Payment Services

Secure processing of card payments in the hotel business

Guidelines from SIX Payment Services

Contents

Foreword

An ever-increasing number of people value the flexibility and independence associated with paying by card – on both sides of reception.

In order that the positives continue to outweigh the negatives we would like to familiarise you with the optimum and correct approach to using cashless payments, as well as provide you with useful tips. There are also a number of security measures to consider. Given that wherever there is success, the fraudsters are never far away: The level of fraudulent activity has increased significantly in recent years, especially in the hotel industry.

As a leading enterprise in the field of cashless payments, SIX Payment Services sees itself obligated to provide you with hands-on support regarding the efficient handling of payments by card as well as dealing with the topic of card data security.

Simple booking process

Step-by-step

SIX has developed a booking process specifically tailored to the requirements of the hotel industry, and offers (among other things) payment processing with tokens (substitute data). The procedures subsequently offer increased data security and additional, useful benefits. Please note that the function has to be activated on your terminal (ep2). If this is not yet the case, please get in touch with SIX.

Status	Using the payment terminal	Comments
Booking by telephone, post, email or an online portal. Cardholder and card are not present.	Reservation*	When placing a reservation a token PAN is generated with the token expiry date. This is listed on the receipt.**
Check-in: Cardholder and card are present.	Reservation*	Repeat the reservation process at the payment terminal and swipe the payment card. A new token PAN with a token expiry date is generated.
	Cancelling the reservation	Finally, cancel the first reservation at the payment terminal, in order that the amount is only reserved once on the card.
When extending the stay	Extending the reservation	
Check-out	Booking the reservation	The card does not necessarily have to be swiped, including for DCC payments. **Important:** The original reservation and any reservation extensions will subsequently be registered and automatically deleted following this process. Therefore, no reservation cancellation has to take place.

* Insofar as no prior online booking and associated charge to the card has taken place.
** The token PAN is a randomly generated, indecipherable 19-digit substitute number for the original card number. Only SIX will know to which original card number the token PAN belongs. A random expiry date is generated for every token PAN which, for security reasons does not correspond to that of the original payment card.

Benefits of the booking process with SIX

The payment card simply has to be swiped during check-in. It is no longer a mandatory requirement during check-out.

DCC payments (dynamic currency conversion) are also possible during check-out, without the need to re-swipe the card.

The card information is transferred and “tokenised” using the secure EFT standard (Electronic Fund Transfer), i.e. substituted with incomprehensible random data. Due to the fact that this information is not sensitive, complying with PCI DSS requirements is rendered significantly easier.

Tips

During check-in, swipe the card whenever possible using the chip or the magnetic strip. By doing so, you are transferring liability to the card-issuing bank in the event of any loss.

When your guests are checking out, offer them the opportunity to pay in the currency of their card (DCC). The guest must be given the opportunity to confirm his or her consent by pressing the confirm button on the payment terminal. Please ensure to alert the guest‘s attention to DCC using simple questions, e.g.: May we settle your bill directly in pounds sterling (card currency)?

Inform the guest that during the reservation process the booking amount was reserved on the card, meaning that the card limit was reduced by this amount (but the amount will not be charged).

Important information

Credits may only be allocated to the same card that was originally charged. Never allocate credits to other credit cards, debit cards or bank accounts.

Using the payment terminal

Quick guide

Reservation

1. Select booking type “Reservation”
2. Enter the amount to be reserved and authorised
3. Swipe the card at the terminal
4. Confirm the amount with PIN or signature
5. “Reservation” confirmation printed off

Extending the reservation

1. Under “Other transactions” select the booking type “Extend reservation”
2. Enter the amount by which the reservation should be extended
3. Enter the “Trx Ref. Number”

4.1 Card present: Scan the card at the terminal

4.2 Card not present: select “manual” and enter the token PAN as well as the token expiry date

5. Confirm the amount
6. The “Reservation extension” confirmation is printed out

Booking (reservation)

1. Select booking type “Booking reservation”
2. Enter final amount (differential amount is subsequently authorised automatically)
3. Select “Manual”
4. Enter the “Trx Ref. Number”
5. Card number is requested
   > Enter token PAN
6. Expiry date is requested
   > Enter token expiry date
7. CVC2/CVV2 is requested
   > Press the “OK” button
8. Check the final amount and select DCC for an international guest. He or she must confirm DCC by pressing the button. Now, no card has to be swiped.

