Sips e-payment solution

Contrôle de lutte contre la Fraude

Guide d'utilisation

Version 2.06 – Mai 2013

Contact

Téléphone : +33 (0) 0811 10 70 33

Mail : sips@atos.net

SOMMAIRE

1. INTRODUCTION

1.1 A PROPOS DES FONCTIONS DE CONTROLES DE LUTTE CONTRE LA FRAUDE

Afin d'aider le commerçant dans sa lutte contre la fraude, **Atos Worldline** offre dans la solution **Sips** la possibilité, lors du paiement par l'internaute, d'associer des contrôles complémentaires à la demande d'autorisation.

Cette offre repose aujourd'hui sur 14 possibilités de contrôles :

- contrôle d'en-cours carte,
- contrôle d'en-cours IP,
- contrôle d'en-cours CustomerID,
- contrôle du nombre maximum de cartes par CustomerID,
- contrôle du nombre maximum de CustomerID par carte,
- contrôle de liste grise de cartes,
- contrôle des cartes mises en opposition (Oppotota),
- contrôle de BIN étranger,
- contrôle du pays de l'adresse IP,
- contrôle de similitude des pays carte et IP,
- contrôle e-Carte Bleue,
- contrôle des cartes à autorisation systématique,
- contrôle carte commerciale,
- contrôle date d'expiration de carte

Ces contrôles peuvent être activés avant ou après la demande d'autorisation. Le fonctionnement de chacun de ces contrôles est détaillé dans la suite de ce document.

Ils sont applicables sous certaines conditions à tous les moyens de paiement acceptés par **Sips**.

En plus de ces contrôles, il existe la possibilité d'obtenir les informations suivantes :

- IP country : information du pays du fournisseur d'accès de l'internaute
- Informations sur la carte bancaire utilisée pour le paiement

Ces informations sont restituées quelle que soit le résultat de la demande d'autorisation. Le fonctionnement de la restitution de ces informations est détaillé dans les chapitres Information IP Country et Information Carte Bancaire.

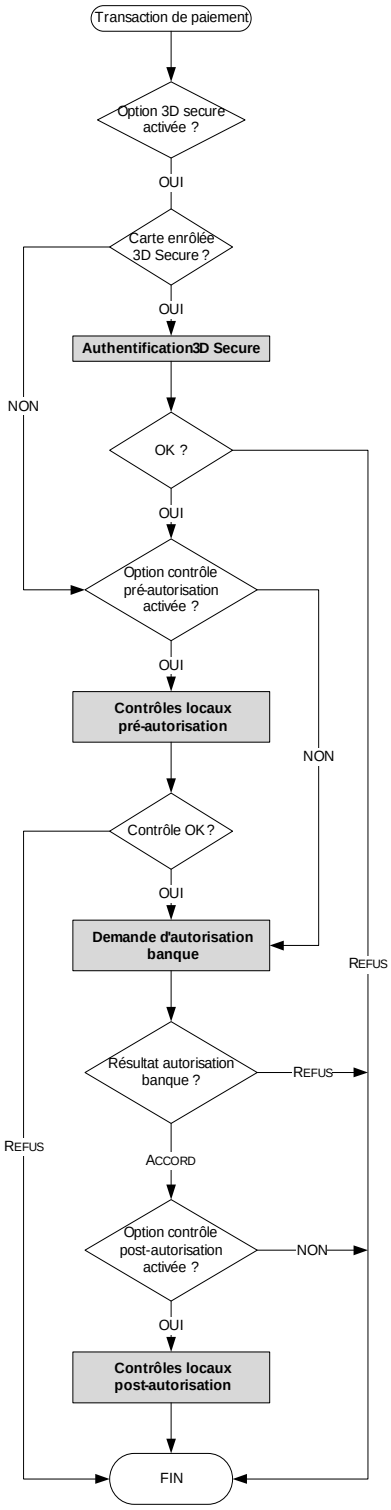
1) A QUI S'ADRESSENT CES CONTROLES ?

Ces contrôles s'adressent à tous les commerçants ayant déjà souscrit à l'offre **Sips** et sensibilisés à un risque éventuel de fraude sur leur site marchand.

