Maintenance Manual

iCT2xx, iPP3xx, iWL2xx and iSMP terminals

PayEx
EXPERTS IN PAYMENTS

Contents

Introduction

Thank you for choosing PayEx as vendor for your payment solution.
This manual provides information and guides you through the maintenance procedures associated with 1st Line Support of your PayEx terminal. Read the manual carefully to perform 1st hand service on your terminal.

This manual is not intended for self-education but prerequisites that proper training has been undergone prior to use of this manual.

PayEx 2nd Line Support can be contacted by using the contact information below. When contacting PayEx 2nd Line Support, please provide so much information about your issue as possible;

- A detailed description of the error and how/if it can be re-produced
- Photo/Scan of the receipt, screenshots/photos/description of what the terminal displays
- PosPay log (where applicable)
- Terminal log (where LLT is used)
- Contact information

Norway: Telephone: **+47 99401150** email: **support.pos@payex.com**.
Sweden: Telephone: **+46 498207878** email: **support.pos@payex.com**.
Finland: Telephone: **+46 498207878** email: **support.pos@payex.com**.
Denmark: Telephone: **+46 498207878** email: **support.pos@payex.com**.

Version 1.0 May 2013.

Terminal overview

PayEx delivers the Ingenico Payment terminal iCT-, iPP-, iSMP and iWL-series.
The terminals are delivered with two different types of keyboard layout.
1. Keyboard with text on the red (CANCEL or STOP), yellow (CLEAR) and green button (ENTER or OK).
MENU key is used to enter menu on standalone terminals.
2. Keyboard without text on the red, yellow and green button.
F key is used to enter menu on standalone terminals.

Regardless of your keyboard layout, entering menu on ECR connected terminals requires the following key combinations: F3 (up arrow) + operator password (default: 1234) + Green key + 2 (Mynt). Note that the transaction menu is disabled for ECR connected terminals, i.e. all financial transactions must be initiated from ECR.

The table below lists properties for the terminals. Keep in mind that some chapters in this document describe settings/procedures that may not be a property of your terminal.

Property	iCT220&250	iPP320&350	iWL220&250	iSMP
Network Ping	Yes	Yes	**No**	Yes
ECR – Ethernet	Yes	Yes	**No**	Yes
ECR – PPP	Yes	Yes	**No**	**No**
Standalone – GPRS	**No**	**No**	Yes	**No**
Standalone - Ethernet	Yes	**No**	**No**	**No**
Printer	Yes	**No**	Yes	**No***

* iSMP can be connected to a Bluetooth printer.

All terminals are delivered with a preinstalled software application.
The terminals are also delivered with a standard administrator and operator code. The administrator code is set default to 1111, and the operator code is set default to 1234. Change the codes as soon as the terminal is deployed at your store/ sale place. The instructions for changing these codes are described in the terminal's user manual.

Terminals

iCT220 &250

iPP320 & 350

iWL220 & 250

iSMP

= Locate terminal type.

Display: For iCT220, iPP320, iWL220 and iSMP, the display is Black and White,-50 series are color terminals.

Physical terminal colors:

iCT220 &250: Black

iPP320: Grey, iPP350: Black

iWL220: Black, iWL250: Grey-White

iSMP: Black

Troubleshooting

This chapter will guide you through how to troubleshoot various problems on your terminal.

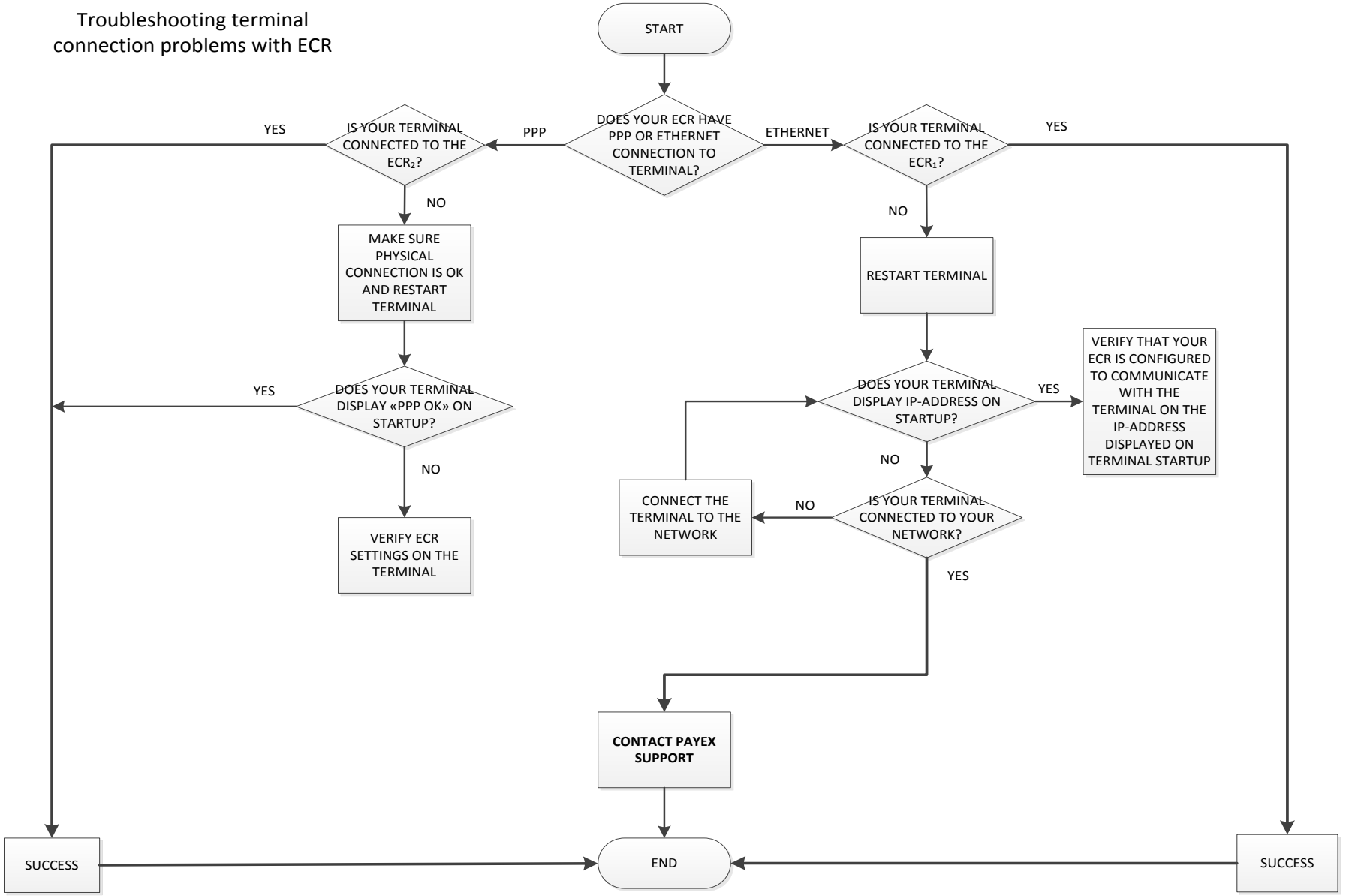
Troubleshooting terminal connection problems with ECR

The flowchart on the next page is a flowchart for (re)connecting the terminal to your ECR.

1. The terminal is connected to the ECR if an IP address is displayed in the terminal window and the ECR is configured to communicate with the terminal on that specific address.
2. The terminal is connected to the ECR if the terminal displays “PPP OK”. “PPP OK” should be displayed within one (1) minute. If not, restart your ECR and Terminal.

If any action does not solve your problem, contact PayEx 2nd Line Support.

