Payment Services

Le traitement sécurisé des paiements par carte dans l'hôtellerie

Un guide de SIX Payment Services

Sommaire

Avant-propos

De plus en plus de gens apprécient la flexibilité et l'indépendance que procure le paiement par carte – devant et derrière le comptoir de la réception.

Pour que vous continuiez de profiter de ces avantages, nous souhaitons vous expliquer la procédure correcte à suivre lors d'un paiement sans numéraire ainsi que vous donner des conseils pratiques. Pa ailleurs, certaines mesures de sécurité doivent être observées. Les fraudeurs ne sont jamais loin, surtout lorsque les affaires sont juteuses : Le secteur de l'hôtellerie a été particulièrement touché par le cumul d'incidents frauduleux au cours des dernières années.

En tant qu'entreprise leader dans le domaine du paiement sans numéraire, SIX Payment Services s'engage à vous soutenir activement dans le traitement efficace des paiements par carte ainsi que dans le domaine de la sécurité des données de carte.

Processus de réservation simple

Pas à pas

SIX a développé un processus de réservation spécialement adapté aux exigences de l'hôtellerie et offre entre autres le traitement des paiements avec un token (données de remplacement). Ainsi, tous les processus sont assurés avec la plus grande sécurité des données et fournissent d'autres avantages utiles. Veuillez observer que la fonction doit être activée sur votre terminal (ep2). Si cela n'est pas encore le cas, veuillez vous renseigner auprès de SIX.

Statut	Procédure au terminal de paiement	Remarques
Réservation par téléphone, courrier, e-mail ou portail en ligne. Titulaire de carte et carte de paiement ne sont pas sur place.	Réservation*	Lors de la réservation, un token PAN avec date d'expiration du token est généré. Ceci est inscrit sur le justificatif.**
Check-in : Titulaire de carte et carte de paiement sont sur place.	Réservation*	Procédez à une nouvelle réservation au terminal de paiement et lisez la carte de paiement. Ce faisant, un nouveau token PAN avec date d'expiration du token est généré.
	Annulation réservation	Annulez ensuite la première réservation au terminal de paiement, afin que le montant ne soit réservé qu'une seule fois sur la carte.
Lors d'un prolongement du séjour	Augmentation de la réservation	
Check-out	Enregistrement réservation	Il n'est pas obligatoire de lire la carte de paiement, même pour les paiements DCC. **Important :** Après ce processus, la réservation initiale et les augmentations éventuelles de la réservation sont enregistrées et automatiquement supprimées. Il n'est donc pas nécessaire de procéder à une annulation de la réservation.

* dans la mesure où la carte n'a pas encore été débitée du montant de la réservation en ligne.

** Le token PAN est un numéro à 19 chiffres, généré de manière aléatoire et incompréhensible pour remplacer le numéro de carte original. SIX est la seule à pourvoir déchiffrer quel token PAN est attribué à quel numéro de carte original. Pour chaque token PAN, une date d'expiration aléatoire est générée, qui, pour des raisons de sécurité, n'est pas la même que celle de la carte de paiement originale.

Avantages du processus de réservation par SIX

Il suffit de lire la carte de paiement lors du check-in. Elle ne sera plus nécessaire lors du check-out.

DCC (conversion automatique des devises) est également possible lors du check-out, sans avoir besoin de lire à nouveau les données de la carte.

Celles-ci sont transmises avec le standard sécurisé EMV et « tokenisées », cela signifie qu'elles sont remplacées par des données aléatoires non compréhensibles.Vu que ces informations ne sont pas sensibles, cela simplifie fortement l'exigence de conformité PCI DSS.

Conseils

Veuillez lire les données de la carte de paiement lors du check-in si possible avec la puce ou la piste magnétique. En cas de dommage, vous vous dégagez de toute responsabilité envers la banque émettrice de la carte (Issuer).

Lors du check-out, proposez à vos clients de payer dans la monnaie de leur carte grâce à DCC. Le client de l'hôtel doit confirmer en appuyant sur une touche du terminal de paiement. Attirez l'attention de votre client sur l'option de paiement avec DCC, en posant par ces exemples ces questions simples : Pouvons-nous procéder au paiement directement en livres (monnaie de la carte) ?

Informez le client que lors de la réservation, le montant sera réservé sur sa carte de crédit et que cela réduit la limite de sa carte en conséquence (mais que le montant n'est pas débité).

