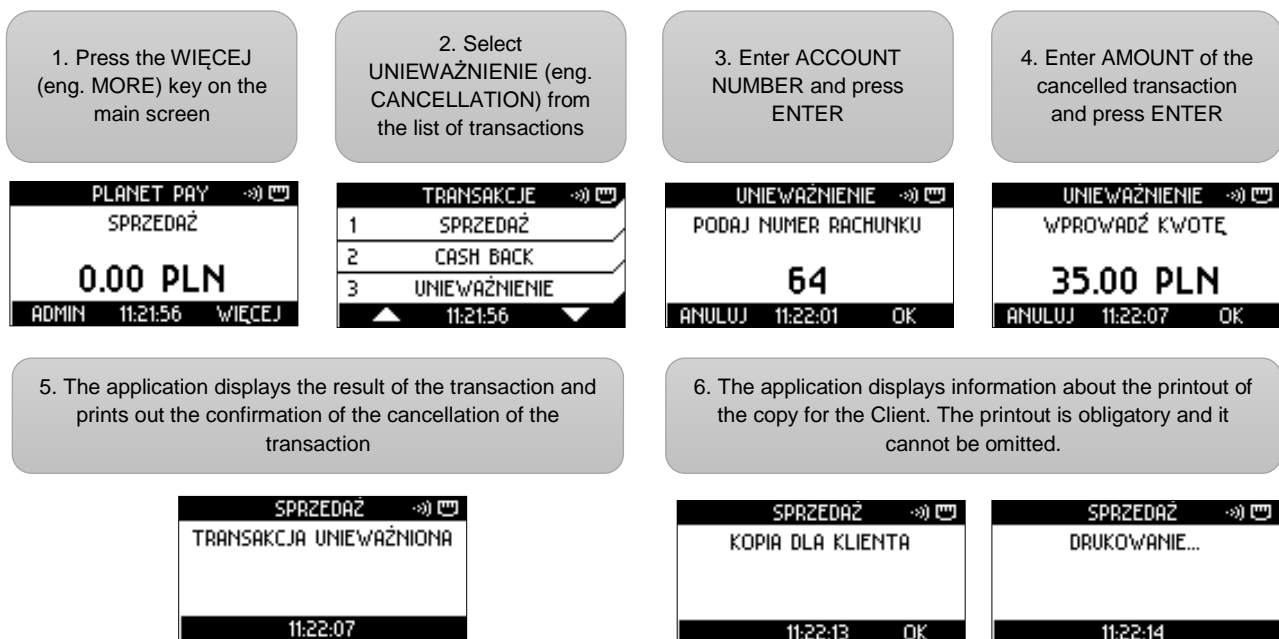


FIGURE 24 CANCELLATION – STANDARD PROCEDURE

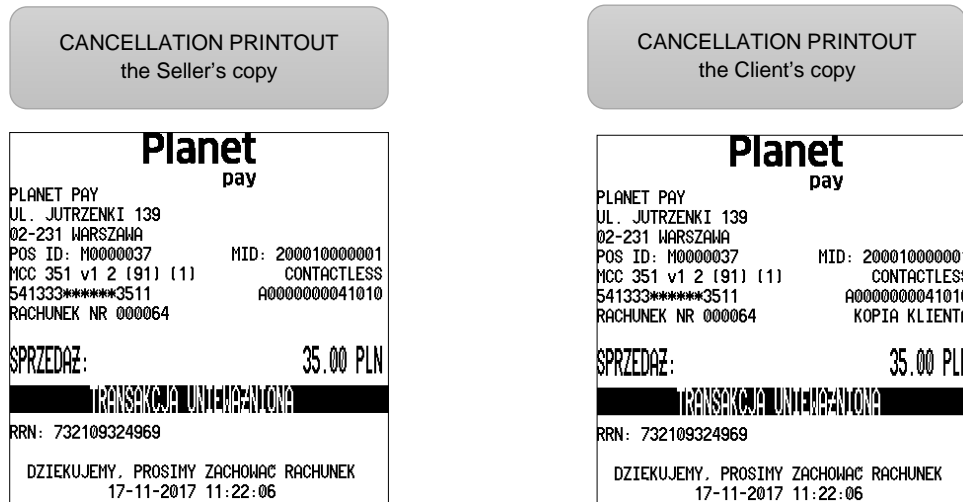


FIGURE 25 CANCELLATION – EXEMPLARY CONFIRMATION PRINTOUTS

In case of the inappropriate data given by the User the application displays one of the following messages:

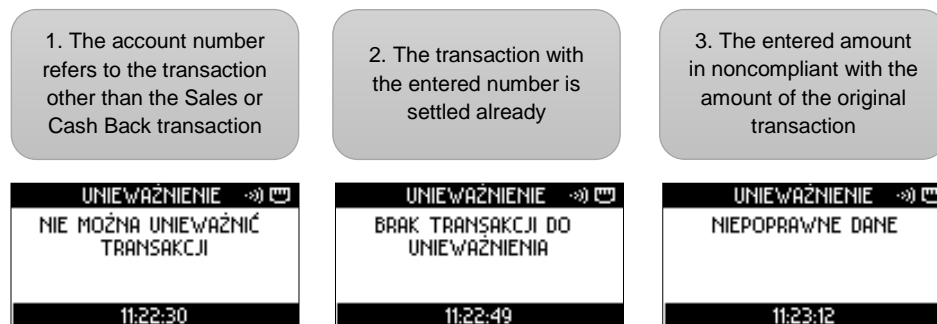


FIGURE 2 CANCELLATION - ERROR MESSAGES



The cancelled transactions are specifically marked on the printouts of the reports and settlements, i.e. by a broken line and “CANCELLED” wording under the data of the withdrawn transaction (see: [Settlement printouts](#))

3.2.4 Copy of the Client's printout

The application allows printing out the copy of every transaction made on the terminal since the last successful Settlement (in practice – performed the same day).

This function is used e.g. when for any reason the original printout is lost or unclear. The copy can be printed out at the Client's request.

When the function is called out, the version of the Client's receipt is printed out.

In order to make the copy of the Client's printout:

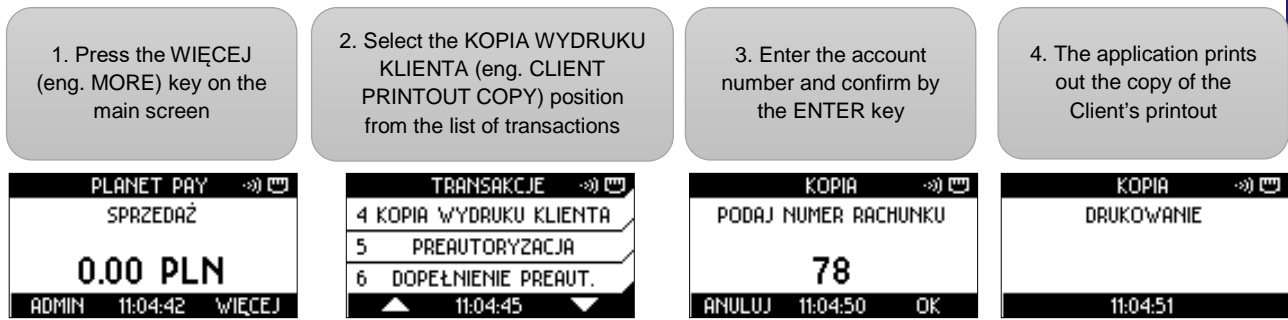


FIGURE 27 COPY OF CLIENT'S PRINTOUT – STANDARD PROCEDURE

i If the Seller or the Client do not remember the account number, it may be helpful to draw a detailed report including the list of transactions, numbers of their accounts and amounts.

If the copy of the Prepaid GSM transaction is printed out, the data of the top-up code are masked with asterisks.

The Client's copy of the settled transaction cannot be printed out.

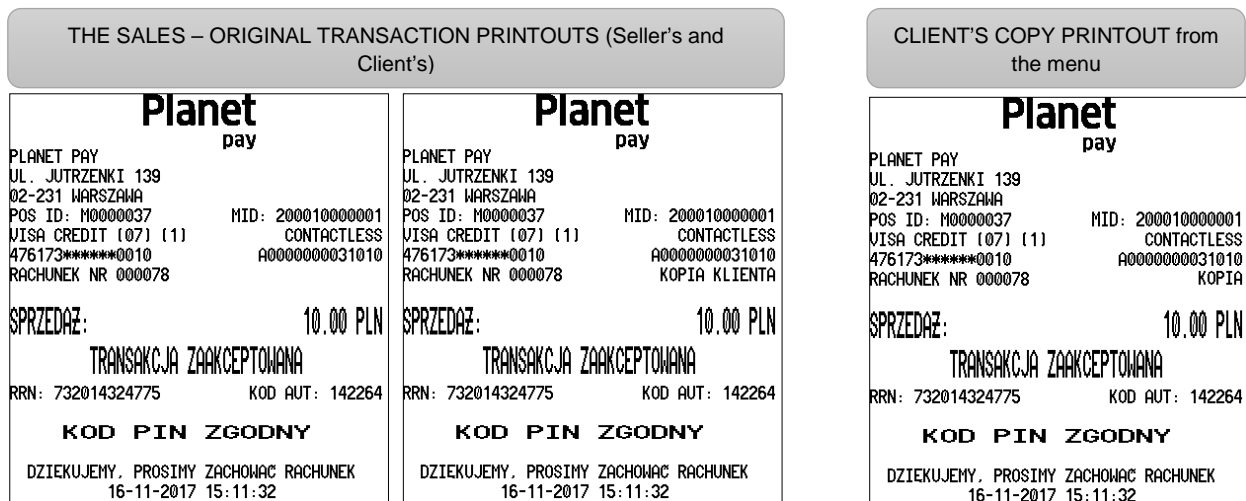


FIGURE 28 COPY OF CLIENT'S PRINTOUT – THE SALES

PREPAID GSM – ORIGINAL TRANSACTION PRINTOUTS (Seller's and Client's)

