Payment Services

Die sichere Abwicklung von Kartenzahlungen in der Hotellerie

Ein Leitfaden von SIX Payment Services

Inhalt

Vorwort

Immer mehr Menschen schätzen die Flexibilität und die Unabhängigkeit beim Bezahlen mit Karte – hinter und vor der Rezeption.

Damit die Vorteile weiterhin überwiegen, möchten wir Ihnen die beste, korrekte Vorgehensweise beim bargeldlosen Bezahlen aufzeigen sowie hilfreiche Hinweise mitgeben. Ausserdem gilt es einige Sicherheitsmassnahmen zu beachten. Denn wo Erfolg ist, sind auch Betrüger nicht fern: Besonders in der Hotellerie haben sich in den letzten Jahren betrügerische Vorfälle gehäuft.

Als führendes Unternehmen im Bereich des bargeldlosen Bezahlens sieht sich SIX Payment Services verpflichtet, Sie bei der effizienten Handhabung von Kartenzahlungen sowie dem Thema Kartendatensicherheit tatkräftig zu unterstützen.

Einfacher Buchungsprozess

Schritt für Schritt

SIX hat einen Buchungsprozess speziell für die Anforderungen in der Hotellerie entwickelt und bietet unter anderem die Zahlungsabwicklung mit Token (Ersatzdaten) an. So sind die Abläufe mit erhöhter Datensicherheit und weiteren nützlichen Vorteilen verbunden. Bitte beachten Sie, dass die Funktion auf Ihrem Terminal (ep2) aktiviert sein muss. Falls dies noch nicht der Fall ist, erkundigen Sie sich bitte bei SIX.

Status	Vorgehen am Zahlterminal	Bemerkungen
Buchung per Telefon, Post, E-Mail oder Onlineportal. Karteninhaber und Zahlkarte sind nicht vor Ort.	Reservation*	Bei der Reservation wird eine Token PAN mit Token Verfalldatum generiert. Diese sind auf dem Beleg vermerkt.**
Check-in: Karteninhaber und Zahlkarte sind vor Ort.	Reservation*	Tätigen Sie erneut eine Reservation am Zahlterminal und lesen Sie die Zahlkarte ein. Dabei wird ein neuer Token PAN mit Token Verfalldatum generiert.
	Annullierung Reservation	Annullieren Sie anschliessend die erste Reservation am Zahlterminal, damit der Betrag nur einmal auf der Karte reserviert ist.
Bei Verlängerung des Aufenthalts	Reservationserhöhung	
Check-out	Buchung Reservation	Die Zahlkarte muss nicht zwingend eingelesen werden, auch nicht für DCC-Zahlungen. **Wichtig:** Nach diesem Prozess werden die ursprüngliche Reservation und allfällige Reservationserhöhungen verbucht und automatisch gelöscht. Es muss also keine Annullierung der Reservation vorgenommen werden.

* sofern keine Online-Buchung mit bereits durchgeführter Belastung der Karte vorliegt.

** Die Token PAN ist eine zufällig generierte, nicht nachvollziehbare 19-stellige Ersatznummer für die Original-Kartennummer. Zu welcher Original-Kartennummer die Token PAN gehört, kann ausschliesslich SIX nachvollziehen. Zu jeder Token PAN wird ein zufälliges Verfalldatum generiert, das aus Sicherheitsgründen nicht demjenigen auf der Original-Zahlkarte entspricht.

Vorteile des Buchungsprozesses bei SIX

Die Zahlkarte muss nur noch beim Check-in eingelesen werden. Sie wird beim Check-out nicht mehr zwingend benötigt.

Auch DCC (Dynamische Währungsumrechnung) ist beim Check-out möglich, ohne die Karte nochmals einzulesen.

Die Kartendaten werden mit dem sicheren EMV-Standard übermittelt und «tokenisiert», das heisst durch nicht nachvollziehbare Zufallsdaten ersetzt. Da diese Informationen nicht sensibel sind, wird das Erfüllen der PCI DSS-Anforderungen erheblich vereinfacht.

Tipps

Lesen Sie die Zahlkarte beim Check-in wenn möglich mit dem Chip oder dem Magnetstreifen ein. Sie treten dadurch im Schadenfall die Haftung an die kartenherausgebende Bank ab.

Bieten Sie Ihren Gästen mit DCC beim Check-out an, in der Kartenwährung zu bezahlen. Der Gast muss die Möglichkeit haben, sein Einverständnis durch Tastendruck am Zahlterminal zu bestätigen. Machen Sie den Gast mit einfachen Fragen auf DCC aufmerksam, zum Beispiel: Dürfen wir direkt in Pfund (Kartenwährung) abrechnen?