2. FONCTIONNEMENT GENERAL

2.1 ENCHAINEMENT DES TRAITEMENTS POUR LA CARTE BANCAIRE

Selon les options sélectionnées par le commerçant, l'enchaînement des traitements d'une transaction de paiement se déroulera comme suit (voir page suivante) :



2.2 CHOIX DE LA STRATEGIE DE CONTROLE

Le comportement du serveur de paiement **Sips** diffère selon que le contrôle complémentaire est placé avant (pré-autorisation) ou après (post-autorisation) la demande d'autorisation bancaire.

Remarque : Pour le commerçant, le choix du contrôle pré ou post autorisation est stratégique :

- un contrôle post-autorisation donne une indication complémentaire à la demande d'autorisation bancaire mais ne bloquera en aucun cas la transaction.
- un contrôle pré-autorisation est décisif quant au résultat de la demande d'autorisation, suivant le résultat du contrôle, la transaction subira une demande d'autorisation ou non.

Le commerçant a la possibilité de combiner des contrôles post-autorisation avec des contrôles pré-autorisation.

La suite de ce paragraphe doit permettre au commerçant de choisir la stratégie de contrôle la mieux adaptée à son besoin.

Remarque : Dans le cas d'un contrôle post-autorisation, il sera conseillé au commerçant de valoriser le champ capture_day à une valeur suffisamment élevée pour lui permettre d'agir sur la transaction (validation, annulation) après réception et analyse du résultat du contrôle d'en-cours restitué dans son journal de fonds des transactions.

1) CONTROLE PLACE AVANT LA DEMANDE D'AUTORISATION

Lorsque des contrôles sont activés en pré-autorisation et que l'un d'eux refuse la transaction alors le serveur de paiement **Sips** ne fait pas de demande d'autorisation.

Par exemple, si une carte est trouvée en liste grise, le serveur de paiement **Sips** refuse la transaction.

De même, dans le cas où plusieurs contrôles sont activés, ils sont effectués les uns après les autres. Si l'un des contrôles refuse une transaction, alors les contrôles suivant ne seront pas effectués.

Par exemple, le commerçant dispose des contrôles en pré-autorisation « liste grise + bin étranger + similitude IP + carte », le porteur n'est pas en liste grise, mais dispose d'une carte dont le bin est étranger, alors la transaction sera refusée et le contrôle de similitude ne sera pas effectué.

Résultat du contrôle de lutte	Résultat de la demande	Etat de la	Opération possible sur la transaction (annulation*,

contre la fraude	d'autorisation	transaction	validation*)
OK	OK	Acceptée	OUI
	KO	Refusée	NON
KO	pas de demande		NON

(*) selon le mode et le délai de capture de la transaction.

a. Contrôle placé après la demande d'autorisation

Le contrôle de lutte contre la fraude placé après la demande d'autorisation (post-autorisation) ne sera déroulé que s'il y a eu accord du serveur d'autorisation bancaire.

Lorsque des contrôles sont activés en post-autorisation et que l'un d'eux retourne une information sur la transaction, alors le serveur de paiement **Sips** renvoie à la fois le résultat d'autorisation du serveur et le résultat du contrôle de lutte contre la fraude.

De même, dans le cas où plusieurs contrôles sont activés, ils sont effectués les uns après les autres. Le premier contrôle négatif retourné stoppe le déroulement des suivants.

Résultat de la demande d'autorisation	Résultat du contrôle de lutte contre la fraude	Etat de la transaction	Opération possible sur la transaction (annulation*, validation*)
OK	OK	Acceptée	OUI
	KO		OUI
KO	pas de contrôle	Refusée	NON

(*) selon le mode et le délai de capture de la transaction.

2.3 RECUPERATION DU RESULTAT DU CONTROLE

Le résultat d'un contrôle de lutte contre la fraude est restitué dans le champ complementary_info et aussi complementary_code du message de réponse à une demande d'autorisation.

On le trouvera donc :

- dans la réponse manuelle et automatique des API **Sips Payment Web** (Version >= 5.00),
- dans le champ complementary_info de la réponse de l'API **Sips Office Server** (version du composant Office >= 3.06),
- dans le journal de fonds des transactions (format table uniquement à partir de la version 5), lors de la consultation de la transaction depuis **Sips Office Extranet**.