CLIENT'S COPY PRINTOUT from the menu

Planet
pay

PLANET PAY
UL. JUTRZENKI 139
02-231 WARSZAWA
POS ID: M0000037 MID: 200010000001
VISA CREDIT (07) (11) CONTACTLESS
476173*****0010 A0000000031010
RACHUNEK NR 000078

PREPAID GSM: 30.00 PLN
TRANSAKCJA ZAAKCEPTOWANA

RRN: 732110325006 KOD AUT: 103489

DZIEKUJEMY. PROSIMY ZACHOWAC RACHUNEK
17-11-2017 11:04:04

Planet
pay

PLANET PAY
UL. JUTRZENKI 139
02-231 WARSZAWA
POS ID: M0000037 MID: 200010000001
VISA CREDIT (07) (11) CONTACTLESS
476173*****0010 A0000000031010
RACHUNEK NR 000078 KOPIA KLIENTA

PREPAID GSM: 30.00 PLN
TRANSAKCJA ZAAKCEPTOWANA

RRN: 732110325006 KOD AUT: 103489

Play
Kod doładowania:
0037 8676 2371 33

JAK DOŁADOWAĆ KONTO?
* WYBIERZ NA KLAWIATURZE *100*
* WPISZ 14-CYFROWY KOD I NACISNIJ #
* ZATWIERDZ OPERACJE TAK, JAK ZATWIERDZASZ
NUMER TELEFONU, GDY DZWONISZ.
PO PRAWIDŁOWYM DOŁADOWANIU OTRZYMASZ
WIADOMOŚĆ O AKTUALNYM STANIE KONTA I
OKRESIE JEGO WAZNOŚCI.
WWW.PLAYMOBILE.PL
OBŚŁUGA KLIENTA-ZADZWON *500

Data ważności: 2018-12-31
Numer seryjny: 136821405878



DZIEKUJEMY. PROSIMY ZACHOWAC RACHUNEK
17-11-2017 11:04:04

Planet
pay

PLANET PAY
UL. JUTRZENKI 139
02-231 WARSZAWA
POS ID: M0000037 MID: 200010000001
VISA CREDIT (07) (11) CONTACTLESS
476173*****0010 A0000000031010
RACHUNEK NR 000078 KOPIA


PREPAID GSM: 30.00 PLN
TRANSAKCJA ZAAKCEPTOWANA

RRN: 732110325006 KOD AUT: 103489

Play
Kod doładowania:
****** * * * * ***

JAK DOŁADOWAĆ KONTO?
* WYBIERZ NA KLAWIATURZE *100*
* WPISZ 14-CYFROWY KOD I NACISNIJ #
* ZATWIERDZ OPERACJE TAK, JAK ZATWIERDZASZ
NUMER TELEFONU, GDY DZWONISZ.
PO PRAWIDŁOWYM DOŁADOWANIU OTRZYMASZ
WIADOMOŚĆ O AKTUALNYM STANIE KONTA I
OKRESIE JEGO WAZNOŚCI.
WWW.PLAYMOBILE.PL
OBŚŁUGA KLIENTA-ZADZWON *500

Data ważności: 2018-12-31
Numer seryjny: 136821405878



DZIEKUJEMY. PROSIMY ZACHOWAC RACHUNEK
17-11-2017 11:04:04

FIGURE 29 COPY OF CLIENT'S PRINTOUT – PREPAID GSM

3.2.5 Preauthorisation

The preauthorisation consists in blocking temporarily the funds on the Client's for the later payment. This means that the funds are not transferred to the Seller's account but only reserved until the payment for the service is made [see: [Completion of preauthorisation](#)] or the expiry of blockade. The fund blockage period can be different depending on the type of the card used

The preauthorisation is often used when booking hotel rooms or renting cars as the Seller's security – the guarantee that there will be sufficient funds on the Client's account for the later settlement.



The data on the confirmation of the Preauthorisation are necessary for the performance of the later settlement (Completion of preauthorisation).

It is recommended to keep the printout and store it until the Completion or release of blockade.

In order to make the Preauthorisation:

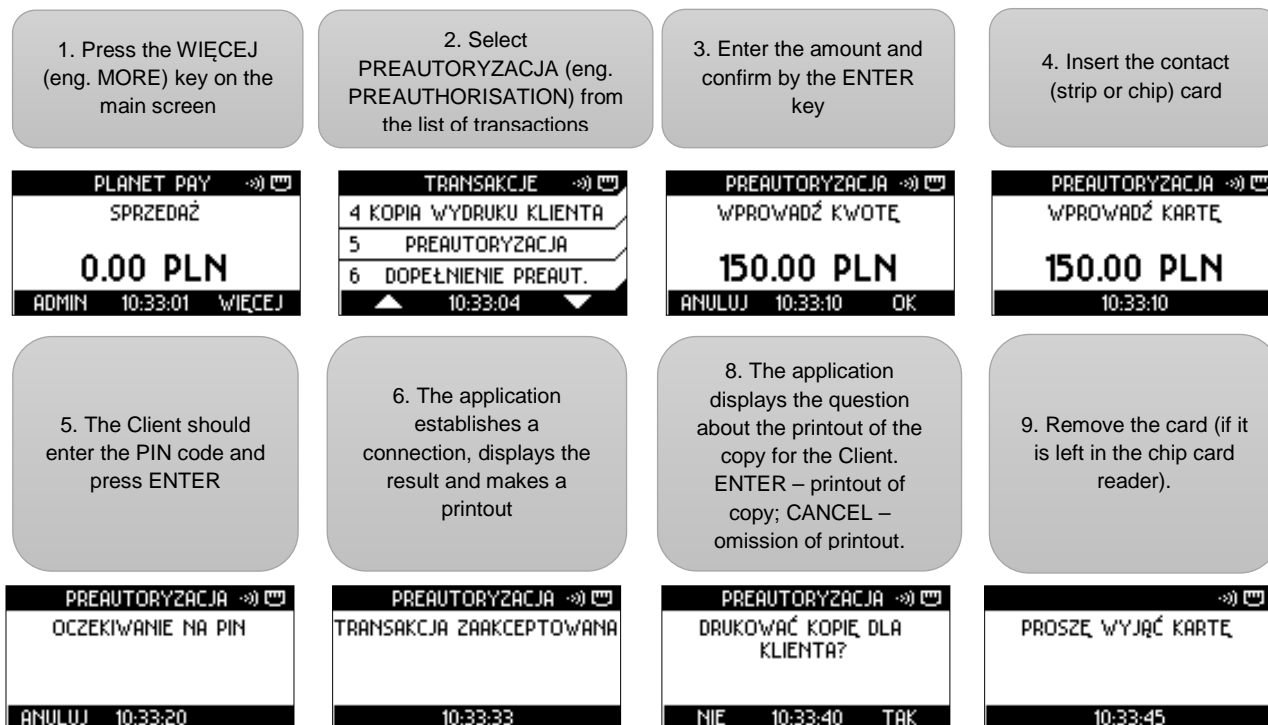


FIGURE 29 PREAUTHORIZATION WITH PIN – STANDARD PROCEDURE

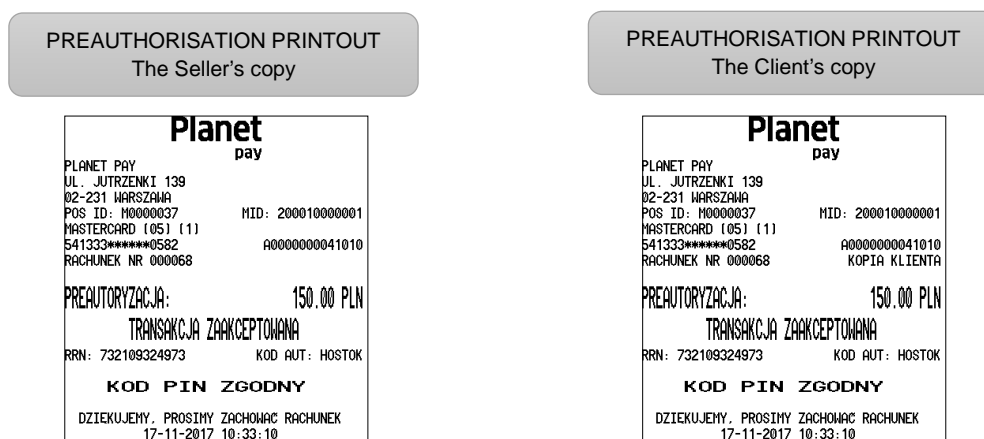


FIGURE 31 PREAUTHORIZATION– EXEMPLARY CONFIRMATION PRINTOUTS

Depending on the application settings the Preauthorisation can be performed also without the physical presence of the payment card, only with the use of the data of the card made available by the Client (e.g. on the basis of the data given by telephone). In such a case the Seller manually enters the required data – card number, card expiry date (located on the card reverse) and CVV2/CVC2 code (located on the card reverse).



The necessity of giving the expiry date and/or CVV2/CVC2 code is optional and depends on the Provider's settings.

In order to make the Preauthorisation without the physical presence of the payment card:



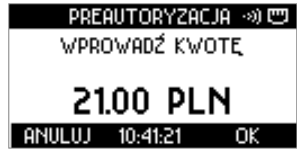

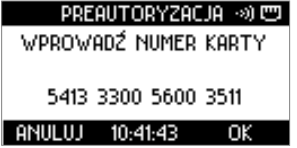

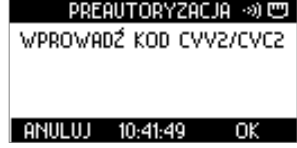

<p>1. Press the WIĘCEJ (eng. MORE) key on the main screen</p>	<p>2. Select PREAUTORYZACJA (eng. PREAUTHORISATION) from the list of transactions</p>	<p>3. Enter the amount and confirm by the ENTER key</p>	<p>4. The application displays the card insertion screen</p>
			
<p>5. Using the 0-9 keys, enter manually the card number. Confirm by the ENTER key</p>	<p>6. Enter the card expiry date (month/year). Confirm by the ENTER key</p>	<p>7. Enter the CVV2/CVC2 code (3 characters). AND confirm by the ENTER key. These data are masked with asterisks. OR skip the entry of the code by pressing ENTER</p>	
			
<p>8. The further part of the transaction procedure is similar to the standard transaction procedure: The application connects with the Authorisation Centre, then displays the result of the transaction and prints out the confirmation.</p>			

FIGURE 32 PREAUTHORIZATION– MANUALLY ENTERING THE CARD DATA



The preauthorisation cannot be performed as the contactless transaction - the icon of the contactless transactions is not visible on the card insertion screen; the BLIK option is also unavailable for this operation.

