Contrôles complémentaires de lutte contre la fraude

Guide d'utilisation

Version 2.03 – 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

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 11 possibilités de contrôles :

- contrôle d'en-cours carte,
- contrôle d'en-cours IP,
- contrôle de liste grise de cartes,
- contrôle de liste grise de codes postaux,
- contrôle de BIN étranger,
- contrôle e-Carte Bleue,
- contrôle du pays de l'adresse IP,
- contrôle des cartes mises en opposition (Oppotota),
- contrôle de similitude des pays carte et IP,
- contrôle des cartes à autorisation systématique,
- contrôle de plages de BIN

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 applicatives 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.*

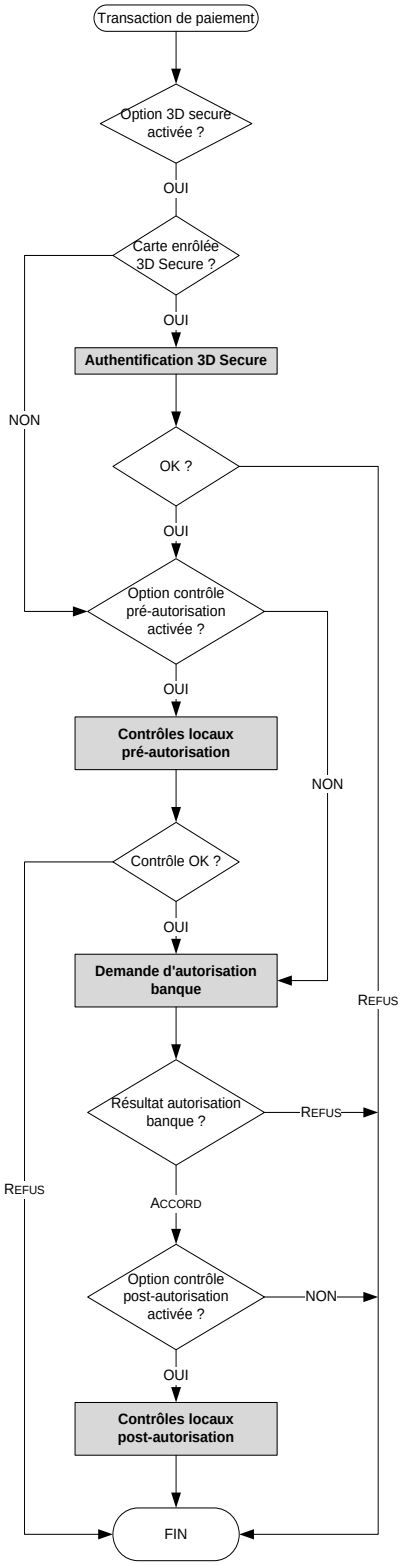
1.2 A QUI S'ADRESSENT CES CONTROLES ?

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.

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

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

2.2.2 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

3.1.1 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).

3.1.1.1 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

3.1.1.2 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

3.1.2 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. 8.4 - 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

3.2.1 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).

3.2.1.1 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

3.2.1.2 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

3.2.2 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

3.3.1 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

- vérifier l'appartenance de la combinaison de ces 2 pays à une liste de combinaisons de pays autorisées ou interdites. Cette liste de combinaisons de pays est fournie par le commerçant lors de la création de la transaction

OU

- vérifier la concordance du pays de la carte et du pays de l'adresse IP dans le cas où le commerçant ne fournit pas de liste de combinaisons de pays autorisées ou interdites.

Les codes pays de la carte et de l'adresse IP sont retournés dans le champ *complementary_info* sous la forme :

<COUNTRY_COMBINATION CARD_COUNTRY=XXX IP_COUNTRY=XXX />

où XXX correspond au code pays iso alphabétique 3166 (cf. annexe) ou à la valeur « UNKNOWN » dans le cas où le code pays n'a pas pu être déterminé (appartenance à aucun plage, adresse IP non transmise).