Informieren Sie Ihren Gast darüber, dass bei der Reservation der Betrag der Buchung auf seiner Kreditkarte reserviert wurde und dass die Kartenlimite um diesen Betrag reduziert wird (der Betrag wird aber nicht belastet).

Wichtige Hinweise

Gutschriften dürfen nur auf dieselbe Kreditkarte ausgestellt werden, die ursprünglich belastet wurde. Nehmen Sie eine Gutschrift keinesfalls auf andere Kredit-, Debitkarten oder Bankkonten vor.

Vorgehen am Terminal

Quick Guide

Reservation

1. Buchungsart «Reservation» wählen
2. Betrag eingeben, der reserviert und autorisiert werden soll
3. Karte am Terminal einlesen
4. Betrag mit PIN oder Unterschrift bestätigen
5. Beleg «Reservation» wird gedruckt

Reservationserhöhung

1. Unter «Andere Transaktionen» die Buchungsart «Erhöhung Reservation» aufrufen
2. Betrag eingeben, um den die Reservation erhöht werden soll
3. «Trx Ref. Nummer» eingeben

4.1 Karte vor Ort: Karte am Terminal einlesen

4.2 Karte nicht vor Ort: «manuell» wählen und Token PAN sowie Token Verfalldatum eingeben

5. Betrag bestätigen
6. Beleg «Reservationserhöhung» wird gedruckt

Buchung (Reservation)

1. Buchungsart «Buchung Reservation» wählen
2. Endbetrag eingeben (Differenzbetrag wird automatisch nachautorisiert)
3. «manuell» wählen
4. «Trx Ref. Nummer» eingeben
5. Kartennummer wird gefragt
   > Token PAN eingeben
6. Verfallsdatum wird gefragt
   > Token Verfalldatum eingeben
7. CVC2/CVV2 wird gefragt
   > Taste «OK» drücken
8. Endbetrag kontrollieren und bei einem ausländischen Gast DCC wählen. Er muss DCC mittels Tastendruck bestätigen. Es muss jetzt keine Karte eingelesen werden.

No show

Vorgehen analog Prozess «Buchung Reservation» mit folgenden Änderungen:

– abgebucht werden darf maximal der Betrag für eine Übernachtung
– «no show» handschriftlich in die Unterschriftenzeile des Belegs notieren

Gutschrift

1. Buchungsart «Gutschrift» wählen
2. Passwort für das Zahlterminal eingeben und «OK» drücken
3. Betrag eingeben und «OK» drücken
4. Datum der ursprünglichen Transaktion eingeben
5. Karte einführen und «OK» drücken
6. Beleg «Gutschrift» wird gedruckt

Buchung (Nachbelastung)

1. Buchungsart «Buchung» wählen
2. Betrag der Nachbelastung eingeben
3. «manuell» wählen
4. Kartennummer wird abgefragt
   > Token PAN eingeben
5. Verfalldatum wird abgefragt
   > Token Verfalldatum eingeben
6. CVC2/CVV2 wird abgefragt > «OK» drücken
7. DCC nicht anbieten, da der Karteninhaber nicht per Tastendruck bestätigen kann
8. Schreiben Sie «Signature on File» in die Unterschriftenzeile auf den Beleg

Annulierung Reservation

1. Unter «Andere Transaktionen» die Buchungsart «Annullierung Res.» wählen
2. «Trx Ref. Nummer» eingeben

3.1 Karte vor Ort:
– Karte am Terminal einlesen
– Reservation wird annulliert

3.2 Karte nicht vor Ort:
– «manuell» wählen
– Kartennummer wird erfragt
  > Token PAN eingeben
– Verfalldatum wird erfragt
  > Token Verfalldatum eingeben
– CVC2/CVV2 wird erfragt > «OK» drücken

Beleg

Snow Mountain Hotel Resort
Crystal Peak
3920 Zermatt
Switzerland

1	Reservation	
	Visa	
2	9756 1348 0110 7483 611	
3	Verfallsdatum	09.18
	12.05.2016	11:05:34
	Buchungsperiode	4
	Trm-Id:	12345678
	Act-Id:	5
	AID:	A0000000041010
4	Trx. Ref. Nummer:	123456789
	Trx. Seq.-Nr:	87974475
	Autorisationscode:	121851
	EPF:	
5	49FAEB10EC70B4099C7B5C167E9E5FCC	
	Total-EFT	EUR 345.00
	Unterschrift	
	SIX Payment Services	

1 Buchungsart
2 «Token Kartennummer»
3 «Token Verfallsdatum»
4 Referenznummer der Transaktion
5 Totalbetrag

Reservationsgarantie per Kreditkarte

So gehen Sie richtig vor

Bei einer Buchung mit Kreditkarte (Visa, Mastercard, UnionPay, JCB, Diners Club Card oder Discover Card) kann die erste Übernachtung garantiert werden.