The amounts of the performed Preauthorisations are not included in the IN TOTAL section on the printouts of the Settlements

The Cancellation cannot be carried out for the Preauthorisation.

If the data entered by the User are incorrect (e.g. card number or expiry date format), after the attempted confirmation the application displays the message with information about the error.

3.2.6 Completion of preauthorisation

The Completion is the transaction consisting in settling the funds reserved earlier during the Preauthorisation [see: [Preauthorisation](#)]. The amount of the Completion is transferred from the Client's account to the Seller's account.



The Completion can be performed for the same or lower amount but not higher than the amount of the Preauthorisation. If the final amount to be paid is higher, apart from the Completion the additional Sales transaction for the remaining amount should be made

The Completion may be performed on the different device than the Preauthorisation (e.g. on the other terminal in the same point of sale or of the same sales network)



The Completion is made without the use of the Client's payment card.

The data included on the confirmation of the earlier completed Preauthorisation are necessary for the performance of the Completion.

In order to make the Completion of the preauthorisation:

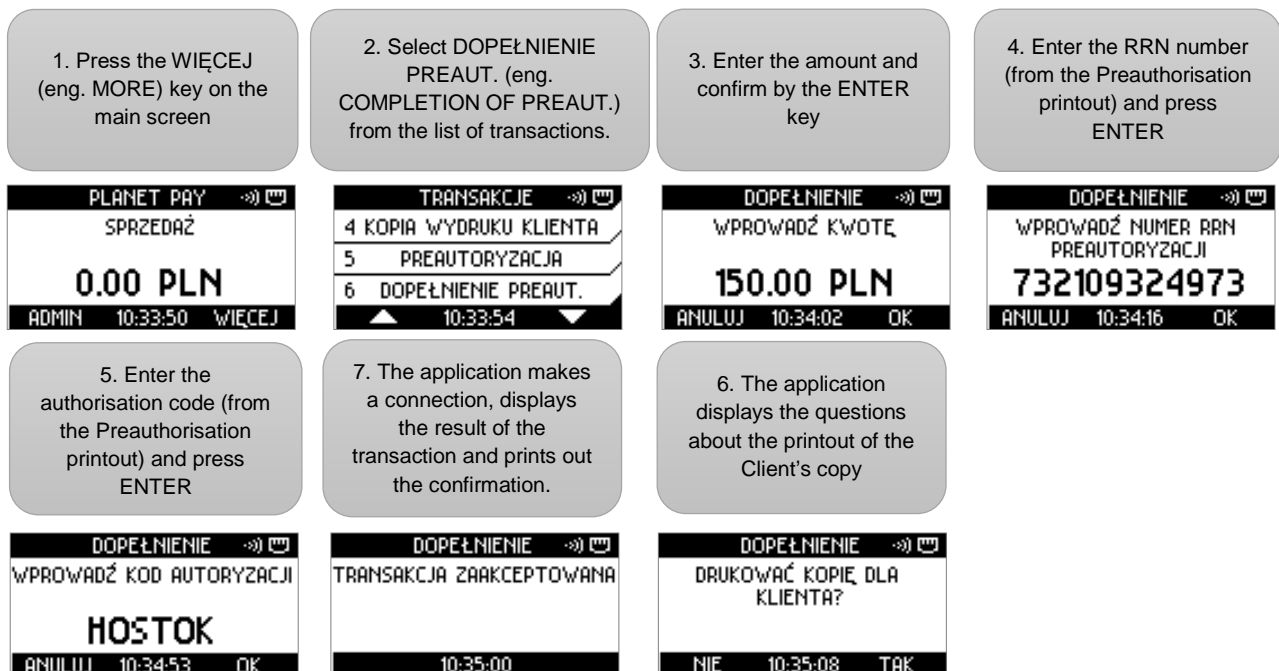


FIGURE 33 COMPLETION OF PREAUTHORISATION – STANDARD PROCEDURE

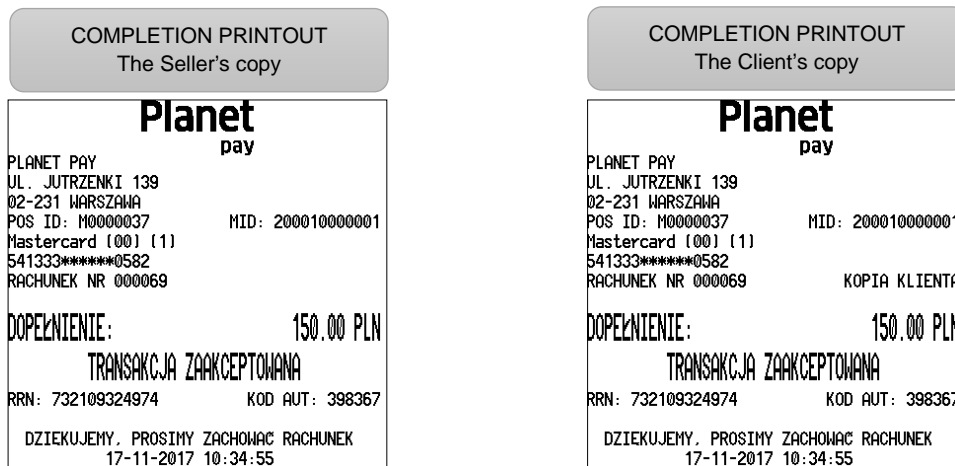


FIGURE 34 COMPLETION OF PREAUTHORISATION – EXEMPLARY CONFIRMATION PRINTOUTS

3.2.7 Prepaid GSM

The Prepaid GSM transaction allows selling the GSM top-ups by using the card- or cash-based payment. The transaction procedure is presented below.

3.2.7.1 Prepaid GSM – card-based payment

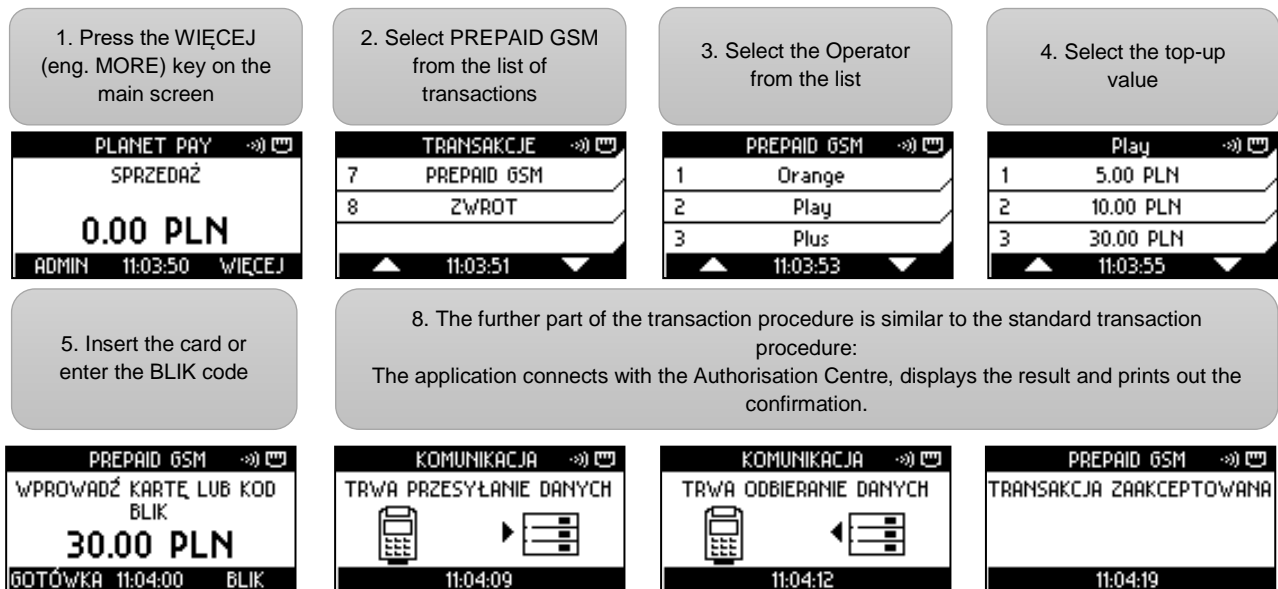


FIGURE 35 PREPAID GSM – CARD-BASED PAYMENT

3.2.7.2 Prepaid GSM – cash-based payment

If the Client declares to pay in cash, on the card insertion screen:

1. Select the GOTÓWKA (eng. CASH) option



2. The application connects with the Authorisation Centre and displays the result of the transaction.



3. The application displays the „Gotówka otrzymana?” (eng. “Cash received?”) question. The confirmations are printed out when the proper value is selected.

If the „NIE” (eng. “NO”) answer is indicated, the code is not printed out, and the transaction is cancelled

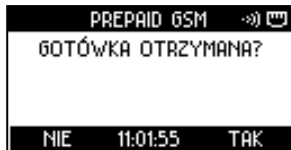


FIGURE 36 PREPAID GSM – CASH-BASED PAYMENT

Prepaid GSM – card-based payment, transaction accepted



Prepaid GSM – copy printout from the menu



FIGURE 37 PREPAID GSM – EXEMPLARY PRINTOUTS

3.2.8 Return

The Return transaction is the transaction opposite of the Sales transaction, i.e. the transaction amount is transferred (returned) to the Client's account.



The access to the Return transaction is protected by the Administrator's password.

The Return transaction is performed when the Client returns the goods for which he/she paid by card, and the original Sales transaction cannot be longer cancelled (the original transaction is already sent for the settlement). The return should be made with the same card which was used earlier during the Sales transaction.