Troubleshooting terminal connection problems with ECR



Troubleshooting TMS

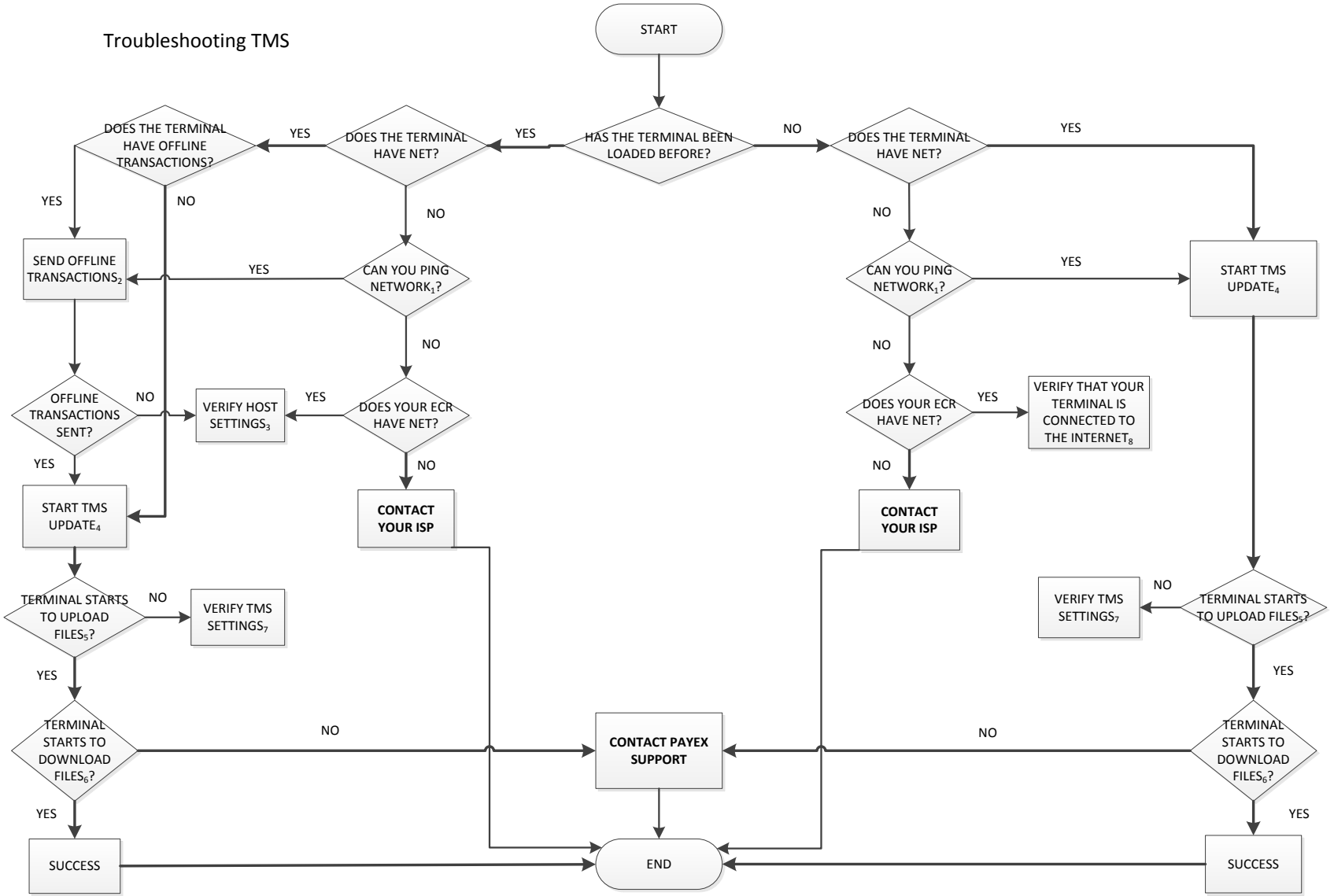
The flowchart on the next page is a step-by-step chart of how to download from TMS. This flowchart is not fully applicable for iWL terminals. Read carefully the numbered instructions for correct TMS download for iWL terminals.

1. Ping network: F3+operator code (1234) + TELIUM MANAGER + Initialization + Hardware + Ethernet Setup + Ping. Enter a valid IP-address and press OK. Received packages shall be 4/4. The terminal might have the wrong protocol selected if the terminal does not connect to the Internet. Press F3 (up arrow) + operator password (default 1234) + TELIUM MANAGER + Initialization + Hardware + Ethernet setup + Boot proto. Select static IP address or DHCP, depending on your terminal setup. Contact PayEx 2nd Line Support if you are not sure if your terminal(s) shall use static IP address or DHCP. iWL terminals do not have the option to ping a network address.
2. Send offline transactions: F+4(send offline) or F3+operator password (default 1234)+4(send offline). Offline transaction must be sent before the terminal can perform a TMS update.
3. Verify Host settings: Enter support menu and verify parameters by entering the Host connection submenu. Contact PayEx 2nd Line Support if the host connection parameters are configured wrong or to verify that they are correct on your terminal.
4. Start TMS update: Standalone terminals: Start TMS update by entering the system menu; F+7+4.. Terminals can also start TMS update from the Telium manager menu, F3+operator code+0+2+2+OK/Green key. **For iWL terminals, the TMS update must be started from the Telium manager menu.**
5. Terminal will start to upload files if filenames (e.g. activity.inf) are shown on the terminal display.
6. Terminal will start to download files if filenames are shown on the terminal display with a progress indicator.
7. TMS settings are located in the Telium Manager menu, F3+0+3+1+T.M.S. Verify that they are correct for your terminal.
8. The terminal must have a physical connection to Internet, either via the ECR, or via Ethernet with SSL.

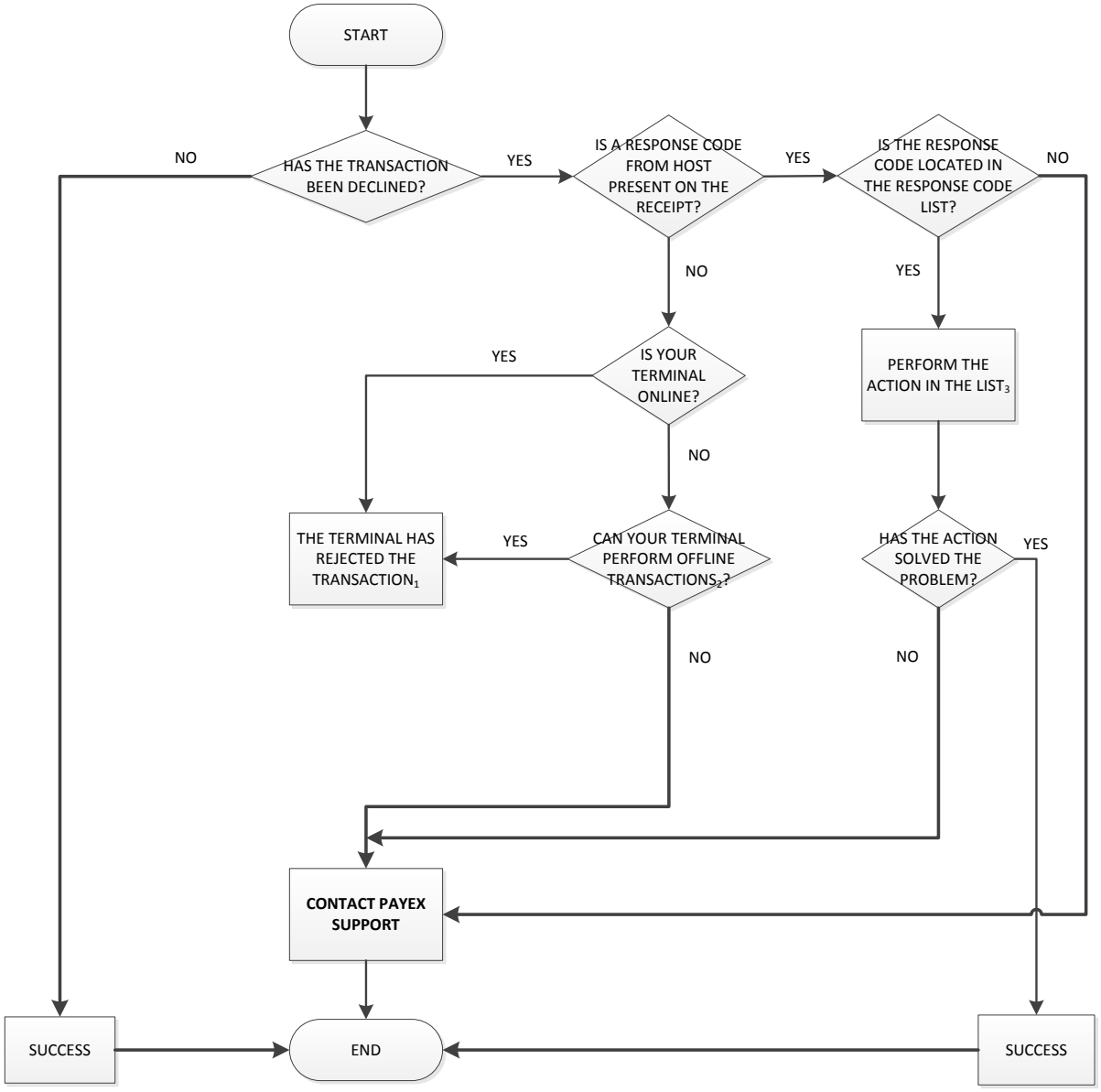
iSMP terminal must be connected to the terminal for the terminal to get Internet connection. It is important that the iOS device is connected to the terminal during the TMS download. If the iOS device is disconnected from the terminal, the TMS download will remain idle for a while before disconnecting. The TMS download will not succeed, and a new TMS update must be performed.

