Atos Worldline
HIGH-TECH TRANSACTIONAL SERVICES

Sips
Présentation fonctionnelle

Version 3.0 – Octobre 2010

REACH YOUR TARGETS »

Contact
By phone: +33 (0)811 107 033
By fax: +33 (0)811 107 033
By email: sips@atosorigin.com

Sips
e-Payment Solution
by Atos Worldline

www.atosworldline.com

SOMMAIRE

Quelles solutions Sips pour quels besoins ?

E-commerce

Sips Payment. La gestion des pages sécurisées avec l'authentification 3D Secure se font sur les serveurs Sips. Le commerçant dispose d'un extranet lui permettant de rembourser ses clients, de faire du paiement différé, du débit à l'expédition etc. Le commerçant n'a jamais connaissance des données carte de ses clients.
Sips Office Server. Avec une connexion de serveur à serveur, le commerçant affiche lui même les pages de paiement. Il dispose d'un identifiant qui lui évite de conserver les données carte. Le commerçant, via son SI, peut ainsi faire du paiement différé ainsi que des opérations de caisse de manière automatisée (remboursement, annulations).

Multicanal, mobilité

Sips Office Server. La connexion de serveur à serveur permet de traiter des paiements en provenance de n'importe quel canal. Ainsi, le commerçant peut connecter à l'API son SVI, une interface minitel, une interface maison pour son centre d'appels, etc. L'échange de données se fait au format XML.
Sips Office Extranet. Cet extranet sécurisé est accessible via un identifiant et un mot de passe. Il permet à un opérateur de centre d'appel ou à un commerçant de disposer d'un terminal de paiement virtuel. Et ainsi de créer des transactions sans avoir à développer une interface de paiement..
Sips Office Batch. Le commerçant peut également créer des transactions et effectuer ses opérations de back-office par l'envoi de fichiers . Cette solution répond aux besoins des commerçants de vente à distance qui souhaitent fonctionner en mode offline.
Sips Payment SVI-s Commande. Donne la possibilité à des téléconseillers de transférer les clients vers le serveur vocal interactif de paiement Sips afin de finaliser la transaction en cours. Le client est invité à saisir les informations de sa carte de paiement sur un serveur vocal interactif sécurisé et n'a donc pas besoin de les communiquer au Téléconseiller
Sips Payment SVI-s Paiement de factures offre la possibilité à des fournisseurs de services de proposer à leurs clients finaux un nouveau moyen de paiement à distance de leurs factures grâce à un SVI de paiement sécurisé, sans passer par un opérateur côté commmerçant.
Sips Payment Mobile permet de proposer du paiement sur des téléphones mobiles. Fonctionne sur le même principe que Sips Payment Web : l'affichage des pages de paiement est effectué par Sips.

Paiement récurrent, abonnement

Sips Office Server. Le commerçant utilise une solution de serveur à serveur et associe un identifiant à chaque transaction. Le numéro de carte est ainsi externalisé sur les serveurs Sips. A chaque échéance de paiement, il lui suffira de faire référence à la transaction initiale pour qu'elle soit dupliquée. Toutes les étapes de l'abonnement sont prévues : préinscription sans débit (vérification de la carte), débit, annulation, remboursement, etc.
Le composant abonnement. Le commerçant associe un identifiant d'abonné à l'inscription d'un client. Il pourra ensuite débiter son client de manière récurrente, en mode online ou par transfert de fichiers.
En offline avec Sips Office Batch. Le commerçant peut envoyer une liste de débits à réaliser, soit à partir de numéros d'abonnés soit à partir des identifiants de transactions précédemment traitées.

Paiement différé Débit à l'expédition Paiement échelonné

Toutes les solutions Sips autorisent le paiement en plusieurs échéances, le débit à l'expédition et le paiement en différé. Seules les méthodes diffèrent en fonction des moyens utilisés. Sips Payment permet de scinder une transaction en plusieurs échéances de manière automatique. Sips Office Server permet d'automatiser la validation des transactions pour débiter le client à l'expédition des produits vendus. Sips Office Batch permet d'effectuer toutes ces opérations via un transfert de fichiers.

I. PRESENTATION DE L'OFFRE ATOS WORLDLINE SIPS

A. A PROPOS DE SIPS

Atos Worldline, fort de son savoir-faire en matière de commerce électronique et de sa forte implication dans le domaine bancaire commercialise depuis 1996 une solution de paiement sécurisé, sous le nom de Sips, conforme aux réglementations interbancaires française et internationale.

D'un point de vue fonctionnel, la solution permet d'accepter des paiements de manière sécurisée sur tous les canaux de vente à distance (Internet, mobile, SVI, couponing). Cette fonctionnalité de base s'accompagne d'outils perfectionnés pour administrer les transactions (rembourser, annuler, valider, différer le paiement, etc) et pour contrôler leur bonne acceptation financière (crédit sur compte commerçant et vérification d'impayés). La richesse de la solution permet d'accepter une multitude de moyens de paiement, locaux et internationaux, et de créditer ces transactions sur des comptes bancaires dans 63 pays dans le monde.

En résumé

Sips permet à tout commerçant d'intégrer une solution de paiement et de gestion de caisse à son système d'information. Il garde le choix de son établissement bancaire dans le monde ainsi que des moyens de paiement acceptés.

Sips est la première solution de paiement française certifiée PCI/DSS, le programme de sécurisation des données mis en œuvre par les réseaux internationaux (Visa, Mastercard, American Express). PCI/DSS impose le respect de règles très strictes dans toute la chaîne de traitement : réseau, données cartes, contrôle des données, traçabilité des accès aux données, politique de sécurité.

La certification PCI/DSS de la solution Sips n'exonère par le commerçant sur ses obligations vis-à-vis du respect de la réglementation en vigueur. Notamment s'il utilise Sips Office pour créer des transactions, le commerçant veillera à demander conseil à son établissement bancaire.

B. A QUI S'ADRESSE CE SERVICE ?

Sips est largement distribué dans le monde. Il est vendu directement aux commerçants par Atos Worldline et est proposé par une multitude d'hébergeurs et d'établissements bancaires. Ce service s'adresse en particulier à :

- un commerçant, souhaitant facilement élargir sa clientèle en vendant ses produits et services par l'Internet, sans se soucier des aspects sécuritaires des transactions, et tout en conservant sa banque ;
- un hébergeur, un intégrateur, un fournisseur d'accès, ou un gérant de galeries marchandes sur l'Internet, souhaitant proposer un service de paiement sécurisé personnalisé à sa clientèle ;

- un établissement bancaire, désirant proposer à sa clientèle commerçante une solution personnalisée et fiable.

En résumé

Des milliers de e-commerçants ont confiance en notre solution. Une multitude de banques et de distributeurs revendent la solution Sips via leur réseau.

C. UN RESEAU D'ACCEPTATION EUROPEEN

Pour effectuer de manière transparente des demandes d'autorisation et des remises en banque, Sips doit aujourd'hui avoir une connexion avec l'acquéreur du commerçant (sa banque ou une autre institution) et son centre de traitement monétique. Sips dispose de multiples connexions dans le monde, ce qui lui permet d'atteindre 63 pays sur tous les continents.

Pour tous vos projets internationaux, nous vous invitons à nous contacter. Nous vous conseillerons sur les moyens de paiement acceptés dans les pays concernés.

Les pays couverts par Sips (en rouge) pour l'acquisition des flux de paiement

D. LES PRE-REQUIS

1. PRE-REQUIS BANCAIRE / FINANCIER

L'utilisation de Sips pour un commerce électronique ne nécessite pas de liaison particulière entre le serveur du commerçant et sa banque ou Atos Worldline. L'internet est le moyen de communication privilégié.

Outre l'immatriculation au registre du commerce et des sociétés, l'utilisation du service Sips nécessite l'obtention d'un contrat de Vente à Distance (eCommerce) / Vente par Correspondance (VPC), d'un contrat avec un établissement financier en vue d'accepter des cartes privatives ou accréditives, ou d'un compte de monnaie électronique auprès d'un établissement bancaire ou financier, au choix du commerçant. Pour souscrire au service 3-D Secure des réseaux Visa et Mastercard, le commerçant doit en faire la demande d'une part à son établissement bancaire (qui doit lui même être inscrit en tant que participant aux programmes 3-D Secure des différents réseaux bancaires concernés) et d'autre part à Atos Worldline.

Pour accepter plusieurs devises, le commerçant doit en faire la demande auprès de son établissement bancaire ou financier. La solution Sips gère les devises les plus couramment acceptées dans le monde.

2. PRE-REQUIS TECHNIQUE ET SECURITAIRE

En fonction des solutions de paiement, le commerçant devra parfois installer une interface permettant la communication entre ses serveurs et la solution Sips. Le détail des pré-requis techniques est précisé dans le guide des interfaces de paiement.

Le certificat délivré au commerçant à son inscription est une clef de sécurité unique permettant au commerçant de communiquer de manière chiffrée avec les serveurs sécurisés Sips. Aussi, le commerçant est responsable de sa conservation et doit prendre toutes les mesures pour :

- en restreindre l'accès,
- le sauvegarder de manière chiffrée,
- ne jamais le copier sur un disque non sécurisé,
- ne jamais l'envoyer (e-mail, courrier) de manière non sécurisée.

La compromission d'un certificat et son utilisation par un tiers malveillant perturberait le fonctionnement normal de la boutique, et pourrait notamment générer des transactions non justifiées sur le site du commerçant ou provoquer des opérations de caisse injustifiées (des remboursements par exemple)

Aussi, en cas de compromission de certificat, le commerçant est tenu d'en demander au plus vite la révocation puis le renouvellement à notre service clients.

Côté sécurité des données, le commerçant ainsi que ses prestataires sont tenus de se conformer à la réglementation PCI/DSS, à des degrés divers en fonction de l'importance de leur activité. La solution Sips, certifiée PCI/DSS, contribue à faciliter au maximum la mise en conformité des marchands en mettant à sa disposition tous les outils pour lui éviter d'avoir à connaître ou à conserver des données sensibles. Toutefois, nous vous invitons à évoquer ce sujet avec votre établissement acquéreur.

E. COMMENT EN PROFITER

Le démarrage d'une boutique commerçant sur Sips se déroule en 5 étapes majeures. Cf l'annexe A page 26 pour plus d'informations sur l'administration des boutiques.

La phase contractuelle

La signature du contrat Sips avec Atos Worldline, soit avec une banque, un hébergeur ou directement avec le commerçant.

La signature

Envoi du kit et inscription

A réception du formulaire d'inscription, Atos Worldline inscrit la boutique et retourne au commerçant un **certificat de production** ainsi qu'un kit de paiement (logiciel, exemples, documentations et certificat de test) pour un environnement technique spécifique (précisé dans le formulaire par le client). Le client reçoit également les codes d'accès à l'outil de gestion de caisse Sips Office Extranet.