The Return transaction is always confirmed by the Client's signature, regardless of the type of the card used.

The dynamic currency conversion (DCC) service is available for the Return transaction. In order to make the Return transaction:







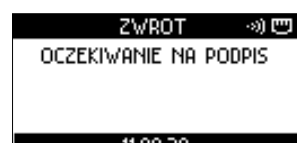
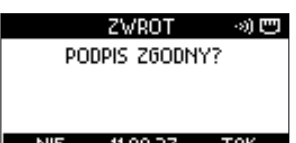


<p>1. Press the WIĘCEJ (eng. MORE) key on the main screen</p>	<p>2. Select ZWROT (eng. RETURN) the list of transactions</p>	<p>3. Enter the Administrator's password</p>	<p>4. The entered characters are masked</p>
			
<p>5. Enter the return amount and confirm by the ENTER key</p>	<p>6. Insert the card into the reader or put the proximity card</p>	<p>7. The application prints out the confirmation with the place for the Client's signature and displays the question about the compliance of the signature. If it is compliant, press ENTER</p>	
			
<p>8. The application displays information about the printout of the Client's copy. The printout is obligatory and cannot be omitted. Press ENTER</p>		<p>10. Remove the cards (if it is left in the reader of the chip cards).</p>	
			

FIGURE 38 RETURN – THE SIGNATURE COMPLIANT

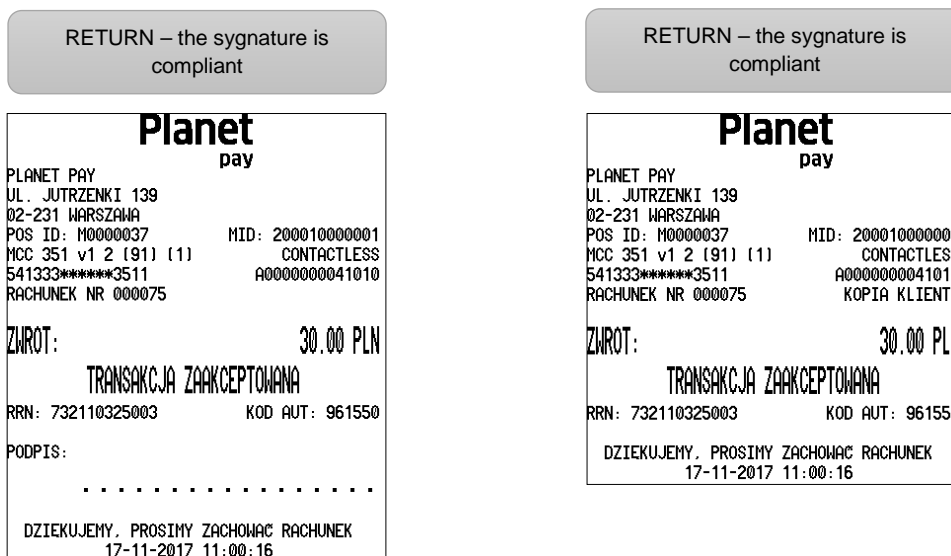


FIGURE 39 RETURN - THE SIGNATURE COMPLIANT – PRINTOUTS

If the Client's signature on the confirmation of the transactions is noncompliant with the signature put on the card:

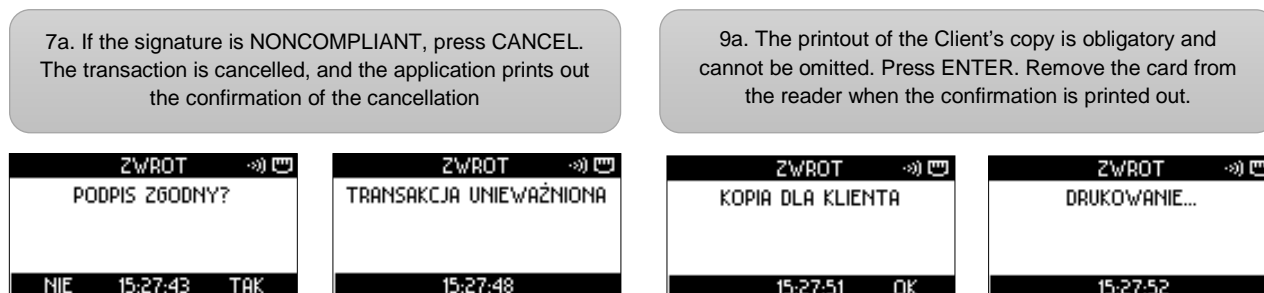


FIGURE 40 RETURN - THE SIGNATURE NONCOMPLIANT

RETURN – Seller's printout with the place for the signature

Planet pay

PLANET PAY
UL. JUTRZENKI 139
02-231 WARSZAWA
POS ID: M0000037 MID: 200010000001
Mastercard (02) (1)
541333*****3511
RACHUNEK NR 000040

ZWROT: 30.00 PLN

TRANSAKCJA ZAACCEPTOWANA

RRN: 732014324793 KOD AUT: HOSTOK

PODPIS:

.....

DZIEKUJEMY, PROSIMY ZACHOWAC RACHUNEK
16-11-2017 15:27:19

RETURN – Seller's printout with the place for the signature

Planet pay

PLANET PAY
UL. JUTRZENKI 139
02-231 WARSZAWA
POS ID: M0000037 MID: 200010000001
Mastercard (02) (1)
541333*****3511
RACHUNEK NR 000040

ZWROT: 30.00 PLN

TRANSAKCJA UNWAZNIWIONA

RRN: 732014324793

DZIEKUJEMY, PROSIMY ZACHOWAC RACHUNEK
16-11-2017 15:27:19

Planet pay

PLANET PAY
UL. JUTRZENKI 139
02-231 WARSZAWA
POS ID: M0000037 MID: 200010000001
Mastercard (02) (1)
541333*****3511
RACHUNEK NR 000040 KOPIA KLIENTA

ZWROT: 30.00 PLN

TRANSAKCJA UNWAZNIWIONA

RRN: 732014324793

DZIEKUJEMY, PROSIMY ZACHOWAC RACHUNEK
16-11-2017 15:27:19

FIGURE 41 RETURN - THE SIGNATURE NONCOMPLIANT - PRINTOUTS

3.3 Dynamic currency conversion – DCC

Depending on the configuration the application makes available the DCC (dynamic currency conversion) service.

This allows the Client to make payments in the foreign currency in which the card is issued (if other than PLN).

If the DCC service is activated in the application, when the data of the card are read, the transaction amount is displayed and printed out in both currencies – PLN and the card's currency, and the Client should be asked to select the currency. The further part of the transaction procedure is similar to the standard transaction procedure.

The exemplary procedure of the transaction with the DCC option is presented below.

1. Enter and confirm the transaction amount

2. Insert the contact card

3. The application displays and prints out the conversion of the currencies. Ask the Client in what currency he/she wants to pay and press the corresponding key.

PLANET PAY →

SPRZEDAŻ

30.00 PLN

ADMIN 10:54:44 WIECEJ

SPRZEDAŻ →

WPROWADZ KARTE LUB KOD BLIK

30.00 PLN

10:54:46 BLIK

DCC →

CHOOSE CURRENCY

30.00 PLN
7.78 EUR

PLN 10:55:02 EUR

DCC Quote

TOTAL: 30.00 PLN

Exchange rate: 1 PLN=0.2593463 EUR

Commission: 0.00 EUR

Fee/Mark-up: 0.000000%

TOTAL: 7.78 EUR

This Currency Conversion is provided by IBANK

17-11-2017 10:54:44

The further part of the transaction procedure is similar to the standard transaction procedure, the application request the Client to enter the PIN or put the signature, displays the result and prints out the confirmation.

FIGURE 42 DCC TRANSACTION - PROCEDURE



If the foreign currency is selected, the Client's copy is printed out in English.

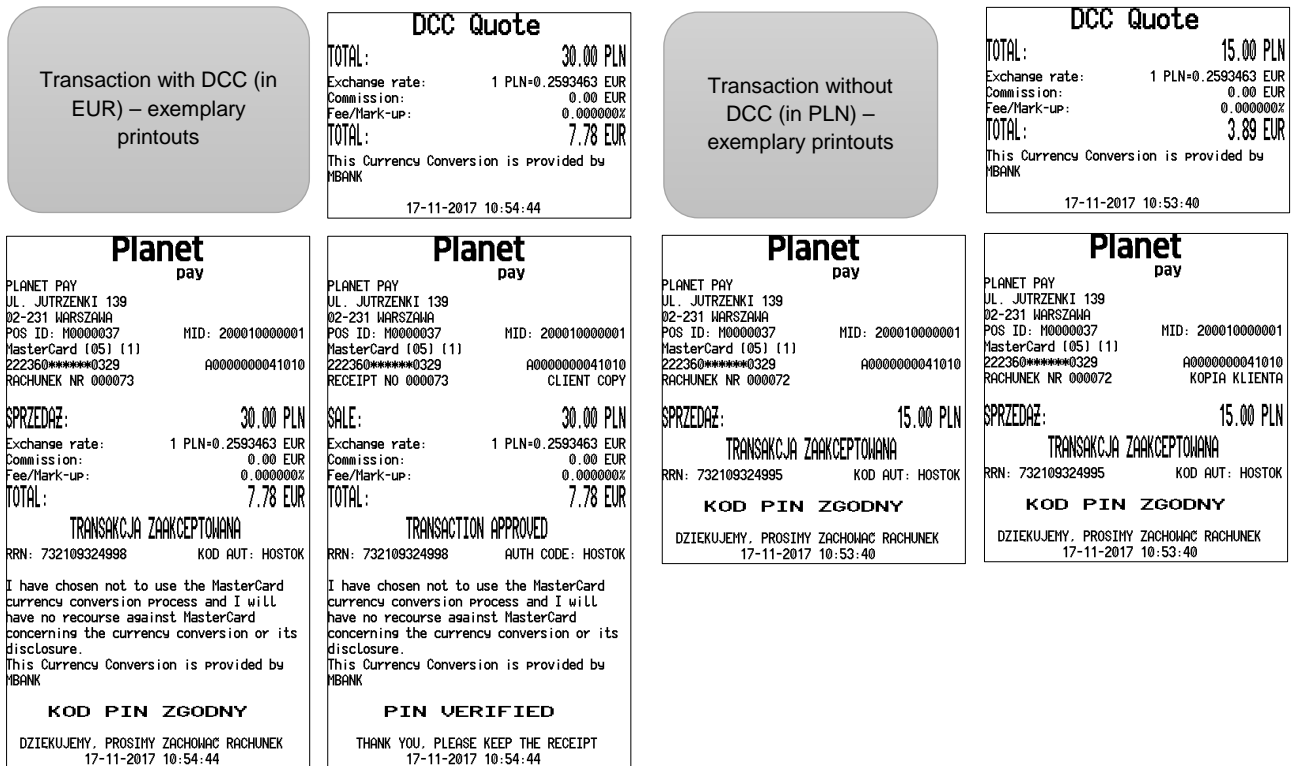


FIGURE 3 DCC - EXEMPLARY PRINTOUTS



The DCC option is always unavailable for the contactless transactions.
The DCC proposition never appears for the cards whose currency is PLN.