If any action does not solve your problem, contact PayEx 2nd Line Support.

Troubleshooting TMS



Troubleshooting declined transactions



1. See the Declined transactions chapter
2. The terminal only accepts transactions that are sent and approved by host.
3. See the response code list on page 21.

If any action does not solve your problem, contact PayEx 2nd Line Support.

Declined transactions

The most common declined (offline) transactions are listed below. If you are experiencing other declined-situations, contact PayEx 2nd Line Support.
If there is something wrong with the keys in the terminal, it can appear in multiple cases listed below.

All display screenshots on the following pages are based on English setup.

Card is inserted or swiped and the transaction is declined without PIN entry

This is most likely a BIN table issue.

Possible errors and screenshots

1. The card used is not found in the BIN table (See the Supported cards chapter).
   This error will display the following screens for *chip cards* that is inserted but not found in the BIN table:

Terminal requires that the card is inserted.

The terminal displays the AID on the chip.

The PAN is not found in the BIN table and the transaction is therefore declined.

This error will display the following screenshots for

- Magnetic stripe cards (1st and last screenshot).

- Chip cards that have been swiped (1st and last screenshot).

- Chip cards that have been misread multiple times and then terminal requested it to be swiped, called fallback (all screenshots). For fallback transactions, the terminal can also decline the transaction based on:

- The terminal is configured to decline all fallback transactions

- Fallback is not allowed for the card used

In addition:

- There is something wrong with the keys in the terminal. A chip card is inserted but the terminal requested fallback on 1st attempt (all screenshots).

Terminal requires that the card is inserted.

Terminal requires that the card is removed because the chip could not be read. Previous and this screenshot will be displayed until the chip is read, or it requires fallback (after 3 attempts).

The terminal requests fallback.

The card is not found in the BIN table and the transaction is declined.

2. The transaction type is not supported by the card.

   This error will display the following screens for *transaction type* not supported for the card used:

Terminal requires that the card is inserted.

The terminal displays the application label of the chip.

The PAN is found in the BIN table, but the transaction type for that card is not supported.

Solution

Contact PayEx 2nd Line Support. Provide information about card(s) used and the transaction type that has been performed.

The transaction has been declined after PIN entry

Possible errors and screenshots

1. The transaction has exceeded maximum offline purchase limit.
2. The terminal has reached maximum number of stored offline transactions.
3. The card used has expired.
4. There is a communication problem with host, and the terminal has declined the transaction based on the communication error code. This code is only located in the debug log.
5. The transaction has been declined with a response code.
6. The transaction has been declined based on TVR and TSI. See the appendix.
7. There is something wrong with the keys in the terminal (i.e. online pin enciphering has failed)

All errors listed above will show the following screenshots (*if the terminal is offline, it will not display the 4th screenshot*):

Terminal requires that the card is inserted.

Application label is displayed

The terminal requests PIN input.

The terminal tries to send the transaction to host.

The transaction has been declined.

Solution

1&2: Attempt to get your terminal online, by following the steps in “Troubleshooting offline terminals” chapter.

3: The terminal is offline and has declined the transaction because the card has expired. If a card has expired and the terminal is online, response code 54 should be present on the receipt.

4: Try the transaction again, it might be approved offline. Attempt to get your terminal online.

5: Locate the transaction in the Response codes list and perform the “action” in the list.

6. Locate the TVR and TSI on the receipt and see if it has been declined based on that, see TVR and TSI

7: Contact PayEx 2nd Line Support

SSL is configured on the terminal, but the transactions are declined.

Possible errors and screenshots

1. The terminal is not configured correctly
2. The host connection and address might be wrong
3. SSL certificates are not loaded on the terminal correctly. Load new certificates.

Declined transactions with SSL will display the following screenshots:

Terminal requires that the card is inserted.

Application label is displayed

The terminal requests PIN input.

The terminal tries to send the transaction to host.

The transaction has been declined.

Solution

1: Verify that the SSL parameters are OK. Enter the support menu→Configuration Parameters→Set parameter. Input parameter "150" and press OK. This parameter shall be"1". Input parameter "155" and press ok. This parameter shall be a password. Restart the terminal and retry the transaction if you have altered these parameters.

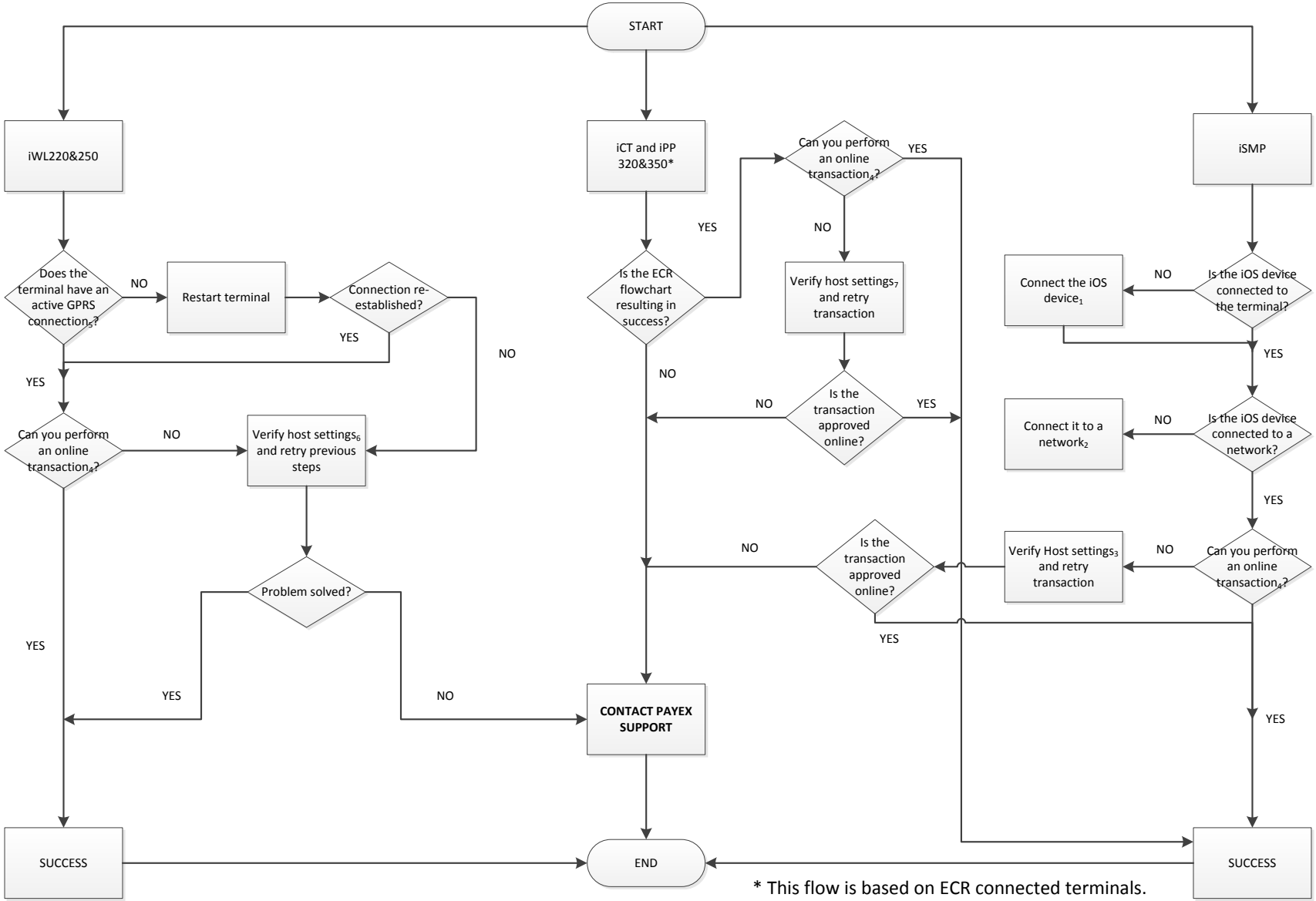
2&3: Contact PayEx 2nd Line Support.

Troubleshooting offline terminals

On the next page is a flowchart for offline terminals, and how to get them online.