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

3.3.1.1 Contrôle Similitude Carte/IP avant la demande d'autorisation

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

Si le couple pays de la carte / pays de l'IP est présent dans la liste des combinaisons interdites ou absent de la liste des combinaisons autorisées, le serveur Sips refuse la transaction et retourne un refus vers le commerçant en indiquant le motif :

Contrôle similitude carte/IP PRE autorisation				
	Résultat			
Contrôle similitude carte/IP	Combinaison interdite	Combinaison autorisée	Pays Inconnu	problème technique
Demande autorisation banque	Pas de demande	xx		
	Réponse			
response_code	05	xx		
complementary_code	12	00	13	99

3.3.1.2 Contrôle Similitude Carte/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 de similitude des pays de la carte et de l'adresse IP post-autorisation :

Contrôle similitude carte/IP POST autorisation					
	Résultat				
Demande autorisation banque	KO	OK			
Contrôle similitude carte/IP		Combinaison autorisée	Combinaison Interdite	Pays Inconnu	problème technique
	Réponse				
response_code	xx	00			
complementary_code		00	12	13	99

3.3.2 Conditions d'utilisation

Si un commerçant Sips désire opter pour le "contrôle Similitude pays carte/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. Le contrôle similitude carte/IP est systématiquement effectué pour toutes les transactions de paiement par carte générées sur 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. **Dans ce cas, le contrôle se limitera à une vérification de concordance entre le code pays de la carte et celui de l'adresse IP**.

Si le commerçant Sips souhaite définir une liste de combinaisons de pays autorisées ou interdites, il lui suffit de notifier le mot-clef correspondant à la liste (une seule liste possible) dans le champ *data* de l'API de la manière suivante :

- Liste de combinaisons de pays à interdire : FORBID_CTRY_COMBI
- Liste de combinaisons de pays à autoriser : ALLOW_CTRY_COMBI

C'est-à-dire le contrôle SIMILITUDE:

- Avec le champ data non valorisé vérifie la concordance du pays de la carte et du pays de l'adresse IP
- Avec le champ data exploité avec une liste ALLOW_CTRY_COMBI **autorise** uniquement une liste de pays contenu dans le champ data
- Avec le champ data exploité avec une liste FORBID_CTRY_COMBI **interdit** uniquement une liste de pays contenu dans le champ data

Le nombre de pays est limite à 25.

Une combinaison de pays est représentée sous la forme (XXX,xxx) où XXX et xxx représentent respectivement le code pays de la carte et celui de l'adresse IP. Chaque code pays doit respecter la norme iso alphabétique 3166 (cf. annexe), la valeur particulière « *** » permettant de désigner l'ensemble des pays. Les combinaisons de pays doivent être séparées 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_CTRY_COMBI=(FRA,***),(BEL,BEL);</CONTROLS>»

permet d'autoriser une carte Française quel que soit le pays de l'adresse IP, ainsi que les cartes Belges depuis la Belgique.

3.4 INFORMATION IP COUNTRY

3.4.1 Fonctionnement

Cette information 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 (calculé dans Sips Payment Web ou fournir par le commerçant dans Sips Office Server).

Une incertitude peut persister sur le pays de l'internaute essentiellement à cause de l'attribution dynamique de 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 du pays où se situe physiquement l'internaute.

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

3.4.2 Conditions d'utilisation

Un commerçant qui désire l'*information IP country* doit en faire la demande auprès du Centre d'Assistance Technique.

La restitution de cette information est opérationnelle dès que l'option est paramétrée sur le serveur Sips suite à la demande du commerçant.

Pour Sips Office Server, la recherche du pays est engagée dès lors que l'adresse IP (customer_ip_address) est fournie et valide (le fonctionnement nécessite au minimum la version 306 du composant Office).

Pour Sips Payment Web, c'est le serveur Sips qui récupère l'adresse IP.

Aucune modification du site marchant 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).

Le code pays est retourné dans le champ *complementary_info* sous la forme : IP_COUNTRY=xxx, où xxx correspond au code pays iso alphabétique 3166 (cf. ***8.2. Annexe 2 : codes pays alphabétique iso 3166***).