4. Administration functions

4.1 Settlement

The SETTLEMENT function consists in transferring the data of all accepted transactions performed on the terminal to the authorisation host.



After the successful Settlement the transactions on the terminal are deleted which means that:

- in each case the data of the transactions performed since the last (successful) Settlement are transmitted
- it is not possible to make the Cancellation and the Copy of the account of the settled transaction

The Settlement is successful, if the "Zgodność z hostem" (eng. "Compliance with host") result is specified on the printout or, in exceptional cases, the "Niezgodność z hostem" (eng. "Noncompliance with host") result.



If the “Niezgodność z hostem” (eng. “Noncompliance with host”) message recurs on the subsequent printouts of Settlements, contact the Service Centre.

If the Settlement error message recurs on the printouts, absolutely contact the Service Centre.

The copy of the Settlement printout cannot be done.

4.1.1 Call of Settlement

Depending on the configuration the Settlement can be carried out by the application automatically once a day on the specific weekdays at the determined time.

If need be, the function can be called manually from the ADMIN menu:

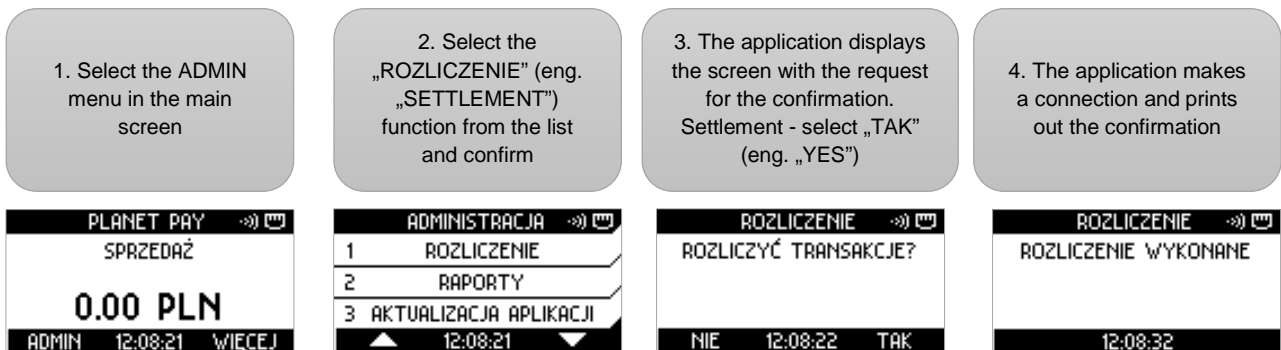


FIGURE 44 SETTLEMENT – STANDARD PROCEDURE

4.1.2 Settlement printouts

The complete Settlement printouts, in addition to the data of the point of sale (address, TID, MID), date and time, include:

- The title of the SETTLEMENT with the result (e.g. “Compliance with host”)
- The number of the Settlement (PACKAGE)
- The IN TOTAL section - the summary of the payments with breakdown into the type and number of the transactions: SALES, RETURN, CASH
- The separate sections with the summary of the BLIK, DCC transactions (if available on the terminal) and GSM TOP-UPS (if available)
- The DETAILED section with the list of all the accepted transactions. The list includes:
 - Transactions account number
 - Transaction type
 - Transaction amount
 - Transaction performance date and time
- The sales amount and cash withdrawal amount are printed out separately in the DETAILED section for the Cash Back (Sales and cash withdrawal) transactions.
- For the convenience of the User the cancelled transactions - marked by the broken line and CANCELLED wording - are specified on the printout in the DETAILED section. The amounts of the cancelled transactions are not included in the Balance in the IN TOTAL section, just like the amounts of the Preauthorisation transactions.

If there are no transactions to be settled on the terminal, the printout includes the zero values of amounts and numbers of transactions, and “Brak transakcji” (eng. “No transaction”) information appears in the DETAILED section.

In addition, depending on the configuration:

- the Settlement printout may not include the DETAILED section.
- if no transaction is made on the terminal since the last successful Settlement, the confirmation of the performance of the Settlement may not be printed out

- PREPAID transactions activated
- DCC service activated
- printout of transaction details activated

Planet
pay

PLANET PAY
UL. JUTRZENKI 139
02-231 WARSZAWA
POS ID: M0000037 MID: 200010000001

ROZLICZENIE
ZGODNOŚĆ Z HOSTEM
Paczka: 24

SUMARYCZNIE

Sprzedaz	14 transakcji	269.00 PLN
Zwrot	2 transakcji	110.00 PLN
Gotówka	1 transakcji	20.00 PLN
SALDO		179.00 PLN

W TYM:

TRANSAKcje DCC

Sprzedaz	1 transakcji	25.00 PLN
Zwrot	1 transakcji	20.00 PLN

TRANSAKcje BLIK

Sprzedaz	0 transakcji	0.00 PLN
Zwrot	0 transakcji	0.00 PLN
Gotówka	0 transakcji	0.00 PLN

DOŁADOWANIA GSM

Karta	2 transakcji	35.00 PLN
Blik	0 transakcji	0.00 PLN
Gotówka	2 transakcji	35.00 PLN

SZCZEGÓLNE

000079	SPRZEDAŻ	15.00 PLN	17.11.11.28
000080	SPRZEDAŻ	25.00 PLN	17.11.11.28
000081	SPRZEDAŻ	30.00 PLN	17.11.11.29
000082	SPRZEDAŻ	7.00 PLN	17.11.11.29
000083	SPRZEDAŻ	4.00 PLN	17.11.11.29
000084	SPRZEDAŻ	8.00 PLN	17.11.11.29
000085	SPRZEDAŻ	9.00 PLN	17.11.11.29
000086	SPRZEDAŻ	46.00 PLN	17.11.11.29
000088	SPRZEDAŻ	30.00 PLN	17.11.12.04
	GOTÓWKA	20.00 PLN	
000089	SPRZEDAŻ	25.00 PLN	17.11.12.04
000090	ZWROT	90.00 PLN	17.11.12.05
000091	ZWROT	20.00 PLN	17.11.12.05
000092	GSM Orange	10.00 PLN	17.11.12.06
000094	GSM T-Mobile	25.00 PLN	17.11.12.06
000095	GSM Heyah	30.00 PLN	17.11.12.06
000096	GSM Play	5.00 PLN	17.11.12.07

17-11-2017 12:08:23

- PREPAID transactions activated
- DCC service activated
- printout of transaction details deactivated

Planet
pay

PLANET PAY
UL. JUTRZENKI 139
02-231 WARSZAWA
POS ID: M0000037 MID: 200010000001

ROZLICZENIE
ZGODNOŚĆ Z HOSTEM
Paczka: 26

SUMARYCZNIE

Sprzedaz	6 transakcji	116.50 PLN
Zwrot	0 transakcji	0.00 PLN
Gotówka	1 transakcji	50.00 PLN
SALDO		166.50 PLN

W TYM:

TRANSAKcje DCC

Sprzedaz	0 transakcji	0.00 PLN
Zwrot	0 transakcji	0.00 PLN

TRANSAKcje BLIK

Sprzedaz	0 transakcji	0.00 PLN
Zwrot	0 transakcji	0.00 PLN
Gotówka	0 transakcji	0.00 PLN

DOŁADOWANIA GSM

Karta	0 transakcji	0.00 PLN
Blik	0 transakcji	0.00 PLN
Gotówka	1 transakcji	5.00 PLN

17-11-2017 12:21:07

- PREPAID transactions deactivated
- DCC service deactivated
- printout of transaction details activated

Planet
pay

PLANET PAY
UL. JUTRZENKI 139
02-231 WARSZAWA
POS ID: M0000037 MID: 200010000001

ROZLICZENIE
ZGODNOŚĆ Z HOSTEM
Paczka: 25

SUMARYCZNIE

Sprzedaz	5 transakcji	88.00 PLN
Zwrot	1 transakcji	60.00 PLN
Gotówka	1 transakcji	25.00 PLN
SALDO		53.00 PLN

W TYM:

TRANSAKcje BLIK

Sprzedaz	0 transakcji	0.00 PLN
Zwrot	0 transakcji	0.00 PLN
Gotówka	0 transakcji	0.00 PLN

SZCZEGÓLNE

000097	SPRZEDAŻ	2.00 PLN	17.11.12:10
000098	SPRZEDAŻ	6.00 PLN	17.11.12:10
000099	SPRZEDAŻ	45.00 PLN	17.11.12:10
000100	SPRZEDAŻ	30.00 PLN	17.11.12:10
	GOTÓWKA	25.00 PLN	
000101	ZWROT	60.00 PLN	17.11.12:11
000102	SPRZEDAŻ	5.00 PLN	17.11.12:11

17-11-2017 12:12:47

FIGURE 45 SETTLEMENT – EXEMPLARY PRINTOUTS

4.2 Reports

The REPORTS function allows making the printout with the summary of the transactions performed on the terminal since the last Settlement until the call of the report [see: [Settlement](#)].