No show

Same approach as “Booking reservation” with the following changes:

– The maximum chargeable amount is for one overnight stay
– “No show” must be noted down by hand on the signature line

Credits

1. Select the booking type “Credit”
2. Enter the password for the payment terminal and press “OK”
3. Enter the amount and press “OK”
4. Enter the date of the original transaction
5. Insert card and press “OK”
6. The “Credit” is printed out

Booking (additional charge)

1. Select booking type “Booking”
2. Enter the additional charge amount
3. Select “Manual”
4. Card number is requested
   > Enter token PAN
5. Expiry date is requested
   > Enter token expiry date
6. CVC2/CVV2 is requested > Press “OK”
7. Do not offer DCC, due to the fact that the cardholder cannot confirm by pressing the button
8. Write “Signature on file” on the signature line on the receipt

Cancelling a reservation

1. Select the booking type “Cancel res.” under the booking type “Other transactions”
2. Enter the “Trx Ref. Number”

3.1 Card present:
- – Swipe the card at the terminal
- – Reservation is cancelled

3.2 Card not present:
- – Select “Manual”
- – Card number is requested
  > Enter token PAN
- – Expiry date is requested
  > Enter token expiry date
- – CVC2/CVV2 is requested > Press “OK”

Receipt

Snow Mountain Hotel Resort
Crystal Peak
3920 Zermatt
Switzerland

1	Reservation	
	Visa	
2	9756 1348 0110 7483 611	
3	Expiry date	09.18
	12.05.2016	11:05:34
	Booking period	4
	Trm-Id:	12345678
	Act-Id:	5
	AID:	A0000000041010
4	Trx. Ref. Number:	123456789
	Trx. Seq.-No:	87974475
	Authorisation code:	121851
	EPF:	
5	49FAEB10EC70B4099C7B5C167E9E5FCC	
	Total-EFT	EUR 345.00
	Signature	
	SIX Payment Services	

1 Booking type
2 “Token card number”
3 “Token expiry date”
4 Transaction reference number
5 Total amount

Reservation guarantee by credit card

The correct approach

When registering a booking with a credit card (Visa, MasterCard, UnionPay, JCB, Diners Club Card or Discover Card) the first overnight stay can be guaranteed.

Reservation

Please request the following information from your guest when making the reservation:

– Last name, first name (as they appear on the card)
– Billing address
– Credit card number and expiry date
– Telephone number, postal address, email address
– Date of arrival and duration of stay

Please provide your guest with the following information (ideally in written form):

– Price of each overnight stay for the desired room category as well as total billing amount (including VAT)
– Exact hotel address
– Booking code (provided by the hotel)
– Hotel cancellation policy conditions, in particular the latest point in time for a free of charge cancellation
– Clarification that once the cancellation deadline has expired and/or should the cancellation conditions not be complied with, the cost of the overnight stay including all taxes will be charged to the card

Cancellation

In principle, you are obligated to accept all cancellations received by you before 18:00 local time on the day of the planned arrival. If this cancellation period is too short for you, you can extend this up to a maximum of 72 hours before the planned arrival of your guest. In such a case you must draw your guest's attention in writing to the special cancellation period. You must make explicit reference to the specific date and time of this cancellation period.

– Execute the "Reservation cancellation" process at the payment terminal
– You must inform the cardholder of the cancellation number (issued by the hotel)

No show

If the guest fails to appear and has also not cancelled his or her reservation within the allotted time, you may charge his or her credit card for the costs of an overnight stay including taxes, and print out the corresponding receipt.

– Execute a "Booking" with the corresponding amount
– In place of the cardholder's signature please write the comment "No show" on the signature line

Tip

Request a signed declaration of consent from your guest, on which he or she provides his or her consent to your conditions of cancellation as well as your General Terms and Conditions.

Important

If the cardholder disputes having made the hotel reservation themselves, you may under certain circumstances be unable to demand payment.