3.4.2.1 Code pays inconnu

Lorsque le système ne trouve pas le pays, le code IP_COUNTRY est valorisé à "XXX".

Un code pays inconnu peut être retourné dans les 4 cas suivants :

- le système n'a pas connaissance de l'adresse IP (non renseignement dans Sips Office Server par exemple)
- l'information IP country est indisponible momentanément
- l'adresse IP n'est pas renseignée correctement
- l'adresse IP est renseignée correctement mais inconnue de la base de données

4. CONTROLER L'ACTIVITE DU CLIENT

4.1 CONTROLE DE L'EN-COURS CARTE

4.1.1 Fonctionnement

Cette fonction complémentaire à la demande d'autorisation permet au commerçant de mesurer le risque sur un achat par le contrôle de l'activité de la carte sur une période.

Pour le commerçant qui demande le contrôle d'en-cours, le serveur Sips va contrôler l'activité du porteur sur une période donnée.

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

4.1.1.1 Contrôle d'en-cours 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 d'en-cours pré-autorisation :

Contrôle en-cours carte PRE autorisation			
	Résultat		
Contrôle en-cours carte	OK	Problème technique	KO
Demande autorisation banque	xx		Pas de demande
	Réponse		
response_code	xx		05
complementary_code	00	99	02

4.1.1.2 Contrôle d'en-cours 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 en-cours carte POST autorisation				
	Résultat			
Demande autorisation banque	KO	OK		
Contrôle en-cours carte		OK	KO	Problème technique

	Réponse			
response_code	xx	00		
complementary_code		00	02	99

4.1.2 Conditions d'utilisation

Si un commerçant Sips désire opter pour le "contrôle en-cours carte" il doit en faire la demande auprès du Centre d'Assistance Technique en précisant les informations suivantes qui permettront de personnaliser le contrôle :

- période (en jours) sur laquelle s'effectue le contrôle d'en-cours,
- montant cumulé maximum (en euro) autorisé sur la période,
- nombre de transactions maximum autorisées sur la période,
- montant maximum (en euro) d'une transaction.

Le paramètre *période* est obligatoire. Les trois autres paramètres sont paramétrés avec des valeurs maximales.

Le tableau suivant définit les valeurs minimum et maximum de ces paramètres :

Paramètre	**Valeur min**	**Valeur max**
PERIODE	1 jour	30 jours
CUMUL-MAX	1,00 euro sur la période	999 999,00 euros sur la période
MONTANT_MAX	1,00 euro sur la période	999 999,00 euros sur la période
NB_MAX	1 transaction sur la période	99 transactions sur la période

Le contrôle est opérationnel dès que l'option est paramétrée sur le serveur Sips suite à la demande du commerçant. Le contrôle en-cours carte est systématiquement effectué pour toutes les transactions de paiement par carte générées sur le site marchand.

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

4.1.3 Mutualisation du contrôle

Le contrôle d'en-cours carte peut être configuré de telle manière qu'il s'effectue sur un ensemble de boutiques d'un même client (exemple : Une enseigne a plusieurs boutiques Web et souhaite effectuer le contrôle encours carte sur l'ensemble des boutiques web)

4.1.4 Limites d'utilisation

Le contrôle d'en-cours carte n'est pas effectué lors des opérations de caisse de type remboursement, annulation ou validation.

L'en-cours de la carte du porteur n'est pas mis à jour lors des opérations remboursement, annulation, validation qu'elles soient partielles ou totales.

Dans le cas d'un paiement en N fois, le contrôle d'en-cours est effectué lors du paiement en ligne (contrôle d'une transaction du montant global de l'achat). Cependant les N transactions sont enregistrées dans l'en-cours du porteur et seront prises en compte lors des éventuels prochains achats dans la période concernée par le contrôle d'en cours.