Reservation

Verlangen Sie von Ihrem Gast bei der Reservation folgende Informationen:

- Name,Vorname (wie auf der Karte angegeben)
- Rechnungsadresse
- Kreditkartennummer und Verfalldatum
- Telefonnummer, Postadresse, E-Mail-Adresse
- Ankunftsdatum und Aufenthaltsdauer

Geben Sie Ihrem Gast folgende Informationen, am besten schriftlich:

- Preis pro Übernachtung für die gewünschte Zimmerkategorie sowie Rechnungstotal (inkl. MwSt)
- Genaue Hoteladresse
- Buchungscode (vom Hotel vergeben)
- Annullierungsbedingungen Ihres Hotels, insbesondere der letztmögliche Zeitpunkt für eine kostenlose Annullierung
- dass ihm nach Ablauf der Annullierungsfrist, bzw. wenn die Annullierungsbedingungen nicht eingehalten werden, eine Übernachtung inkl. Taxen belastet wird

Annullierung

Sie sind grundsätzlich verpflichtet, alle Annullierungen anzunehmen, die bis 18.00 Uhr Ortszeit des geplanten Ankunftstages bei Ihnen eintreffen. Falls Ihnen dieser Annullierungszeitraum nicht genügt, können Sie diesen auf maximal 72 Stunden vor das geplante Eintreffen des Gastes verlegen. In diesem Fall müssen Sie Ihren Gast schriftlich auf den besonderen Annullierungstermin aufmerksam machen. Weisen Sie ausdrücklich auf das konkrete Datum und die Uhrzeit dieses Termins hin.

- Führen Sie am Zahlterminal eine «Annullierung Reservation» aus
- Sie müssen dem Karteninhaber die Annullierungsnummer (vom Hotel ausgestellt) bekannt geben

No show

Erscheint der Gast nicht und hat er die Reservation auch nicht rechtzeitig annulliert, können Sie seiner Kreditkarte die Kosten für eine Übernachtung inkl. Taxen belasten und einen entsprechenden Beleg ausstellen.

- Führen Sie eine «Buchung» über den entsprechenden Betrag aus
- Anstelle der Unterschrift des Karteninhabers tragen Sie handschriftlich den Vermerk «No show» in die Unterschriftenzeile ein

Tipp

Verlangen Sie von Ihrem Gast eine unterschriebene Einwilligungserklärung, in der er Ihren Annullierungsbedingungen und AGB zustimmt.

Wichtig

Sollte der Karteninhaber bestreiten, die Hotelreservation selbst getätigt zu haben, steht Ihnen unter Umständen kein Vergütungsanspruch zu.

Reservation mit Anzahlung per Kreditkarte (Advance Deposit)

So gehen Sie richtig vor

Möchten Sie für eine Reservation eine Anzahlung verlangen, können Sie das über die Kreditkarte des Gastes tun. Es gibt dafür zwei Möglichkeiten: Am Zahlterminal oder online. Bei beiden Optionen ist es wichtig, dass Sie die folgenden Schritte genau befolgen, damit sich Rückfragen oder gar Rückbuchungen vermeiden lassen.

Reservation

Verlangen Sie von Ihrem Gast bei der Reservation folgende Informationen:

- Name,Vorname (wie auf der Karte angegeben)
- Rechnungsadresse
- Kreditkartennummer und Verfalldatum
- Telefonnummer, Postadresse, E-Mail-Adresse
- Ankunftsdatum und Aufenthaltsdauer

Geben Sie Ihrem Gast folgende Informationen, am besten schriftlich:

- Preis pro Übernachtung für die gewünschte Zimmerkategorie sowie Rechnungstotal (inkl. MwSt)
- Genaue Hoteladresse
- Buchungscode (vom Hotel vergeben)
- Annullierungsbedingungen Ihres Hotels, insbesondere der letztmögliche Zeitpunkt für eine kostenlose Annullierung
- Betrag der Anzahlung, den Sie seiner Kreditkarte belasten werden (darf den Preis für 14 Nächte nicht übersteigen). Verzichten Sie in der Bestätigung auf die Angabe der vollständigen Kreditkartennummer und geben Sie maximal die letzten vier Ziffern an.
- dass die Anzahlung von der Schlussrechnung abgezogen wird
- dass die Unterkunft für den Zeitraum, der von der Anzahlung gedeckt ist, für ihn freigehalten wird
- dass die Anzahlung nach Ablauf der Annullierungsfrist, bzw. wenn die Annullierungsbedingungen nicht eingehalten werden, ganz oder teilweise verfällt

Anzahlung am Zahlterminal buchen

- Nehmen Sie am Zahlterminal eine «Buchung» vor
- Auf dem Beleg schreiben Sie von Hand «Advance Deposit» in die Unterschriftenzeile
- Sie sind verpflichtet, dem Gast innerhalb von drei Arbeitstagen eine schriftliche Anzahlungsbestätigung sowie eine Kopie des Buchungsbelegs zukommen zu lassen.
- Die von Ihnen ausgestellte Anzahlungsbestätigung muss folgende Angaben enthalten:
  - Hotelname
  - Name, Rechnungsadresse und Telefonnummer des Karteninhabers
  - voraussichtliches Ankunftsdatum
  - Anzahlungsbetrag
  - Datum der Transaktion
  - Buchungscode der Anzahlung (vom Hotel vergeben)
  - spätester Zeitpunkt für eine Annullierung
  - vereinbarte Annullierungsbedingungen
  - Angaben zu Rechten und Pflichten bei Anzahlungen über Kreditkarten

Tipp

Verlangen Sie von Ihrem Gast eine unterschriebene Einwilligungserklärung, in der er Ihren Annullierungsbedingungen und AGB zustimmt.

Anzahlung online buchen

Diese Möglichkeit steht Ihnen offen, wenn Sie ein passendes E-Commerce-Paket von SIX Payment Services besitzen. Dabei können Sie entweder ein Angebot über den Anzahlungsbetrag im Backoffice der Applikation erstellen, das Sie dem Gast per E-Mail zustellen, oder der Gast bucht über Ihren Online-Shop.

In beiden Fällen wird Ihr Gast auf das Zahlfenster verwiesen, indem er seine Kartendaten eingeben kann. Im Anschluss wird der Gast aufgefordert, im 3-D-Secure-Fenster sein Passwort einzugeben – so können Sie sicher stellen, dass der Gast die Buchung persönlich vorgenommen hat. Im Backoffice können Sie die getätigte Buchung einsehen und bearbeiten.

Annullierung am Zahlterminal und online:

- Teilen Sie dem Karteninhaber den Annullierungscode mit (vom Hotel vergeben) und weisen Sie darauf hin, dass der Code für mögliche Rückfragen aufbewahrt werden sollte
- Versehen Sie die Anzahlungsbestätigung mit dem Vermerk «cancelled» und dem Annullierungscode
- Berechnen Sie den zu erstattenden Betrag
- Führen Sie eine Gutschrift am Zahlterminal durch
- Senden Sie dem Gast innerhalb von drei Arbeitstagen eine Kopie beider Belege (Buchungsbeleg Advance Deposit und Gutschriftenbeleg der Annullation) begleitet von einem Text, der erklärt, dass eine Gutschrift vorgenommen wurde

Wichtig

Grundsätzlich hat der Gast Anrecht auf das von ihm gebuchte Zimmer oder die Zimmerkategorie. Ist die vom Gast reservierte Unterkunft bei seiner Ankunft nicht verfügbar, sind Sie verpflichtet, ihm die gesamte geleistete Anzahlung gutzuschreiben.

Transaktionsabwicklungen mittels manueller Kartendatenerfassung sind mit Risiken belastet, die das Hotel zu tragen hat. Insbesondere dann, wenn sich nachträglich herausstellen sollte, dass die Kartendaten missbräuchlich ohne Einverständnis des Karteninhabers verwendet wurden. Die Risiken können Sie massgeblich vermindern, indem Sie die Anzahlung online abwickeln.

Nachträgliche Abbuchungen (Late Charges)

So gehen Sie richtig vor

Stellen Sie nach dem Check-out fest, dass in der Endabrechnung nicht berücksichtigte Kosten entstanden sind, so können Sie die Kreditkarte nachträglich belasten.