Remarques importantes

Les crédits ne peuvent être établis que sur la même carte de crédit qui a été initialement débitée. Ne procédez en aucun cas à un crédit sur une autre carte de crédit ou de débit ou un autre compte bancaire.

Procédure au terminal

Quick Guide

Réservation

1. Sélectionner le type de transaction « Réservation »
2. Entrer le montant qui doit être réservé et autorisé
3. Lire les données de la carte au terminal
4. Confirmer le montant avec PIN ou signature
5. Impression du justificatif « Réservation »

Augmentation de la réservation

1. Accéder dans « Autres transactions » au type de transaction « Augmentation de la réservation »
2. Saisir le montant duquel la réservation doit être majorée
3. Entrer « Numéro Trx. Ref. »

4.1 Carte sur place : lire les données de la carte au terminal

4.2 Carte non sur place : sélectionner « manuellement » et saisir le token PAN ainsi que la date d'expiration token

5. Saisir le montant
6. Impression du justificatif « Augmentation de la réservation »

Enregistrement (réservation)

1. Sélectionner le type de transaction « Enregistrement réservation »
2. Saisir le montant final (le montant différentiel est automatiquement autorisé rétroactivement)
3. Sélectionner « Manuellement »
4. Entrer « Numéro Trx. Ref. »
5. Le numéro de carte est demandé
   > Entrer le numéro token PAN
6. La date d'expiration est demandée
   > Entrer la date d'expiration token
7. CVC2/CVV2 est demandé (code au dos de la carte)
   > appuyer sur la touche « OK »
8. Contrôler le montant et sélectionner DCC pour un client étranger. Confirmer DCC en appuyant sur la touche. Les données de la carte n'ont pas besoin d'être lues.

No show

Procédure comparable à « Enregistrement réservation » avec les différences suivantes :

– le montant maximal autorisé est le prix d'une nuitée
– noter « no show » à la main sur la ligne de signature du justificatif

Crédit

1. Sélectionner le type de transaction « Crédit »
2. Entrer le mot de passe pour le terminal de paiement et appuyer sur « OK »
3. Saisir le montant et appuyer sur « OK »
4. Entrer la date de la transaction initiale
5. Introduire la carte et appuyer sur « OK »
6. Impression du justificatif « Crédit »

Réservation (débit rétroactif)

1. Sélectionner le type de transaction « Réservation »
2. Saisir le montant du débit rétroactif
3. Sélectionner « Manuellement »
4. Le numéro de carte est demandé
   > Entrer le numéro token PAN
5. La date d'expiration est demandée
   > Entrer la date d'expiration token
6. CVC2/CVV2 est demandé > appuyer sur « OK »
7. Ne pas proposer DCC vu que le titulaire de carte ne peut pas confirmer sur simple pression d'un bouton
8. Écrire « Signature on File » sur la ligne de signature du justificatif

Annulation réservation

1. Accéder dans « Autres transactions » au type de transaction « Annulation réserv. »
2. Entrer « Numéro Trx. Ref. »

3.1 Carte sur place :
   – Lire les données de la carte au terminal
   – La réservation est annulée

3.2 KCarte non sur place :
   – Sélectionner « Manuellement »
   – Le numéro de carte est demandé
   > Entrer le numéro token PAN
   – La date d'expiration est demandée
   > Entrer la date d'expiration token
   – CVC2/CVV2 est demandé > appuyer sur « OK »

Justificatif

Snow Mountain Hotel Resort
Crystal Peak
3920 Zermatt
Suisse

1	Réservation	
	Visa	
2	9756 1348 0110 7483 611	
3	Date d'expiration	09.18
	12.05.2016	11:05:34
	Période comptable	4
	Trm-Id:	12345678
	Act-Id:	5
	AID:	A0000000041010
4	Numéro Trx. Ref. :	123456789
	N° Trx. Seq. :	87974475
	Code d'autorisation :	121851
	EPF:	
5	49FAEB10EC70B4099C7B5C167E9E5FCC	
	Total-EFT	EUR 345.00
	Signature	
	SIX Payment Services	

1 Type de transaction
2 «Token numéro de carte»
3 «Token date d'expiration»
4 Numéro de référence de la transaction
5 Montant total

Garantie de la réservation par carte de crédit

Voici la procédure correcte

Lors d'une réservation par carte de crédit (Visa, Mastercard, UnionPay, JCB, Diners Club Card ou Discover Card), la première nuit est garantie.

