



PCI PASSPORT 2026

THE SECURITY OF CARD PAYMENTS



The guide is intended for the use of S Group.

Provided by SOK Payment Solutions
Layout Pirre Liukka

January 2026



CONTENT OF THIS COURSE

- Ensuring secure card payments 5
- What does S Group’s PCI Passport training consist of? 5
- Safety considerations 6
 - 1. Checking and storing payment terminals 6
 - 2. Visits by maintenance personnel 7
 - 3. Using workplace computers and devices and secure work practices 7
- Secure payment 8
- Use of S-mobiili 9
- Security factors to consider during payment disruptions 10
- Information security management in S Group 11
- PCI DSS standard and information security 11
- Issues to be considered in the hotel business, the sales service for the travel and hospitality business, and customer service for online stores 13



Verifone

Kokonaissumma
€ 0.86

Valitse vaihtoehto

VISA CREDIT

VISA DEBIT

1 OZ.

2 ABC

3 DEF

4 GHI

5 JKL

6 MNO

7 PRS

8 TUV

9 WXY

* ' "

0 -SP

#

X

<

○

P400

S-ETUKORTTI
S-Pankki

ENSURING SECURE CARD PAYMENTS

Customers must be able to trust that they can pay securely with their payment card at S Group outlets and online stores **without fear of misconduct**. At S Group, we want to be worthy of our customers' trust and abide by the Payment Card Industry Data Security Standard (PCI DSS).

By following standard guidelines and practices, **we can reduce misconduct and improve the security of card payments**.

The standard sets the requirements for both secure technical solutions and practices and the training of personnel.

An independent **PCI auditor** makes random visits to selected S Group locations annually to check that correct practices are being followed, and that everyone handling payment cards is familiar with the PCI passport guidelines.

WHAT DOES S GROUP'S PCI PASSPORT TRAINING CONSIST OF?

PCI Passport training is S Group's own training course on secure card payments, which aims to ensure that **everyone who handles payment cards, payment card details or payment terminals in their work is familiar with secure card payment practices**.

Everyone who handles payment cards as part of their work must complete the PCI passport every year. New employees must participate in PCI Passport training before starting work.

For more information about card payments, contact the cash manager or the manager at your location, or read checkout instructions and PCI guidelines.

SAFETY CONSIDERATIONS

1. CHECKING AND STORING PAYMENT TERMINALS

Criminals try to gain access to payment card details by installing auxiliary devices on payment terminals to read and store card details, and by stealing payment terminals, for example.

PREVENTION:

- **Check daily** that all payment terminals are in place and show no signs of alteration, such as extra parts or wires, tool marks, broken parts or missing screws.
- **Payment terminals that are temporarily out of service** must be kept in a secure place or in a place that is monitored by the CCTV system.
- **If a payment terminal is found to be missing**, a closure request must be immediately made to the service provider or other party instructed to process such communications. A report of an offence must also be filed with the police if necessary. Do not forget to file an incident report for the missing payment terminal in SFalcony.
- If a **stolen payment terminal is returned** to the place of business, it must not be used or connected to the local network. In such a case, the payment terminal must be reported for suspected tampering and SFalcony's instructions must be followed.
- If you notice that a **CCTV camera is pointed at a payment terminal's keyboard, and the keyboard is not masked**, please report the situation appropriately in accordance with your cooperative's guidelines.
- The keyboards of all payment terminals on Veikkaus slot machines and ATMs visible in the location's CCTV cameras should also be masked.

2. VISITS BY MAINTENANCE PERSONNEL

From time to time, people visit our places of business to service the equipment there, but criminals may also impersonate service personnel.

PREVENTION:

- Always **verify** the identities of maintenance personnel and their work orders. You must do this even if you know the person from previous maintenance visits.
- **Report** any unauthorised persons who use payment terminals or cash registers.
- **Make sure** that doors lock behind you to prevent unauthorised persons entering the personnel facilities.

