



EMV PAYMENT TERMINAL SYSTEM FUNCTIONAL DESCRIPTION 21 October 2011 / V 4.2





table of contents

1. Introduction	2
2. Definitions	3
3. Payment terminal system	6
4. Agreements and accepted cards	6
5. Identifying cards and verifying their authenticity	7
6. Purchases and cash withdrawals	8
6.1 Purchases	8
6.2 Cash withdrawals with bank cards	9
6.3 Cashback with Visa and MasterCard cards	10
6.4 Correcting transactions	10
6.5 Payee's receipt	10
7. Authorisation	11
7.1 Automated authorisation	11
7.2 Manual authorisation	11
8. Forwarding hot card information	12
9. Forwarding transactions	12
9.1 Principles for transmission of transactions	12
9.2 Transmitting transactions	12
9.3 Check-ups for bank card transactions	13
10. Refunding transactions	13
11. Monitoring card payments	13
12. Storing receipts	17
13. Issuing complaints over transactions	17
14. Exceptional situations in transaction transmission	17
14.1 Processing old bank card transactions	17
14.2 Batch adjustments	18
15. Security	18
15.1 PCI requirements	18
15.2 Guidelines for merchants	18
15.3 Using the PIN	18
15.4 Data communication encryption	19
15.5 Data storage	19
15.6 Deletion of data	19
16. Further information	19

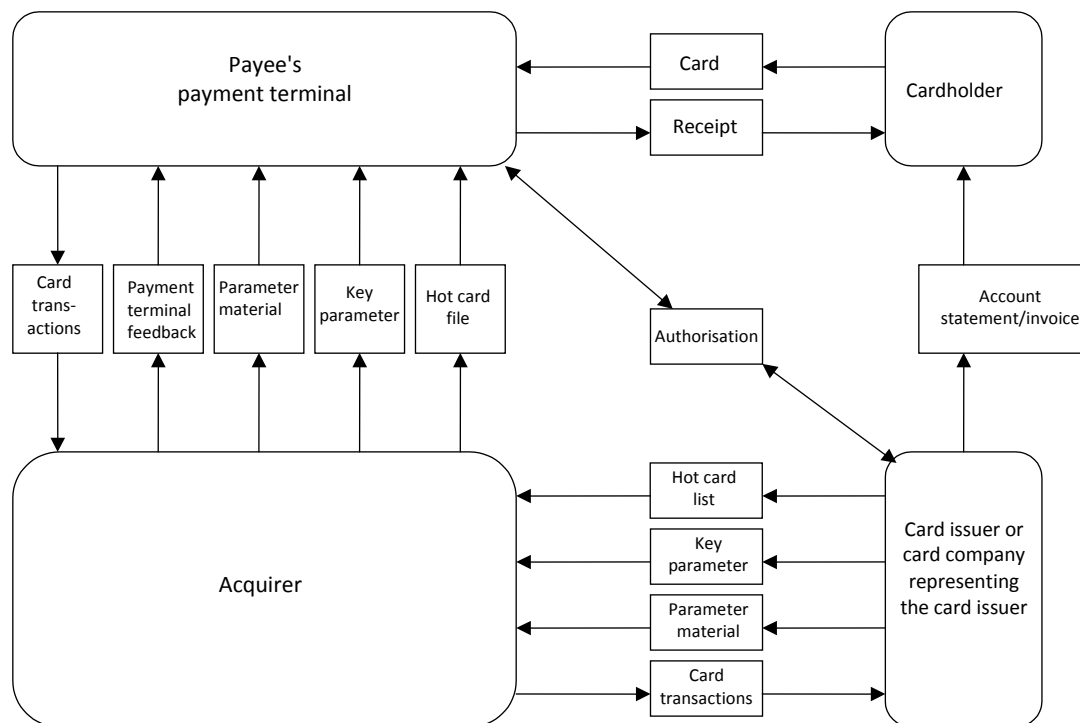
1. Introduction

This functional description is to be appended to a payment terminal agreement. This document describes the general principles of the banks' EMV payment terminal system.

This description focuses on the processing of bank card transactions. Each card issuer has its own terms and conditions, which must be observed when processing transactions made with the issuer's cards.