Réservation

Lors de la réservation, demandez à votre client les informations suivantes :

– Nom, prénom (comme indiqué sur la carte)
– Adresse de facturation
– Numéro de carte de crédit et date d'expiration
– Numéro de téléphone, adresse postale, adresse e-mail
– Date d'arrivée et durée du séjour

Donnez à votre client les informations suivantes, dans la mesure du possible par écrit :

– Prix d'une nuitée pour la catégorie de chambre ainsi que le montant total de la facture (TTC)
– Adresse exacte de l'hôtel
– Code de réservation (donné par l'hôtel)
– Conditions d'annulation de votre hôtel, en particulier la date limite pour une annulation sans frais
– que, passée cette date limite, ou si les conditions d'annulation n'ont pas été observées, une nuit TTC sera débitée

Annulation

Vous êtes contraint par principe d'accepter toutes les annulations qui ont été signalées avant 18h00 heure locale de la date d'arrivée prévue dans votre hôtel. Si cette période d'annulation ne vous suffit pas, vous pouvez l'allonger à 72h maximum avant la date d'arrivée du client prévue. Dans ce cas, vous devez signaler par écrit à votre client la date spécifique d'annulation. Spécifiez explicitement la date concrète et l'heure en question.

– Procédez à une « Annulation réservation » sur le terminal de paiement
– Vous devez communiquer au titulaire de carte le numéro d'annulation (donné par l'hôtel)

No show

Si le client n'est pas venu et qu'il n'a pas annulé la réservation à temps, vous pouvez débiter sa carte de crédit des coûts pour une nuitée TTC et éditer le justificatif correspondant.

– Procédez à une « Réservation » du montant correspondant
– Inscrivez à la place de la signature du titulaire de carte la mention « No show » sur la ligne de signature

Conseil

Demandez à votre client un consentement par écrit, dans lequel il accepte les conditions d'annulation et les CGV.

Important

Si le titulaire de carte nie avoir procédé lui-même à la réservation, vous ne serez éventuellement pas en droit d'exiger une compensation.

Réservation avec acompte par carte de crédit (Advance Deposit)

Voici la procédure correcte

Si vous souhaitez demander un acompte pour une réservation, vous pouvez le faire via la carte de crédit du client. Deux possibilités sont à votre disposition : Auterminal de paiement ou en ligne. Pour les deux options, il est important de suivre exactement les étapes suivantes, pour éviter des questions ou même des rétrofacturations.

Réservation

Lors de la réservation, demandez à votre client les informations suivantes :

- Nom, prénom (comme indiqué sur la carte)
- Adresse de facturation
- Numéro de carte de crédit et date d'expiration
- Numéro de téléphone, adresse postale, adresse e-mail
- Date d'arrivée et durée du séjour

Donnez à votre client les informations suivantes, dans la mesure du possible par écrit :

- Prix d'une nuitée pour la catégorie de chambre ainsi que le montant total de la facture (TTC)
- Adresse exacte de l'hôtel
- Code de réservation (donné par l'hôtel)
- Conditions d'annulation de votre hôtel, en particulier la date limite pour une annulation sans frais
- Montant de l'acompte à débiter sur sa carte de crédit (ne doit pas dépasser le prix de 14 nuitées). N'inscrivez pas le numéro complet de la carte de crédit dans la confirmation et donnez à la place uniquement les quatre derniers chiffres.
- que l'acompte est déduit de la facture finale
- que la chambre est réservée pour toute la durée du séjour couverte par l'acompte
- que, passée cette date limite, ou si les conditions d'annulation n'ont pas été observées, l'acompte sera perdu partiellement ou complètement

Conseil

Demandez à votre client un consentement par écrit, dans lequel il accepte les conditions d'annulation et les CGV.