3. USING WORKPLACE COMPUTERS AND DEVICES AND SECURE WORK PRACTICES

Computers and devices in the workplace are intended for work purposes. You must not attach other equipment or install your own programs on them.

- Do not use the cash register for anything other than work purposes. Do not use it to access the internet or email.
- Always lock all devices when you leave them unattended, even for just a moment.
- Do not disclose user IDs or passwords to anyone. IT support will never ask for them.
- Learn good password practices (information security instructions) and learn how to create your own passwords in line with them.
- Be sceptical about requests, queries and phone calls in languages other than Finnish.
- The information security policy, the data security guidelines and other data security-related materials can be found in **sPoint**.

SECURE PAYMENT

When making a payment, the customer normally handles their own payment card. If necessary, you can advise the customers how to use the payment terminal. When advising the customer on how to make a payment, **you must never ask the customer for their PIN or enter it on their behalf.**

- Ensure that the customer can make the payment and enter their PIN undisturbed.
- Payment terminals instruct customers during the payment transaction, and you can follow the progress of the payment on the cash register display.
- **The magnetic stripe on payment cards with a chip must not be used for payments.** If a payment terminal is unable to read the card's chip, you must agree on another payment method with the customer.
- If it is not possible to read the card details from the chip, **you must not charge the card by entering the card number into the payment terminal.**
- If a customer does not remember their PIN, and payment cannot be approved without it, **it is not recommended that you bypass the PIN.** However, this practice may vary between cooperatives, so check the up-to-date instructions for your location.
- Please note that for some payment cards, bypassing the PIN is technically prevented. In this case, it is impossible to pay without the PIN.

If a customer is paying for their purchases without an S-Etukortti card, remember to ask if they have one. The customer will only receive co-op member benefits if they use their S-Etukortti card.

A customer can register as a co-op member online, on the S-Business mobile app, or at the co-op member service point and S Bank outlet. You can check the nearest service point in the S-mobiilli app.

THE FULL PAYMENT CARD NUMBER IS ALWAYS CONFIDENTIAL

- One of the central principles of the PCI DSS standard is that **a full card number is always confidential.**
- At S Group, **full card numbers are never printed on cashier receipts.** Only the last four digits are visible on the receipt.

NEVER

- Write down or store full card numbers, unless your location's instructions require this in certain situations.
- Take a photo of a payment card.
- Send full card numbers or photos of payment cards by email or through other electronic communication channels.
- Write down the security code on the back of a card.

USE OF S-MOBIILI

S-MOBIILI – THE CO-OP MEMBER'S OWN APPLICATION

S-mobiili is the co-op members' own app that you can use to

- earn cashback (Bonus) for your purchases when you use a contactless S-Etukortti Card or the barcode of your S-Etukortti Card
- add your S-Etukortti Card to your Apple Wallet
- view your electronic receipts and enable paperless transactions
- monitor your cashback status
- make use of your favourite stores' discounts and campaigns
- manage your S-Bank accounts and cards, as well as your savings and investments.

CUSTOMERS MUST ALWAYS HANDLE THEIR SMART DEVICES THEMSELVES

- When redeeming a coupon, make sure that the customer presses the button to use it.
- The S-Etukortti barcode must be read before proceeding to the subtotal.
- Check regularly whether there are any coupons in the S-mobiili app that are valid at your location.
- Tell your customers about the discounts and campaigns and help them use them.
- Note that the S-mobiili app is constantly evolving, so you should regularly check it for new features and changing benefits.

MOBILE S-ETUKORTTI CARD

S-mobiili users can accrue cashback and take advantage of co-op member benefits on their phones. **Android users** can use their contactless S-Etukortti Card via S-mobiili, while **iPhone users** can add their S-Etukortti Card to their Apple Wallet or also use it with their Apple Watch.

S-mobiili also has an **S-Etukortti barcode** available to all users.