Envoi postal + e-mail

Le développement

Le développeur du commerçant implémente la solution, à l'aide du certificat de test obtenu avec le kit.

Le commerçant effectue des tests Sips de démonstration, permettant de vérifier la bonne communication avec Atos Worldline

Une fois le développement terminé et les tests concluants, le commerçant installe le certificat de production.

Intégration client

Les tests de Pré-production

Le commerçant effectue des tests en pré-production avec son certificat de production et avec des numéros de carte réels. Les tests de pré-production vont générer des demandes d'autorisation vers sa banque sans provoquer de remise, donc de débit carte.

Le client envoie à Atos Worldline ses préférences graphiques

Tests bancaires

Le passage en production

Le commerçant envoie le Procès Verbal de recette, 24 heures avant la date à laquelle il souhaite passer en production (tous les jours sauf les Vendredi, Samedi, Dimanche et jours fériés).

Après avoir vérifié que le commerçant a bien effectué un test OK (une demande d'autorisation acceptée par la banque), Atos Worldline effectue le passage en production à la date précisée par le commerçant.

Lancement

F. PRESENTATION DES INTERFACES SIPS

Sips Payment Web

Sips Payment Web permet au commerçant de vendre en toute sécurité dans le monde Internet sans avoir à connaître des données sensibles de la transaction. Les pages de paiement sont sécurisées par Atos Worldline.

Sips Payment Mobile

Sips Payment Mobile est une réplique de Sips Payment Web adaptée au monde du mobile. Il permet ainsi d'accepter des paiements sur des terminaux mobiles, sur des pages de paiement sécurisées par Atos Worldline

Sips Payment SVI-s

Sips Payment SVI-s est un Serveur Vocal Interactif sécurisé qui permet d'accepter des paiements via une interface vocale. Il peut être utilisé de manière autonome en paiement de factures émises ou en fin de parcours d'achat d'une hotline.

Sips Office Server

Sips Office Server permet un dialogue de machine à machine entre le commerçant et Sips. Et donc d'accepter des paiements sur tous les canaux de vente, ou d'automatiser les opérations de gestion des transactions.

Sips Office Batch

Sips Office Batch permet l'envoi de fichiers par le commerçant vers Sips. Ces fichiers peuvent contenir des transactions de paiement ou des opérations de gestion.

Sips Office Extranet

Sips Office Extranet permet la gestion des paiements. Il est accessible via une adresse sécurisée (HTTPS). Il permet également au commerçant de créer des transactions via un TPE virtuel.

Les interfaces Sips Payment sont multicanal et permettent de créer des transactions uniquement. Sips est en relation directe avec le client acheteur et sécurise le processus de capture des données sensibles.

Les interfaces Sips Office permettent à la fois de créer des transactions et d'effectuer des opérations de caisse. Ces interfaces mettent le commerçant en relation avec les serveurs Sips.

	Canal de paiement			
	Internet	Mobile	Téléphone & SVI	Courrier
Sips Payment				
- Web	✓	✓	×	×
- Mobile	×	✓	×	×
- SVI-s	×	×	✓	×
Sips Office				
- Extranet	×	×	✓	✓
- Server	✓	✓	✓	✓
- Batch	✓	✓	✓	✓

Toutes ces interfaces sont documentées dans le guide *Présentation des interfaces.*

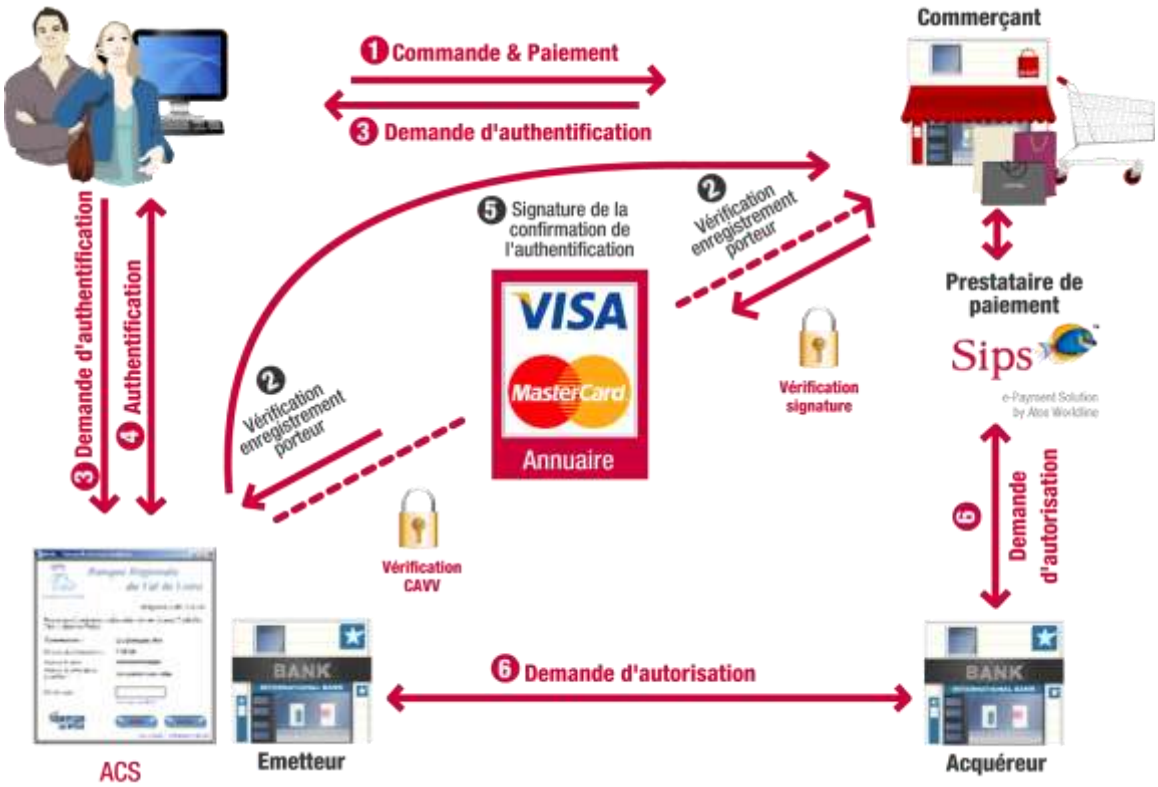
II. LE PAIEMENT

A. VISION D'ENSEMBLE DES FLUX DE PAIEMENT

1. POUR UNE TRANSACTION VIA INTERNET

Une transaction de paiement initiée par l'acheteur, pour une carte de paiement internationale devant être authentifiée 3-D Secure (*Verified by Visa* et *Mastercard Secure Code*), met en relation 4 acteurs pour aboutir. Le prestataire de paiement, Atos Worldline, se positionnant aux côtés du Commerçant :

- Pour lui donner accès à de multiples moyens de paiement, dans un pays ou dans le monde entier. Certains moyens de paiement étant spécifiques à des pays, un lien avec l'établissement émetteur de ce moyen de paiement est indispensable ;
- Pour simplifier le traitement et les échanges. Une transaction 3-D Secure implique 7 échanges de données entre les 4 interlocuteurs. Grâce à la solution Sips, le commerçant n'a besoin de gérer qu'une interface de communication entre son système d'informations et Sips. D'autant que la complexité des échanges croît avec le nombre de moyens de paiement acceptés ;
- Pour bénéficier d'outils complémentaires au paiement : de lutte contre la fraude par exemple ;
- Pour obtenir un reporting uniforme pour l'ensemble de ses moyens de paiement.



Les échanges de flux pour une transaction internet 3D-Secure

2. POUR UNE TRANSACTION EN VENTE A DISTANCE HORS INTERNET

Hors internet, le commerçant dispose de plusieurs interfaces pour accepter des paiements avec la même facilité. Le commerçant a le choix entre :

- Utiliser une interface unique pour l'ensemble de ses transactions. L'interface Sips Office Server met le commerçant au cœur de ce processus transactionnel. Il concentre les informations de paiement et les transmet à l'interface Sips pour traitement vers les acquéreurs dans le ou les pays choisis. Cette solution implique que le commerçant gère lui-même l'interface avec son client final pour capturer les informations de paiement (numéro de carte, de compte, etc). Elle impose donc au commerçant une gestion rigoureuse et une politique de sécurité sans faille (notamment les règles de PCI/DSS des réseaux internationaux Visa et Mastercard) étant donné que les informations sensibles comme le numéro de carte transitent via son système d'information.

  Cette gestion de l'interface client n'impose toutefois pas au commerçant de conserver ces données sensibles dans la mesure où la solution Sips apporte au commerçant tous les outils pour agir sur ces transactions à partir d'un alias attribué lors de sa création. Ainsi, un remboursement ou un nouveau débit du moyen de paiement utilisé est effectué sans conservation et utilisation de données sensibles par le commerçant.

- Opter pour l'utilisation de plusieurs interfaces de paiement en fonction des canaux, et ainsi :
  - **Sips Payment Mobile** pour le paiement sur des téléphones portables,
  - **Sips Payment SVI-s** pour le paiement via le canal vocal, soit en routage d'appel soit en appel autonome,
  - **Sips Office Server** et **Sips Office Batch** pour le paiement via des coupons, via le minitel ou tout autre canal
  - **Sips Office Extranet** pour la création de toutes transactions par le commerçant sur un TPE virtuel Internet sécurisé

  Ces interfaces étant pour la plupart spécifiques à un canal de paiement, l'acheteur bénéficie d'un parcours optimisé et totalement adapté à ce canal. En dehors des interfaces Sips Office lorsqu'elles sont utilisées pour créer des transactions, le commerçant n'a jamais connaissance des données sensibles du paiement.

Le guide *Présentation des interfaces* décrit les avantages de chaque interface et vous permet de discerner lesquelles correspondent le mieux à vos besoins.

B. LES PARAMETRES ET OPTIONS DU PAIEMENT

Le commerçant a la possibilité de proposer à son client plusieurs modes de paiement, qui lui permettent de proposer des **facilités de paiement**, **du paiement récurrent**, et de rapprocher au mieux le débit de l'internaute de la livraison d'un produit (**paiement à l'expédition**).

1. LE CHOIX DU JOUR ET DES MODALITES DE REMISE EN BANQUE DES TRANSACTIONS

Le commerçant peut choisir :

- le jour d'envoi en banque de la transaction (la remise en banque). Le commerçant peut ainsi faire du paiement immédiat ou différé.
- le mode d'envoi en banque de cette transaction (après Validation par le commerçant ou de manière automatique).