1) Connect the iOS device:
    1. Dock the iOS device (iPod, iPhone) in the iOS device slot on the iSMP.
    2. Connect the iOS device to a Wi-Fi network. See 2).
    3. Start the payment application on the iOS device. Also make sure that the terminal is powered on.
2) Connect the iOS device to any Wi-Fi network.
3) Enter support menu→Settings→Host connection. Connection parameters shall be:
   With SSL:
   - IP address: pospaytx.payex.com and port: 443.
   Connection type: Ethernet.
4) A response code will be present on the receipt. See the example of receipts chapter on where to find the response code from host.
   Note that if the terminal has performed (several) offline transaction, this transaction may also be approved/declined offline. Please wait a while to let the terminal send offline transactions.
5) GPRS connection is active if a GPRS signal (bars) is displayed in the top left corner of the screen (iWL 250, opposite position on iWL 220), along with the SIM card name. The GPRS signal is optimal if 5 (five) bars is displayed. In addition, a phone connection must be active in the top center of the screen. It is not unusual that the phone connection is dropped if the terminal has been idle for a while. When sending a transaction after being idle, it shall re-establish the connection.
6) Enter support menu→Settings→Host connection.
   Connection parameters shall be:
   With SSL; IP address: pospaytx.payex.com, port: 443, GPRS apn is individual, based on what SIM card you have received from PayEx. Login and password are left blank.
   Connection type: GPRS.
   Without SSL: IP address: 195.225.0.42, port 9034, GPRS apn is individual, based on what SIM card you have received from PayEx. Login and password are left blank.
   Connection type: GPRS.
7) Depending on your terminal setup, host settings shall be:
   PPP (USB) connected terminals:
   Connection parameters: IP address 1.1.1.1 and port 9034.
   Connection type: Ethernet
   Ethernet (LAN) connected terminals:
   Connection parameters:
   With SSL: IP address: pospaytx.payex.com, port: 443
   Without SSL: 195.225.0.42, port 9034 (*Or 9033*)

Troubleshooting offline terminals



Using the Telium manager

The Telium manager can also be used to verify that a terminal is online. This is applied for all terminals, except iWL terminals.

- Enter the following key combination to enter the Telium menu:
  F3(up) + 1234 + Telium manager (0)
- **Ping a network address** to verify that the terminal has Internet connection:
  Initialization + Hardware + Ethernet setup + Ping. Enter a valid IP address and press OK/Enter. Received packages shall be 4/4.
- A terminal can be offline if the **boot protocol** is not configured correctly in the terminal. Verify that this is correct by entering:
  Initialization + Hardware + Ethernet setup + Boot Proto. Static address or DHCP can be selected.

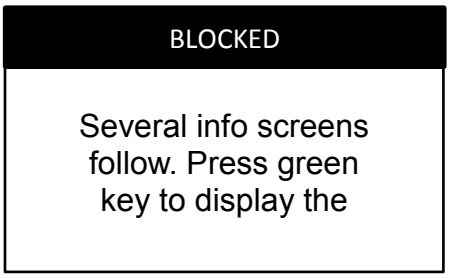
Blocked terminals

A terminal can be blocked in two ways:

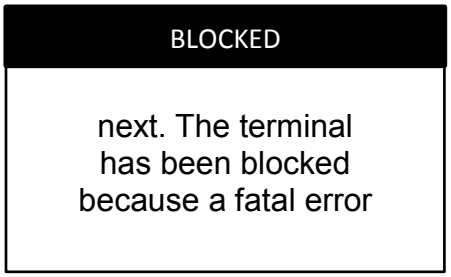
1. Transaction block – The terminal can be operated normally, except performing transactions.
2. Full block – The terminal will be fully blocked because a major incident has occurred on the terminal. The terminal will not be usable until it has been unblocked.

Warning! If a terminal gets blocked, contact PayEx 2nd Line Support immediately for further assistance.

The following screens will appear if your terminal gets blocked. If it is a full block, the terminal will restart before displaying:

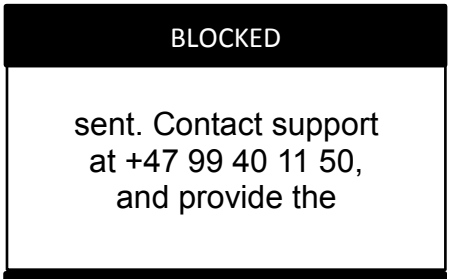


A blocked message will appear. Terminals with printer will print out terminal information that continues on the next info screens.



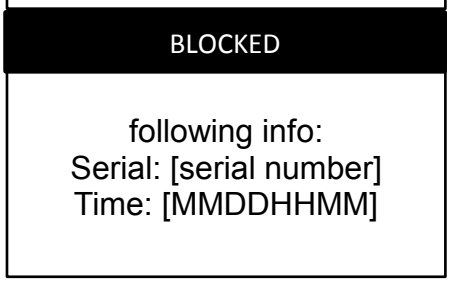
[press green key]

[press green key]



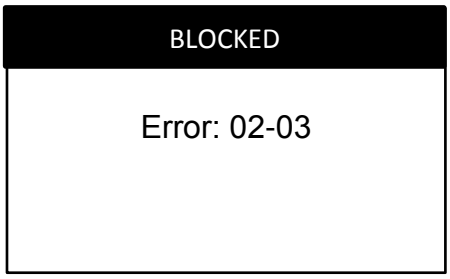
[press green key]

See Introduction chapter for correct phone number



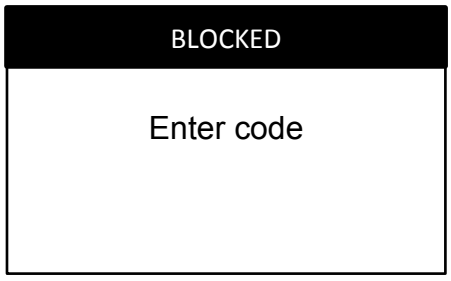
[press green key]

The serial number of the terminal will appear
The time will appear in format: Month, Month, Day, Day, Hour, Hour, Minutes, Minutes

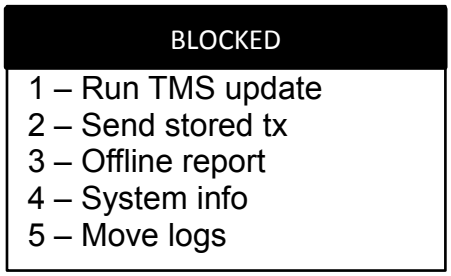


[press green key]

The error type will appear. In this example case, it is an offline approved transaction that has been sent, and host has responded with code 03 – Invalid merchant number.



Press green key and then press menu/F. This screen shall appear.
Enter the code provided by PayEx 2nd Line Support if you are requested to do so.



A blocked menu will appear. PayEx 2nd Line Support will provide information about what you shall select.

A Transaction blocked terminal will display “TERMINAL BLOCKED” on the idle screen (start screen).
A “unblock” menu will appear below “support” in the menu where the unblock code can be entered.

Support menu

The support menu provides possibility to change different types of settings, configuration and more if it has occurred errors or problems on the terminal and is listed below.
In order to access the support menu, contact PayEx 2nd Line Support for a support code.
Note: A support menu password will only work for one day, attempting to access the support menu with the same password a different day will not work.

9-1 Settings

9-1-1 Setup ECR

Disable (Standalone operating mode)
Serial mode (Not used)
PPP mode (USB connection between ECR and terminal)
Ethernet mode (Ethernet connection between ECR and terminal)

9-1-2 TMS management

Configure (Sets the communication parameters for TMS connection)
Connect (Connects the terminal to TMS for downloading upgraded application and/or files)

9-1-3 Host connection

Connection parameters (Sets the address and port (and apn) to host)
Connection type (Select between Ethernet and GPRS)

9-2 Configuration parameters

9-2-1 Print all parameters (Prints all parameters in the terminal)
9-2-2 Set parameter (Sets an existing parameter to a different value, or verifies that a parameter is correct)
9-2-3 Delete parameter (Deletes a parameter that is not in use)
9-2-4 Print EMV configuration (Prints EMV configuration on the terminal)

9-3 File management

9-3-1 List all files (Prints out the files on the terminal. Also asks for it to be stored on the HOST disk)
9-3-2 Delete sales report (Deletes current sales report)
*9-3-3 Delete offline transactions (**DO NOT USE THIS FUNCTION UNLESS EXPLICITLY ADVISED SO BY PAYEX 2ND LINE SUPPORT**)*
9-3-4 Delete total amount (Deletes total amount of the sales report)
9-3-5 Delete logs (Deletes the log file on the terminal)
9-3-6 Move logs (Moves the log files to the HOST disk. They can be recovered if you have LLT*)*

9-4 Stored transactions

9-4-1 Print offline transactions
*9-4-2 Delete offline transactions (**DO NOT USE THIS FUNCTION UNLESS EXPLICITLY ADVISED SO BY PAYEX 2ND LINE SUPPORT**)*
9-4-3 Delete reversal (Deletes the reversal file (if any) on the terminal)

9-5 System info

9-5-1 System info (Displays and prints out system information; App version, Operating System and Telium system information)
9-5-2 List components (Prints out components on the terminal)
9-5-3 Security info (Prints out security information on the terminal)

9-5-2&9-5-3 are only applied if your terminal must be sent to PayEx for service.