Reservation/Check-in

Um nachträglich Abbuchungen zu tätigen, müssen Sie dem Kunden spätestens beim Check-in die Allgemeinen Geschäftsbedingungen im Zusammenhang mit Zusatzkosten erläutern. Wir empfehlen Ihnen deshalb, den Gast am besten bereits bei der Reservation eine Einwilligungserklärung unterzeichnen zu lassen, in der er Ihren die Annullierungsbedingungen und AGB zustimmt.

Nach der Abreise

- Nehmen Sie am Zahlterminal eine «Buchung» vor
- Vermerken Sie «Signature on File» in der Unterschriftenzeile
- Wird die Buchung bzw. die Autorisation abgelehnt, kontaktieren Sie den Karteninhaber und fragen Sie nach einem anderen Zahlungsmittel
- Senden Sie dem Karteninhaber folgende Informationen:
  - Kopie des Belegs mit Vermerk «Signature on File» in der Unterschriftenzeile
  - Kopie der Rechnung(en) über die Zusatzkosten mit detaillierter Aufschlüsselung

Wichtig

Nachgebuchte Zusatzkosten dürfen sich nur auf Zimmer, Essen oder Getränke beziehen. Die Hotelrechnung darf sich durch diese Nachbuchung um maximal 15% erhöhen.

Belaufen sich die Zusatzkosten auf mehr als 15% oder fallen Kosten aufgrund von Verlust, Diebstahl oder Beschädigungen im Hotelzimmer an, dürfen diese nur dann nachgebucht werden, wenn Sie den Gast nach seiner Abreise nochmals kontaktiert und sich mit ihm geeinigt haben. Die Einwilligung, dass diese Kosten der Karte belastet werden dürfen, muss in schriftlicher Form vorliegen.

Wirksamer Kartendatenschutz dank PCI DSS

Der Payment Card Industry Data Security Standard (PCI DSS) ist ein Regelwerk im elektronischen Zahlungsverkehr, das sich auf die sichere Abwicklung von Kartentransaktionen bezieht und dessen Einhaltung von den führenden Kartenorganisationen – Visa, Mastercard, JCB International, American Express und Discover Financial Services – zwingend verlangt wird. Herausgegeben und weiterentwickelt wird das Regelwerk vom Payment Card Industry Security Standards Council.

Alle Unternehmen, die Kartendaten speichern, übermitteln oder verarbeiten, müssen die Sicherheitsrichtlinien dieses Regelwerks erfüllen. Werden die Anforderungen nicht eingehalten, können die Kartenorganisationen in letzter Konsequenz die Akzeptanz von Kartenzahlungen untersagen.

Das Regelwerk hat den Zweck, Sie vor den unangenehmen Folgen eines Kartendatendiebstahls zu schützen; mit einem Kartendatenverlust gehen neben finanziellen Verlusten auch Reputationsschäden einher.

Dieses Regelwerk besteht aus zwölf Anforderungsgruppen und bezieht sich auf die IT-Infrastruktur, die Prozesse sowie die Mitarbeiter Ihres Hotels:

Anforderung 1: Installation und Pflege einer Firewall-Konfiguration zum Schutz von Karteninhaberdaten

Anforderung 2: Keine vom Anbieter gelieferten Standardeinstellungen für Systemkennwörter und andere Sicherheitsparameter verwenden

Anforderung 3: Schutz gespeicherter Karteninhaberdaten

Anforderung 4: Verschlüsselung bei der Übertragung von Karteninhaberdaten über offene, öffentliche Netze

Anforderung 5: Schutz sämtlicher Systeme vor Malware und regelmässige Aktualisierung von Antivirensoftware und Programmen

Anforderung 6: Entwicklung und Wartung sicherer Systeme und Anwendungen

Anforderung 7: Beschränkung des Zugriffs auf Karteninhaberdaten je nach Geschäftsinformationsbedarf

Anforderung 8: Identifizierung und Authentifizierung des Zugriffs auf Systemkomponenten

Anforderung 9: Physischen Zugriff auf Karteninhaberdaten beschränken

Anforderung 10: Verfolgung und Überwachung des gesamten Zugriffs auf Netzwerkressourcen und Karteninhaberdaten

Anforderung 11: Regelmässiges Testen der Sicherheitssysteme und -prozesse

Anforderung 12: Pflegen einer Informationssicherheitsrichtlinie für das gesamte Personal.