The payment terminal system includes the following functions and properties:

- Purchases and cash withdrawals and the related forwarding procedures
- Payment terminal authorisation
- Feedback and payee account credit
- Forwarding key and parameter material data
- Procedure for forwarding hot card information



The payee must observe the agreement and safety regulations, and any instructions issued by the acquirer or card issuer.

As regards bank cards, the bank card guarantee conditions and payment terminal agreement describe the mutual liabilities of the bank and the acquirer.

The EMV payment terminal system description, which has been distributed to software suppliers, describes the properties required of payment terminal systems and equipment.



2. Definitions

Acquirer refers to the party who negotiates together with the payee (company) upon how card transactions are credited and how materials (payment transactions, safety data, key parameters and parameter materials) are received, transferred and processed. The issuer determines the routing of authorisations. The acquirer or the party authorised by the acquirer certifies payment terminals. The acquirer can arrange the forwarding of transactions with a router.

Authorisation requester is a payee who sends an authorisation request to the card issuer.

Authorisation service is used by the payee in accordance with the terms and conditions governing the card to verify the card data and the sufficiency of funds in the account that is linked to the card that is paying for goods or services or making a cash withdrawal, as well as to place the funds on hold. Authorisation is made automatically through a payment terminal or by telephone.

Bank card is a national payment card that is issued by the bank and linked to the customer's bank account. The card can be used in Finland for shopping and for cash withdrawals. Bank cards cannot be used to make payments on the Internet.

Bank card warranty means that the bank verifies that the payee has operated in accordance with the valid bank card warranty conditions prevailing at the time, before paying the sum to the payee. The bank card warranty does not cover cash withdrawals at points of sale.

Card issuer (Issuer) is a bank or another institution which issues cards and is responsible for their distribution and life cycle, as well as for the debiting of purchases and cash withdrawals to the cardholder's account. The issuer specifies the terms and conditions applied to the use of its cards.

Cashback refers to a cash withdrawal that is made in connection with a credit or debit card purchase at a point of sale. A cashback transaction cannot be made independently of a purchase (cf. cash withdrawal with a bank card at a point of sale).

Cash withdrawal refers to cash withdrawal with a bank card, executed at a point of sale, which does not require a concurrent purchase (cf. cashback).

Certificate is a component used in PKI encryption. The certificate allows parties to identify each other, and the TCP/IP connection is encrypted with a banks' certification service certificate that is ordered from the bank. The authenticity of EMV cards is verified by means of a certificate issued by Visa/MasterCard. DDA cards also include the card issuer's own certificate.

Chip card (Integrated Circuit Card, IC Card, Smart Card, Chip Card) is a plastic card which contains an embedded security processor with memory (i.e. a chip). The chip contains one or more EMV payment applications for use in payment terminals. The chip may also contain other applications (e.g. authentication application or e-purse application). The Single Euro Payments Area rules require that all general-purpose credit cards are equipped with an EMV-standardised chip.



21 October 2011 / V 4.2

Combination card contains two or more payment applications or payment methods. These include cards which combine e.g. a bank card together with a Visa or MasterCard credit card, or a Visa or MasterCard credit card with a Debit card.

Credit card is a card used for payment of goods and services utilising the credit granted to the cardholder. Credit cards come in two types, general purpose cards and store cards or retail credit cards. If the credit is interest-free and the purchases are paid in full against each invoice, the credit card can also be referred to as interest-free card or grace period card.

Debit card is a chipped payment card issued by the bank to the customer for international use on a bank account. Debit card payments require online authorisation either always (like Visa Electron/Maestro) or where the card parameters or payment terminal parameters so require.

EMV refers to a payment card standard developed by international card companies (MasterCard and Visa) for chip payments.

EMV payment terminal system refers to a device or set of equipment that is in the possession of the acquirer and has been certified by an organisation approved by the acquirer. The system enables the automated retrieval of key parameters and parameter materials, card payments, hot card list checks, forwarding transactions to the bank, and transaction verification. The payment terminal reads the card data either from a chip or magnetic stripe, performs the necessary verifications, stores the purchase transaction and forwards the transactions.

General-purpose credit card refers to a card that the holder may use at any point of sale that will accept the card regardless of its line of business. *Retail credit card* and *store card*, instead, refer to cards that are only accepted by certain points of sale.

Hot card file and list

A hot card file contains information on blocked payment cards. The file is delivered electronically to the payment terminal. A hot card list is a paper document which contains information on all blocked payment cards, and is used in a similar fashion with a manual imprinter.