Réserver l'acompte au terminal de paiement

- Procédez à une « Réservation » sur le terminal de paiement
- Ecrivez à la main sur le justificatif « Advance Deposit » sur la ligne de signature
- Vous êtes tenu de faire parvenir au client de l'hôtel sous trois jours ouvrables une confirmation écrite de l'acompte ainsi qu'une copie du bon de réservation.
- La confirmation de l'acompte établie par vos soins doit contenir les informations suivantes :
  - Nom de l'hôtel
  - Nom, adresse de facturation et numéro de téléphone du titulaire de carte
  - Date d'arrivée prévue
  - Montant de l'acompte
  - Date de la transaction
  - Code de réservation de l'acompte (donné par l'hôtel)
  - Date limite pour une annulation
  - Conventions d'annulation
  - Droits et obligations pour les acomptes par carte de crédit

Réserver l'acompte en ligne

Cette possibilité est à votre disposition si vous possédez un pack e-commerce de SIX Payment Services. Ainsi, vous pouvez soumettre une offre portant sur le montant de l'acompte dans le backoffice de l'application, que vous envoyez par e-mail au client, ou bien le client réserve directement sur votre cyberboutique.

Dans les deux cas, votre client doit être redirigé vers la fenêtre de paiement dans laquelle il doit entrer ses données de carte. Ensuite, le client doit saisir son mot de passe dans la fenêtre 3-D-Secure – ainsi, vous pouvez vous assurer que c'est bien le client qui a procédé personnellement à la réservation. Vous pouvez consulter et modifier la réservation effectuée dans le backoffice.

Annulation au terminal de paiement et en ligne :

- Indiquez au titulaire de carte le code d'annulation (attribué par l'hôtel) et rappelez que le code doit être conservé pour toute demande ultérieure
- Inscrivez sur la confirmation d'acompte la mention « annulé » et le code d'annulation
- Calculez le montant à rembourser
- Procédez à une note de crédit sur le terminal de paiement
- Envoyez au client au sein de trois jours ouvrables une copie des deux justificatifs (bon de réservation Advance Deposit et note de crédit de l'annulation), accompagnés d'un texte expliquant qu'une note de crédit a été effectuée

Important

D'une manière générale, le client a droit à la chambre qu'il a réservée ou la catégorie de chambre. Si lors de son arrivée la chambre n'est pas disponible, vous êtes tenu de lui rembourser entièrement l'acompte.

Le traitement des transactions effectuées par saisie manuelle des données de carte comportent un certain risque à la charge de l'hôtel. En particulier si il s'avérait par la suite que les données de carte ont été utilisées de façon frauduleuse sans le consentement du titulaire de carte. Les risques peuvent être largement évités si vous procédez à la réservation en ligne.

Réservations rétroactives (Late Charges)

Voici la procédure correcte

Si vous constatez après le check-out que des coûts n'ont pas été pris en compte dans le décompte final, vous pouvez débiter la carte de crédit de façon rétroactive.

Réservation / Check-in

Pour procéder à un débit rétroactif, vous devez avoir expliqué au client au plus tard lors du check-in les conditions générales de vente et notamment en rapport avec les frais supplémentaires. Nous vous recommandons donc de faire signer au client dès sa réservation une déclaration de consentement dans laquelle il consent aux conditions d'annulation et aux CGV.

Après le départ

- Procédez à une « Réservation » sur le terminal de paiement
- Apposez dans la ligne de signature « Signature on File »
- Si la réservation ou selon l'autorisation est annulée, contactez le titulaire de carte et demandez-lui un autre moyen de paiement
- Envoyez au titulaire de carte les informations suivantes :
  - Copie du justificatif avec la mention « Signature on File » dans la ligne de signature
  - Copie de la facture/des factures concernant les coûts additionnels avec le détail des positions

Important

Les coûts additionnels débités rétroactivement ne peuvent concerner que la chambre, des repas ou boissons. Cependant, la facture de l'hôtel ne peut être majorée que de 15 % grand maximum.

BSi les coûts additionnels s'élèvent à plus de 15 % ou si des coûts ont été occasionnés en raison d'une perte, un vol ou de dommages dans la chambre de l'hôtel, ces coûts ne peuvent être débités qu'après avoir recontacté le client après son départ et si vous avez trouvé un accord avec ce dernier. Le consentement du client concernant le débit de la carte de crédit doit être disponible par écrit.

Protection effective des données de carte grâce à PCI DSS

Le Payment Card Industry Data Security Standard (PCI DSS) est un ensemble de dispositions relatif aux paiements électroniques, qui s'occupe du traitement sécurisé des transactions par carte. La conformité à PCI DSS est une exigence impérative de toutes les principales organisations internationales de cartes : Visa, Mastercard,JCB International, American Express et Discover Financial Services. Les dispositions sont éditées par le Payment Card Industry Security Standards Council.