Lorsque le commerçant choisit d'être ainsi en *mode Validation*, les transactions ne partent pas en banque automatiquement (comme dans le *mode de capture automatique*), mais attendent une validation de sa part. Ce qui permet par exemple au commerçant de débiter son client à l'expédition des produits.

Dans un cas comme dans l'autre, le commerçant détermine un délai. Dans le mode de capture automatique (ou *mode Annulation*), la transaction sera envoyée en banque lorsque le délai sera atteint. Dans le mode Validation, le commerçant pourra décider d'envoyer en banque la transaction à tout moment avant expiration du délai.

La demande d'autorisation réalisée le jour du paiement permet d'informer la banque du porteur que le commerçant souhaite débiter la carte client pour le montant demandé et de s'assurer que la carte du porteur est bien valide et autorise le débit pour le montant indiqué.

La validité de la demande d'autorisation est variable d'un moyen de paiement à l'autre. Elle est par exemple de 6 jours pour les cartes Visa, Mastercard, American Express et Diners.

Cf. Annexe C qui précise pour chaque moyen de paiement la durée de validité d'une demande d'autorisation

Aussi, lorsque le commerçant souhaite débiter son client plusieurs jours après la date d'achat, Sips déroule des scénarios différents.

a. Le paiement différé inférieur ou égal à la durée de validité de la demande d'autorisation

Dans cette situation, Sips effectue une demande d'autorisation du montant réel de la transaction au moment où elle est réalisée.

Le commerçant a la possibilité de valider ou annuler partiellement ou totalement ce paiement dans les *n* jours qui suivent la transaction (sachant que n est inférieur ou égal à la durée de validité de la demande d'autorisation) en fonction du mode choisi.

En mode Validation, si le commerçant ne valide pas la transaction pendant ce délai, elle expirera et ne sera pas envoyée en banque. A l'inverse, en mode de capture automatique (mode *annulation*), si la transaction n'est pas annulée pendant cette période de paiement différé, elle sera automatiquement envoyée en banque au bout de cette échéance.

b. Le paiement différé supérieur à la durée de validité de la demande d'autorisation

Si le paiement différé est supérieur à la durée de validité de la demande d'autorisation, Sips effectue une demande d'autorisation pour la carte de l'internaute d'un montant de deux Euros seulement – elle représente une prise d'empreinte, l'internaute n'étant pas débité de cette somme. Cette prise d'empreinte permet de vérifier la validité de la carte au moment du paiement, sans faire subir à l'internaute deux demandes d'autorisation du montant réel, ce qui risquerait de lui faire dépasser son plafond de paiement carte autorisé.

A échéance, ou lorsque la validation (déclenchée par le commerçant) aura lieu, Sips effectuera la demande d'autorisation avec le montant réel ou final de la transaction. Ce montant sera envoyé pour remise le jour même.

A noter que plus le délai d'envoi en banque est élevé, plus le risque que la transaction soit refusée *in fine* est grand. Le commerçant est informé du résultat de la demande d'autorisation effectuée à l'échéance ou lors de sa validation. Le commerçant doit donc veiller à intégrer ce résultat avant de fournir le bien ou service à son client.

Points-clefs

Pour des raisons réglementaires, le différé de paiement d'une transaction authentifiée 3D Secure est systématiquement porté à 6 jours si le commerçant a renseigné une valeur supérieure.

Le paiement en différé n'est pas disponible pour certains moyens de paiements (cf. la liste page 35).

2. LE PAIEMENT EN PLUSIEURS FOIS

Le commerçant a la possibilité de scinder une transaction en plusieurs parties, qui seront envoyées en banque à des intervalles déterminés.

Ainsi, une transaction de paiement en *n* fois génère *n* transactions, ayant le même identifiant mais effectuées à des dates différentes. Chaque transaction est indépendante des autres et comprend une demande

d'autorisation systématique. En cas d'accord, la transaction en question est envoyée en banque. En cas de refus, la transaction n'est pas représentée.

La mise en œuvre de ce genre de paiement est subordonnée à la détermination par le commerçant du montant de la première transaction, du nombre total de prélèvements ainsi que de la périodicité des prélèvements.

Le montant de chaque transaction dépendra de la différence entre le montant total diminué de la première transaction et divisé par le nombre de prélèvements moins un (la première transaction étant comprise dans le nombre total d'échéances).

Points-clefs

La date de validité de la carte doit être inférieure à la date de la dernière échéance

Le commerçant garde la possibilité, pour une transaction donnée, d'annuler chacun des prélèvements à venir avant leurs échéances respectives.

Le nombre maximal d'échéances est de 3. Les échéances ne peuvent pas s'étendre sur plus de 90 jours.

Le commerçant pourra également faire du paiement en plusieurs fois par ses propres moyens, en étant lui-même à l'initiative de chacune des échéances, via l'opération de duplication. Ainsi, après un premier paiement (ou une première prise d'empreinte), le Commerçant pourra dupliquer à chaque échéance la transaction initiale et lui donner le montant correspondant (cf., la fonction de Duplication page 19).

Le commerçant devra rester prudent en proposant du paiement en plusieurs fois dans la mesure où, comme en cas de paiement différé, il n'a aucune garantie de règlement sur les échéances ultérieures. Une carte mise en opposition ou avec un solde insuffisant pourrait lui infliger des pertes conséquentes. Par ailleurs, si la première transaction a fait l'objet d'une authentification 3-D Secure, les échéances suivantes ne pourront pas bénéficier du transfert de responsabilité.

En résumé

Des fonctions Sips avancées permettent de reporter le délai de remise en banque d'une transaction donnée, de manière partielle ou totale.

III. LA GESTION DE CAISSE AVEC SIPS OFFICE

La gestion de caisse consiste pour un commerçant à créer ou modifier l'état et ainsi le devenir d'une transaction réalisée sur Sips.

Les outils de gestion de caisse permettent au commerçant d'agir sur les transactions jusqu'à quinze mois après leur création. Ce délai correspond au temps de conservation des transactions Sips en base de données. Sips propose ainsi trois interfaces de gestion de caisse : Sips Office Extranet, Sips Office Server et Sips Office Batch.

- **Sips Office Extranet**, qui est fourni en standard avec toutes les offres, est une interface sécurisée accessible via l'Internet. Le commerçant se connecte grâce à un nom d'utilisateur et un mot de passe qui lui sont propres. Cette interface implique une intervention manuelle du commerçant.
- **Sips Office Server** est une interface online de serveur à serveur, qui consiste en un programme installé sur le serveur commerçant et auquel il fait appel de manière transparente, autonome et automatisée. La solution peut être totalement intégrée au système d'informations du commerçant.
- **Sips Office Batch** est une interface offline par échange de fichiers, qui permet au commerçant de collecter sur un même fichier des opérations de caisse, qu'il transmettra de manière sécurisée aux serveurs Sips. Elle permet donc une intégration complète au système d'informations du commerçant.

Ces trois interfaces permettent de créer des transactions (avec demande d'autorisation) ainsi que de générer des opérations de back-office (la gestion de caisse). Plusieurs fonctions sont disponibles pour intervenir sur les transactions afin d'optimiser la gestion de caisse des commerçants et d'améliorer le service rendu aux internautes (pour proposer par exemple du débit à l'expédition).

Les interfaces de gestion de caisse permettent :

- la consultation/le diagnostic des transactions
- la validation totale ou partielle des transactions pour qu'elles soient remisées
- l'annulation totale ou partielle des transactions avant qu'elles ne soient remisées
- le remboursement total ou partiel des transactions lorsqu'elles ont déjà été remisées
- la création ou la duplication de transactions
- Le forçage de transactions

Certaines cartes ou réseaux peuvent avoir des règles de gestion qui n'autorisent pas certaines des opérations de caisse. Pour une liste détaillée des moyens de paiement et des opérations autorisées, cf. en Annexe C page 35.

A. DESCRIPTIF DES FONCTIONS

1. LA CONSULTATION ET LE DIAG

La consultation (via Sips Office Extranet) et le Diag (via Sips Office Server) permettent de visualiser les principales caractéristiques d'une transaction, tels que le montant, la devise, le type de carte utilisé, l'état de la transaction (accord, refus, remisé, expiré) etc.

Sur Sips Office Extranet, le commerçant peut également consulter une liste de transactions à partir de plusieurs critères qu'il détermine, et même rechercher une transaction à partir d'un numéro de carte qu'il possède.

2. L'ANNULATION

Cette fonction permet de modifier le montant à envoyer en banque. Cette fonction est utile pour les commerçants qui doivent s'assurer de la présence des produits dans leurs stocks. Lorsqu'un client a commandé plusieurs produits, le commerçant peut annuler partiellement la transaction du montant d'un produit indisponible afin de débiter l'internaute uniquement du montant des produits réellement livrés.

L'annulation d'une transaction doit être effectuée avant son envoi en banque. Si la transaction a déjà été remisée en banque, l'annulation est impossible ; le commerçant conserve la possibilité de rembourser totalement ou partiellement son client.

Par défaut, la capture différée est inactive, ce qui signifie que l'envoi en banque des transactions se fait le jour même. Afin de différer la date d'envoi en banque des transactions, le commerçant doit s'assurer que ce paramètre est correctement renseigné.

Le serveur Sips contrôle deux paramètres lorsqu'une annulation est demandée:

- le **montant** : on ne peut annuler un montant supérieur au montant d'origine de la transaction.
- le **délai** pour annuler une transaction : il a été défini au moment de la demande d'autorisation. Lorsque ce délai est dépassé, la transaction est remisée et ne peut plus être annulée.

Il est possible d'annuler une transaction en plusieurs fois, tant que le délai de capture n'est pas atteint et que le solde de la transaction n'est pas nul. Dans le cas d'une annulation partielle, le solde de la transaction part automatiquement en banque à expiration du délai de capture.

Points-clefs

Une opération d'annulation ne peut être annulée

Toute transaction non annulée est envoyée en banque automatiquement à expiration du délai de capture déterminé par le commerçant

Cette fonctionnalité n'est pas disponible pour certains moyens de paiement.

3. LA VALIDATION

La fonction de validation permet de déclencher l'envoi en banque d'une transaction. Elle permet ainsi au commerçant de faire du paiement différé en débitant son client à l'expédition des produits achetés.

En choisissant le mode validation, il est nécessaire de valider chacune des transactions pour les envoyer en banque. Si un commerçant ne valide pas une transaction donnée avant que son délai de capture choisi ne prenne fin, cette transaction expirera. Il sera alors impossible de l'envoyer en banque.

Si le commerçant omet de valider dans les délais, il pourra représenter la transaction grâce à l'opération de duplication.