Issuer – see Card issuer.

Key parameters ensure the authenticity of the chip card at the payment terminal.

Manual imprinter is used to transfer customer and payee information onto a payment form. The imprinter makes a carbon copy of the embedded (raised) characters on the customer's payment card. The payee's information is copied from a name plate, which has e.g. the payee's member shop number, trade registry number or business ID, name, address (and account number). Banks and acquirers who accept bank card transactions will provide a guide on the use of the payment form and the manual imprinter.

Online authorisation is used for the real-time verification of a card's validity.

Parameter materials are used by EMV payment terminals to identify the payment cards accepted by the terminal.



Payee provides products and services, which the cardholder purchases with their payment card. The payee must have valid agreements on the approval of bank card transactions and forwarding them to the bank (payment terminal agreement) with its account-holding bank and, as concerns other cards, with the card company in question.

Payment application is an application stored on the chip, which contains the payment features of the card (e.g. Visa Credit, Debit MasterCard, etc.) and its processing rules, for example on the use of the card in payment terminals and ATMs, as specified by the bank or the card entity. In addition to common processing rules, the chip's payment may contain restrictions and risk management parameters that individual card issuers may have imposed on the use of the card.

Payment card is a general term for bank, credit, combination, cash and charge cards.

Payment terminal – see EMV payment terminal system.

PA-DSS (Payment Application Data Security Standard) is a data security standard which applies to card payment systems and focuses on software houses in particular.

PCI/DSS (Payment Card Industry / Data Security Standard) is a data security standard which protects card payment data. The standard applies to all parties who process card payment data.

PCI PTS (Payment Transaction Security Requirements) is a data security standard for card payment transactions which applies to all device manufacturers whose devices allow the use of personal information numbers (PIN codes).

PCI data security standards are issued by international card organisations (American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc.) for the protection of card payment data. The standards include technical and functional requirements. The PCI standards include PCI Data Security Standard (PCI DSS), PIN Transaction Security Requirements (PCI PTS) and Payment Application Data Security Standard (PA-DSS). Further information on the PCI standards can be found on the website of the PCI Security Standards Council and/or requested from the acquirer.

PIN (Personal Identification Number) is a code known only by the cardholder. The PIN code is checked when the card is used in cash dispensing ATMs and payment terminals to verify the card user and to approve the payment.

PIN pad is a number pad that is used to enter the PIN on a payment terminal.

Quasi-Cash transaction refers to selling commodities/services that can be exchanged into cash, for example gaming rights, chips, foreign currency, etc.

Reference numbers allow the payee to monitor refunds automatically. The payee must agree on the use of a reference number together with the bank, card company and payment terminal supplier.



21 October 2011 / V 4.2

Router forwards authorisations from the payee to the appropriate card issuer and payment transactions to the acquirer or receiver of card transactions. The router delivers the received response back to the payee. One transaction may involve several routers. It is also possible that no router is used.

Surcharge is an additional charge by the payee.

TCP/IP (Transmission Control Protocol / Internet Protocol) refers to a protocol used by data communication networks on the Internet.

3. Payment terminal system

The EMV payment terminal system function is based on the EMV payment terminal system description (POS 03001) maintained by the Federation of Finnish Financial Services.

All EMV payment terminals and payment terminal systems that accept bank cards must be certified by an organisation authorised by the Federation of Finnish Financial Services. Payees are advised to refer to Luottokunta's website (www.luottokunta.fi) for information on Visa and MasterCard -certified terminals.

Payees can purchase an EMV payment terminal or payment terminal system from software houses or equipment suppliers. The terminal or system consists of the following components:

- card reader for chip and magnetic stripe cards
- PIN pad
- display
- key pad
- receipt printer
- payment terminal software
- line connection (transaction transmission and authorisation)

Detailed user instructions for the payment terminal or payment terminal system are supplied by the equipment manufacturer or payment terminal software supplier.

4. Agreements and accepted cards

The payee must agree on the following issues with its account-holding bank:

- the payment terminal service
- accepting bank cards as a form of payment
- cash withdrawal service, when necessary.

The bank and payee agree on the following issues in the payment terminal service agreement: forwarding and authorising payment card transactions approved by the payee, hot card information updates and the key and parameter materials, as well as feedback material.