Reservation with an advance deposit paid by credit card

The correct approach

If you wish to request an advance deposit for a reservation, you can do so using the guest's credit card. There are two options here: Via the payment terminal or online. When using either option it is important to stick to the following steps exactly, in order to avoid any queries or return debits.

Reservation

Please request the following information from your guest when making the reservation:

- Last name, first name (as they appear on the card)
- Billing address
- Credit card number and expiry date
- Telephone number, postal address, email address
- Date of arrival and duration of stay

Please provide your guest with the following information (ideally in written form):

- Price per overnight stay for the desired room category as well as the total billing amount (incl. VAT)
- Exact hotel address
- Booking code (provided by the hotel)
- Hotel cancellation policy conditions, in particular the latest point in time for a free of charge cancellation
- Advance deposit amount, which you will charge to his or her credit card (this may not exceed the price for 14 nights). Please avoid stating the complete card number on the confirmation, and only provide a maximum of the last four digits.
- That the advance deposit is deducted from the final bill
- That the room for the period covered by the advance deposit is kept free for the guest
- That the advance deposit will, in whole or in part, be withheld after the cancellation period has expired and/or if the conditions of the cancellation policy are not complied with

Booking the "Advance deposit" at the payment terminal

- Execute a "Booking" at the payment terminal
- Write the words "Advance deposit" on the signature line on the receipt by hand
- You are obligated to send a written advance deposit confirmation and a copy of the booking receipt to the guest within three working days.
- The advance deposit confirmation printed out by you must contain the following information:
  - Hotel name
  - Name, billing address and telephone number of the cardholder
  - Scheduled date of arrival
  - Advance deposit
  - Date of the transaction
  - Booking code of the advance deposit (issued by the hotel)
  - The latest point in time for a cancellation
  - Agreed cancellation conditions
  - Statement of rights and obligations when paying an advance deposit via credit card

Tip

Request a signed declaration of consent from your guest, on which he or she provides his or her consent to your conditions of cancellation as well as your General Terms and Conditions.

Booking an advance deposit online

This option is available to you if you have access to the correct e-commerce package from SIX Payment Services. This allows you to either generate an offer through the application's back office using the advance deposit, which you can then send to the guest by email, or the guest can register a booking via your online shop.

In both cases, the guest is referred to the payment window where he or she can enter their card details. The guest is then requested to enter his or her password in the 3-D-SecureWindow – which allows you to ascertain that the guest has made the booking themselves. In the back office you can view and process the booking.

Cancelling at the payment terminal and online:

- Inform the cardholder of the cancellation code (issued by the hotel) and inform them that the code should be stored safely in the event of any possible queries
- Please ensure that you write the comment "Cancelled" and the cancellation code on the advance deposit confirmation
- Calculate the amount to be reimbursed
- Issue a credit at the payment terminal
- Ensure that you send the guest a copy of both receipts within three working days (advance deposit booking receipt and credit note for the cancellation) accompanied by a text explaining that a credit has been issued

Important

In principle, the guest has a right to the room or the room category booked by him or her. If the accommodation reserved by the guest is unavailable at the point in time of his or her arrival, you are obligated to credit the full advance deposit paid by the guest.

Transaction settlements using manually entered card information involve risks, which are to be borne by the hotel. In particular if it subsequently emerges that the card data has been fraudulently used and without the cardholder's consent. You can significantly reduce such risks by processing the advance deposit online.

Late charges

The correct approach

Should you discover at check-out that a number of additional costs have not been accounted for in the final bill, you may charge so-called late charges to the credit card.

Reservation/Check-in

In order to charge any late charges, you must have explained to the customer no later than at the point in time of check-in your General Terms and Conditions in connection with additional costs. We therefore recommend obtaining a signed declaration of consent from the guest (at best at the point in time the reservation is made) through which the guest declares their consent to your conditions of cancellation and your T&Cs.

After the guest's departure

- Execute a "Booking" at the payment terminal
- Note down "Signature on file" on the signature line
- If the booking and/or authorisation is rejected, please contact the cardholder and request another form of payment
- Please send the cardholder the following information:
  - Copy of the receipt with the comment "Signature on file" on the signature line
  - Copy of the bill(s) regarding the additional costs with a detailed breakdown

Important

Late charges for additional costs may only relate to the room, food and drink. The hotel bill may only be increased by a maximum of 15% as a result of these late charges.