Le commerçant peut valider tout ou partie du montant de la transaction. Le montant validé partira en banque le jour de cette validation. Il est bien entendu impossible de valider un montant supérieur au montant d'origine de la transaction.

Points-clefs

Une opération de validation ne peut être annulée. Toutefois, le commerçant peut annuler le montant qui a été validé tant que la transaction n'a pas été envoyée en banque. Une transaction ne peut être validée qu'en une seule fois.

Toute transaction validée est systématiquement enregistrée dans la liste de transactions à remiser.

Cette fonctionnalité n'est pas disponible pour certains moyens de paiement.

4. LE REMBOURSEMENT

Le remboursement permet de créditer un internaute qui a précédemment été débité (produit non parvenu, indisponible, détérioré, retour etc.).

Le compte de l'internaute sera crédité du montant remboursé et le compte du commerçant est débité de ce même montant. Le remboursement est envoyé en banque le jour même de l'opération.

Le commerçant peut rembourser un client dans les quinze mois qui suivent sa commande. Il peut faire autant de remboursements partiels qu'il souhaite tant qu'il ne dépasse pas ce délai de quinze mois et que le solde est supérieur à zéro.

Points-clefs

Une opération de remboursement ne peut pas peut être annulée ou validée.

Le montant à rembourser ne doit pas dépasser le montant de la transaction initiale.

5. LE FORÇAGE OU L'AUTORISATION PAR TELEPHONE

Le forçage permet d'envoyer en banque une transaction qui, pour une demande d'autorisation, a reçu un *code referral* d'appel phonie. Ce code intervient lorsqu'un internaute a dépassé le plafond de dépenses autorisées de sa carte.

Pour procéder à un forçage, le commerçant doit récupérer le numéro de la carte porteur et appeler son centre d'appel referral (le numéro de téléphone du centre d'appel est fourni par la banque du commerçant). En communiquant les données de la transaction (numéro de carte, montant de la transaction), le centre d'appel contacte la banque de l'acheteur afin d'obtenir une autorisation. Si cette dernière est accordée, le commerçant peut alors forcer l'envoi en banque de la transaction.

Si la transaction forcée est en mode validation, le commerçant doit ensuite la valider pour l'envoyer en banque.

Le montant ainsi envoyé en banque est nécessairement le montant d'origine de la transaction, il n'est pas modifiable. Le commerçant a 36 jours pour forcer une transaction.

Cette fonction est facultative et doit être paramétrée sur la boutique du commerçant.

Points-clefs

Une opération de forçage ne peut être annulée. Une transaction ne peut être forcée qu'une seule fois

Cette fonctionnalité n'est pas disponible pour certains moyens de paiement.

6. LA CREATION A PARTIR D'UN NUMERO DE CARTE

Le commerçant peut lui-même effectuer une transaction qui sera créditée sur son compte. Il doit disposer du numéro et de la date de validité de la carte de l'acheteur.

Cette fonction est notamment utile lorsqu'un commerçant prend des commandes par téléphone ou reçoit des bons de commande avec des données cartes. Le commerçant peut donc réaliser ce paiement soit depuis l'interface Sips Office Extranet soit directement avec Sips Office Server.

Lorsque le commerçant utilise ces outils de création de transaction, il doit prendre toutes les mesures nécessaires à la sécurisation des données sensibles (numéro de carte notamment) et ainsi respecter la réglementation PCI/DSS (cf Annexe A page 33). C'est notamment pour éviter ces contraintes que Sips met à la disposition de ses clients des interfaces multi-canal, permettant d'accepter des transactions provenant des canaux web, mobile et téléphone.

Le commerçant doit par ailleurs être en accord avec son établissement bancaire et financier quant au canal de paiement utilisé dans le cadre de son contrat de vente à distance. Une transaction réalisée sur internet via Sips Payment Web n'a pas les mêmes caractéristiques qu'une transaction effectuée via Sips Office Extranet et doit pouvoir être distinguée comme telle. Cette dernière interface permet, à la création de la transaction, de préciser le canal utilisé pour le paiement. Le canal courrier étant le canal le plus fréquemment utilisé dans la mesure où tous les autres canaux disposent d'une solution adéquate et sans contrainte pour le commerçant.

Points-clefs

Le commerçant doit disposer des coordonnées bancaires du client

La création d'une transaction carte par Sips Office Extranet ne pourra pas bénéficier d'une authentification 3D-Secure (le client ne partageant pas son secret).

7. LA DUPLICATION

Un commerçant peut créer une nouvelle transaction à partir d'une ancienne. Il lui suffit de connaître l'identifiant ainsi que la date de création de cette ancienne transaction.

La duplication d'une transaction est possible pendant les quinze mois qui suivent la date de sa création. La transaction créée lors de la duplication est une nouvelle transaction, dont on peut changer toutes les caractéristiques à l'exception des informations carte qui ne sont pas connues du commerçant. Une transaction créée par duplication peut à son tour être dupliquée.

La duplication d'une transaction entraîne une nouvelle demande d'autorisation, sur la base du numéro de carte correspondant à la transaction d'origine. Le sort de la transaction dupliquée ne dépend en aucun cas de l'issue de la transaction d'origine : si la transaction initiale avait été refusée, il est possible qu'elle soit acceptée après une duplication, et vice-versa.

Une transaction associée à un paiement en plusieurs fois peut être dupliquée. Le paiement de cette nouvelle transaction sera effectué en une seule fois.

A titre d'exemple, si une transaction n'a – par erreur ou omission – pu être validée dans le délai de capture renseigné par le commerçant, elle a expiré et ne sera donc pas envoyée en banque. Il reste au

commerçant souhaitant rattraper cette transaction la possibilité de dupliquer cette transaction expirée. A condition qu'elle soit autorisée, cette nouvelle transaction sera envoyée en banque.

La duplication permet également au commerçant de proposer à ses clients de faire des **paiements récurrents** (abonnement) sans disposer du numéro de carte, ou proposer un paiement en complément de commande sans nouvelle saisie du client. L'opération de duplication pouvant être automatisée avec Sips Office Server ou Sips Office Batch, le commerçant peut aussi proposer du **paiement en plusieurs fois** à ses clients.

Points-clefs

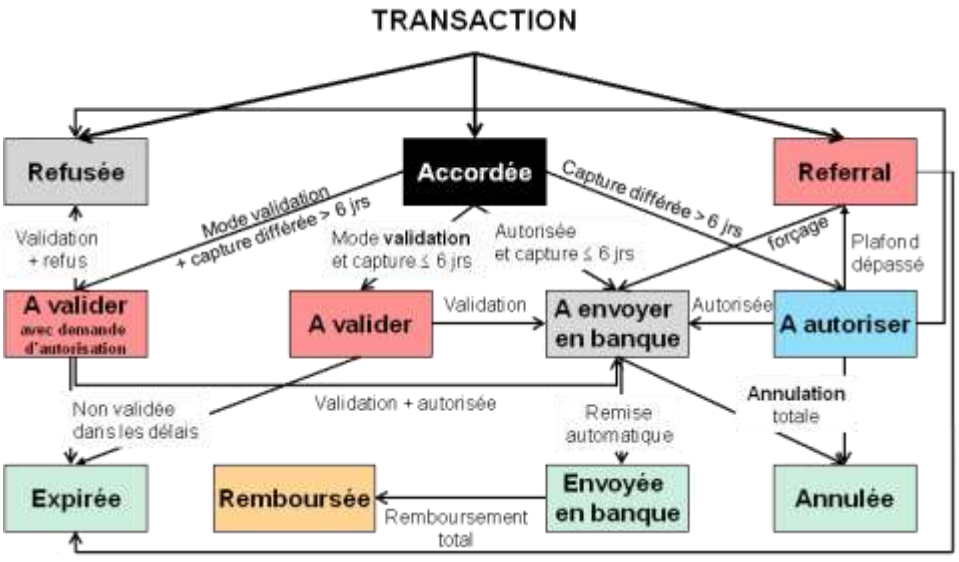
Le commerçant doit renseigner l'identifiant ainsi que la date de la transaction d'origine.

Des transactions en refus ou ayant expiré faute de validation dans les délais de capture peuvent être dupliquées.

L'opération de duplication n'est pas disponible pour certains moyens de paiement.

B. LE CYCLE DE VIE DES TRANSACTIONS

Au vu du descriptif des opérations, et étant donné qu'une même transaction peut avoir des parcours très différents en fonction surtout des préférences et des manipulations du commerçant mais aussi du fait de l'acheteur, le diagramme ci-dessous permet de suivre les états possibles dans la vie d'une transaction.



Le cycle de vie des transactions Sips

1. IDENTIFICATION ET SUIVI DES TRANSACTIONS

Le commerçant utilisant la solution SIPS peut aisément suivre la trace de chaque transaction à partir de deux données principales: le **Transaction ID** (TID) ainsi que la **date** de la transaction. Ces données permettent de suivre le parcours d'une transaction, tant à partir de l'outil de recherche de l'interface Sips Office Extranet que sur les journaux des transactions et des opérations ou encore sur un relevé bancaire. Le TID est composé de six chiffres et est être unique (pour une boutique commerçant) sur une journée.

Le commerçant peut également utiliser des **données métiers** lui permettant d'identifier les transactions, tel qu'un numéro de commande, une description, une référence de panier, un identifiant de client, etc. Ce genre de données peut être véhiculé d'un bout à l'autre du processus de paiement et se retrouver dans les différents journaux et sur l'extranet Office.

2. LA REMISE EN BANQUE

La remise en banque, qui consiste à créditer le compte du commerçant et à débiter celui du client acheteur (ou l'inverse dans le cas d'un remboursement), a lieu toutes les nuits. Ensuite, libre à chaque établissement bancaire d'appliquer une date de valeur au crédit du compte commerçant.

L'envoi en banque des transactions du commerçant dépend de la valeur du délai de capture renseigné (cf. 1 Le choix du jour et des modalités de remise en banque des transactions page *12*) ainsi que du mode d'envoi en banque choisi (validation ou annulation).

A noter que le commerçant peut suivre au jour le jour les transactions que Sips envoie en remise (pour traitement du paiement par l'acquéreur) Il suffit pour cela qu'il en fasse la demande à la cellule d'assistance.

Points-clefs

Cette liberté de choix permet au commerçant d'ajuster au plus près une transaction de la fourniture d'un bien ou service à l'Internaute. Il peut donc automatiser l'envoi en banque des transactions.

IV. LES OUTILS DE LUTTE CONTRE LA FRAUDE

Sips met à la disposition du commerçant des outils de lutte contre la fraude qui lui permettent de mieux mesurer les risques d'une transaction donnée.