9-6 Keys

9-6-1 Delete DUKPT keys (Deletes DUKPT keys on the terminal. DO NOT USE THIS FUNCTION UNLESS EXPLICITLY ADVISED SO BY PAYEX 2ND LINE SUPPORT)
9-6-2 Delete TGKIT keys (Deletes TGKIT keys on the terminal. Only applied if DUKPT keys are not loaded on the terminal. DO NOT USE THIS FUNCTION UNLESS EXPLICITLY ADVISED SO BY PAYEX 2ND LINE SUPPORT)

9-7 Print EMV tags *(Prints EMV tags on the terminal)*

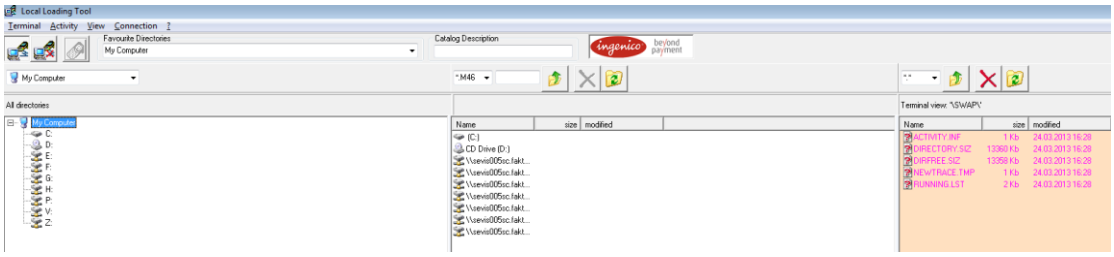
LLT

LLT is a tool for loading files and applications on a terminal.
Please note that not all 1st line support have access to this program.

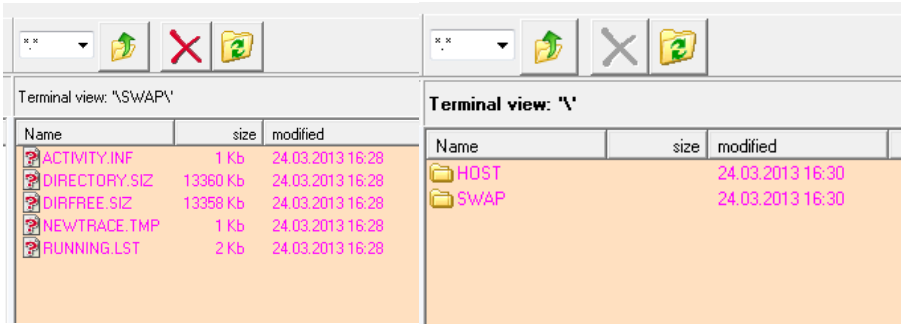
In order to load files on a terminal, the terminal must be set in LLT modus.

1. Restart the terminal by pressing comma key and yellow button simultaneously.
2. Press and hold F3 (up arrow) until "LLT" is displayed on the terminal.
3. Connect the terminal to the PC with an USB cable. Cables used;
   iWL & iSMP: Micro USB, iCT: standard-B USB cable (USB cable with a square shape)
   iPP: USB type A straight powered cable.
4. Start LLT and connect the terminal. This can be done in three different ways:
   a. With mouse by clicking the icon on the top left corner.
   b. By pressing F4
   c. From the LLT menu: Terminal →connection

   The terminal's swap disk will appear in the right pane, and an active connection icon is shown in the top left corner.



5. The terminal has two disks, HOST and SWAP. When the terminal has connected, it automatically opens the SWAP disk in the right pane, press the folder up icon to show both disks.



6. Move the right files to the right disk. The following files shall be added to which disk:

HOST	SWAP
CONFIG	CONFIG.BIN
EMV.PAR	***.AGN
BIN.CSV	***.M**
SALESREPORT	
SURBINS	
SURCHARGES	

.AGN files are payment application files. .M files are catalogue files, e.g. it can contain all the files listed in the table above. It shall always be loaded on the SWAP disk; its containing files will be automatically moved to the right disk. .M file endings are unique for each terminal type. LLT will automatically recognize the connected terminal, and will list only the right .M file(s) that can be loaded on that terminal:

Terminal series	iCT 220&250	iPP320&350	iWL 220&250	iSMP
.M file ending	.M40	.M46	.M44	.M42

7. Disconnect the terminal from LLT. The terminal will restart. If the terminal has a printer, it will print out new files loaded on the host disk on the terminal.

LLT must also be used to recover Log files from the terminal:

1. Select “Move the log files” in the Support menu.
2. Set the terminal in LLT mode
3. Start the LLT program on your PC
4. Connect the terminal to the PC
5. Locate the HOST folder on the right pane in LLT (Terminal view). This is done by clicking the folder up icon when the terminal is connected and double clicking the HOST folder
6. Drag and drop the DEBUG.LOG file to a suitable place on your hard drive
7. Send an email to PayEx 2nd Line Support, **support.pos@payex.com**, with the debug file attached

Communication

There are two different types of network communication that the terminals use, GPRS or Ethernet.

GPRS

iWL terminals are normally configured with GPRS connection. This network communication type requires a SIM card, which is preinstalled on the terminal on delivery.

Ethernet

The terminals can communicate with host using a network cable connected to the Internet, using SSL.

SSL

SSL is a cryptographic protocol for secure data transfer over the Internet. SSL is based on client certificates that have to be correctly downloaded in the terminal. See the “Troubleshooting declined transactions” chapter if you are experiencing declined transactions if your terminal setup requires that the terminal uses SSL.

TMS

All the terminals PayEx deliver are registered in TMS. TMS enables downloading of software, terminal Operating System, Manager, Keys and other files/applications. See the “Troubleshooting TMS” chapter for a step-by-step guide if your terminal has problems with TMS update.

Transaction types

This chapter describes the transaction types supported by PayEx, and how they are initiated in the terminal. If a transaction is declined, se the “Troubleshooting declined transactions” chapter.

Cards and transaction types supported

PayEx terminals support a wide range of card types and functions. Each merchant have their unique card acceptance agreements and supported functions defined by the acquirer.

Purchase

Purchase is a transaction type where a customer receives a merchandise or service in exchange for money.
A Purchase can be performed with the possibility for the customer to add extra amount to the total. If an acquirer has special rules and restrictions for extra limits, their threshold values are used. E.g. if the purchase amount is below x, where x is the threshold value set by acquirer, the extra limit is a fixed amount. If the amount is over x, the extra limit is a percentage of the purchase amount.
If the acquirer does not have any extra limit restrictions, maximum extra limit is 99% of the purchase amount. A purchase can also include Surcharge.

Depending on your terminal setup, a purchase is initialized in two ways:

1. Purchase on ECR connected terminals:
   A purchase is initiated from the ECR. The ECR sends the purchase amount to the terminal.
2. Purchase on standalone terminals:
   A purchase amount is entered by the person performing the sale, and hands over the terminal to the customer.

In both cases the customer then inserts card (bank, credit, debit, gift card etc.). After card insertion it is either usual that;

- The customer enters PIN code, sign the receipt or uses Chip & Go.
- The customer inputs a total purchase amount which includes extra and then enters PIN code or sign the receipt.

After this step, the transaction is normally sent to host and approved or declined with a response code.

Purchase with Cash Back

Purchase with Cash Back is a transaction type where a customer can withdraw cash in the same transaction along with the purchase. Special rules and restrictions exist, e.g. in Norway it’s not allowed to perform this transaction type if the terminal is offline. It’s not possible to add extra for this transaction type, the Cash Back amount replaces the extra amount described above.

Refund

Refund is a transaction type where an account is credited when the customer returns merchandise. A refund normally takes 3-5 working days before the credited amount is available on the cardholder’s account. Special rules and restrictions exist, not all merchants support this transaction type.

Withdrawal

Withdrawal is a transaction type where a customer can withdraw money from a card without performing a purchase. Special rules and restrictions exist, not all cards support this transaction type.