If these additional costs exceed 15% or are the result of any loss, theft or damage to the hotel room, these may only be charged as late charges if you have contacted the guest after his or her departure, and have reached an agreement on the matter. Any consent to allowing these costs to be charged to the card must be presented in written form.

Effective card data privacy thanks to PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is a set of regulations governing electronic payment transactions, which regulates the secure processing of card transactions and to which absolute compliance is demanded by leading card organisations – Visa, Mastercard, JCB International, American Express and Discover Financial Services. This set of regulations is issued by and subject to further development under the Payment Card Industry Security Standards Council.

All businesses that store, transfer or process card data must fulfil the security requirements stipulated by these regulations. If the regulations are not complied with, the card organisations may ultimately prohibit the acceptance of such card payments.

This set of regulations is intended to protect you against the undesirable consequences of card data theft; the loss of any card data is associated with both financial loss and reputational damage.

This set of regulations consists of 12 sets of requirements and relates to your hotel's IT infrastructure, the the processes and your members of staff:

Requirement 1: Installation and maintenance of a firewall configuration to protect cardholder data

Requirement 2: Do not use any of the standard settings and security parameters offered by the provider for system passwords

Requirement 3: Protection of stored cardholder data

Requirement 4: Encryption during transfer of cardholder data via open, public networks

Requirement 5: Protection of all systems against malware and regular updating of antivirus software and programmes

Requirement 6: Development and maintenance of secure systems and applications

Requirement 7: Limitation of access to cardholder data depending on the business information requirement

Requirement 8: Identification and authentication of access to system components

Requirement 9: Limit physical access to cardholder data

Requirement 10: Tracking and monitoring of all access to network resources and cardholder data

Requirement 11: Regular testing of security systems and processes

Requirement 12: Maintain an information security guideline for all members of staff.

Compliance with the requirements is checked on the basis of three validation measures:

- Hotels with transactions exceeding 6 million transactions per year or contractual partners who have been the victim of card data theft, shall conduct an on-site audit. This must be implemented by a qualified auditor or a qualified certification body respectively (QSA – Qualified Security Assessor).
- Hotels with fewer than 6 million transactions per year can declare compliance with the guideline via a SAQ – Self Assessment Questionnaire. Depending on the form of card acceptance there are corresponding versions of this document SAQ.
- For those hotels whose infrastructure comes into contact with card data, there are so-called network scans. On a quarterly basis and in consultation with you an ASV (Approved Scanning Vendor) will conduct so-called friendly hacking attacks. The objective is to be able to identify weak links at an early stage.

Staying on the safe side

In terms of security, those solutions are deemed appropriate where your hotel has absolutely no involvement with the complete or unencrypted card data of your guests. This allows you to ensure that the amount of effort associated with the certification process is significantly reduced.

The following tips should support you in reducing the riskof card data theft and the effort involved in certification:

PCI Proxy Server

Reservation platforms are important distribution partners. Unfortunately, not everyone ensures secure conduct: Sensitive data is often transferred without encryption – by email or via XML interfaces.

If this is the case, the effort associated with fulfilling PCI DSS security requirements increases significantly. In order to avoid such additional effort, there is a simple and cost-effective alternative: the PCI Proxy Server. This collects the card data en route from the booking platform to you, and replaces it with incomprehensible random numbers (tokens). The associated sensitive card data is stored in a PCI DSS-certified environment. This ensures that you benefit from a more straightforward validation procedure, while allowing you to process bookings via the portals as normal.

Hotel Software – Property Management System (PMS)

Please check as to whether your hotel software is certified in accordance with the PA-DSS (Payment Application Data Security Standard). This subsequently ensures that the card data is stored in encrypted format in compliance with regulations. It is best to contact your PMS provider.

Outsourcing

If you are unable to omit the need to electronically store card data, please discuss the option of outsourcing together with your service provider. If card data storage is undertaken by the service provider, all PCI DSS-relevant requirements must be fulfilled. Request the corresponding verification (certificate). Protect yourself with the PCI certification of your partner and service provider.