Ces outils, appelés *contrôles complémentaires* peuvent pour la plupart être paramétrés de deux façons :

- En mode **pré-autorisation**, les contrôles ont un caractère décisif. Dès qu'un contrôle est négatif, la transaction est refusée et n'est pas envoyée en demande d'autorisation.

  La **demande d'autorisation** est envoyée si tous les tous les contrôles pré-autorisation sont positifs. Si la demande d'autorisation est refusée, la transaction se termine.

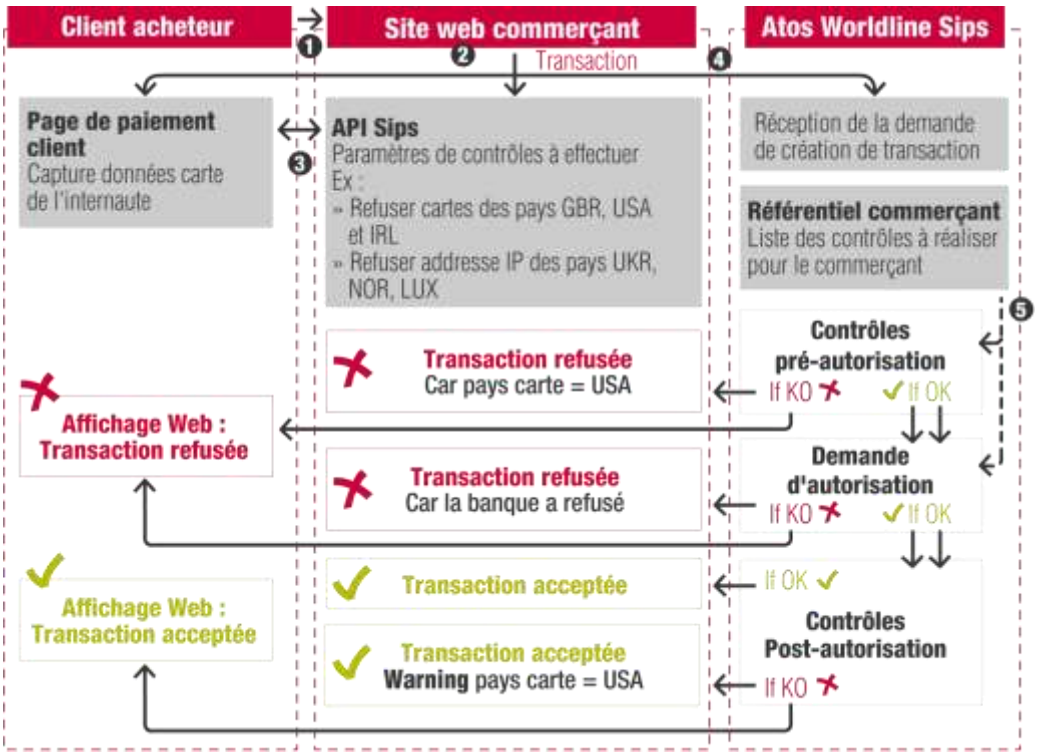
- En mode **post-autorisation**, les contrôles ont un caractère simplement informatif. Si la réponse à la demande d'autorisation est correcte, les contrôles complémentaires sont lancés mais ne font pas blocage au bon déroulement de la transaction en cas de contrôle négatif.

Points-clefs

Dans tous les cas, le commerçant est informé du résultat du contrôle en temps réel.

Le résultat des contrôles est restitué dans les journaux et affiché sur l'extranet.

Avec une transaction 3-D secure, l'authentification est effectuée avant les contrôles de pré-autorisation.



Les contrôles complémentaires peuvent avoir plusieurs objectifs :

A. LOCALISER LE CLIENT GÉOGRAPHIQUEMENT

1. LE CONTROLE DU PAYS D'ORIGINE DES CARTES

Ce contrôle permet à un commerçant :

- En pré-autorisation, de refuser les cartes bancaires émises par un établissement financier établi à l'étranger.
- En post-autorisation, d'obtenir une information quant à la nationalité d'une carte. Le commerçant est informé en temps réel si la carte est originaire d'un pays prédéterminé ou si elle est étrangère à ce pays. A posteriori, dans le reporting quotidien des transactions, il est informé du pays d'émission de la carte.

Ce contrôle complémentaire est souvent utilisé dans les solutions de scoring qui mettent en rapport la nationalité d'une carte avec le pays de destination d'un bien commandé et/ou la langue choisie par l'acheteur sur le site commerçant. Le commerçant peut fournir une liste des pays autorisés (liste positive) ou une liste de pays refusés (liste négative) qui serviront de référence.

2. LE REPERAGE DU PAYS DE L'ADRESSE IP DU CLIENT

Ce contrôle, disponible seulement en post-autorisation, permet au commerçant de récupérer le pays associé à l'adresse IP du fournisseur d'accès de l'internaute. Cette fonction se base sur l'adresse IP de l'appelant.

Une incertitude peut persister sur le pays de l'internaute essentiellement en raison de l'attribution dynamique d'adresses IP par certains fournisseurs d'accès ou d'adresses IP dynamiques. Atos Worldline met régulièrement à jour sa base de données d'adresses IP. Le taux de fiabilité annoncé par le fournisseur de notre base de données d'adresses IP est de plus de 95%. A noter que le pays restitué n'est pas forcément du pays où se situe physiquement l'internaute.

Cette information est calculée avant même l'engagement dans un premier contrôle local et n'a aucune conséquence sur le déroulement des autres contrôles complémentaires ou sur la demande d'autorisation.

3. COMBINAISON DES CONTROLES PAYS DE LA CARTE ET DE L'ADRESSE IP

Sips propose également un contrôle comparant le pays d'émission de la carte du client avec le pays de l'adresse IP utilisée. Le commerçant peut demander au serveur Sips de l'alerter lorsque les pays ne correspondent pas.

B. CONTROLER L'ACTIVITE DE LA CARTE DU CLIENT : LE CONTROLE D'EN-COURS

Ce contrôle permet à un commerçant d'être informé (en post-autorisation) ou de limiter (en pré-autorisation) soit le montant maximal d'un achat sur une boutique soit le nombre ou le montant total des achats réalisés avec un même numéro de carte sur une ou plusieurs boutiques Sips et sur une période donnée.

Ainsi, le commerçant définit une période glissante de X jours sur laquelle le contrôle est effectué, ainsi que : soit un nombre soit un montant maximal d'achats sur cette période.

Ce contrôle est également un complément idéal des solutions de scoring qui affectent un risque plus important à un client inconnu ayant déjà réalisé une ou plusieurs transactions sur une très courte période.

✍ **A noter**

La période glissante maximale de contrôle est de 30 jours.

C. CONTROLER LA PRESENCE DE CARTES DANS DES LISTES POSITIVES

1. LE CONTROLE EN LISTE GRISE COMMERÇANT

Sips permet au commerçant de créer et gérer sa propre liste grise de numéros de cartes à risque. Via l'interface Office Extranet, le commerçant peut ajouter et gérer des numéros de cartes correspondant à des clients avec lesquels il aurait eu par le passé des difficultés de paiement (l'ajout d'une carte en liste grise peut se faire soit à partir d'un numéro de carte soit à partir d'une référence de transaction).

Le commerçant peut affecter à chaque numéro de carte inscrit dans sa liste un motif particulier (client douteux, impayé, etc).

Ce contrôle sera donc utilisé par les commerçants qui souhaitent s'assurer que la carte utilisée par l'acheteur n'est pas référencée dans une liste des cartes *indésirables* appelée *liste grise des cartes*.

Le client peut inscrire les numéros de carte individuellement ou bien enregistrer des plages entières de cartes. Le commerçant sera ainsi informé (en post-autorisation) ou refusera systématiquement (en pré-autorisation) l'utilisation d'un numéro de carte enregistré ou appartenant à la plage de BIN de sa liste grise.

2. LE CONTROLE EN LISTE NOIRE

Ce contrôle permet au commerçant de décider d'honorer ou non une prestation payée par un porteur d'une carte en opposition.

Le commerçant peut demander à ce que ce contrôle soit réalisé à chaque validation de transaction. En cas de débit à l'expédition, la validation peut intervenir plusieurs jours après la demande d'autorisation ; le risque que la carte du porteur ait fait l'objet d'une mise en opposition est donc plus élevé. Ce contrôle permettra donc au commerçant de limiter les risques d'un débit sur une carte perdue ou volée.

En France, le fichier des cartes en opposition utilisé est le fichier OPPOTOTA (**Oppo**sition **Tota**le). Il contient toutes les cartes françaises et étrangères en opposition déclarées par les réseaux (CB, Visa et Mastercard). Il y a plus de 5 millions de cartes en opposition répertoriées. Le fichier Oppotota est mis à jour à 14 reprises au cours d'une journée.

D. CONNAITRE LES PROPRIETES DE LA CARTE

1. LES CARACTERISTIQUES DE LA CARTE BANCAIRE

Cette information permet au commerçant de récupérer des caractéristiques de la carte bancaire utilisée pour le paiement. Elle n'est valable que pour les cartes CB, Visa et Mastercard.

Les caractéristiques renvoyées sont :

- le nom de la banque émettrice (pour certains pays)
- le code pays de la banque émettrice (code iso alphabétique 3166)
- le code produit (par exemple Maestro, Electron, Visa Gold, Mastercard Corporate Card, …)

Cette information est calculée avant même l'engagement dans un premier contrôle local et n'a aucune conséquence sur le déroulement des autres contrôles complémentaires ou sur la demande d'autorisation.

2. DETECTION DES E-CARTES BLEUES FRANÇAISES

La e-Carte Bleue, la carte virtuelle dynamique proposée par la SAS Carte Bleue via ses membres, établissements bancaires Français, permet à un porteur de carte de générer de manière dynamique un numéro de carte pour chaque achat effectué à distance. Le numéro de carte généré par son établissement bancaire lui permet ainsi de faire un achat pour un montant donné et chez un seul commerçant.

Ces cartes ne permettant pas (ou rarement) à un commerçant de débiter plusieurs fois son client (en mode abonnement ou paiement en plusieurs fois avec un différé important), le commerçant peut souhaiter en être informé. Le commerçant peut également souhaiter être informé de (ou refuser) l'utilisation d'une e-carte lorsqu'il propose un paiement à distance avec retrait en magasin/guichet sur présentation de la carte utilisée sur internet (le client n'ayant qu'un numéro et non une carte).

Ce contrôle permet ainsi au commerçant de proposer à son client un moyen de paiement alternatif ou de l'informer des limites en cas de paiement par e-Carte Bleue (pas d'abonnement possible par exemple).