The agreement concerning acceptance of bank cards as a form of payment covers all bank cards issued by all banks in Finland. As concerns other payment cards, the payee agrees on



their acceptance as a form of payment with the card company in question. Each card company issues its own terms and conditions and other guidelines.

In addition to a bank card application, combination cards also contain a payment card application for international use. Banks may also issue co-branding cards together with certain enterprises. In addition to a bank card or other card feature, these cards also contain the partner's payment card feature. The bank card feature is subject to warranty conditions and the instructions above.

The implementation and routing of the authorisation must be agreed with the bank, a teleoperator or other service supplier.

The payee must observe the terms and conditions and guidelines for the payment card.

The Payment Card Subcommittee at the Federation of Finnish Financial Services decides on the approval of cards for the banks' payment terminal system. The Federation of Finnish Financial Services maintains a list of cards which are valid for use in Finnish payment terminals. The list is made available to software houses maintaining payment terminal systems.

If the payee has issued cards which have not been accepted in the system, the payee can, at its discretion, agree on a software modification with the payment terminal software supplier to ensure that such cards will also be accepted in the payee's payment terminal system.

5. Identifying cards and verifying their authenticity

Bank cards display the name of the bank and the word 'Pankkikortti' or 'Bankkortt'. Combination cards also display the identifiers of the relevant international card system.

An increasing number of payment cards contain a chip as well as a magnetic stripe on the back, which serves as a backup system.

The card number is embossed on the card. The first four digits of the card number are also printed on card.

The period of validity is given in the format MM/YY.

The bank card is embossed with the letters 'PK' or 'BK'. A combination card may contain further embossment.

The name of the cardholder is embossed on the card, and his/her signature is displayed on the back.



21 October 2011 / V 4.2



Further information concerning card identification is available from Visa and MasterCard acquirers and the relevant card companies.

The EMV payment terminal system identifies accepted cards by means of parameter material data. The system verifies the authenticity of chip cards using key parameters. The card issuer maintains the key and parameter material data. The payee's bank or other acquirer makes the material available for retrieval by the payee. The payment terminal system retrieves new material automatically.

The payee must always contact the software/equipment supplier when making an agreement concerning the acceptance of a new payment card or when the agreement with the card company expires.

When a payment terminal is withdrawn from use or the payment terminal agreement expires, the payee must notify the acquirer and the software/equipment supplier.

The payee is responsible for ensuring that the key and parameter material data in the payment terminal system is up to date.

6. Purchases and cash withdrawals

6.1 Purchases

When a chip card is used, the data must be read from the chip in the first place. The cardholder inserts the chip card into the payment terminal's card reader, verifies the amount to be charged, selects the form of payment (if asked to do so by the terminal) and enters his/her PIN to authorise the payment to be debited from his/her account. The use of the PIN corresponds to signature and verification of identity. The terminal prints a receipt on the payment for the customer.

When the customer pays with a magnetic stripe card that does not contain a chip, the cashier reads the card data using a magnetic stripe reader. If necessary, the cashier asks the customer for the preferred form of payment and selects the specified option. The payer accepts the transaction by signing the receipt. The cardholder's identity is to be verified and authorisation requested if required by the card's warranty conditions or when necessary for security reasons.

The payee is required to keep receipts for bank card payments or electronic data related to the payment for a minimum of eighteen (18) months. The payee must present a receipt or



21 October 2011 / V 4.2

printout for a given transaction upon request free of charge. The receipts must be stored and disposed of safely, ensuring that the data in the receipts cannot fall into the hands of outsiders.

Other card companies issue separate guidelines for the use of their cards and storage of payment terminal receipts.

Chip cards control the operation of the payment terminal. The use of chip cards may be subject to various restrictions set by the bank or the cardholder.

6.1.1 Exceptional situations

When using a chip card the customer approves the charge by his/her PIN or, in exceptional situations, by his/her signature, in which case the transaction is authorised and the cashier verifies the customer's identity and the authenticity of his/her signature. The customer may approve transactions by his/her signature if he/she cannot remember his/her PIN or it cannot be used for other reasons.

If the chip does not work, the card data can be read from the magnetic stripe, which acts as a backup system, and the payer approves the transaction by signing the receipt. The cashier should verify the identity of the payer. The transaction must always be authorised.