Exemple :

Le tableau suivant décrit l'évolution de l'en-cours d'un porteur dans le cas où un commerçant a choisi de limiter les achats sur son site à 4 transactions/mois pour un montant max de 100 000 Euro:

Date de l'achat	Description du paiement	Résultat du contrôle d'en-cours	Etat de l'en-cours carte après enregistrement du paiement
01/10/2003	50 000 E, paiement en 3 fois (1 paiement /semaine)	**OK**	TR1 01/10/2003 10 000 TR2 08/10/2003 20 000 TR3 15/10/2003 20 000
07/10/2003	10 000 E, paiement standard	**OK**	TR1 01/10/2003 10 000 TR2 08/10/2003 20 000 TR3 15/10/2003 20 000 TR4 07/10/2003 10 000
12/10/2003	5 000 E, paiement standard	**KO (NB_MAX)**	TR1 01/10/2003 10 000 TR2 08/10/2003 20 000 TR3 15/10/2003 20 000 TR4 07/10/2003 10 000
01/11/2003	2 000 E, paiement standard	**OK**	TR2 08/10/2003 20 000 TR3 15/10/2003 20 000 TR4 07/10/2003 10 000 TR5 01/11/2003 2 000
02/11/2003	12 000 E, paiement standard	**KO (NB_MAX)**	TR2 08/10/2003 20 000 TR3 15/10/2003 20 000 TR4 07/10/2003 10 000 TR5 01/11/2003 2 000
07/11/2003	60 000 E, paiement standard	**KO (CUMUL_MAX)**	TR2 08/10/2003 20 000 TR3 15/10/2003 20 000 TR5 01/11/2003 2 000
07/11/2003	1 500 E, paiement standard	**OK**	TR2 08/10/2003 20 000 TR3 15/10/2003 20 000 TR5 01/11/2003 2 000 TR6 07/11/2003 1 500

Paramètres du commerçant dans cet exemple : PERIODE=30j, NB_MAX=4, CUMUL_MAX=100 000

4.2 CONTROLE DE L'EN-COURS IP

4.2.1 Fonctionnement

Cette fonction complémentaire à la demande d'autorisation permet au commerçant de mesurer le risque sur un achat par le contrôle de l'activité d'un client à partir d'une adresse IP sur une période.

Pour le commerçant qui demande le contrôle d'en-cours, le serveur Sips va contrôler l'activité du client sur une période donnée.

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

4.2.1.1 Contrôle d'en-cours 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 d'en-cours pré-autorisation :

Contrôle en-cours IP PRE autorisation			
	Résultat		
Contrôle en-cours IP	OK	Problème technique	KO
Demande autorisation banque	xx		Pas de demande
	Réponse		
response_code	xx		05
complementary_code	00	99	16

4.2.1.2 Contrôle d'en-cours 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 en-cours IP POST autorisation				
	Résultat			
Demande autorisation banque	KO	OK		
Contrôle en-cours IP		OK	KO	Problème technique
	Réponse			
response_code	xx	00		
complementary_code		00	16	99

4.2.2 Conditions d'utilisation

Si un commerçant Sips désire opter pour le "contrôle en-cours IP" il doit en faire la demande auprès du Centre d'Assistance Technique en précisant les informations suivantes qui permettront de personnaliser le contrôle :

- période (en jours) sur laquelle s'effectue le contrôle d'en-cours,
- montant cumulé maximum (en euro) autorisé sur la période,
- nombre de transactions maximum autorisées sur la période,
- montant maximum (en euro) d'une transaction.

Le paramètre *période* est obligatoire. Les trois autres paramètres sont paramétrés avec des valeurs maximales.Le tableau suivant définit les valeurs minimum et maximum de ces paramètres :

Paramètre	**Valeur min**	**Valeur max**
PERIODE	1 jour	30 jours
CUMUL-MAX	1,00 euro sur la période	999 999,00 euros sur la période
MONTANT_MAX	1,00 euro sur la période	999 999,00 euros sur la période
NB_MAX	1 transaction sur la période	99 transactions sur la période

Le contrôle est opérationnel dès que l'option est paramétrée sur le serveur Sips suite à la demande du commerçant. Le contrôle en-cours IP est systématiquement effectué pour toutes les transactions de paiement par carte générées sur le site marchand.