3. DETECTION DES CARTES A AUTORISATION SYSTEMATIQUE

La CAS (Carte à Autorisation Systématique) est une carte devant faire l'objet d'une demande d'autorisation, quels que soient le montant de la transaction et le canal de vente (paiement de proximité ou à distance). La demande d'autorisation permet pour ces cartes de vérifier la provision disponible sur le compte de dépôt du client afin d'en vérifier la solvabilité.

La détection des CAS (parmi lesquelles les cartes Electron, Maestro ainsi que les cartes cadeau) permet ainsi au commerçant de mieux cerner la qualité de l'acheteur.

✍ **A noter**

Ces contrôles complémentaires permettent au commerçant de mieux apprécier les risques associés à une transaction.

E. L'APPORT DE 3-D SECURE

Pour les commerçants ayant souscrit au service 3-D Secure, désigné par les réseaux Visa et MasterCard sous les appellations respectives « Verified By Visa » et « MasterCard SecureCode », la transaction de paiement fait également l'objet d'une authentification du titulaire de la carte, au cours de laquelle la banque émettrice de la carte ainsi que le réseau (Visa ou Mastercard) vont intervenir.

Le programme présente plusieurs avantages. D'un côté, l'internaute est assuré de communiquer ses coordonnées bancaires à sa banque. De l'autre, le commerçant est assuré que son client est bien le porteur vu qu'il aura été authentifié par sa banque. Pour ce type de transaction, le commerçant peut bénéficier de la garantie de paiement, sous certaines conditions dépendantes de la réglementation bancaire en vigueur.

✍ **A noter**

L'authentification via 3D-Secure est totalement intégrée à l'interface Sips Payment et ne nécessite aucun développement supplémentaire pour le commerçant.

Avec L'interface Sips Office Server, le commerçant dispose d'un kit de développement lui simplifiant la mise en place.

La transfert de responsabilité dont bénéficie le commerçant est indiqué dans le reporting Sips par le champ 3D_LS (pour *Liability Shift*). Il n'est pas systématique et ne doit pas supplanter les contrôles de lutte contre la fraude mis en place par le commerçant. Un taux d'impayés trop important pourrait remettre en cause l'acceptation des moyens de paiement par le commerçant.

3-D Secure ne permet par ailleurs pas de répondre à toutes les cinématiques de paiement. Il n'est pas effectif notamment pour :

- Les paiements différés de plus de 6 jours

- Les paiements en plusieurs fois ou capturées en plusieurs échéances
- Les transactions récurrentes (par l'utilisation de la fonction de duplication par exemple)
- Les paiements hors internet (saisie manuelle par le commerçant, par SVI sécurisé, créés par le commerçant, etc)
- Les transactions ayant été forcées (opération de forçage)

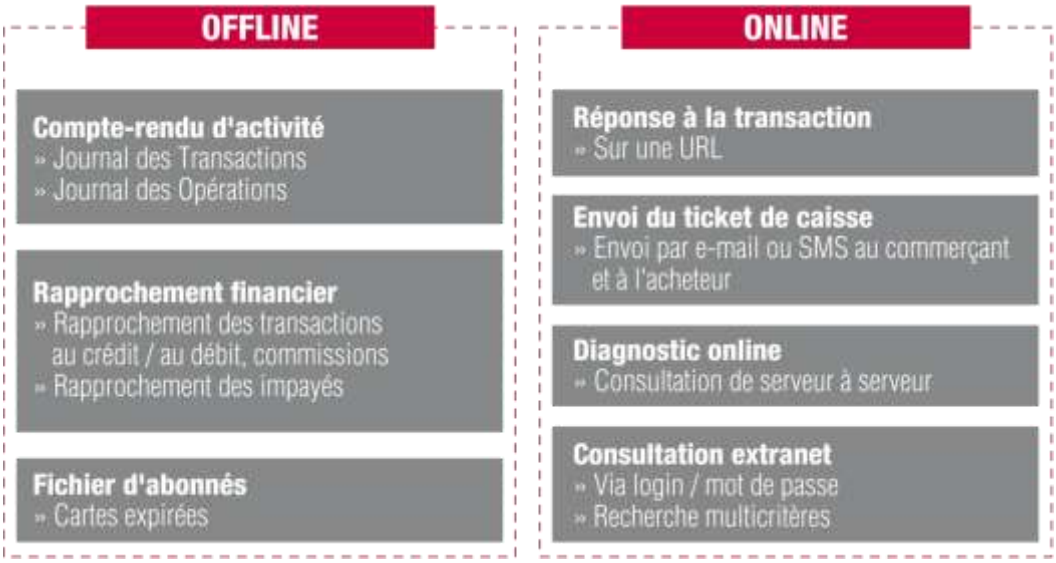
Pour plus d'information sur les outils de lutte contre la fraude, nous vous invitons à consulter ***Le guide des contrôles complémentaires***.

V. LE REPORTING

Le reporting sur Sips est très riche : le commerçant dispose de plusieurs outils lui permettant de suivre à la trace les transactions effectuées sur sa boutique : les réponses automatique et manuelle, les journaux de fonds, l'outil de consultation des transactions (Office Extranet) et le diag (Office Server), le journal de rapprochement des transactions ainsi que le journal de rapprochement des impayés. Il est donc bien informé de ce que ses clients lui achètent ainsi que ce qui sera crédité ou débité sur son compte.

A noter

Le commerçant peut insérer des **données métier** qui lui sont propres dans les flux de transactions et opérations. Sips les lui retournera inchangées ; il pourra ainsi retrouver ces informations jusqu'en fin de chaîne, dans toutes les formes de reporting existantes.



Vue d'ensemble des différentes formes de reporting Sips

A. LA REPONSE AUTOMATIQUE ET LA REPONSE MANUELLE

Sur Sips Payment, le résultat de la demande d'autorisation d'une transaction est immédiatement envoyé par Sips à une adresse URL choisie par le commerçant, qui peut ainsi constituer un historique des transactions en temps réel : c'est l'objet de la **réponse automatique**. Cette adresse doit faire référence à un programme du commerçant qui réceptionne et traite les informations retournées par le serveur Sips

Le commerçant peut également recevoir la **réponse manuelle** si l'internaute clique sur le bouton *« Retour à la boutique »* des pages de paiement Sips. Il sera redirigé sur une page du commerçant qui reçoit de

nouveau le résultat de la demande d'autorisation et peut afficher un message personnel en fonction de ce résultat.

A noter que le contenu des réponses automatique et manuelle de Sips Payment Web est identique. Le commerçant peut également profiter de ces réponses pour afficher lui-même le ticket de paiement à son client.

Avec Sips Office Server, il n'existe pas de réponse manuelle étant donné que le commerçant gère les écrans de capture des informations carte. Aussi, le commerçant obtient systématiquement une réponse à ses requêtes.

L'utilisation de Sips Payment Web provoquant l'envoi d'une réponse sur une URL, et étant donné que l'envoi dépend d'une part de la validation de la transaction par l'internaute et d'autre part du bon fonctionnement de l'internet et des réseaux, le commerçant garde la possibilité d'utiliser en complément le composant Diag de Sips Office Server afin d'interroger la base de données Sips sur l'issue du paiement. A titre d'exemple, si le commerçant n'a pas reçu la réponse automatique au bout d'un temps déterminé, il pourra utiliser le composant Diag pour demander à la base Sips d'Atos Worldline si la transaction est toujours en cours, terminée et quel est son statut.

B. LES JOURNAUX DES TRANSACTIONS ET DES OPERATIONS

L'offre de paiement Sips comprend l'envoi de deux journaux distincts : l'un des **transactions** de paiement effectuées par les clients, l'autre des **opérations** (validation, remboursement, etc) effectuées par le commerçant à l'aide des interfaces Office.

En résumé

Ces deux journaux permettent au commerçant d'effectuer un suivi complet de l'activité de sa boutique en ligne, tant du point de vue des ventes que pour la vérification de ses relevés bancaires.

Pour la majorité des commerçants, ces journaux sont envoyés une fois par jour, le matin, entre 4h00 et 6h00, et contiennent la liste des transactions/opérations effectuées depuis l'envoi des journaux de la veille. Le journal est envoyé même si aucune transaction/opération n'est intervenue la veille.

Ces informations sont généralement envoyées par e-mail en fichier attaché (le client peut en choisir le nom). Par défaut, les fichiers ont pour identité *transactions.xls ou operations.xls.*

Les journaux sont au format dit *Excel*, constitué d'autant de colonnes qu'il y a de champs, séparés par un même caractère et aisément exploitable par le logiciel du même nom.

Points clés

Le commerçant peut également recevoir dans son journal des opérations la liste des opérations de remise en banque réalisées par le service Sips. Il doit pour cela en faire la demande auprès du service clients.

C. LA CONSULTATION

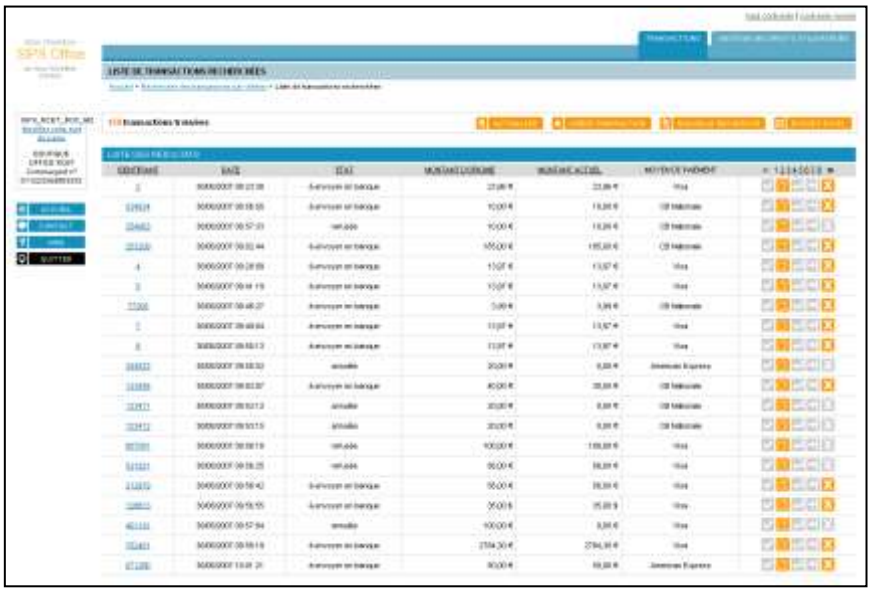
Afin d'améliorer le suivi des transactions, le commerçant dispose également d'un outil de consultation des paiements effectués sur sa boutique en ligne, via l'extranet Office Client. Il peut ainsi :

- consulter une transaction, à partir du numéro de la transaction ou de la carte ainsi que de la date de la transaction ;
- consulter une liste de transactions, à partir d'un ensemble de critères (numéro de transaction, date, référence commerçant, statut de la transaction, etc).