Toutes les entreprises qui enregistrent, transmettent ou éditent des données de carte, doivent satisfaire aux règles de sécurité définies dans ces dispositions. Si les exigences ne sont pas remplies, les organisations de carte peuvent alors en fin de compte interdire l'acceptation des paiements par carte.

Cet ensemble de dispositions a pour but de vous protéger des conséquences désagréables d'un vol de vos données de carte ; dans le cas d'un vol des données de carte, les pertes financières engendrées sont souvent accompagnées d'un préjudice de réputation.

Cet ensemble de dispositions est constitué de douze groupes d'exigences et porte sur l'infrastructure IT, les processus ainsi que les employés de votre hôtel :

Exigence 1 : Installation et entretien d'une configuration pare-feu pour la protection des données du titulaire de carte

Exigence 2 : Ne jamais utiliser les paramètres par défaut fournis pour les mots de passe système et autres paramètres de sécurité

Exigence 3 : Protection des données de titulaire de carte enregistrées

Exigence 4 : Cryptage des données de titulaire de carte lors de la transmission sur des réseaux non protégés, publics

Exigence 5 : Protection de tous les systèmes contre les malware et mise à jour régulière des logiciels antivirus et programmes

Exigence 6 : Développement et maintenance de systèmes et applications sécurisés

Exigence 7 : Restriction de l'accès aux données de titulaire de carte suivant le besoin d'information

Exigence 8 : Identification et authentification de l'accès aux composants du système

Exigence 9 : Restreindre l'accès physique aux données du titulaire de carte

Exigence 10 : Suivi et surveillance de tout l'accès aux ressources réseau et données de titulaire de carte

Exigence 11 : Tester régulièrement les systèmes et procédures de sécurité

Exigence 12 : Mettre en œuvre une directive sur la sécurité de l'information pour l'ensemble du personnel.

Le respect des exigences est vérifié à l'aide de trois mesures de validation :

- Les hôtels ayant plus de 6 millions de transactions par an ou les partenaires qui ont été victimes d'un vol de leurs données de carte, doivent participer à un On-Site Audit. Celui-ci doit être conduit par un auditeur qualifié, respectivement par une entreprise de certification accréditée (QSA – Qualified Security Assessor).
- Les hôtels ayant moins de 6 millions de transactions par an peuvent déclarer respecter les directives en remplissant un formulaire d'auto-évaluation(SAQ – Self-Assessment Questionnaire).En fonction de l'acceptation de carte donnée, il existe plusieurs versions de ce document SAQ.
- Pour les hôtels dont l'infrastructure est en contact avec des données de carte, il existe des network-scans. Tous les trimestres et sur consultation un ASV (Approved Scanning Vendor) procède à un piratage amical. L'objectif est de détecter à temps les points faibles.

En toute sécurité

Concernant la sécurité, il est recommandé d'envisager des solutions conçues de telle façon que votre hôtel n'entre pas du tout en contact avec des données de cartes non cryptées et complètes. Ainsi, vous pouvez réduire considérablement le temps investi pour la certification.

Les conseils suivants vous aident à réduire le risque d'un vol de données de carte et le temps investi pour la certification :

PCI Proxy Server

Les plateformes de réservation sont des partenaires de distribution importants. Hélas, elles ne respectent pas toujours les règles de sécurité : Les données sensibles sont souvent transmises sans cryptage – par e-mail ou par des interfaces XML.

Si c'est le cas, la charge à investir pour satisfaire les normes de sécurité PCI DSS augmente fortement. Pour éviter cette charge supplémentaire, il existe une alternative simple et moins couteuse : le PCI Proxy Server. Celui-ci intercepte les données de carte en cours de route entre la plateforme de réservation et votre établissement et les remplace par un numéro (token) aléatoire. Les données de carte sensibles sont alors enregistrées dans un environnement certifié PCI DSS. Ainsi, vous profitez d'une validation simplifiée et pouvez toutefois procéder à des réservations par des portails en ligne.

Hotel Software – Property Management System (PMS)

Vérifiez si votre logiciel hôtelier est certifié PCI PA-DSS (Payment Application Data Security Standard). Ainsi, vous assurez que les données de carte sont enregistrées avec cryptage conformément aux directives. Le mieux est de contacter votre fournisseur PMS.