The call of the report does NOT result in sending the transactions for the settlement and does NOT delete the transactions from the terminal.

The reports can be done many times through the day and their content can be different, especially, if the new transaction is performed on the terminal between the calls of the Reports.

The printouts of the Reports are not numbered.

4.2.1 Summary

The Summary Report printouts, in addition to the data of the point of sale (address, TID, MID), date and time, include:

- The title of the Report
- The IN TOTAL section - the summary of the payments with breakdown into the type and number of the transactions: SALES, RETURN, CASH
- The separate sections with the summary of the BLIK, DCC transactions (if available on the terminal) and GSM TOP-UPS (if available)

4.2.2 Detailed

The Detailed Report printouts, in addition to the data specified in the Summary report, include the DETAILED section described in the chapter [Settlement printouts](#).

4.2.3 GSM top-up report

The GSM TOP-UP Report printouts, in addition to the data of the point of sale (address, TID, MID), date and time, include the summary of the accepted Prepaid GSM transactions with breakdown into:

- payment methods – CARD, BLIK, CASH (Operator, denomination, number of transactions, total amount)
- individual Operators (number of transactions and total amount) - IN TOTAL section

The GSM top-up report is visible in the REPORTS menu, if the Prepaid GSM transaction is available on the terminal.

4.2.4 Generation of report

The individual reports can be generated from the ADMIN menu, REPORTS submenu:

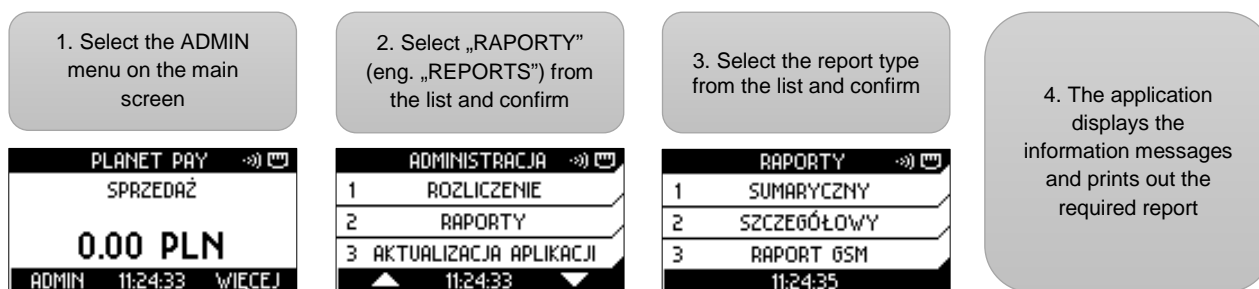


FIGURE 56 GENERATION OF THE REPORT

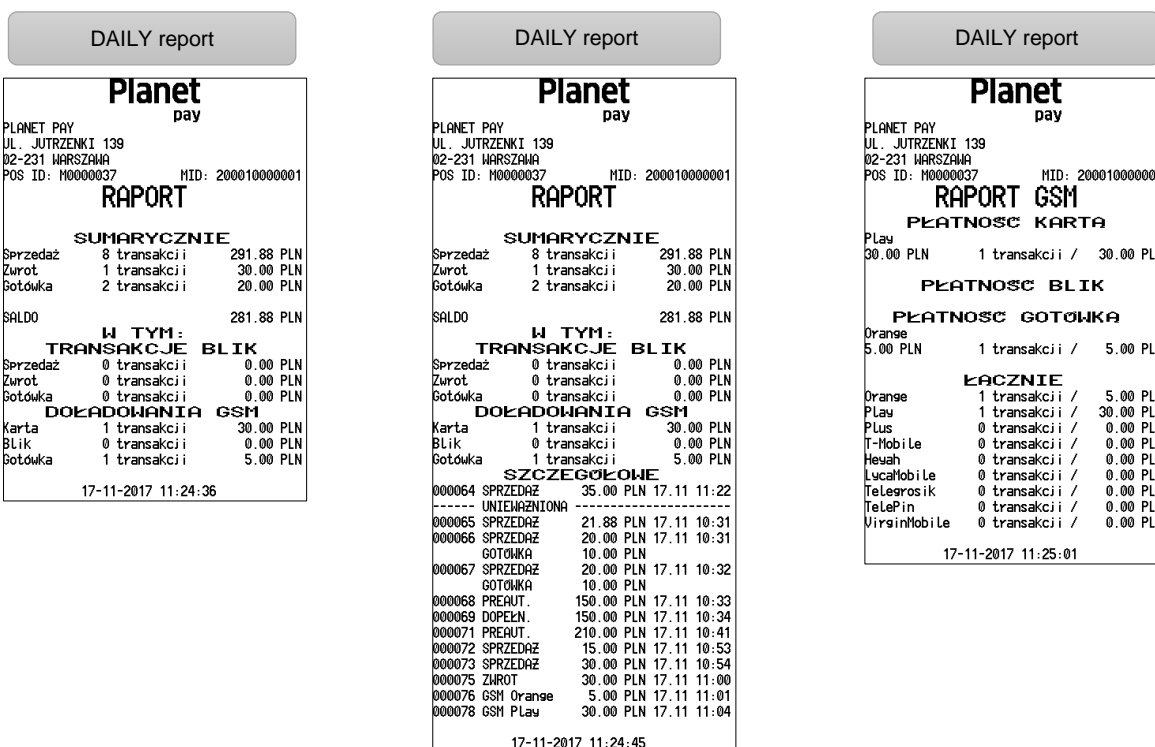


FIGURE 67 REPORTS – EXEMPLARY PRINTOUTS

4.3 Update of application

The update consists in connecting the application with TMS to download the latest parameters (settings) and/or the new version of the application as well as in sending information about the terminal status.

Depending on the configuration the application may perform the update once a day on the specific weekdays at the determined time.

The update is usually performed every day at night.

If need be, the update can be called manually from the ADMIN menu.



If at the time of the call of the update there are unsettled transactions on the terminal, the application displays the question about the confirmation and the performance of the Settlement.

The update cannot be done if there are unsettled transactions on the terminal.

In order to make the Update of the application:

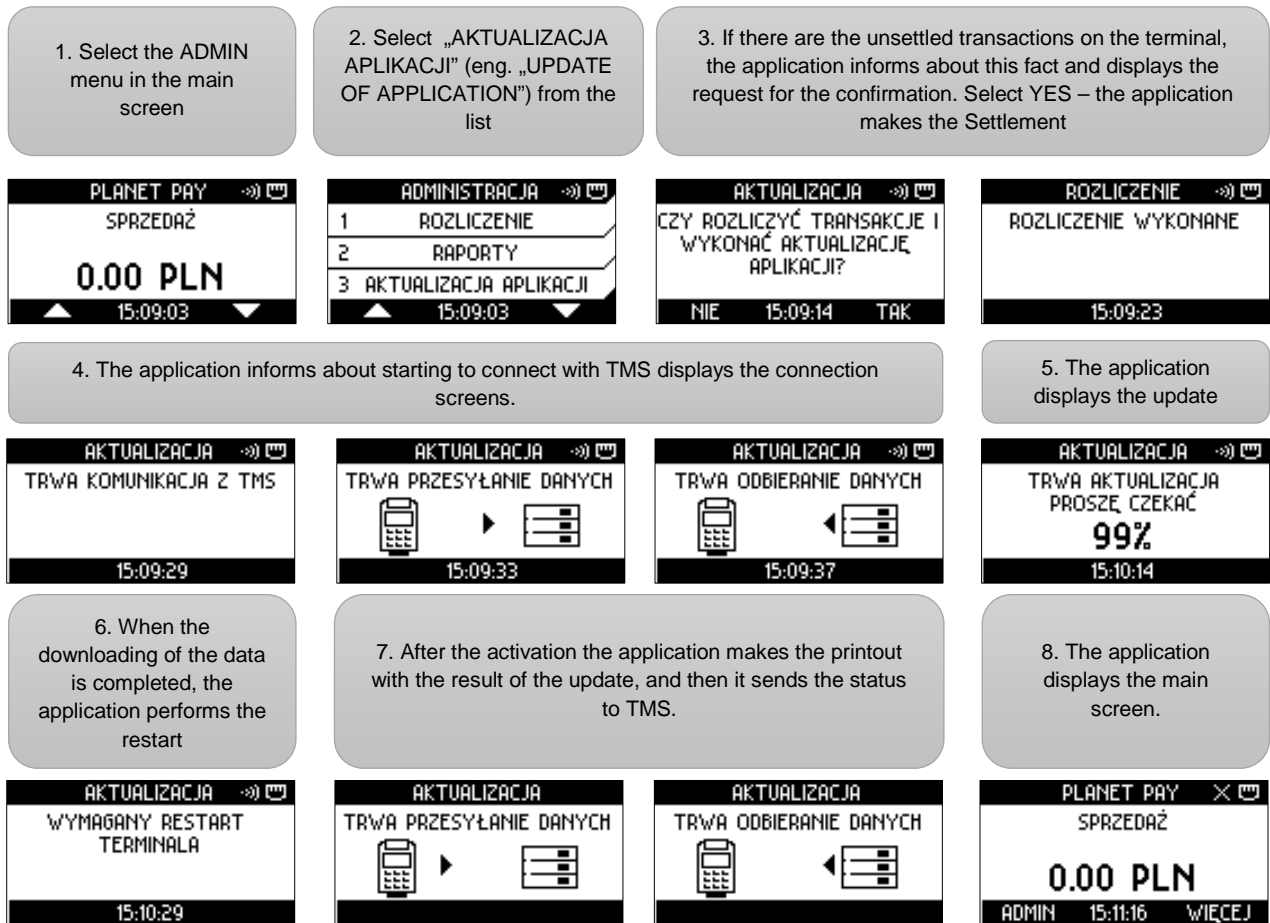


FIGURE 78 UPDATE OF APPLICATION – STANDARD PROCEDURE

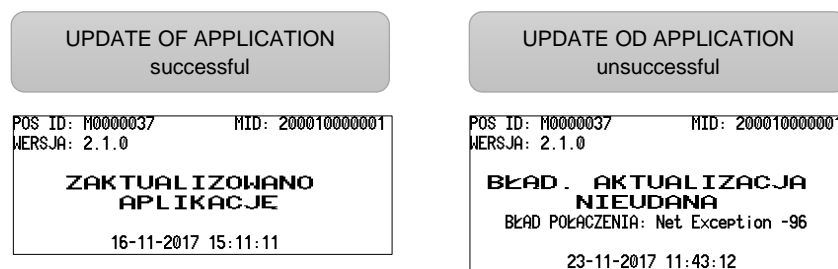


FIGURE 89 UPDATE OF APPLICATION – EXEMPLARY PRINTOUTS



If there is an error or the application update error recurs, keep the printout, contact the Service Centre and inform about the error mentioning the error code specified on the printout.