The S-Etukortti card can be used on mobile devices in a large part of S Group locations, but it is not yet possible to accrue cashback or utilise co-op member benefits in all ways in some business areas.

SECURITY FACTORS TO CONSIDER DURING PAYMENT DISRUPTIONS

IT IS ESSENTIAL TO REPORT ANY PROBLEMS WITH PAYMENT AS ACCURATELY AND QUICKLY AS POSSIBLE!

- Disruptions must be reported to Ässätuki, which can initiate communications about payment disruptions based on the information received.
- Ässätuki will inform the outlets about the scope of the disruption and its end by email and via S Group's internal communications channel.
- You'll receive more information about disruptions in card payment from the cash manager or the manager at your location.



INFORMATION SECURITY MANAGEMENT IN S GROUP

Information security management aims to ensure the confidentiality, accuracy and availability of S Group's data. An information security management system, which is based on the ISO/IEC 27001 standard, is in place to achieve the objectives for information security.

Employees play a critical role in ensuring information security, which is why it is important that everyone knows and follows the correct procedures.

It is important that employees familiarise themselves with the information security guidelines and the requirements of the PCI Passport each year.

SOK Risk Management informs about current information security issues and abuse trends, and promotes the employees' ability to identify phishing messages, for example.

|| **Every S Group employee is personally responsible for following the information security guidelines.**

PCI DSS STANDARD AND INFORMATION SECURITY

Securing the payment card data is a part of S Group's information security management. By following secure practices and instructions, S Group employees also participate in securing payment card information.

Through systematic management of information security, we ensure that the information security requirements of the PCI DSS are met. PCI DSS stands for Payment Card Industry Data Security Standard.

Employees are obliged to report any deficiencies in information security, threats or procedural errors to their immediate manager or to SOK Risk Management (riskienhallinta@sok.fi).

Employees who handle payment card data must report any anomalies or irregularities related to payment cards to their manager or the cash manager immediately.



14.27

5G

Credit

S PANKKI



VISA

.... 5105



Pidä lähellä lukijaa

Bonus

S-ETUOIKETTI

ISSUES TO BE CONSIDERED IN THE HOTEL BUSINESS, THE SALES SERVICE FOR THE TRAVEL AND HOSPITALITY BUSINESS, AND CUSTOMER SERVICE FOR ONLINE STORES

Never ask the customer to send payment card details by instant messaging, email or e-fax. Ask the customer to provide their card details securely using a payment link (Mama). The payment link will be sent to the customer from the outlet, sales service or online store customer service. This will also be done even if the customer had sent their card details on their own initiative by instant messaging, email or e-fax.

If a customer's message contains payment card details, these must be deleted before you reply to the message or forward it. You must also immediately delete the customer's message containing the card details, also from the folder for deleted messages.

If the customer cannot provide their card details via the payment link, the card details can exceptionally be received by telephone. If the customer reads out their card number during a phone call, please ensure that you do not repeat it. If calls are recorded, **any recorded call containing payment card details must be deleted immediately.**

In the hotel business, full card numbers are stored in the card number field in Opera for confirming arrival. **Payment card details cannot be saved in any other fields in Opera or in any other systems.** Charging the card number saved in the card number field in Opera must be carried out in Netaxept, if required. **The card number must not be copied from Opera to Netaxept.** Instead, the card number must be entered manually to ensure that no card details are saved in the workstation's cache. As the payment reform progresses, the need for Netaxept will be reduced or eliminated altogether.



A series of horizontal dotted lines spanning the width of the page, intended for writing or notes. The lines are evenly spaced and extend from the left margin to the right edge of the page.



A series of horizontal dotted lines for writing, spanning the width of the page. The lines are evenly spaced and extend from the left margin to the right edge of the page.



CONTENTS OF THIS GUIDE:

Ensuring secure card payments

Security considerations

Secure payment

Information security management in S Group

Security factors in the hotel business, the sales service for the travel and hospitality business, and customer service for online stores

© S Group

Confidential material for training purposes only.