Outsourcing

Si vous ne pouvez pas renoncer à l'enregistrement des données de carte, clarifiez avec votre prestataire si un outsourcing est possible. Si l'enregistrement des données de carte est pris en charge par le prestataire, celui-ci doit remplir toutes les exigences PCI DSS. Demandez-lui un justificatif (certificat). Assurez-vous que votre partenaire et fournisseur de services soit bien agréé PCI.

Portail web SAQ

SIX Payment Services opère en coopération avec un partenaire un portail web SAQ (Self-Assessment-Questionnaire).

Le portail vous guide pas à pas dans toutes les étapes nécessaires à la certification PCI DSS. Dans les archives de documents du portail, vous pouvez à la fin consulter et télécharger tous les documents faisant partie de la procédure, tels que l'attestation de certification, le Self-Assessment et le cas échéant, les résultats du scan réseau.

Le portail est à la disposition de tous les clients SIX et ceci gratuitement.

En cas de questions techniques ou concernant le contenu, adressez-vous directement à l'équipe PCI de SIX : pci-support.ch@six-payment-services.com

Secure PayGate

Si vous prenez la réservation par téléphone, fax, e-mail ou courrier, vos clients peuvent payer facilement en ligne et en toute sécurité sans que votre hôtel ait besoin des données de carte. La solution s'appelle Secure PayGate.

Secure PayGate joint aux avantages d'une transaction communément appelée Mail/Phone Order la sécurité d'une transaction Secure e-commerce protégée par mot de passe. Cela signifie pour vous : plus de sécurité et traitement facilité.

Pour en savoir plus sur Secure PayGate, rendez-vous sur : **www.paymentforyou.com**

Conseil

Offrez à vos clients le paiement par procédure 3D Secure. Pour que vous soyez sûr que le client de l'hôtel a procédé lui-même à la réservation et que le renversement de responsabilité opère en votre faveur.

Compte tenu de la croissance constante de la cybercriminalité, le secteur hôtelier est également dans le collimateur des fraudeurs. L'examen des incidents a montré que la majeure partie aurait pu être évitée avec les bons mécanismes de sécurité. Les conseils suivants du standard de sécurité international PCI DSS vous concernent si vous stockez des données de carte dans votre infrastructure (la vérification est recommandée néanmoins également indépendamment de PCI DSS) :

1. Modifier les paramètres par défaut

Les intégrateurs programment souvent les systèmes PMS et POS avec des mots de passe par défaut. Si un criminel se procure ce mot de passe, il pourra facilement accéder à vos systèmes. N'utilisez donc jamais le mot de passe fourni par votre fournisseur. Définissez avant l'installation d'une application un nouveau mot de passe très complexe : Utilisez des majuscules et minuscules ainsi que des chiffres et caractères spéciaux. Le mot de passe doit contenir au moins huit caractères.

2. Configurer correctement le pare-feu

Configurez le pare-feu de sorte que le trafic de données entrant et sortant soit uniquement limité aux services nécessaires à cette opération. Ne connectez pas directement vos systèmes PMS et POS à Internet. Bloquez le trafic de données entrant et filtrez le trafic sortant. Cette mesure limite considérablement les activités d'un attaquant.

3. Segmentation du réseau

Segmentez votre réseau : Empêchez la communication des systèmes de traitement de cartes avec les autres systèmes par des pare-feux et routeurs. L'objectif est d'interdire l'accès direct aux systèmes de traitement de cartes et ainsi de minimiser le risque d'un piratage des données. Un réseau non segmenté signifie également que PCI DSS doit être appliqué à l'ensemble du réseau.

4. Configurer l'authentification à facteurs multiples

Configurez pour toutes les solutions d'accès distant une authentification à facteurs multiples aussi bien pour les employés internes que pour les fournisseurs de services. La protection par un simple mot de passe ne suffit généralement pas à dissuader les criminels. Combinez toujours le mot de passe à d'autres méthodes d'authentification : L'utilisation de certificats PKI (Public Key Infrastructure) ou de clé physique est largement répandue aujourd'hui dans beaucoup d'entreprises. Renseignez-vous auprès de votre fournisseur si d'autres solutions sont possibles.