Die Einhaltung der Anforderungen wird anhand von drei Validierungsmassnahmen überprüft:

- Hotels mit mehr als 6 Mio. Transaktionen pro Jahr oder Vertragspartner, die Opfer eines Kartendatendiebstahls wurden, führen einen On-Site Audit durch. Dieser muss durch einen ausgebildeten Auditor durchgeführt werden, respektive durch ein akkreditiertes Zertifizierungsunternehmen (QSA – Qualified Security Assessor).
- Hotels mit weniger als 6 Mio. Transaktionen pro Jahr können die Einhaltung der Richtlinien mittels eines Selbstbeurteilungsfragebogens (SAQ – Self-Assessment Questionnaire) deklarieren. Je nach Form der Kartenakzeptanz gibt es korrespondierende Versionen dieses Dokuments SAQ.
- Für Hotels, deren Infrastruktur mit Kartendaten in Berührung kommt, gibt es zudem die sogenannten Network-Scans. Vierteljährlich und nach Absprache mit Ihnen führt ein ASV (Approved Scanning Vendor) freundliche Hacking-Angriffe durch. Ziel davon ist, dass Schwachstellen rechtzeitig ermittelt werden können.

Auf der sicheren Seite

In Bezug auf die Sicherheit sind Lösungen erstrebenswert, bei denen Ihr Hotel gar nicht erst mit vollständigen und unverschlüsselten Kartendaten in Berührung kommt. Damit können Sie dies sicherstellen, dass sich der Zertifizierungsaufwand erheblich reduziert.

Folgende Tipps unterstützen Sie dabei, das Risiko eines Kartendatendiebstahls und den Aufwand der Zertifizierung zu reduzieren:

PCI Proxy Server

Reservationsplattformen sind wichtige Distributionspartner. Leider verhalten sich jedoch nicht alle immer sicher: Sensible Daten werden oft unverschlüsselt übermittelt – per E-Mail oder über XML-Schnittstellen.

Ist dies der Fall, erhöht sich der Aufwand, die PCI DSS Sicherheitsbestimmungen zu erfüllen, erheblich. Um diesen zusätzlichen Aufwand zu vermeiden, gibt es eine einfache und kostengünstige Alternative: den PCI Proxy Server. Dieser fängt Kartendaten auf dem Weg von der Buchungsplattform zu Ihnen ab und ersetzt sie mit einer nicht nachvollziehbaren Zufallsnummer (Token). Die dazugehörigen sensiblen Kartendaten werden in einer nach PCI DSS zertifizierten Umgebung gespeichert. Dadurch profitieren Sie von einer einfacheren Validierung und können dennoch ganz normal Buchungen über Portale abwickeln.

Hotel Software – Property Management System (PMS)

Überprüfen Sie, ob Ihre Hotelsoftware nach PA-DSS (Payment Application Data Security Standard) zertifiziert ist. Damit stellen Sie sicher, dass die Kartendaten den Vorgaben entsprechend verschlüsselt abgespeichert sind. Kontaktieren Sie am besten Ihren PMS-Anbieter.

Outsourcing

Falls Sie auf die elektronische Speicherung von Kartendaten nicht verzichten können, klären Sie mit Ihrem Dienstleister die Möglichkeit eines Outsourcings ab. Wird die Kartendatenspeicherung durch den Dienstleister übernommen, muss er alle PCI DSS-relevanten Anforderungen erfüllen. Verlangen Sie den entsprechenden Nachweis (Zertifikat). Sichern Sie sich bezüglich PCI-Zertifizierung Ihres Partners und Dienstleistungserbringers ab.

SAQ Webportal

SIX Payment Services betreibt in Kooperation mit einem Partner ein SAQ-Webportal (Self-Assessment-Questionnaire).

Das Portal führt Sie schrittweise durch alle für die PCI DSS-Zertifizierung notwendigen Prozesse. Im Dokumentenarchiv des Portals können Sie im Anschluss alle bei der Durchführung angefallenen Dokumente, wie die Zertifizierungsbescheinigung, das Self-Assessment und falls für Sie relevant die Ergebnisse der Netzwerk-Scans, einsehen und herunterladen.

Das Portal steht allen SIX-Kunden kostenlos zur Verfügung.

Bei technischen oder inhaltlichen Fragen, wenden Sie sich am besten direkt an das PCI Team von SIX:
pci-support.ch@six-payment-services.com

Secure PayGate

Falls Sie Reservationen via Telefon, Fax, E-Mail oder Post entgegennehmen, können Ihre Gäste im Voraus schnell, bequem und sicher online bezahlen, ohne dass Ihr Hotel mit Kartendaten in Berührung kommt. Die Lösung heisst Secure PayGate.