If the magnetic stripe is unreadable, the cashier can enter the card number manually on the number pad, if this is permitted by the card company. In this case the transaction must be authorised and a manual imprint taken using a manual imprinter to prove that the card was present during the transaction. The cashier should affix the imprinted payment slip to the receipt from the payment terminal. The customer only signs the receipt.

If the card is embossed and the card issuer allows it, the manual imprinter can be used as backup to the payment terminal system. If a manual imprinter is used, special care should be taken when identifying acceptable cards and checking the blacklists. Transactions must always be authorised.

6.2 Cash withdrawals with bank cards

The payee may offer its customers the opportunity to withdraw cash at the shop's cash register with their bank cards. The payee must agree on this service with its account-holding bank: The cash withdrawal service must be made available to all customers using a bank card, irrespective of their bank. Customers may also choose to withdraw cash only, and the payee must not require a purchase of goods or services to be made.

For the payee to be able to offer the service, the payment terminal must support automated authorisation. Cash withdrawals are always verified regardless of the amount. The cash cashier should verify the customer's identity. Entering the card number manually on the number pad is not permitted.

The payee may advertise the cash withdrawal service and charge a fee from the customer for the service. A notice stating the availability of the service and it being subject to a fee must be clearly displayed at the cash register. The amounts of the cash withdrawal and the service fee must be separately stated on the cash withdrawal receipt.



The payee can refuse to offer the cash withdrawal service, or lower the maximum amount of withdrawals, if cash funds at the cash registers are running low. If the payee is temporarily prevented from offering the cash withdrawal service, the customers must be informed without delay.

Cash withdrawals are not covered by the bank card guarantee.

The cardholder's bank sets the minimum amount for cash withdrawals. The maximum amount is EUR 400.

The bank verifies the authorisation code included in the payment terminal message. If the authorisation code is incorrect or missing, the system rejects the transaction and returns it to the payee.

6.3 Cashback with Visa and MasterCard cards

Cashback transactions with Visa and MasterCard cards differ from cash withdrawals made with bank cards. The acquirers of Visa and MasterCard cards specify the terms and conditions for cashback transactions and issue the relevant instructions.

6.4 Correcting transactions

An erroneous bank card transaction can be corrected by cancelling the original transaction and then making the correct transaction. When a bank card transaction is cancelled, the cancelling transaction must always refer to the original transaction of the same amount (counter-entry) and be sent to the bank together with the data on the original transaction. Single correction transactions made later are not permitted for bank card payments; instead, the customer must be refunded by means of a cash refund, gift voucher, account transfer from the payee to the payer, etc.

If the original transaction was authorised, the authorisation must also be cancelled.

Card companies issue their own instructions for correcting payment transactions made with their cards.

6.5 Payee's receipt

The payee is required to keep receipts for bank card payments or electronic data related to the payment for a minimum of eighteen (18) months. The payee must present a receipt or printout for a given transaction to the bank upon request free of charge. The receipts or data must be stored and disposed of safely, ensuring that the data cannot fall into the hands of outsiders.

The payee's and cardholder's receipts can be distinguished from each other by means of the card number, for example. The payee's copy shows the card number in full, while the cardholder's copy shows the last four digits.



7. Authorisation

In the EMV system the chip card controls the operation of the payment terminal and requests the terminal to send an authorisation request based on the risk management parameters set by the card issuer.

All purchases must be authorised if they exceed the limit specified in the bank card guarantee conditions. Smaller amounts may also be authorised, if required by the payee, and random authorisation requests be made for transactions that remain below the guarantee limit. All cash withdrawals made using a bank card and transactions made with Visa Electron or Maestro cards must always be authorised electronically. The authorisation limits for other cards are set by each card company.

The authorisation must apply to the total amount of the purchase. If the amount is changed (for example, a tip is added to a restaurant bill), the original purchase and its authorisation must be cancelled and a new transaction (and a new authorisation) be made with the final amount.

All bank card transactions made on unattended self-service machines (such as oil companies' fuel pumps) must always be authorised electronically. At a fuel pump, the final amount of the purchase is not known in advance. For this reason, oil companies have agreed to advance authorisation and partial cancellation of transactions.

7.1 Automated authorisation

Payment terminal authorisation is based on the EMV payment terminal system description maintained by the Federation of Finnish Financial Services. Payment terminal authorisation uses the encrypted TCP/IP connection or a closed X.25 packet switched network. The payee must contact the equipment/software supplier to ensure that the authorisation connections have been directed to the bank or other card issuer using the most direct route.