2.4 LIMITES D'UTILISATION

Etant donné que le résultat des contrôles est retourné dans le seul champ complementary_code, il ne sera pas aisé pour un commerçant optant pour l'enchaînement de plusieurs contrôles de connaître l'exhaustivité des contrôles passés sauf s'il garde en mémoire leur séquencement exact.

Supposons qu'un commerçant opte pour le contrôle de liste grise carte et contrôle d'en-cours carte. S'il reçoit la valeur 02 (cf. Annexe 1) dans le champ complementary_code, il doit se souvenir que le contrôle de liste grise carte s'est bien déroulé. Si par contre, il reçoit la valeur 03 dans le champ complementary_code, il doit savoir que le contrôle d'en-cours carte n'a pas été effectué.

Les contrôles ne sont effectués que pour les nouvelles transactions (y compris duplication), ils ne concernent pas les opérations (validation, annulation, remboursement).

Remarque : si un commerçant est paramétré en pré-production et qu'il a opté pour les contrôles complémentaires, ceux-ci seront effectués et facturés au moment de ses tests. Par contre, les en-cours cartes de test ne seront pas mis à jour.

3. LOCALISER LE CLIENT GEOGRAPHIQUEMENT

3.1 CONTROLE BIN ETRANGER

1) FONCTIONNEMENT

Cette fonction complémentaire à la demande d'autorisation permet au commerçant de décider d'honorer ou non une prestation en fonction du pays d'émission de la carte du porteur.

Cette fonction ne sera activée que pour les transactions de paiement par carte du réseau CB (CB nationale, VISA, Mastercard). La fonction ne sera pas activée lors d'un paiement par carte de type privatif ou hors réseau CB (Amex, Cetelem, Solo, Switch…).

Pour les commerçants qui demandent le contrôle de BIN étranger, le serveur **Sips** va interroger une base de donnée des plages porteur afin de :

- déterminer si la plage de BIN porteur de la carte existe

  ET

- vérifier l'appartenance du pays d'origine de la carte à une liste de pays autorisés ou interdits. Cette liste de pays, ainsi que leur caractère autorisé ou interdit, est fournie par le commerçant lors de la création de la transaction. Si la liste n'est pas fournie, alors le contrôle se fera sur le code pays du commerçant (cf. ci-dessous).

  OU

- comparer le code du pays d'origine de la carte avec le code pays du commerçant (champ *merchant_country*).

Une plage de BIN sera déclarée étrangère si son pays d'origine est interdit ou différent de celui du commerçant.

Le contrôle de BIN étranger peut être effectué avant ou après la demande d'autorisation, c'est le commerçant qui choisit son mode de fonctionnement.

Le code pays de la carte est retourné dans le champ complementary_info sous la forme : CARD_COUNTRY=XXX, où XXX correspond au code pays iso alphabétique 3166 (cf. annexe).

Contrôle de BIN étranger avant la demande d'autorisation

Le commerçant demande ce contrôle pour limiter les demandes d'autorisation vers la banque.

Le tableau suivant résume le comportement du serveur **Sips** selon le résultat du contrôle de BIN étranger pré-autorisation :

Contrôle BIN étranger PRE autorisation				
	Résultat			
Contrôle BIN étranger carte CB	OK	problème technique	BIN inconnu	BIN non autorisé
Demande autorisation banque	xx		Pas de demande	
	Réponse			
response_code	xx		05	
complementary_code	00	99	05	06

ii. Contrôle de BIN étranger après la demande d'autorisation

Le commerçant demande ce contrôle pour mesurer la prise de risque sur la transaction.

Le tableau suivant résume le comportement du serveur **Sips** selon le résultat du contrôle de BIN étranger post-autorisation :

Contrôle BIN étranger POST autorisation					
	Résultat				
Demande autorisation banque	KO	OK			
Contrôle BIN étranger carte CB		OK	BIN inconnu	BIN non autorisé	Problème technique
	Réponse				
response_code	xx	00			
complementary_code		00	05	06	99

2) CONDITIONS D'UTILISATION

Si un commerçant **Sips** désire opter pour le "contrôle de BIN étranger" il doit en faire la demande auprès du Centre d'Assistance Technique.