Reversal

If any of transaction types above have been performed, a reversal transaction can be performed. This will reverse the **last** transaction that has been performed.

Balance inquiry

Balance inquiry is a transaction type where a customer can view available funds on a card. This will also be printed on the receipt. Special rules and restrictions exist, not all cards support this transaction type.

Surcharge

Surcharge is an extra fee charged by card acceptant explicitly when payment is done with a credit card.
Surcharge is added to the purchase amount. This may be a fixed value, and/or a percentage of the purchase amount. These values and percentages may vary between card issuers and card types.
Surcharge is preconfigured for the merchants and it can be turned on or off in the support menu.
If surcharge parameters needs to be altered, a TMS update must be performed.

Chip & Go

Chip & Go (also known as “No CVM”) excludes PIN and/or signature, and is intended to save time for both customers and persons performing the transaction. It is only applied for low value transactions, PIN shall be used as identification method for transactions over threshold value set by acquirer.
How it works: A customer inserts the card as if it was a normal transaction. The customer confirms the amount by pressing OK (green button) if the transaction is below threshold value set by acquirer.
No Cash Back amount may be added when using Chip & Go. Chip & Go is only available for merchants with one of the following MCC:

- 4111 Local and Suburban Commuter Passenger Transportation, including Ferries
- 4112 Passenger Railways
- 4131 Bus Lines
- 5812 Eating Places and Restaurants, mainly lunch restaurants not fine dining
- 5814 Fast food restaurants
- 5994 News Dealers and Newsstands

Deposit

Deposit is a transaction type where a customer has won money on a bet/lottery and wishes to withdraw the money from the customer's player's account to the customer's bank account. Deposit can only be performed if the terminal is online and the card used is domestic in the region where it is used (i.e. the card's country code equals the terminal's country code).

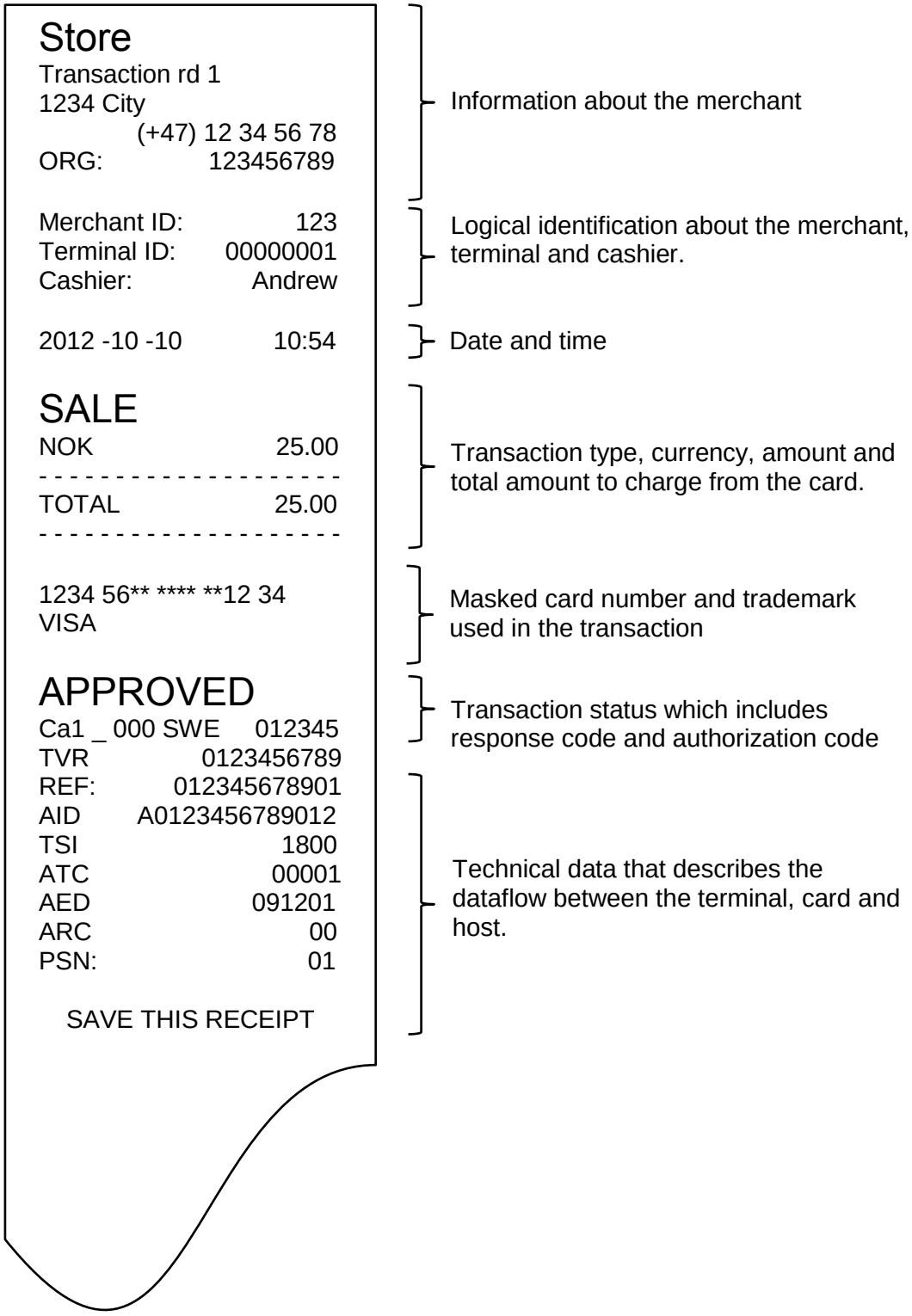
Deposit is only available for merchants with MCC 7995. This includes industries such as Lotteries, Casinos, Off-Track Betting and Wagers at Race Tracks.

Pin Before Amount

Pin Before Amount is an authorization type where the customer enters PIN before the amount is delivered to the terminal. After PIN is entered and verified, the purchase amount is sent to the terminal, and the customer confirms the amount with OK/Cancel.

Appendix

Receipt example – sale receipt



Response codes

This is a complete list of possible response codes from host.

If you can't find the response code in the table below, contact PayEx 2nd Line Support.

Response code	Response	Action
00	Transaction approved	
01	Transaction needs further authorization	Contact acquirer
03	Invalid merchant number	Contact your bank
04	Declined	Use a different card
05	Declined	Use a different card
06	Declined	Use a different card
07	Declined	Use a different card
12	Declined	Use a different card
13	Invalid amount	Enter another amount
14	Invalid card	Use a different card
15	Card issuer not defined	Use a different card
17	Customer aborts card sequence	Retry transaction
19	Declined	Use another card
20	Transaction aborted	Retry transaction
25	Original transaction not found	Contact PayEx 2nd Line Support
29	Wrong session number	Contact PayEx 2nd Line Support
30	Format error	Contact PayEx 2nd Line Support
33	Card expired	Use a different card
34	Wrong CDV (check digit verification)	Retry transaction or use a different card
36	Declined	Use a different card
38	Number of possible PIN exceeded	Use a different card
39	Declined	Use a different card
41	Declined	Use a different card
43	Declined	Use a different card
51	Declined	Use a different card
54	Card expired	Use a different card
55	Wrong PIN	Retry PIN or use a different card
56	No card record	Use a different card
57	Service not allowed for acquirer	Transaction type not allowed. Contact PayEx 2nd Line Support
58	Service not allowed for the merchant	Transaction type not allowed. Contact PayEx 2nd Line Support
61	Refused by card issuer	Use a different card
62	Service not allowed for this card	Use a different card
63	CSN error (Security violation)	Retry transaction. Contact PayEx 2nd Line Support if this is continuous
65	Too many transactions	Use a different card
67	Card blocked	Use a different card
68	Declined	Use a different card
75	Too many PIN attempts	Use a different card
77	Wrong MAC	Contact PayEx 2nd Line Support