SAQ Webportal

SIX Payment Services operates an SAQ Webportal (Self-Assessment-Questionnaire) in collaboration with a partner.

The portal will take you step-by-step through all the processes deemed necessary for PCI DSS certification. In the portal's document archive you can view and download all documents generated during the execution, such as the accreditation certificate, the self-assessment and, if relevant for the result, the network scan.

The portal is available free of charge to all SIX customers.

Should you have any technical or content-related questions, it is best that you contact the PCI Team at SIX directly: pci-support.ch@six-payment-services.com

Secure PayGate

If you have received reservations by telephone, fax, email or by post, your guests are able to pay in advance easily, conveniently and securely online, without the hotel having anything to do with the card data. The solution is called Secure PayGate.

Secure PayGate combines the benefits of the so-called Mail/Phone Order Transaction with the security of a password-protected secure e-commerce transaction. This means for you: increased security and convenient processing.

More information on Secure PayGate can be found at: **www.paymentforyou.com**

Tip

Offer your guests the option to pay with the 3-D-Secure Window.
This ensures that you, as a hotel, are certain that the guest has undertaken the booking themselves, which leads to a reversal of liability in your favour.

The hotel industry remains the focus of hackers as cyber criminality continues to grow. An investigation into such incidences has revealed that a significant proportion of attacks could have been avoided had there been appropriate security measures in place. The following tips from the international PCI DSS security standard are important for you if your infrastructure hosts card data (this check is also recommended irrespective of PCI DSS):

1. Change standard settings

PMS and POS systems are often configured by integrators using standard passwords. If a criminal gains access to such a password, he or she is granted easy access to your systems. Therefore, please never use the standard password provided by the supplier. Before the installation of an application, please set a new password with a high level of complexity: Please use capital letters and lower-case letters as well as numbers and special characters. The password must be at least eight characters long.

2. Securely set up your firewall

Configure the firewall in such a way that the in- and outflow of data is limited to those services, which are required for conducting business activity. Do not make your PMS and POS systems directly accessible via the Internet. Block any incoming data flow and filter any outgoing data flow. This measure significantly inhibits the activities of an attacker.

3. Network segmentation

Segment your network: Prevent any communication between the card processing systems and others by way of firewalls and routers. The objective is to prohibit direct access to the card processing systems, thereby minimising the risk of data being accessed. An unsegmented network also means that PCI DSS has to be applied across the entire network.

4. Set up multi-factor authentication

Establish a multi-factor authentication process for all remote access solutions, for internal members of staff and for service providers. Security with simply one password is mostly not enough to deter criminals. Combine the password with other methods of authentication: The use of PKI certificates (Public Key Infrastructure) or hardware tokens is well-established across many businesses today. Enquire with your solutions provider regarding possible extensions.

5. Check logs

Please ensure that the event protocols (logs) are generated, monitored and stored. Do not assume that criminals only act inconspicuously. Your activities are often registered via logs. Please check this regularly. This subsequently allows you to identify risks at an early stage and reduce them to a minimum.

6. Handling printouts and paper receipts

Please ensure that any printouts, faxes and receipts containing card data are kept securely under lock and key – in drawers or cupboards. Members of staff must be sensitised to the use of such confidential data, and it must be defined and checked as to which members of staff require access to such documentation due to their work. The proper disposal of documentation must also be safeguarded.

7. Service providers

Please contact your service provider who transfers, processes or stores card data on your behalf, and request the submission of a PCI-Compliance verification. Co-responsibility should be regulated. Maintain a list of your suppliers, in order that you can retain an overview.

Questions

Do you have any questions regarding the topic of security? Your PMS provider and the PCI Team from SIX are happy to help.

Payment Services

Declaration of consent
Credit card authorisation (template)

By way of a declaration of consent the guest is providing his or her consent to any authorised bookings without physically presenting the card. You will find a corresponding template below.

Your hotel name / your hotel logo:

This form must be kept in a secure environment.