The TCP/IP connection is encrypted by means of a certificate issued by the Banks' Certificate Service.

If authorisation routing is provided by an external supplier, the payee and the service supplier agree on the implementation of the authorisation traffic and the related division of responsibilities.

7.2 Manual authorisation

If the payment terminal does not support electronic authorisation, manual authorisation via a telephone must be used as a backup. The telephone number of the authorisation service is +358 100 3100.

The cashier must enter the authorisation code obtained from the authorisation service on the payment terminal's number pad or write it on the payment slip. The authorisation codes for bank cards include a verification digit to prevent errors when keying in the number.

8. Forwarding hot card information

The acquirer makes hot card information available for retrieval by the payee's payment transfer system. Hot card files are compiled daily, including the weekend.

The Payment Card Subcommittee at the Federation of Finnish Financial Services decides on the hot card information forwarded in the payment terminal system.

The payee should agree on the retrieval of a printed hot card list, which serves as backup, with its bank.

The hot card information is available for retrieval by the payee from 00.00 am. The payee is obliged to retrieve the information before accepting any card transactions. If the sales outlet is not open every day, the payee must also ensure retrieval of hot card lists issued for those days during which the outlets was closed.

The payee's liability for hot card information issued by the bank begins immediately upon retrieval of the information, yet nevertheless no later than 24 hours after the bank has made the information available for retrieval by the payee. The beginning of the liability period concerning other cards is set by each card company.

Each card company is responsible for the authenticity of its hot card information.

9. Forwarding transactions

9.1 Principles for transmission of transactions

All EMV payment terminals and payment terminal systems used in Finland must be certified by an organisation authorised by the Federation of Finnish Financial Services. The payee is responsible for the authenticity of the transaction material, transmitting the material and retrieving feedback. The bank is responsible for processing the material it receives, refunding bank card transactions, creating feedback and making transactions to be transmitted available to card companies.

As a rule, bank cards are accepted in Finland. However, a Finnish company may place a payment terminal certified in Finland in its office abroad which accepts Finnish debit and payment cards. This must nevertheless be separately agreed with the receiving bank. Bank card transactions transmitted from abroad must be denominated in euro. The bank card guarantee does not apply to transactions made abroad. The transmission of transactions other than bank card transactions must be separately agreed with each card issuer.

If authorisation routing is provided by an external supplier, the payee and the service supplier agree on the transfer of payment terminal files and the related division of responsibilities.

9.2 Transmitting transactions

Banks recommend data be transmitted once a day. Banks receive transactions around the clock each day of the week. If the transactions are transmitted as timed, it is advisable not to send them on the hour in order to avoid congestion in data communication.



Bank card transactions must be delivered within 20 days of the date of the transaction. If this is not possible, the payee must immediately contact its bank, as well as the card companies whose cards the delayed delivery concerns.

The payment terminal system generates a transmission report, which the payee must check, see section 11.

9.3 Check-ups for bank card transactions

Banks are not obliged to approve transactions in the following cases :

- The transaction is older than 20 days
- The payment terminal message does not comply with the current payment terminal transaction
- The check digits for the card number are incorrect
- The payee has failed to observe the limits specified in the bank card guarantee conditions
- The amount of the transaction exceeds the authorisation limit, but the transaction has not been authorised or the check digit for the authorisation code is incorrect
- A cash withdrawal has not been authorised
- The date of the transmission batch sent to the bank is more than five (5) days old.

For cards other than bank cards, the issuer's conditions and guidelines are to be observed.

10. Refunding transactions

The bank receiving the transactions refunds the payee for all purchases and cash withdrawals made with any bank card once the data verification has been completed. Transactions sent on banking days are refunded on the date of transmission, provided the material arrives at the bank by the deadline stipulated by the bank; otherwise, the bank refunds the payee on the following banking day. The bank informs the payee of the refund by means of payment terminal feedback and account statement.

The bank makes transactions other than bank card transactions available to the card issuer or the card company representing the card issuer within the agreed schedule. The card issuer carries out verifications for these transactions. Approval limits, refund time and methods are based on the agreement between the payee and the card issuer.