La consultation d'une liste de transactions l'autorise à renseigner un grand nombre de critères de recherche, tels que la date, l'identifiant, l'état de la transaction, le type de carte, la devise. La page de résultat lui permet de consulter l'ensemble des informations rattachées à une transaction précise.

Le commerçant peut ainsi rechercher :

- une transaction à partir de son identifiant
- une transaction à partir du numéro de carte
- une liste de transactions à partir de multiples critères



La page de résultats de la recherche de transactions

En utilisant Sips Office Server, le commerçant peut interroger de manière unitaire la base de données Sips en utilisant la fonction DIAG.

✍ **A noter**

Le back-office étant d'une grande richesse, il offre au commerçant tous les outils de gestion de caisse nécessaires pour suivre et agir au mieux sur ses transactions.

D. LES JOURNAUX DE RAPPROCHEMENT

1. LES JOURNAUX DE RAPPROCHEMENT DES TRANSACTIONS

Atos Worldline a mis en place, avec certains établissements bancaires et financiers partenaires, un système de rapprochement des transactions réalisées sur Sips des débits et crédits sur le compte du commerçant.

Cette solution permet au commerçant de s'assurer que toutes les transactions acceptées et envoyées en remise par Sips sont bien créditées sur son compte.

L'établissement partenaire met à disposition quotidiennement un fichier Relevé de Gestion Informatique, qui contient toutes les transactions créditées et débitées sur les comptes de ses commerçants. Sips collecte ce fichier et le rapproche des transactions (débits et crédits) envoyées en remise. A cela vont s'ajouter des données propres à la transaction Sips (références transaction, montant, devise), des données métier (références client ou de la commande) ainsi que des données financières (montant brut et net de commissions).

Ainsi, le commerçant est informé en détail des transactions rapprochées et est alerté en cas de non-rapprochement. Une transaction non-rapprochée génère une alerte que l'établissement bancaire ou financier pourra rapidement traiter. A partir de ce rapprochement, Sips envoie un *Journal de Rapprochement des Transactions* (JRT) à chaque commerçant.

2. LES JOURNAUX DE RAPPROCHEMENT DES IMPAYES

Les journaux de rapprochement des impayés contiennent les transactions effectuées sur le site du commerçant et créditées sur son compte et apparaissent désormais comme impayées (par exemple en raison d'une contestation client). Sips recevant le fichier des impayés de la banque du commerçant, un rapprochement avec ses transactions permet d'enrichir les données de la banque avec le contexte Sips de la transaction (numéro de la transaction, références propres au commerçant, etc.).

Points clés

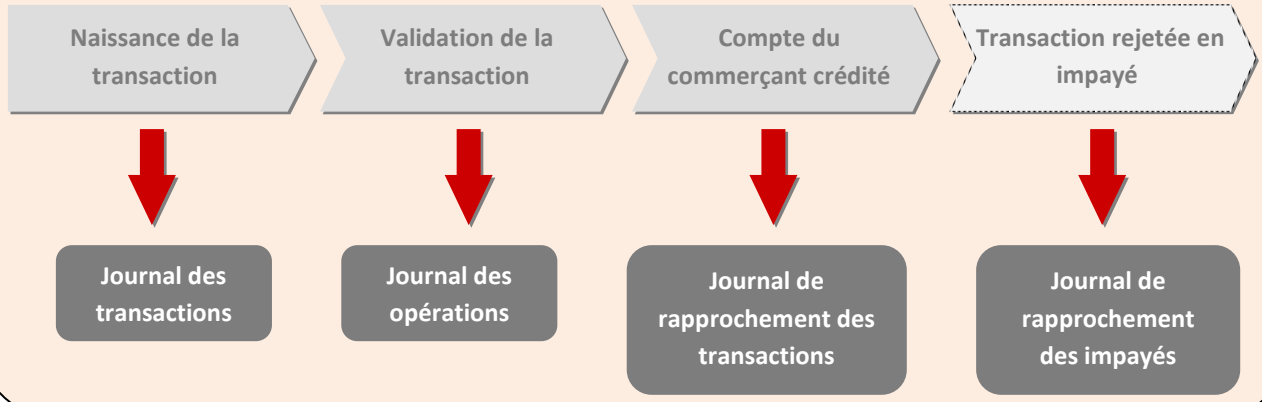
L'outil de rapprochement des transactions et des impayés est disponible pour un certain nombre d'établissements bancaires et financiers partenaires. Nous vous invitons à nous consulter pour valider que votre établissement le propose

Certains moyens de paiement ne font pas partie des journaux de rapprochement.

E. LES FICHIERS D'ABONNÉS

Les fichiers d'abonnés dont la carte arrive prochainement à expiration (2 mois) permettent au commerçant utilisant la solution d'abonnement de proposer à ses clients un renouvellement de la carte enregistrée sur les serveurs Sips. Le fichier permet ainsi aux commerçants d'anticiper un refus d'autorisation sur des cartes expirées.

La traçabilité d'une transaction dans le reporting Sips.



VI. ANNEXES

A. LA SECURITE DES DONNEES : PCI/DSS

PCI/DSS est un standard de sécurité international dont les objectifs sont d'assurer la confidentialité et l'intégrité des données des porteurs de cartes, et ainsi de sécuriser la protection des données cartes et de transaction. Les e-marchands ainsi que les prestataires de paiement sont tenus de s'y conformer, à des degrés divers en fonction de l'importance de leur activité. La solution Sips est ainsi certifiée PCI/DSS depuis 2006.

Les e-marchands Sips sont également tenus de se conformer à ce standard de sécurité. Nous vous invitons à évoquer ce sujet avec votre établissement acquéreur. La protection des données des porteurs de carte étant au cœur de ce standard de sécurité, Sips contribue à faciliter au maximum la mise en conformité des marchands :

- Par l'interface Sips Payment, les données des porteurs de carte ne sont pas connues du marchand ;
- Par la personnalisation très poussée offerte sur ces pages de paiement sécurisées par Sips, de la personnalisation graphique à la personnalisation de l'URL de paiement ;
- Par les facilités de paiement proposées (paiement différé à l'expédition, paiement en plusieurs fois) réalisées à partir d'un identifiant de transaction ;
- Par les fonctions d'abonnement et de paiement récurrent disponibles.

De ce fait, un e-commerçant peut exercer son activité sur de multiples canaux (internet, téléphone/SVI, mobile) et proposer des facilités de paiement, du paiement par abonnement ou en plusieurs fois, sans avoir à connaître des données sensibles des porteurs de carte. Ce qui permet de grandement faciliter le processus de certification PCI/DSS de l'e-commerçant.

Pour plus d'information sur PCI/DSS :

https://www.pcisecuritystandards.org/

B. LA SECURITE DE VOTRE IDENTITE SIPS

Les clefs de la sécurité Sips reposent sur quatre piliers essentiels : **l'authentification du commerçant**, la **demande d'autorisation** auprès de la banque du porteur de la carte ainsi que la **confidentialité** des données, qui transitent chiffrées sur l'Internet (numéro de carte, date de validité etc).

Afin d'éviter toute altération des messages échangés, Atos Worldline vérifie également leur **intégrité**.

Le Certificat Sips caractérise de façon unique chaque commerçant, le partage de ce même secret permet l'authentification du commerçant par le serveur de paiement Sips. Le commerçant est donc responsable de sa conservation et doit donc prendre toutes les précautions sur le stockage et l'utilisation de ce fichier certificat. Le commerçant doit donc faire le nécessaire pour :

- En restreindre l'accès sur votre serveur
- Le sauvegarder de manière chiffrée
- Ne jamais le copier sur un disque non sécurisé
- Ne jamais l'envoyer (e-mail, courrier) de manière non sécurisée

La compromission d'un certificat et son utilisation par un tiers malveillant perturberait le fonctionnement normal de la boutique, et pourrait notamment :

- générer des transactions non justifiées sur le site du commerçant
- provoquer des opérations de caisse injustifiées (des remboursements par exemple)

En cas de compromission du fichier certificat, le commerçant doit désactiver la fonction paiement et demander un renouvellement de certificat à Atos Worldline.

C. LES MOYENS DE PAIEMENT ACCEPTES

Réseau d'appartenance	Cartes / moyens de paiement	Fonctions autorisées						Validité demande d'autorisation
		C	A	V	R	F	D	
Les cartes interbancaires internationales								
MASTERCARD	Carte MASTERCARD	√	√	√	√	√	√	6 jours
VISA	Carte VISA	√	√	√	√	√	√	6 jours
Les cartes accréditives et corporate internationales								
American Express	American Express	√	√	√	√	√	√	6 jours
DINERS	Diners Club	√	√	√	√	√	√	6 jours
JP : JCB - Japanese Credit Bureau	JCB	√	*	√	√	√	√	30 jours
Les moyens de paiement avec acceptation nationale								
FR : Carte Bleue	Carte Bleue Nationale	√	√	√	√	√	√	6 jours
BE : Banksys	Bancontact/Mistercash	√	*	*	*	*	*	6 jours
DE : Débit direct ELV	ELV (Elektronische Lastschriftenverarbeitung)	√	√	√	√*	*	√	-
UK : NatWest, Barclays	Solo (Visa Electron) Delta (Visa)	√	√	√	√	*	√	6 jours
UK : NatWest, Barclays	Switch (Maestro)	√	√	√	√	*	√	6 jours
Les cartes privatives et d'enseignes								
CETELEM	Aurore	√	*	*	√	*	√	6 jours
COFIDIS	4 Etoiles	√	√	√	√	*	√	99 jours
COFINOGA	COFINOGA, BHV, Casino Géant, CDGP, GL, Gosport, Monoprix, MrBricolage, Soficarte, Sygma	√,	√	√	√	*	*	21 jours
FINAREF	Finaref, FNAC, Cyrillus, Printemps, Kangourou, Surcouf, Pocketcard (Belgique), Conforama, Nuitea, Clubmed, OK Shopping, La Maison de Valérie	√	√	√	√	√	√	6 jours
FRANFINANCE	Pluriel, Toysrus, Connexion, Hypermedia, Delatour, Nouvelles Frontières, Serap, Bourbon, Aubert, Music and Film, Internity, Expert, Digital, Helium, Golf Plus, Pixmania, Digixo, Mobiscount, Ubaldi	√	√	√	√	√	√	90 jours
S2P	PASS	√	*	*	√	*	*	6 jours
	PASS2	√	√	√	√	*	√	6 jours
	CBPASS	√	√	√	√	*	√	6 jours
Les solutions de crédit en ligne								
CETELEM	Presto	√	*	*	*	*	*	-
COFIDIS	1Euro.com	√	*	*	*	*	*	-
FRANFINANCE	Solution Sprint Secure	√	*	*	*	*	*	-
Les autres moyens de paiement								
PayPal	PayPal	√	√	√	√	*	*	-

√ Fonction active	
* Fonction indisponible	

C: Consultation	**R**: Remboursement
A: Annulation	**F**: Forçage
V: Validation	**D**: Duplication

D. LES DEVISES ACCEPTÉES

Toutes les devises peuvent être potentiellement acceptées sur Sips. Entre autres, et pourvu que le contrat commerçant (avec son acquéreur) les accepte :

Code Devise	Nom Devise
978	Euro
840	Dollar Américain
756	Franc Suisse
826	Livre Sterling
124	Dollar Canadien
392	Yen Japonais
484	Peso Mexicain
949	Livre Turque
036	Dollar Australien
554	Dollar Néo-Zélandais
578	Couronne Norvégienne
986	Real Brésilien
032	Peso Argentin
116	Riel Cambodgien
901	Dollar de Taïwan
752	Couronne Suédoise
208	Couronne Danoise
410	Won Coréen
702	Dollar de Singapour
952	Franc CFA
953	Franc Polynésien

E. GUIDE D'ADMINISTRATION DES BOUTIQUES

1. INSCRIPTION DE BOUTIQUE


J - 16:00 maxi


J+2


10:30

Cette opération a pour objectif de déclarer une boutique en pré-production et fait suite à un formulaire d'inscription complété et envoyé par le commerçant.