Secure PayGate verbindet die Vorteile der sogenannten Mail-/Phone-Order-Transaktion mit der Sicherheit einer passwortgeschützten Secure E-Commerce Transaktion. Das bedeutet für Sie: mehr Sicherheit und bequeme Abwicklung.

Weitere Informationen zu Secure PayGate finden Sie unter:
www.paymentforyou.com

Tipp

Bieten Sie Ihren Gästen die Bezahlung mit dem 3-D-Secure-Verfahren an. Damit sind Sie als Hotel sicher, dass der Gast die Buchung selbst vorgenommen hat und es erfolgt die Haftungsumkehr zu Ihren Gunsten.

Durch das stetige Wachstum der Cyberkriminalität steht auch die Hotellerie weiter im Fokus der Angreifer. Die Untersuchung der Vorfälle hat ergeben, dass ein Grossteil der Angriffe mit den richtigen Sicherheitsmechanismen hätte vereitelt werden können. Folgende Tipps aus dem internationalen Sicherheitsstandard PCI DSS sind für Sie wichtig, wenn sich Kartendaten auf Ihrer Infrastruktur befinden (die Überprüfung empfiehlt sich allerdings auch unabhängig von PCI DSS):

1. Standardeinstellungen ändern

PMS- und POS-Systeme werden von Integratoren oft mit Standard-Passwörtern konfiguriert. Kommt ein Krimineller an ein solches Passwort, kann er sich vereinfacht Zugang zu Ihren Systemen verschaffen. Nutzen Sie deshalb niemals das vom Anbieter gelieferte Standard-Passwort. Definieren Sie vor der Installation einer Anwendung ein neues Passwort mit hoher Komplexität: Verwenden Sie Gross- und Kleinschreibung sowie Zahlen und Sonderzeichen. Das Passwort sollte mindestens acht Zeichen lang sein.

2. Firewall sicher einstellen

Konfigurieren Sie die Firewall so, dass der ein- und ausgehende Datenverkehr auf jene Dienste beschränkt ist, die für die Geschäftsausübung erforderlich sind. Machen Sie Ihre PMS- und POS-Systeme nicht direkt über das Internet zugänglich. Blockieren Sie den eingehenden Datenverkehr und filtern Sie den ausgehenden. Diese Massnahme schränkt die Aktivitäten eines Angreifers massiv ein.

3. Netzwerksegmentierung

Segmentieren Sie Ihr Netzwerk: Unterbinden Sie die Kommunikation zwischen den kartenverarbeitenden Systemen und anderen durch Firewalls und Router. Ziel ist es, den direkten Zugriff auf die kartenverarbeitenden Systeme zu verbieten und dadurch das Risiko eines Datenabgriffs zu minimieren. Ein unsegmentiertes Netzwerk bedeutet zudem, dass PCI DSS auf das gesamte Netzwerk angewendet werden muss.

4. Multi-Faktor-Authentifizierung einrichten

Richten Sie für alle Remote-Access-Lösungen eine Multi-Faktor-Authentifizierung ein, für interne Mitarbeiter als auch für Dienstanbieter. Die Sicherung mit lediglich einem Passwort genügt meist nicht, um Kriminelle abzuhalten. Kombinieren Sie das Passwort mit weiteren Methoden zur Authentifizierung: Der Einsatz von PKI-Zertifikaten (Public Key Infrastructure) oder Hardware-Tokens ist heute bereits in vielen Unternehmen verbreitet. Erkundigen Sie sich bei Ihrem Lösungsanbieter über mögliche Ergänzungen.

5. Logs überprüfen

Stellen Sie sicher, dass Ereignisprotokolle (Logs) erstellt, überwacht und gespeichert werden. Gehen Sie nicht davon aus, dass Kriminelle nur versteckt agieren. Ihre Aktivitäten werden oft in den Logs registriert. Überprüfen Sie diese regelmässig. Dadurch können Sie Ihr Risiko frühzeitig erkennen und auf ein Minimum reduzieren.

6. Umgang mit Ausdrucken und Papierbelegen

Stellen Sie sicher, dass Ausdrucke, Faxe, Belege mit Kartendaten unter Verschluss – in Schubladen oder Schränken – aufbewahrt werden. Die Mitarbeiter müssen in Bezug auf den Umgang mit diesen vertraulichen Daten sensibilisiert werden und es muss definiert und kontrolliert werden, welche Mitarbeiter aufgrund ihrer Tätigkeit Zugriff zu diesen Unterlagen benötigen. Die sachgemässe Entsorgung der Unterlagen muss ebenfalls gewährleistet sein.