80	Declined	Use a different card
81	Copied card	Use a different card
82	Wrong card format	Use a different card. Contact PayEx 2nd Line Support if this response code continues
83	Wrong session number	Contact PayEx 2nd Line Support
84	Reversal not possible, transaction declined	Contact PayEx 2nd Line Support
86	Duplicate transaction	Retry transaction
87	Reconciliation must be performed	Contact PayEx 2nd Line Support
88	Missing PIN code	Retry transaction. Contact PayEx 2nd Line Support if this is continuous
90	Reconciliation in progress	Wait for reconciliation to finish. Retry transaction
91	No contact with acquirer	Retry transaction. Contact PayEx 2nd Line Support if this is continuous
95	Accumulator overflow	Contact PayEx 2nd Line Support
96	Error/Problem on Host	Retry the transaction. Contact PayEx 2nd Line Support if this is continuous
97	Timeout	Retry transaction. Contact PayEx 2nd Line Support if this is continuous
98	Error in card	Use a different card
99	Invalid card	Use a different card
9A	Wrong time in terminal (+/- 15 min)	Retry the transaction. The terminal should have updated the time when receiving this response code from host
9B	Declined – too many fallback attempts	Use a different card
9C	Card read error	Retry transaction
9D	Terminal blocked. Terminal must be upgraded.	Contact PayEx 2nd Line Support
A0	Error in card	Use a different card
A1	Card not found in card register	Use a different card
A3	Declined – Error in safety values	Use a different card
A9	Wrong EMV cryptogram	Contact PayEx 2nd Line Support
D2	EMV security error	Contact PayEx 2nd Line Support
D4	Cryptogram error	Contact PayEx 2nd Line Support
F1	Card Blacklisted	Use a different card
F2	Incorrect KID	Contact PayEx 2nd Line Support
F3	KID missing	Contact PayEx 2nd Line Support
FF	Declined	Use a different card
G5	Declined, magstripe on chipcard	Retry with chip or use a different card
G6	Invalid card – chip missing	Use a different card
J1	The bank does not have a bank access agreement	Contact PayEx 2nd Line Support
J2	The merchant does not have a bank access agreement	Contact PayEx 2nd Line Support

TVR and TSI

TVR and TSI is a series of tests that the terminal performs when a chip card is inserted during a transaction. If the test fails, the transaction might be declined based on the TVR. TVR and TSI will always be present on the receipt when a chip card is used.

In the "Detailed description/Impact" pane in the table below, there is a detailed technical description for each TVR BIT. Pay therefore notice to whether the transaction can or will be declined or not. Not all TVR BITS concludes whether the transaction will be declined because they appear rarely. Contact PayEx 2nd Line Support if you experience any of these. See the example on page 36 on how to locate the TVR and extract the information.

TVR

TVR BIT	Description	Detailed description/Impact
8000000000	*Offline data authentication was not performed*	**The transaction was not authenticated offline. Transaction is only authenticated online; otherwise signature is used as CVM. *Transactions will not be declined based on this TVR BIT by itself.***
4000000000	*SDA failed*	**Static Data Authentication failed**
2000000000	*ICC data missing*	**ICC data is missing.**
1000000000	*Card appears on terminal exception file*	**The card or an application on the card is blacklisted, and is not usable. The transaction will be declined**
0800000000	*DDA failed*	**Dynamic Data Authentication failed**
0400000000	*CDA failed*	**Combined Data Authentication failed**
0080000000	*ICC and terminal have different application versions*	**The terminal cannot find the application version on the card, or it's different than the terminal. *Transactions will most likely not be declined***
0040000000	*Expired application*	**The card has an expired application. Transactions will most likely be declined**
0020000000	*Application not yet effective*	**The application on the card is prior to the date from which the application may be used. Transactions will be declined**
0010000000	*Requested service not allowed for card product*	**Service not allowed. Transactions will be declined**
0008000000	*New card*	**The card has never performed an online transaction. *Transactions will not be declined***
0000800000	*Cardholder verification was not successful*	**CVM condition code was not recognized/known by the terminal. *Will most likely not result in a declined transaction***

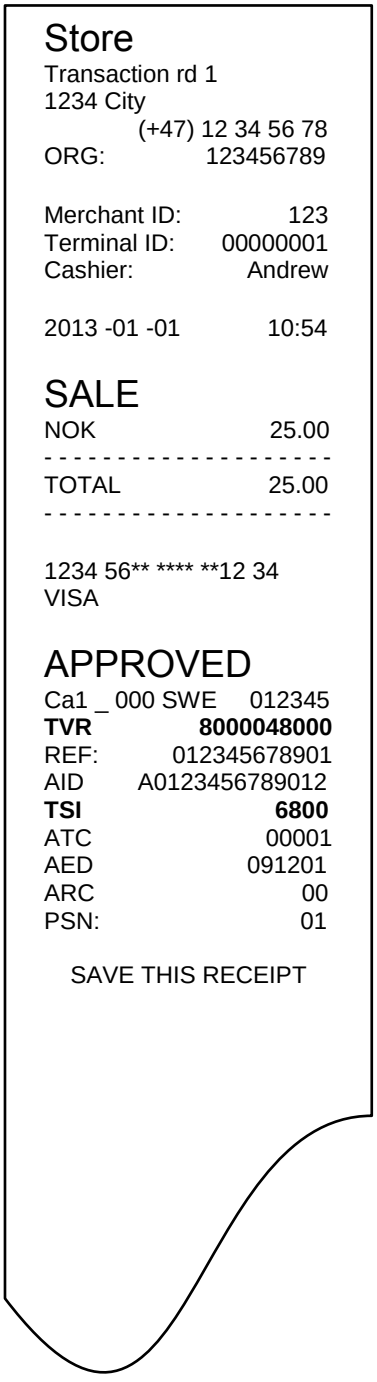
0000400000	*Unrecognized CVM*	**Method number in the CVM code is not known, but CVM condition code is known. *Will most likely not result in a declined transaction***
0000200000	*PIN try limit exceeded*	**Number of PIN tries exceeded. Transactions will be declined, and the customer must contact the card issuer**
0000100000	*PIN entry required and PIN pad not present or not working*	**Bypassing PIN is not supported by PayEx**
0000080000	*PIN entry required, PIN pad present, but PIN was not entered*	**Bypassing PIN is not supported by PayEx**
0000040000	*Online PIN entered*	**The card has online PIN. *Transactions will not be declined based on this TVR BIT by itself.***
0000008000	*Transaction exceeds floor limit*	**Transaction amount exceeds floor limit. The transaction must be verified online. *Transaction will not be declined if terminal is online.* Transactions will be declined if the terminal is offline**
0000004000	*Lower consecutive offline limit exceeded*	**Maximum number of consecutive offline transactions for this ICC application allowed in a terminal with online capability. Transactions will be declined.**
0000002000	*Upper consecutive offline limit exceeded*	**Maximum number of consecutive offline transactions for this application allowed in a terminal without online capability. Transactions will be declined.**
0000001000	*Transaction selected randomly for online processing*	**The transaction is below floor limit, but it has been randomly selected for online processing. *Transactions will not be declined***
0000000800	*Merchant forced transaction online*	**Merchant forced the transaction online. Transactions will be declined if the terminal is offline**
0000000080	*Default TDOL used*	**Default TDOL is used by the terminal if the card does not provide a TDOL**
0000000040	*Issuer authentication failed*	**The card was not authenticated by the Issuer. Transactions will be declined**
0000000020	*Script processing failed before final GENERATE AC*	**Issuer script failed**
0000000010	*Script processing failed after final GENERATE AC*	**Issuer script failed**

TSI

The TSI on the receipt provides information about which of these tests that has been performed during a transaction. If multiple TSI tests have been performed, the TSI will have a hexadecimal value, from 0-F; see the example on the next page.

TSI BIT	Description
8000	*Offline data authentication was performed*
4000	*Cardholder verification was performed*
2000	*Card risk management was performed*
1000	*Issuer authentication was performed*
0800	*Terminal risk management was performed*
0400	*Script processing was performed*

Example



Store
Transaction rd 1
1234 City
(+47) 12 34 56 78
ORG: 123456789

Merchant ID: 123
Terminal ID: 00000001
Cashier: Andrew

2013 -01 -01 10:54

SALE
NOK 25.00
- - - - - - - - - - - - - - - - - - - -
TOTAL 25.00
- - - - - - - - - - - - - - - - - - - -

1234 56** **** **12 34
VISA

APPROVED
Ca1 _ 000 SWE 012345
TVR 8000048000
REF: 012345678901
AID A0123456789012
TSI 6800
ATC 00001
AED 091201
ARC 00
PSN: 01

SAVE THIS RECEIPT

In this Example we can extract the information from the TVR:
8000000000 *Offline data authentication was not performed* – This bit will be set if the terminal cannot authenticate the card offline (i.e. the card has online PIN). The transaction is only verified online, or by signature if the terminal is offline.
0000040000 *Online PIN entered* – Online PIN was performed.
0000008000 *Transaction exceeds floor limit*- Some card schemes has 0 in Floor Limit. This means that all transactions must be approved online. If the terminal is offline, all transactions must be verified with signature. (It might be necessary to call the acquirer to request an authentication code as well).