Le contrôle est opérationnel dès que l'option est paramétrée sur le serveur **Sips** suite à la demande du commerçant. Par défaut le contrôle compare le code du pays d'origine de la carte avec le code pays du commerçant. Le contrôle de BIN étranger est systématiquement effectué pour toutes les transactions de paiement par carte du réseau CB (CB nationale, VISA, Mastercard) générées par le site marchand.

Aucune modification du site marchand n'est nécessaire hormis, si ce n'est déjà fait, l'exploitation des valeurs des champs complementary_code et complementary_info du message réponse à demande d'autorisation (réponse manuelle et automatique).

Si le commerçant **Sips** souhaite définir une liste de pays autorisés ou interdits, il lui suffit de notifier le mot-clef correspondant à la liste (une seule liste possible) dans le champ DATA de l'API :

- Liste (de codes) de pays à interdire : FORBID_CARD_CTRY
- Liste (de codes) de pays à autoriser : ALLOW_CARD_CTRY

C'est-à-dire le contrôle bin étranger:

- Avec le champ data non valorisé bloque **tous** les paiements de carte du réseau CB (CB nationale, VISA, Mastercard) ayant un BIN différent du pays du commerçant
- Avec le champ data exploité avec une liste ALLOW_CARD_CTRY **autorise** uniquement une liste de pays contenu dans le champ data
- Avec le champ data exploité avec une liste FORBID_CARD_CTRY **interdit** uniquement une liste de pays contenu dans le champ data

Les codes pays seront indiqués dans la liste sous la forme XXX, où XXX correspond au code pays iso alphabétique 3166 (cf. annexe), et séparés par une virgule. Il est également possible d'utiliser des listes préétablies destinée à certaines activités (cf.

Annexe 4 : Listes préétablies des codes pays). Il est également possible de cumuler les deux possibilités.

Le mot-clef doit être inséré entre les balises <CONTROLS> et </CONTROLS>, à la suite de mots-clef éventuellement présents entre les balises et séparés de ceux-ci pas un point-virgule.

Exemple pour le passage de plusieurs pays :

data= «<CONTROLS>ALLOW_CARD_CTRY=FRA,BEL,GBR;</CONTROLS>»

Exemple de passage d'une liste pré-établie :

data= «<CONTROLS>ALLOW_CARD_CTRY=#FRJEL;</CONTROLS>»

Le nombre de pays est limite à 60.

Le format des journaux de fonds n'est pas modifié. Les valeurs des champs complementary_code et complementary_info apparaissent dans le journal de fonds des transactions au format table depuis les versions respectivement V2 et V5.

Remarque : Dans le cas d'un contrôle post-autorisation, il sera conseillé au commerçant de valoriser le champ *capture_day* à une valeur suffisamment élevée pour lui permettre d'agir sur la transaction (annulation, validation) après réception et analyse du résultat du contrôle d'en-cours restitué dans son journal de fonds des transactions.

.

3.2 CONTROLE DU PAYS DE L'ADRESSE IP

1) FONCTIONNEMENT

Cette fonction complémentaire à la demande d'autorisation permet au commerçant de décider d'honorer ou non une prestation en fonction du pays affecté à l'adresse IP de l'appelant (calculée dans **Sips Payment Web** ou fournie par le commerçant dans **Sips Office Server**).

Une incertitude peut persister sur le pays de l'internaute essentiellement à cause de l'attribution dynamique d'adresses IP par certains providers ou d'adresses IP dynamiques.

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 le pays où se situe physiquement l'internaute.

Pour les commerçants qui demandent ce contrôle, le serveur **Sips** va :

- Déterminer si l'adresse IP de l'appelant figure dans une plage d'IP existante

Et

- vérifier l'appartenance du pays de l'adresse IP à une liste de pays autorisés ou interdits. Cette liste, **obligatoire**, est fournie par le commerçant lors de la création de la transaction.

Le contrôle du pays de l'adresse IP peut être effectué avant ou après la demande d'autorisation, c'est le commerçant qui choisit son mode de fonctionnement.

Le code pays de l'adresse IP est retourné dans le champ *complementary_info* sous la forme : *<COUNTRY_IP IP_COUNTRY=XXX />*, où XXX correspond au code pays iso alphabétique 3166 (cf. annexe).

a. Contrôle du pays de l'adresse IP avant la demande d'autorisation

Le commerçant demande ce contrôle pour limiter les demandes d'autorisation vers la banque.