Kreditkarten-Autorisierung / Prise en charge / Credit Card Authorization

Karteninhaber / Nom du détenteur de la carte / Credit Card Holder _____ Zimmer / Chambre / Room _____

☐ Zahlung / Payment
oder / ou / or
☐ Garantie / Guarantee

Kartentyp / Type ☐ Visa ☐ Mastercard ☐ American Express ☐ Diners ☐ JCB ☐ UnionPay

Nummer / Numéro / Number _____ Verfallsdatum / Expiration _____

Für folgende Services / Pour les services suivants / For the following charges

Zimmer und Taxen / Chambres et Taxes / Room and Tax ☐
Express Check-Out ☐
Frühstück / Petit-déjeuner / Breakfast ☐
Übrige Gebühren / Autres charges / All incidentals ☐
Payment in the card's currency (DCC - Dynamic Currency Conversion)* ☐

* With DCC your payment is made in the card's currency – instead of in the local currency of the above-stated hotel. By marking the service with a cross you are authorising the above-stated hotel to charge the payments listed in this document in the card's currency. You are aware of the fact that both the final amount to be settled as well as the applicable exchange rate at the point in time of signing this declaration of consent are not yet known.

Für folgende Gäste / Pour les hôtes suivants / For the following guests

Name / Nom / Name _____ Zimmer / Chambre / Room _____
Name / Nom / Name _____ Zimmer / Chambre / Room _____
Name / Nom / Name _____ Zimmer / Chambre / Room _____

Hiermit bestätige ich, dass nebst meiner Zimmerrechnung auch die auf diesem Formular markierten Zusatzkosten sowie die Zimmerrechnung für die anderen aufgeführten Gäste gemäss den allgemein gültigen Geschäftsbedingungen des Hauses zu Lasten meiner oben erwähnten Kreditkarte abgebucht werden dürfen.

Par la présente je confirme qu'en plus de la facture pour ma chambre, vous pouvez également déduire les coûts supplémentaires ainsi que les frais des chambres de nos invités figurant sur les documents joints. Selon les conditions générales nous vous autorisons à débiter ma carte de crédit mentionnée.

I hereby confirm that, excepting my room costs, the additional costs marked above and room costs for the other guests listed on this document can be charged to my above mentioned creditcard in accordance to the general business terms and conditions.

_____ _____
Ort, Datum / Lieu, date / Place, date Vorname, Name / Nom, prénom / Forename, last name

_____
Unterschrift / Signature

SIX Payment Services Ltd
Hardturmstrasse 201
P.O. Box
CH-8021 Zurich

Data protection agreement (sample)

Below you will find a non-binding example of a possible data protection agreement. For a legally binding version, please contact a lawyer of your choice.

On the basis of contractual and statutory confidentiality obligations, the undersigned is required to maintain confidentiality about the facts/information which he or she has attained or become aware of by working at *Hotel Musterhof;* facts/information, that is, which are not generally known, where an interest in its confidentiality is worthy of protection and about which maintaining confidentiality is expressly or tacitly the will of *Hotel Musterhof.*

– Any information relating to the subject, contents and function of the technical or software-supported resources and equipment of *Hotel Musterhof* as well as relating to the organization and processing of all types of business at the *Hotel Musterhof* is covered by the obligation of professional secrecy.
– All personal customer data, including credit or debit card data, are to be especially protected.

Contravening the confidentiality obligation can represent individually or cumulatively a breach of the obligation of professional secrecy or the law on data protection. The corresponding legal provision is reproduced in the appendix to this declaration of confidentiality.

The undersigned commits to treat in strict confidentiality facts/information of which he or she has become aware that are relevant to confidentiality and to use them for no other purpose than for the task for which they were entrusted to him or her.

Place and date

Name of the person signing

Signature

1100116 CHE_EN/01.2018

We would be happy to advise you on all aspects of your tailor-made solution for cashless payment.

Find your local point of contact at: www.six-payment-services.com/contact

SIX Payment Services Ltd
Hardturmstrasse 201
P.O. Box
CH-8021 Zurich

SIX Payment Services (Europe) S.A.
10, rue Gabriel Lippmann
5365 Munsbach
Luxembourg

SIX Payment Services (Austria) GmbH
Marxergasse 1B
AT-1030 Vienna
Austria

SIX Payment Services (Europe) S.A
Branch Office Germany
Theodor-Heuss-Allee 108
D-60486 Frankfurt on the Main