5. Vérifier les logs

Assurez-vous que des protocoles d'évènements (logs) soient bien établis, contrôlés et sauvegardés. Gardez bien en tête que les criminels agissent toujours cachés. Leurs activités sont souvent enregistrées dans les logs. Contrôlez-les régulièrement. Ainsi, vous pouvez identifier le danger à temps et en réduire les effets au minimum.

6. Traitement des imprimés et documents écrits

Assurez-vous que les imprimés, fax, justificatifs comportant des données de carte sont toujours gardés sous clé dans des tiroirs ou des armoires. Les employés doivent être sensibilisés à la manipulation correcte de ces données sensibles et il faut définir et contrôler quelles personnes ont besoin d'un accès à ces données en raison de leurs activités. L'élimination appropriée des documents doit également être assurée.

7. Prestataires de services

Contactez votre prestataire chargé de transmettre, traiter ou sauvegarder les données de carte et demandez-lui une attestation de PCI compliance. La coresponsabilité doit être réglée. Tenez une liste de vos prestataires afin de conserver une vue d'ensemble.

Questions

Avez-vous des questions concernant la sécurité ? Votre fournisseur PMS et l'équipe PCI de SIX vous aideront volontiers.

Payment Services

Déclaration de consentement
Autorisation de carte de crédit (modèle)

Avec une déclaration de consentement, le client donne son accord concernant toute réservation éventuelle justifiée sans présentation physique de la carte. Le modèle correspondant se trouve ci-dessous.

Le nom/le logo de votre hôtel: _____

Ce formulaire doit être conservé dans un endroit sûr.

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 ☐
Paiement en monnaie de la carte (DCC - Dynamic Currency Conversion)* ☐

* Avec DCC, votre paiement est effectué dans la monnaie de votre carte - au lieu de la monnaie locale de l'hôtel précité. En cochant le service, vous autorisez l'hôtel précité à débiter les paiements indiqués dans ce document dans la monnaie de la carte. Vous êtes conscient du fait que le montant final tout comme le cours du change utilisé au moment de la signature de cette déclaration de consentement ne sont pas encore connus.

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 SA
Hardturmstrasse 201
Case Postale
CH-8021 Zurich

Charte de protection des données (spécimen)

Vous trouverez ci-dessous, sans engagement, un modèle de charte de protection des données. Si vous souhaitez une version juridiquement valable, veuillez prendre contact avec un juriste de votre choix.

En raison de l'obligation contractuelle et légale de garder le secret, le/la signataire est tenu(e) de ne pas divulguer les faits/informations portés à sa connaissance dans le cadre de son activité à l'*hôtel ABC.* Il s'agit de faits/d'informations qui ne sont pas connus de tous, pour lesquels il existe un intérêt légitime de garder le secret et pour lesquels le maintien du secret dépend expressément ou tacitement de l'*hôtel ABC.*

– Le secret d'affaires s'applique à toutes les informations obtenues lors de l'utilisation des moyens et des équipements techniques ou informatisés de l'*hôtel ABC* ainsi qu'à toutes les informations relatives à l'organisation et à l'exécution des tâches de l'*hôtel ABC* dans le cadre de la marche de ses affaires.
– Il convient de protéger tout particulièrement les données personnelles des clients, y compris les données relatives à leurs cartes de crédit ou de débit.

Pris individuellement ou de manière cumulative, tout manquement à l'obligation de garder le secret peut représenter une violation du secret d'affaires. La disposition légale correspondante est mentionnée dans l'annexe au présent accord de confidentialité.

Le/la signataire est tenu(e) de traiter de manière strictement confidentielle tous les faits/informations relevant de l'obligation de garder le secret et dont il/elle aurait connaissance. Il/elle ne doit pas les utiliser à d'autres fins que celles en relation avec la tâche qui lui a été confiée.

Lieu et date

Nom du/de la signataire

Signature

1100116 CHE_FR/01.2018

Nous vous conseillons volontiers pour vous offrir la solution qui vous convient avec le paiement sans espèces.

Les coordonnées de votre interlocuteur local sont disponibles sous: www.six-payment-services.com/contact

SIX Payment Services SA
Hardturmstrasse 201
Case postale
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 Vienne
Autriche

SIX Payment Services (Europe) S.A.
Succursale Allemagne
Theodor-Heuss-Allee 108
D-60486 Francfort-sur-le-Main