4.4 Display of version

The function allows displaying the version number of the payment application and making the printout including information about the versions of the individual components of the software installed currently on the terminal.

In order to display the application version:

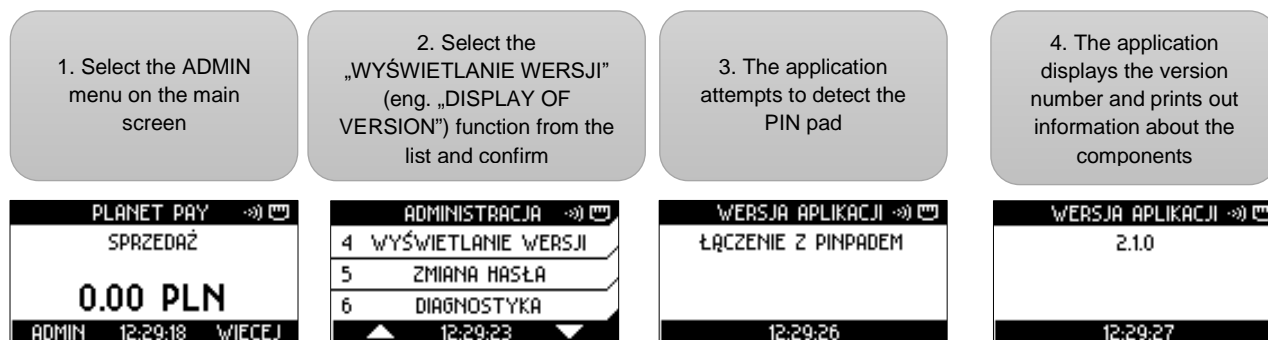


FIGURE 50 DISPLAY OF APPLICATION VERSION

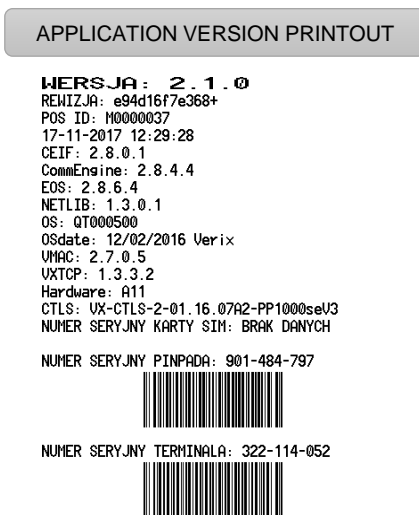


FIGURE 51 EXEMPLARY PRINTOUT OF APPLICATION VERSION

4.5 Change of password

The function allows changing the Administrator's password used to unblock the access to the [Return](#) transaction and [DEMO mode](#). In order to change the Administrator's password:

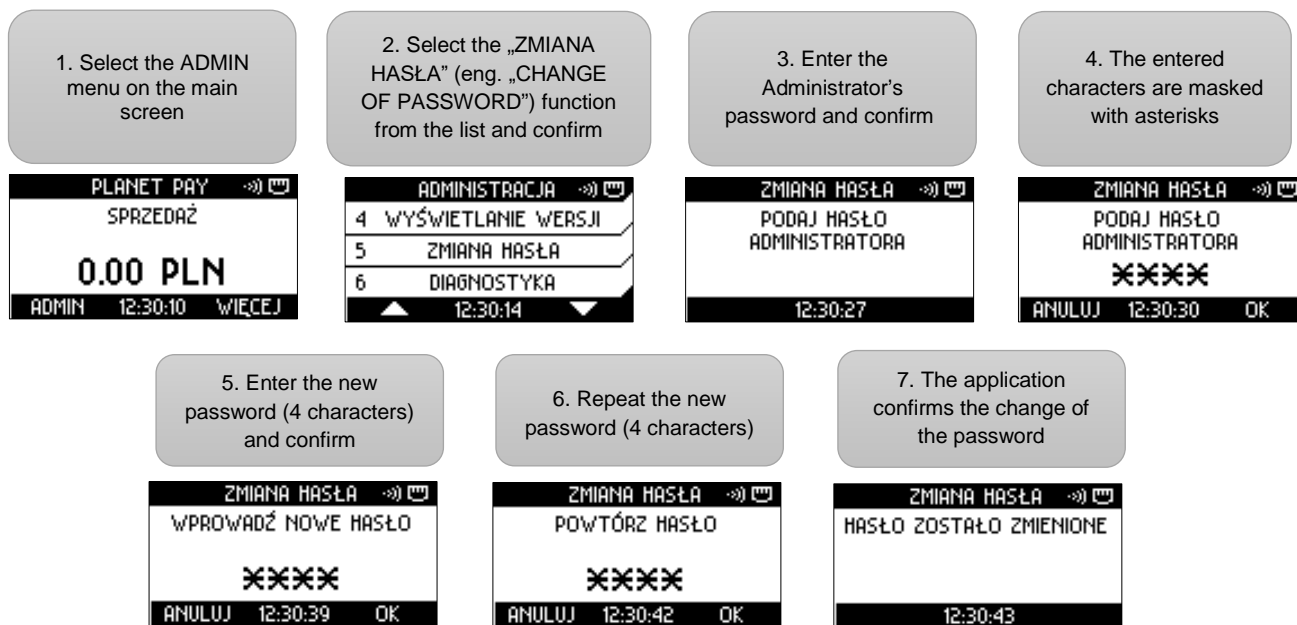


FIGURE 52 CHANGING THE ADMINISTRATOR'S PASSWORD - PROCEDURE



The CHANGE OF PASSWORD function does not allow changing the service password.

4.6 Diagnostics

The DIAGNOSTICS function allows conducting a set of tests to determine a current condition of the device. The Diagnostics function is also available on the terminal when it is not initialised. [see also: [Initialisation](#)]

A part of tests is conducted automatically in the background (e.g. the application does not display the additional messages during the battery test while the test result is specified on the printout). The parts of tests requires the User's operations – the subsequent steps are described below.

4.6.1 Call of Diagnostics and Diagnostics procedure

The single tests cannot be called; however, the User can omit some of them by pressing CANCEL. The possible operations and the results of the individual tests are described below. In order to start DIAGNOSTICS:



FIGURE 53 DIAGNOSTICS – CALLING THE FUNCTION

4.6.1.1 Keyboard test

The objective of the keyboard test is to check the proper function of every key of the device. The application displays the list of symbol corresponding to the individual buttons except the CANCEL key. When the User presses the key, its symbol is “marked off” – disappears from the list of symbols on the screen.

When the last symbol is marked off, the application switches to the printer test.

The possible results of the keyboard test specified on the final printout include:

- OK – every key is pressed and every symbol on the screen is marked off
- NOK (failure) – when the User presses the CANCEL button at any time during the test (e.g. in the absence of the terminal reaction to pressing the button or in order to accelerate the diagnostics procedure)

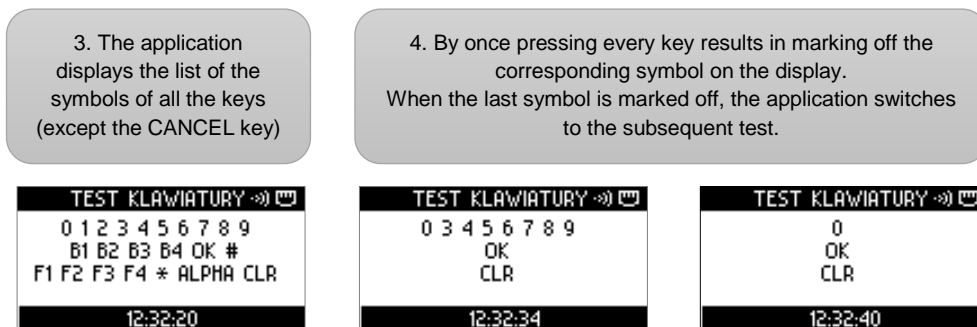


FIGURE 54 DIAGNOSTICS – KEYBORD TEST

4.6.1.2 Printer test

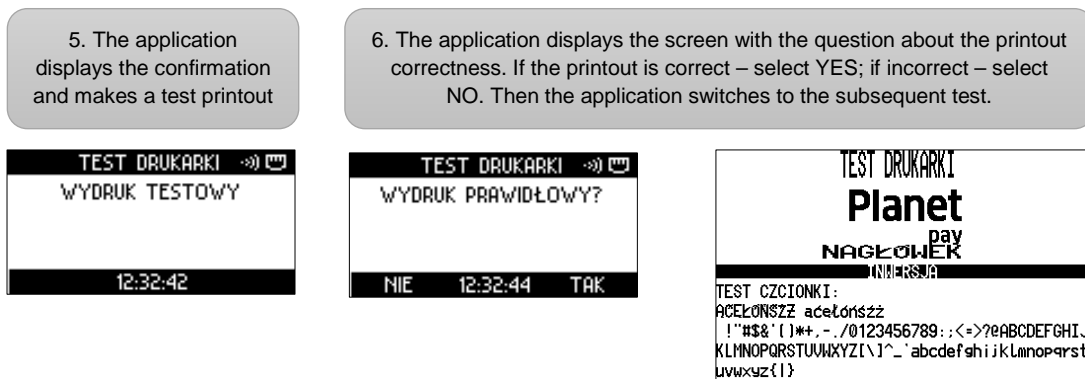


FIGURE 9 DIAGNOSTICS - PRINTER TEST

4.6.1.3 Connection test

<p>7. The application displays the question about the test connection. Select YES.</p>	<p>8. The application displays the authorisation HOST IP ADDRESS obtained from the currently set parameter. If need be, edit it, then confirm Perform the same steps for the HOST PORT field.</p>	<p>10. The application makes a connection and displays the test result.</p>

FIGURE 10 DIAGNOSTICS - CONNECTION TEST

4.6.1.4 Reader test and PIN pad diagnostics

The test of the readers helps to ensure that card readers in the terminal and in the PIN pad are able to read the card proper for their type (microprocessor, magnetic, contactless card).