The payee can automate refund supervision using a reference. The payee is to agree on the use of the reference and its contents with the bank, card company and equipment supplier.

11. Monitoring card payments

The payee monitors the card payments by means of delivery reports, feedback provided by the bank and account statements.

The payment terminal delivery report displays the number of card transactions sent to the bank and their amounts per settlement batch and card type. Failed transmissions are also stated on the delivery report.



21 October 2011 / V 4.2

The bank creates feedback data on received transactions for the payee. The data displays the following information per settlement batch:

- amount credited to the account,
- number of forwarded transactions per card company,
- breakdown of rejected transactions.

The payee can ensure that all payments have been processed and approved by the bank by comparing the delivery report with the feedback data created by the bank. The payee is obliged to check that the feedback data and the corresponding delivery report match the refund data on the account statement.

Approved materials are displayed by settlement batch on the account statement.

Example of payment supervision

The payment terminal makes an automated transmission at 1.05 a.m. on Wednesday. The material contains Tuesday's card transactions.

Transmission report		
26.07.2006 01:05		
SETTLEMENT BATCH 0001009		
BANK CARDS	ITEMS	€
CHARGED	25	1,000.00
ADJUSTMENT	0	0.00
=====	=====	=====
TOTAL	25	1,000.00

SETTLEMENT BATCH 0001010		
LUOTTOKUNTA	ITEMS	€
CHARGED	12	480.00
ADJUSTMENT	1	40.00
=====	=====	=====
TOTAL	13	440.00

- Tuesday's bank card payments are credited to the shop's account on Wednesday.
- The payment terminal retrieves the feedback at 1.05 a.m. on Thursday, transmitting Wednesday's transactions at the same time.



21 October 2011 / V 4.2

Feedback report		
26.7.2006 15:30 Settlement batch 0001009		
REJECTED CARD € FILING REFERENCE DESCRIPTION BANK CARDS CHARGED ADJUSTMENT =====	0004920510032370746 15,00 960723K12T0556 CARD NUMBER ERROR ITEMS 24 0 =====	€ 985.00 0.00 =====
TOTAL	24	985.00
Settlement batch 0001010		
LUOTTOKUNTA CHARGED ADJUSTMENT =====	ITEMS 12 1 =====	€ 480.00 40.00 =====
TOTAL	13	440.00

- On Thursday morning the shop compares the feedback report printed by the payment terminal during the night with the transmission report printed on Wednesday night, noticing that one of the payment transactions made on Tuesday was rejected at the bank and the amount credited to the account is EUR 15 short.
- The shop identifies the transaction on the basis of the filing reference and determines the cause of the error.



Account statement		
Payment date Value date -----	Payee/Payer Message -----	Amount -----
2607	COMPANY LTD	985.00
2707	Payment terminal service 0001009 PURCHASES 24 ITEMS 0 ITEMS	985.00 0.00

- The shop can now acknowledge Tuesday's bank card transactions as received, except for the unclear card payment of EUR 15. Refund by Luottokunta shows on the account statement a few days later. The card companies' refund consists of charges and their adjustments. The commission charged by the card company is also deducted from the refund.

For example:

Charged 480.00 €
- Adjustments 40.00 €
- Commission x%

The shop may set off the amount against its receivables. The shop and card company settle any problems with credit card payments together.

12. Storing receipts

According to Section 70 of the payment services act (Maksupalvelulaki 290/2010), customers are entitled to a 13-month rectification period, during which they may issue a complaint and obtain rectification from their bank due to an unauthorised or incorrectly executed payment transaction. The rectification period begins on the debit date, not on the date of purchase. The seller's obligation to store receipts begins on the date of purchase, however.

Receipts must be stored for a minimum period of 18 months because the 13-month rectification period begins on the debit date, not on the date of purchase.

Accounting legislation does not require that payment terminal receipts are stored (the Accounting Board's opinion). However, these receipts are important material for the processing of old transactions or cases of unauthorised card use.

13. Issuing complaints over transactions

If the cardholder or cardholder's account-holding bank issues a complaint over a payment on the basis of the payment terminal agreement and/or bank card guarantee conditions, it can be charged to the payee for the duration of the settlement process. The final decision is made after the investigation. The payee is obliged to make the receipt for or transaction data on the payment in question available to the bank for investigation purposes free of charge.