Le pays de l'adresse IP est considéré comme interdit s'il figure dans la liste des pays interdits ou ne figure pas dans la liste des pays autorisés.

Le tableau suivant résume le comportement du serveur **Sips** selon le résultat du contrôle du pays de l'adresse IP en pré-autorisation :

Contrôle pays de l'IP PRE autorisation				
	Résultat			
Contrôle pays de l'adresse IP	OK	Problème technique	pays IP inconnu	pays IP interdit
Demande autorisation banque	xx		Pas de demande	
	Réponse			
response_code	xx		05	
complementary_code	00	99	09	10

b. Contrôle du pays de l'adresse IP après la demande d'autorisation

Le commerçant demande ce contrôle pour mesurer la prise de risque sur la transaction.

Le tableau suivant résume le comportement du serveur **Sips** selon le résultat du contrôle d'en-cours post-autorisation :

Contrôle pays de l'IP POST autorisation				
	Résultat			
Demande autorisation banque	KO	OK		
Contrôle pays de l'adresse IP		Problème technique	Pays IP inconnu	Pays IP interdit
	Réponse			
response_code	xx	00		
complementary_code	00	99	09	10

2) CONDITIONS D'UTILISATION

Si un commerçant **Sips** désire opter pour le "contrôle du pays de l'adresse IP" il doit en faire la demande auprès du Centre d'Assistance Technique.

Le contrôle est opérationnel dès que l'option est paramétrée sur le serveur **Sips** suite à la demande du commerçant et que la liste des pays est renseignée par le commerçant. Le contrôle du pays de l'adresse IP est systématiquement effectué pour toutes les transactions de paiement générées par le site marchand. Outre les modifications du site marchant nécessaires pour l'exploitation des valeurs du champ complementary_code des réponses manuelles ou automatiques lors de demande d'autorisation, le commerçant **Sips** devra également définir la liste de pays autorisés ou interdits. Si la liste n'est pas définie, alors le contrôle ne sera pas effectué. Pour cela, il lui suffit de notifier le mot-clef correspondant à la liste (une seule liste possible) dans le champ data de l'API:

- Liste (de codes) de pays à interdire : FORBID_IP_CTRY
- Liste (de codes) de pays à autoriser : ALLOW_IP_CTRY.

C'est-à-dire le contrôle IP COUNTRY:

- Avec le champ data non valorisé n'est pas effectué

- Avec le champ data exploité avec une liste ALLOW_IP_CTRY **autorise** uniquement une liste de pays contenu dans le champ data
- Avec le champ data exploité avec une liste FORBID_IP_CTRY **interdit** uniquement une liste de pays contenu dans le champ data

Le nombre de pays est limite à 60.

Dans le cas de l'utilisation de ce contrôle avec la solution **Sips Office Server**, il faut valoriser le champ customer_ip_adress.

Les codes pays doivent être indiqués dans la liste sous la forme XXX, où XXX correspond au code pays iso alphabétique 3166 (cf. annexe), et séparés par une virgule.

Le mot-clef choisi doit être inséré entre les balises <CONTROLS> et </CONTROLS>, à la suite de mots-clef éventuellement présents entre les balises et séparés de ceux-ci pas un point-virgule.

Exemple : data= «<CONTROLS> ALLOW_IP_CTRY=FRA;</CONTROLS>»

3.3 CONTROLE DE SIMILITUDE DES PAYS CARTE ET IP

1) FONCTIONNEMENT

Cette fonction complémentaire à la demande d'autorisation permet au commerçant de décider d'honorer ou non une prestation en se basant sur la combinaison du pays d'émission de la carte du porteur et du pays affecté à l'adresse IP de l'appelant.

Cette fonction ne sera activée que pour les transactions de paiement par carte du réseau CB (CB nationale, VISA, Mastercard). La fonction ne sera pas activée lors d'un paiement par carte de type privatif ou hors réseau CB (Amex, Cetelem, Solo, Switch…).

Pour les commerçants qui demandent ce contrôle, le serveur **Sips** va interroger la base de données des plages porteurs et celle des plages d'adresses IP afin de :

- déterminer le pays de la carte

  ET

- déterminer le pays de l'adresse IP

  ET