Une fois inscrit et les tests de démonstration effectués, le commerçant effectue des tests en pré-production avec son certificat de production définitif en utilisant de vrais numéros de carte. Des demandes d'autorisation réelles sont alors effectuées sans remise bancaire (veillez à ne pas utiliser des montants importants afin de ne pas impacter le plafond de votre carte).

Les inscriptions sont enregistrées les jours ouvrés à JO+2 à 10h30 à compter de la date de réception du formulaire d'inscription, dûment rempli. Les formulaires doivent être transmis avant 16h00.

2. INSTALLATION DE LOGO ET TEMPLATE


J - 16:00 maxi


J+1


10:30

Le client peut envoyer à Atos Worldline ses préférences graphiques pour personnaliser ses pages de paiement.

Cette opération est effectuée pendant les jours ouvrés à JO+1 à 10:30. Les logos doivent être envoyés **par e-mail** les jours ouvrés avant 16:00.

3. PASSAGE EN PRODUCTION


J - 16:00 maxi


J+1


10:00

Afin de valider son passage en production, le commerçant envoie un Procès Verbal de recette dûment rempli et signé, par fax. Il doit être transmis à JO-1 et avant 16h00 la veille du démarrage. Toute demande de passage en production reçue après cet horaire sera prise en compte à JO+2.

Attention, nous n'effectuons pas de démarrage les Vendredi, Samedi, Dimanche, jours fériés ainsi que la veille de jours fériés.

Les demandes transmises le jeudi après 16:00 et le vendredi avant 16:00 seront prises en compte le lundi suivant. Le passage en production s'effectue à 10:00, du Lundi au Jeudi, et sous réserve que le commerçant a bien effectué au moins un test de pré-production positif (une demande d'autorisation acceptée par la banque).

Atos Worldline envoie une confirmation (mail ou courrier) au client pour lui notifier ce démarrage.

Le lendemain, le commerçant reçoit son premier journal de fonds.

Pour la création de transaction à partir d'Office Client, un test en pré-production doit être réalisé pour le passage en production si le client n'a pas effectué de test avec Sips Payment.

4. MODIFICATIONS D'INSCRIPTION

Les modifications d'inscription concernent les modifications de contrat, de format ou d'adresse destinataire de journaux de fonds, d'ajouts de carte, d'ajout ou de modification d'utilisateurs office, etc.

Ces opérations sont effectives les jours ouvrés à JO+1 à 10h00, si la demande de modification d'inscription est parvenue avant 16h00.

En synthèse :

	Prise en compte	Délai	Horaire de passage de la procédure
Installation logos	avant 16h00	JO+1	10h30 tous les jours ouvrés
Passage en production		JO+1	10h00 tous les jours ouvrés **sauf** le Vendredi et la veille de jours chômés
Modification inscription		JO+1	10h00 tous les jours ouvrés
Inscription boutique		JO+2	10h30 tous les jours ouvrés

Toutes les demandes doivent être communiquées au Service Clients dont vous trouverez les coordonnées en page 41.

F. LEXIQUE DES TERMES UTILISÉS

3-D Secure : Programme (Visa et Mastercard) d'authentification tripartite (émetteur / réseau / acquéreur) de l'internaute, qui s'identifie en ligne avec un mot de passe pendant la phase de paiement. Le commerçant adhérant à ce programme, via sa banque, bénéficie d'une protection contre certains impayés.

Acheteur : L'acheteur est un utilisateur d'Internet qui se connecte sur le site Web du Commerçant et effectue le paiement d'un bien ou d'un service donné.

Acquéreur : Etablissement financier (ou son agent) qui reçoit de l'accepteur (le commerçant, son prestataire de paiement) les données financières relatives à une transaction et introduit ces données dans un système d'échange.

Capture : Voir *remise.*

Certificat de Production : Certificat composé d'une clé de sécurité permettant d'assurer la confidentialité et l'intégrité du paiement sur Internet.

Commerçant : Personne physique ou morale tenant une boutique sur Internet. Le commerçant Sips est inscrit auprès d'Atos Worldline et bénéficie du service de paiement sécurisé par Internet.

CVV2, CVC2 ou CBN2 (Cryptogramme visuel) : Clef sur trois chiffres numériques située sur le panneau signature au dos des cartes VISA, MASTERCARD et CB nationales. Il ajoute un niveau de sécurité supplémentaire dans la vente à distance. Sur les cartes American Express, le cryptogramme est sur 4 chiffres (le 4DBC).

Demande d'autorisation : vérification auprès des institutions financières de la validité de la carte du porteur. Outre la vérification du numéro de carte, cette demande consiste à vérifier que la carte est bien un moyen de paiement valide et qu'elle ne fait pas l'objet d'une mise en opposition.

Emetteur (de carte) : Organisme (ou son agent) qui a émis une carte d'identification au profit d'un porteur de carte.

Hébergeur : Société de services hébergeant un ou plusieurs sites Internet sur ses propres serveurs, connectés à l'Internet. Un hébergeur propose parfois des services de création/gestion de site Internet.

Internaute : Client du Commerçant sur Internet.

Journal de rapprochement des transactions : journal envoyé quotidiennement et mettant en correspondance les transactions réalisées sur Sips et envoyées en remise des transactions effectivement créditées ou débitées sur le compte bancaire ou financier du commerçant.

Journal des opérations : journal généralement envoyé par e-mail quotidiennement au commerçant et contenant toutes les opérations effectuées par celui-ci à partir de l'interface Office Client (opérations de remboursement, validation, annulation etc.) depuis l'envoi du journal de la veille.

Journal des transactions : journal envoyé quotidiennement au commerçant, généralement par e-mail, contenant l'ensemble des transactions effectuées sur un site donné depuis l'envoi du journal de la veille.

Journal de rapprochement des transactions : journal pouvant être envoyé quotidiennement au commerçant. Il permet de rapprocher les transactions réalisées par le commerçant sur sa boutique Sips des transactions effectivement traitées par le centre de traitement commerçant de son établissement bancaire. Il correspond à ce qui sera effectivement crédité/débité sur son compte et alerte le commerçant en cas de transaction non rapprochée. Ce journal permet de faciliter la comptabilité des commerçants.

Merchant_ID: Identifiant commerçant unique utilisé par Atos Worldline, formé à partir du numéro de SIRET préfixé d'un zéro.

Paiement Sécurisé : Les transactions effectuées sur le réseau Internet sont protégées contre les interceptions non autorisées et également contre les modifications et altérations non autorisées du contenu original des messages.

Pré-production : phase pendant laquelle le commerçant utilise le certificat de production qui lui a été délivré à la création de sa boutique Sips. Les tests de pré-production permettent de valider que le contrat commerçant est bien opérationnel.

Remise : Opération d'envoi en banque de transactions, signifiant le crédit/débit du compte du commerçant et le débit/crédit du compte de l'internaute. La capture d'une transaction traduit son envoi en remise, donc son envoi vers son centre de traitement commerçant bancaire.

Réseaux (monétiques) : Regroupement d'organismes émetteurs de moyens de paiement ayant conclu un accord d'échange réciproque des mouvements porteur(émetteur) et commerçant (accepteur).

Transaction ID : Identifiant caractéristique de chaque transaction. Le commerçant peut suivre le parcours de chaque transaction à partir du TID ainsi que de la date de ladite transaction.

Sips : Solution internationale et multi-canal de paiement sécurisé proposée par Atos Worldline.

G. PLUS D'INFORMATIONS & CONTACTS

Pour plus d'informations sur les solutions Sips, il existe d'autres documents fonctionnels de référence :

- La présentation des interfaces Sips
- Le guide utilisateur de Sips Office Extranet

Par ailleurs, il existe des documents plus techniques sur la solution :

- Les guides d'implémentation des interfaces (Guides du programmeur, d'installation et dictionnaire des données)
- Description des journaux de fonds (des transactions, des opérations et de rapprochement)
- Guide des contrôles complémentaires de lutte contre la fraude
- Guide de personnalisation des pages de paiement

Les offres Sips faisant l'objet de constantes évolutions, nous vous invitons à contacter votre interlocuteur technico-commercial pour tout renseignement sur les fonctionnalités ici décrites ainsi que sur vos besoins complémentaires. Des dossiers d'actualité sont également à votre disposition sur notre site internet :

www.sips.atosorigin.com

Contacts

Pour obtenir toute information complémentaire à propos de Sips, vous pouvez contacter :

Un chargé de clientèle pour un **support commercial et fonctionnel :**

- par téléphone au **0 811 10 70 72** (coût d'un appel local).
- par e-mail à l'adresse **Sips-contact@atosorigin.com**

Notre service clients pour un **support technique :**

- par téléphone au **0 811 10 70 33** (coût d'un appel local).
- par fax au **0 811 370 981** (coût d'un appel local).
- par e-mail à l'adresse **Sips@atosorigin.com**

Si vous êtes déjà client, nous vous inviterons à nous indiquer votre numéro de marchand (Merchant_ID), la phase d'installation (démo, pré-production ou production) ainsi que l'interface de paiement de votre boutique. Ces informations nous permettront de vous identifier rapidement et de mieux répondre à vos besoins.