7. Dienstleister

Kontaktieren Sie Ihre Dienstleister, die in Ihrem Auftrag Kartendaten übermitteln, verarbeiten oder speichern und verlangen Sie einen PCI-Compliance-Nachweis. Die Mitverantwortung sollte geregelt sein. Führen Sie eine Liste Ihrer Dienstleister, um die Übersicht zu bewahren.

Fragen

Haben Sie Fragen zum Thema Sicherheit? Ihr PMS-Anbieter und das PCI Team von SIX helfen Ihnen gerne.

Payment Services

Einwilligungserklärung Kreditkarten-Autorisierung (Vorlage)

Mit einer Einwilligungserklärung gibt der Gast sein Einverständnis über allfällige, berechtigte Buchungen ohne physisches Vorliegen der Karte. Untenstehend finden Sie eine entsprechende Vorlage.

Ihr Hotelname / Ihr Hotellogo: _____

Dieses Formular muss in einer gesicherten Umgebung aufbewahrt werden.

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 ☐
Bezahlung in Kartenwährung (DCC - Dynamic Currency Conversion)* ☐

* Mit DCC wird Ihre Zahlung in der Kartenwährung getätigt – statt in der lokalen Währung des oben genannten Hotels. Durch das Ankreuzen des Services ermächtigen Sie das oben genannte Hotel, die in diesem Dokument festgehaltenen Zahlungen in der Kartenwährung abzubuchen. Sie sind sich darüber bewusst, dass sowohl der zu begleichende Endbetrag also auch der angewendete Wechselkurs zum Zeitpunkt der Unterzeichnung dieser Einwilligungserklärung noch nicht bekannt sind.

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 AG
Hardturmstrasse 201
Postfach
CH-8021 Zürich

Datenschutz-Vereinbarung (Muster)

Untenstehend finden Sie ein unverbindliches Beispiel einer möglichen Datenschutz-Vereinbarung. Bitte wenden Sie sich für eine rechtsgültige Version an einen Juristen Ihrer Wahl.

Die/der Unterzeichnende ist aufgrund vertraglicher und gesetzlicher Geheimhaltungspflichten angehalten, Stillschweigen über die ihm durch seine Tätigkeit beim *Hotel Musterhof* zur Kenntnis gelangten bzw. gebrachten Tatsachen/ Informationen zu wahren. Diese dürfen nicht allgemein bekannt sein, es muss ein schutzwürdiges Interesse an deren Geheimhaltung bestehen und diese muss ausdrücklich oder stillschweigend im Willen des *Hotel Musterhof* liegen.

– Unter das Geschäftsgeheimnis fällt jede Information bezüglich Gegenstand, Inhalt und Funktion der technischen bzw. softwaregestützten Mittel und Einrichtungen des *Hotel Musterhof* sowie bezüglich der Ausgestaltung und Abwicklung aller Arten von Geschäften des *Hotel Musterhof*.
– Besonders zu schützen sind alle persönlichen Kundendaten, inklusive Kredit- bzw. Debitkartendaten.

Die Verletzung der Geheimhaltungspflicht kann einzeln oder kumulativ einen Verstoss gegen das Geschäftsgeheimnis oder Datenschutzgesetz darstellen. Die entsprechende gesetzliche Bestimmung ist im Anhang zu dieser Geheimhaltungserklärung wiedergegeben.

Die/der Unterzeichnende ist verpflichtet, ihr/ihm zur Kenntnis gebrachte geheimhaltungsrelevante Tatsachen/ Informationen streng vertraulich zu behandeln und für keinen anderen Zweck zu verwenden, als in Verbindung mit der anvertrauten Aufgabe.

Ort und Datum

Name der unterzeichnenden Person

Unterschrift

1100116 CHE_DE/01.2018

Wir beraten Sie gerne rund um Ihre massgeschneiderte Lösung für das bargeldlose Bezahlen.

Ihren lokalen Ansprechpartner finden Sie unter: www.six-payment-services.com/kontakt

SIX Payment Services AG
Hardturmstrasse 201
Postfach
CH-8021 Zürich

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

SIX Payment Services (Austria) GmbH
Marxergasse 1B
1030 Wien
Österreich

SIX Payment Services (Europe) S.A.
Zweigniederlassung Deutschland
Theodor-Heuss-Allee 108
D-60486 Frankfurt am Main