14. Exceptional situations in transaction transmission

14.1 Processing old bank card transactions

In order to prevent transactions from expiring, it is recommended that the payee continuously monitors the settlement of card payments in accordance to section 11 in this document.

14.1.1 Transactions over 20 days but less than 3 months old

If a transaction transmission to the bank is delayed by more than 20 days, the payee must contact its account-holding bank beforehand to agree on the time of the delivery.

14.1.2 Transactions over 3 months old

If a transaction transmission to the bank is delayed by more than three months, the payee must deliver a report on the reasons for the delay to the bank, as well as the data concerning the transactions, for the purpose of obtaining cardholders' contact information. The payee must inform the cardholders of the delay in charging the card payment at least two weeks before sending the transactions to the bank.

The bank is entitled to charge the payee for expenses incurred due to the processing of delayed transactions.

14.1.3 Transactions over 12 months but less than 3 years old

The bank is not obliged to process transactions that are more than twelve months old, even though the payee's claim usually becomes statute-barred after three years from the purchase date, as provided in the Act on Time-Barring of Debts. The payee may recover the claim directly from the payer.

14.1.4 Other cards

Card company-specific guidelines are to be observed for other cards.

14.2 Batch adjustments

To adjust a fully erroneous batch or a batch that has been sent to the bank twice, the payee must contact its account-holding bank in advance to agree on the transmission of the entire adjustment batch.

Card company-specific guidelines are to be observed for other cards.

15. Security

15.1 PCI requirements

All the recipients, acquirers, recorders and issuers of card transactions must meet the requirements of international security standards such as the PCI.

PCI DSS (Payment Card Industry Data Security Standard) is a security standard approved by international card organisations. Further information on the standard is available on <https://www.pcisecuritystandards.org>.

PCI DSS is a technical standard, while PA-DSS is the functional standard.

15.2 Guidelines for merchants

The Federation of Finnish Financial Services, Luottokunta and the Federation of Finnish Commerce have jointly issued recommendations drafted for merchants in an effort to facilitate their choice of payment terminals and to ensure that the terminals are placed as conveniently as possible from the perspective of both the merchant and the customer. These guidelines are available in Finnish on the Federation of Finnish Financial Services website at http://www.fkl.fi/materiaalipankki/ohjeet/Dokumentit/Sirukortti_kauppiasohje.pdf. (FI/SWE)

15.3 Using the PIN

The PIN pad is to be placed in such a manner that outsiders cannot see the PIN entered on the terminal. Most PIN pads are portable by design; they are mounted on a swivel base or can be tilted, ensuring that the customer can safely enter his/her PIN. The needs of special groups should also be taken into account when considering the placement of the terminal.

The cashier can guide the cardholder in the use of the card during the payment transaction. The cardholder must always enter his/her PIN himself/herself. The cashier must never enter the PIN on behalf of the customer, even when asked to do so.



15.4 Data communication encryption

Transaction transmissions are to be protected as specified in the banking security standard (PATU) issued by the Federation of Finnish Financial Services. Payees obtain the transmission keys needed for encryption from their own banks.

All data communications using wireless networks, public Internet networks or foreign connections must be encrypted using strong encryption. The encryption techniques used by the WLAN, GSM and GPRS systems are not sufficient as such. The encryption must cover the entire transmission connection from one end to the other.

15.5 Data storage

The payee is responsible for ensuring that all data concerning card payments is stored in accordance with the PCI DSS standard and does not fall into the hands of outsiders.

15.6 Deletion of data

When the payment terminal is removed from use, the payee must inform the acquirer of the removal and remove all public keys from the terminal. This removal function is available on the terminal.

When the payee's agreement with the card entity terminates, the payee must remove the card entity's public keys from the payment terminal. This function is available on the terminal.

16. Further information

For further information on card payments, please see the publications and guides available on the website of the Federation of Finnish Financial Services www.fkl.fi.

For user instructions for the payment terminal, please contact the software supplier.

For instructions concerning the acceptance of Visa and MasterCard cards, please contact the card acquirer (e.g. Luottokunta). For instructions concerning other international cards, please contact the card company in question.

Other links:

<https://www.americanexpress.com/finland/>

<http://www.dinersclub.fi/dof/>

<http://www.luottokunta.fi>

<http://www.mastercard.com/fi/personal/fi/>

<http://www.visa.fi/fi.aspx>