In order to make the test of the readers:

<p>11. Pull the card through the magnetic card reader</p>	<p>12. Insert the card to the microprocessor card reader</p>	<p>13. Put the contactless card against the CTLS reader on the PIN pad</p>	<p>13. The application asks about the PIN pad diagnostics. Select YES or NO</p>

FIGURE 57 DIAGNOSTICS – READERS' AND PIN PAD TEST

When every read of the card is successful, the application switches to the subsequent test.



The lack of the reader reaction to the inserted, pulled or put card proper for the type of the reader means failure. In such a case in order to switch to the subsequent test, press CANCEL.

4.6.2 Diagnostics printouts

The exemplary printout of the GPRS terminal diagnostics result

```

POS ID: M0000037      MID: 200010000001
DIAGNOSTYKA
OK - KŁAWIATURA
OK - DRUKARKA
OK - POŁĄCZENIE
  ADRES IP HOSTA: 10.180.82.107
  PORT TCP HOSTA: 7026
  APN: pos.itcard.pl
  SSL: CN=itcsr1pk01pos9test
OK - MAGSTRIPE
OK - ICC
OK - CTLS
OK - PINPAD
  PP BAUDRATE: BaudRate::BR_19200
  PP PARITY: Parity::EVEN
  PP WORD: DataBits::BIT7
  CTLS BAUDRATE: BaudRate::BR_115200
  CTLS PARITY: Parity::NO
  CTLS WORD: DataBits::BIT8



NUMER SERyjNY PINPADA: 901-484-797

NUMER SERyjNY TERMINALA: 322-114-052


17-11-2017 15:04:28
  
```

The exemplary printout of the Ethernet terminal diagnostics result

```

POS ID: M0000037      MID: 200010000001
DIAGNOSTYKA
OK - KŁAWIATURA
OK - DRUKARKA
OK - POŁĄCZENIE
  ADRES IP HOSTA: 192.168.70.13
  PORT TCP HOSTA: 4443
  ADRES IP TERMINALA: 192.168.70.99
  DHCP: 1
  SSL: CN=itcsr1pk01pos9test
OK - MAGSTRIPE
OK - ICC
OK - CTLS
OK - PINPAD
  PP BAUDRATE: BaudRate::BR_19200
  PP PARITY: Parity::EVEN
  PP WORD: DataBits::BIT7
  CTLS BAUDRATE: BaudRate::BR_115200
  CTLS PARITY: Parity::NO
  CTLS WORD: DataBits::BIT8

NUMER SERyjNY PINPADA: 901-484-797

NUMER SERyjNY TERMINALA: 322-114-052


17-11-2017 12:33:31
  
```

FIGURE 58 DIAGNOSTICS' RESULTS – EXEMPLARY PRINTOUTS

4.7 Demo mode

For the training purposes the application provides the special DEMO mode to follow the procedure of some most common used functions and to make the exemplary printouts.

To minimise the risk of mistake, when the DEMO Mode function is activated:

- the DEMO wording is specified on every application screen and every printout
- the amount of every transaction cannot be higher than PLN 1 (except the Cash Back transaction whose total amount is PLN 2)
- the number of the package is zero on every printout of the settlement
- the application does not make real connections but only simulates the connections displaying the connection screens
- some functions are deactivated (e.g. Update of application)

After the exit from the DEMO mode all the transactions made for training purposes are removed and never are specified on the printouts of the reports and the settlements of the real transactions. After the re-entry to the DEMO mode the numbers of the accounts of the transactions start from 1

Besides, the main screen and the list of functions in the menu is the same as in the normal operation mode of the application.

The entry to the DEMO mode is protected with the Administrator's password.

In order to enter the DEMO mode:

1. Press ADMIN on the main screen

2. Select DEMO MODE from the list of transactions

3. Enter the password and confirm by the ENTER key

4. The application confirms the activation of the DEMO mode

FIGURE 59 DEMO MODE - ENTRY

The procedure of the exit from the DEMO mode is similar to its activation:

1. Press ADMIN on the main screen

2. Select DEMO MODE from the list of transactions

3. Enter the password and confirm by the ENTER key

4. The application confirms the activation of the DEMO mode

FIGURE 60 DEMO MODE - EXIT

The exemplary printouts in the DEMO mode:

Exemplary printouts in DEMO mode

Planet pay

PLANET PAY
UL. JUTRZENKI 139
02-231 WARSZAWA

TRYB DEMO

POS ID: M0000037 MID: 200010000001
MCC 351 v1 2 (911) (1) CONTACTLESS
541333*****3511 A0000000041010
RACHUNEK NR 000001

SPRZEDAŻ: 1.00 PLN

TRANSAKCYJA ZAARKEPTOWANA

RRN: 012345678912 KOD AUT: AUTHOK

DZIEKUJEMY. PROSIMY ZACHOWAC RACHUNEK
17-11-2017 12:35:19

Planet pay

PLANET PAY
UL. JUTRZENKI 139
02-231 WARSZAWA

TRYB DEMO

POS ID: M0000037 MID: 200010000001
MCC 351 v1 2 (911) (1) CONTACTLESS
541333*****3511 A0000000041010
RACHUNEK NR 000002 KOPIA KLIENTA

SPRZEDAŻ: 1.00 PLN
CASH BACK: 1.00 PLN
RAZEM: 2.00 PLN

TRANSAKCYJA ZAARKEPTOWANA

RRN: 012345678912 KOD AUT: AUTHOK

DZIEKUJEMY. PROSIMY ZACHOWAC RACHUNEK
17-11-2017 12:35:55

Planet pay

PLANET PAY
UL. JUTRZENKI 139
02-231 WARSZAWA

TRYB DEMO

POS ID: M0000037 MID: 200010000001

ROZLICZENIE
ZGODNOŚĆ Z HOSTEM

Paczka: 0

SUMARYCZNIE

Sprzedaz	2 transakcji	2.00 PLN
Zwrot	0 transakcji	0.00 PLN
Gotówka	1 transakcji	1.00 PLN
SALDO		3.00 PLN

W TYM:

TRANSAKCYJE DCC

Sprzedaz	0 transakcji	0.00 PLN
Zwrot	0 transakcji	0.00 PLN

TRANSAKCYJE BLIK

Sprzedaz	0 transakcji	0.00 PLN
Zwrot	0 transakcji	0.00 PLN
Gotówka	0 transakcji	0.00 PLN

DOKADOWANIA GSM

Karta	0 transakcji	0.00 PLN
Blik	0 transakcji	0.00 PLN
Gotówka	0 transakcji	0.00 PLN

17-11-2017 12:36:23

FIGURE 61 DEMO MODE - EXEMPLARY PRINTOUTS

5. Additional functions

5.1 Printout of the data of terminal and point of sale

In order to facilitate the communication with the Customer Service Office the printout including the identification data of the terminal and point of sale can be made:

- TID
- MID
- model of device
- version of application installed on the terminal
- name and address of point of sale

The function is available from the main screen of the application:

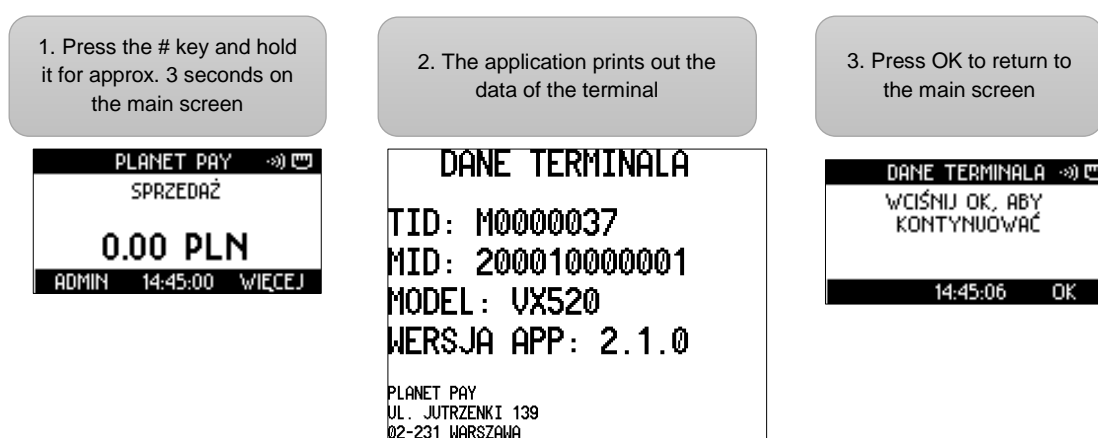


FIGURE 62 PRINTOUT OF THE DATA OF TERMINAL AND POINT OF SALE

5.2 Automatic return to main screen and screen saver

In order to reduce the energy consumption the application is equipped with the function of the automatic return to the main screen and the screen saver.

When the terminal is unused and displays the main screen of the application, after 20 seconds of the inactivity the screen is dimmed, and after next 10 seconds - it is darkened, and the screen saver appears on the display (usually the Provider's logo is set up).

In order to start the transaction, enter the first digit of the amount – the application backlights the screen of terminal and displays the entered digit.

If the user, after the previous function (e.g. after the printout of the report), did not return to the main screen by pressing CANCEL, after 30 seconds of the inactivity the application switches to the administration menu, and after next 30 seconds – to the main screen. This allows the User to start immediately the transaction without navigating the application in order to switch to the main screen.

5.3 Time synchronisation with host

The application allows synchronising the date and time set on the terminal with the Provider's authorisation host. The date and time are synchronised during every transaction.