From the TSI:
6000 6000 is not directly listed in the list of TSI. If multiple TSI tests have been performed, the TSI will have a hexadecimal value, from 0-F. In this case, **2000** – *"Card risk management was performed"* **AND 4000** – *"Cardholder verification was performed",* ***has been performed.***
0800 – *Terminal risk management was performed.*

AID

All EMV cards can contain multiple applications. Application selection is either automatically selected by the terminal when a customer inserts a card, or the customer selects the preferred application.

Card Scheme	RID	Product	PIX	AID
VISA	A000000003	Visa credit or debit	1010	A0000000031010
		Visa Electron	2010	A0000000032010
		V PAY	2020	A0000000032020
		Plus	8010	A0000000038010
MasterCard	A000000004	MasterCard credit or debit	1010	A0000000041010
		MasterCard	9999	A0000000049999
		Maestro (debit card)	3060	A0000000043060
American Express	A000000025	American Express	01	A00000002501
Dankort	A000000121	Debit card	1010	A0000001211010
Diners Club	A000000152	Diners Club	3010	A0000001523010
Discover	A000000152	Discover	3010	A0000001523010
BankAxept	D578000002	BankAxept	1010	D5780000021010

Configuration parameters list

This is a list of configuration parameters loaded on the terminal. Parentheses indicate the (maximum) length of the parameter. This is an example list, and is not valid for your terminals.

```
CLEAR;                    // Used to clear all parameters already present on a
terminal.
16=578027;                // (10) PSP code. Required for IK loading
28=578;                   // (3) Currency code. 578=no, 752=se, 208=dk.
36=00000001;              // (8) Terminal ID.
43=0123456;               // (10) Acquiring inst. identifier.
60=PayEx;                 // (??) Merchant name
61=Wergelandsvn 1;        // (??) Merchant address
62=0167 Oslo;             // (??) Merchant address 2
63=194.248.134.48;        // (16) IP address.
64=9034;                  // (5) IP port.
65=NOK;                   // (3) Currency text.
71=1234;                  // (4) Supervisor password.
74=0;                     // (1) Toggle: Extra.
75=55;                    // (2) Extra limit as percentage.
77=1;                     // (1) Toggle: Cents.
78=0;                     // (1) Toggle: VAT.
79=25;                    // (2) VAT percentage.
100=0;                    // (1) Host connection type. Ethernet=0, GPRS=1.
109=0;                    // (1) ECR mode. 0=off, 2=PPP, 3=Ethernet.
110=6000;                 // (4) TMS port.
111=217.109.89.152;       // (15) TMS IP.
112=payex.apn.telenor.se; // (22) TMS GPRS apn
115=0;                    // (1) TMS connection type. Ethernet=0, GPRS=1.
122=1;                    // (4) Interval between offline transaction sending.
Minutes
123=0;                    // (1) Toggle: PIN/CVM before amount.
127=1445;                 // (4) Time for automatic TMS call. Format: HHMM or HH.
129=p;                    // (1) ECR client
130=0;                    // (1) Require card present on manual reversal.
131=5541;                 // (4) Merchant Category Code.
132=NO;                   // (2) Terminal language
136=987654321;            // (9) Standalone receipts: Merchant org. number.
                              Recommended max length is 9 characters.
137=Cashier;              // (12) Standalone receipts: Cashier name.
                                Recommended max length is 12 characters.
138=3;                    // (1) Number of allowed tries to enter Voice Auth
Code.
140=D5780000021010;       // (14) If an AID is found, auto select it. BAX:
D5780000021010, Dankort: A0000001211010
141=0;                    // (1) Toggle: Print merchant copy when CVM is
signature.
144=2;                    // (1) DHCP on/off. 0=off, 1=on, 2=User controlled.
145=0;                    // (3) Max amount for doing "No CVM" purchase.
146=1;                    // (1) Enable surcharge on the terminal. 0=off, 1=on.
147=+47 99 40 11 50;      // (20) Phone number for 2nd line support
148=0;                    // (1) Toggle: Enable/Disable beeping on PIN entry
149=1;                    // (1) Toggle: Decline when call for auth 0=off, 1=on.
150=0;                    // (1) Toggle: Enable/Disable SSL for HOST
communications.
155=;                     // (64) Password for SSL client certificate
167=1107;                 // (4) Time to perform terminal time update.
168=0;                    // (1) Toggle: Beep when a transaction is not approved
187=5;                    // (4) Maximum number of stored offline trx in terminal
251=0;                    // (1) Toggle: Use serial packet with PPP.
```

Accessories

Below is a list of accessories. Contact your supplier to order these products.

Terminal type	Category	Product name/description	Product number
iWL2xx	PSU	Terminal monoplug (PSU via micro USB)	192010793
iWL2xx	PSU	Base monoplug (PSU via a Base)	192010579
iWL2xx	PSU	Car charger (via micro USB)	192013244
iWL2xx	PSU	Travel adapter (Use the Base PSU to directly charge the terminal)	296110863
iWL2xx	Battery	Li-ions Battery	295006044
iWL2xx	Cable	Ethernet cable 3m	293500052
iWL2xx	Cable	Modem cable	179900087
iWL2xx	Cable	USB cable, female to micro USB (Connect the terminal to a USB device)	296109807
iWL2xx	Cable	USB cable, male to micro USB (Connect the terminal to a USB Host)	296109815
iWL2xx	Base	Charging base	iWL200-01P1481A
iWL2xx	Base	Ethernet modem base	iWL200-01P1482A
iWL2xx	Base	Bluetooth Ethernet modem base	iWL200-01P1483A
iWL2xx	Misc.	Paper feeder iWL	192000053
iPP3xx	Cable	Ethernet cable with External PSU	Cable: 296 114 829 PSU: 192011109
iPP3xx	Cable	USB type A Powered straight cable	296 100 039

Supported cards

Below is a list of supported cards by PayEx. Please note that not all merchants support all cards listed below.

Card	Card
VISA	Universal Presentkort
VISA Electron	YX
MasterCard	Blackhawk Gift cards and value codes
American Express	EVC Gift cards and value codes
Diners Club	Habbo
Handelsbanken Finans	Kicks
VW	Spotify
SKODA	Stadium
Ikano kortet	iTunes
Rikslunchen	DKV
Resursbank	PREEM
FINAX GE CAPITAL	Union Tank
Maestro	yX
JCB	OoB-Card
AgriCard (VISA)	Coop Bonus
SVENSKE BANKKORT	LO Favør
Shell Mastercard	NAF
Ticket Rikskortet	PayEx Loyalty
Vardetryck	Trumf
RIK	Aktiiviraha
ACCEPTCARD	Aurinkomatkat
Bankkort (GE Kapital Bank)	Beoscan
Bankkort	Esso
Bankkort (Coop)	Finnair
COOP Mastercard	Hemtex
COOP Visa	Japan Credit Bureau
Cashcomspresentkort	K-Luotto
China Union Pay	Käyttöluotto
DANKORT	Luottokunta
FDM (Statoil)	Meritarahoitus 2S
Forbrugsforeningen	Neocard
Sentrumsgavekort	OP-Kotipankki
Gavekort Kjede	Pankkikortti
Gavekort Senter	S-Business Card Manage
Gavekort 1	S-Etu
HB Finans	S-Lahjakortit
Ikano	S-Pankki
Shell Mastercard	S-Tili
BBS Kjedegavekort	SOK Gift Card
LIC Mastercard	ST1
Lindex kortet	Spar kortti
Lyngby Storcenter Konto	Stockmann
PBS Centerkort	Taksikortti
PBS Handelstand	Tiliraha
PBS Kjedekort	Tradeka
PayEx Gavekort	PosPay Value cards and -codes
BBS Sentergavekort	Esso Fuel
SparXpres	Metax
Trumf	EuroShell

Abbreviations and acronyms

AID – Application ID
APN – Access Point Name
DDA – Dynamic Data Authentication
DHCP – Dynamic Host Configuration Protocol
DUKPT – Derived Unique Key Per Transaction
ECR – Electronic Cash Register
EMV – Europay, Mastercard, VISA

GPRS – General Packet Radio Service
IP – Internet Protocol
ISP – Internet Service Provider
LAN – Local Area Network
LLT – Local Loading Tool
MAC – Message Authentication Code
MCC – Merchant Category Code. MCC is located in parameter no. 131.
PIN – Personal Identification Number
PPP – Point to Point Protocol
PSU – Power Supply Unit
SIM – Subscriber Identity Method
SDA – Static Data Authentication
SSL – Secure Sockets Layer
TDOL – Transaction certificate Data Object List
TMS – Terminal Management System
TSI – Transaction Status Information
TVR – Terminal Verification Results
USB – Universal Serial Bus

Notes