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

4.2.3 Mutualisation du contrôle

Le contrôle d'en-cours IP peut être configuré de telle manière qu'il s'effectue sur un ensemble de boutiques d'un même client.

4.2.4 Limites d'utilisation

Le contrôle d'en-cours IP n'est pas effectué lors des opérations de caisse de type remboursement, annulation ou validation.

L'en-cours de l'adresse IP d'un client n'est pas mis à jour lors des opérations remboursement, annulation, validation qu'elles soient partielles ou totales.

Dans le cas d'un paiement en N fois, le contrôle d'en-cours est effectué lors du paiement en ligne (contrôle d'une transaction du montant global de l'achat). Cependant les N transactions sont enregistrées dans l'en-cours du porteur et seront prises en compte lors des éventuels prochains achats dans la période concernée par le contrôle d'en cours.

Exemple :

Le tableau suivant décrit l'évolution de l'en-cours d'un client dans le cas où un commerçant a choisi de limiter les achats sur son site à 4 transactions/mois avec la même adresse IP pour un montant max de 100 000 Euro :

Date de l'achat	Description du paiement	Résultat du contrôle d'en-cours	Etat de l'en-cours carte après enregistrement du paiement
01/10/2003	50 000 E, paiement en 3 fois (1 paiement /semaine)	**OK**	TR1 01/10/2003 10 000 TR2 08/10/2003 20 000 TR3 15/10/2003 20 000
07/10/2003	10 000 E, paiement standard	**OK**	TR1 01/10/2003 10 000 TR2 08/10/2003 20 000 TR3 15/10/2003 20 000 TR4 07/10/2003 10 000
12/10/2003	5 000 E, paiement standard	**KO (NB_MAX)**	TR1 01/10/2003 10 000 TR2 08/10/2003 20 000 TR3 15/10/2003 20 000 TR4 07/10/2003 10 000
01/11/2003	2 000 E, paiement standard	**OK**	TR2 08/10/2003 20 000 TR3 15/10/2003 20 000 TR4 07/10/2003 10 000 TR5 01/11/2003 2 000
02/11/2003	12 000 E, paiement standard	**KO (NB_MAX)**	TR2 08/10/2003 20 000 TR3 15/10/2003 20 000 TR4 07/10/2003 10 000 TR5 01/11/2003 2 000
07/11/2003	60 000 E, paiement standard	**KO (CUMUL_MAX)**	TR2 08/10/2003 20 000 TR3 15/10/2003 20 000 TR5 01/11/2003 2 000
07/11/2003	1 500 E, paiement standard	**OK**	TR2 08/10/2003 20 000 TR3 15/10/2003 20 000 TR5 01/11/2003 2 000 TR6 07/11/2003 1 500

Paramètres du commerçant dans cet exemple : PERIODE=30j, NB_MAX=4, CUMUL_MAX=100 000

5. CONTROLER LA PRESENCE DE CARTES DANS DES LISTES INDESIRABLES

5.1 CONTROLE LISTE GRISE CARTE

5.1.1 Fonctionnement

Ce contrôle sera utilisé par les commerçants qui souhaitent vérifier que la carte utilisée par l'acheteur n'est pas référencée dans une liste des cartes "indésirables" appelée "liste grise des cartes". Cette liste est gérée par le commerçant.

5.1.1.1 Contrôle de liste grise carte avant la demande d'autorisation

Cette fonction de type "accepteur" (domaine commerçant) est effectuée par le serveur Sips **avant** la demande d'autorisation vers la banque pour toute transaction de paiement effectuée par carte.

Si la carte est présente dans la liste grise, le serveur Sips refuse la transaction et retourne un refus vers le commerçant en indiquant le motif :

Contrôle liste grise carte PRE autorisation			
	Résultat		
Contrôle liste grise carte	OK	Problème technique	KO
Demande autorisation banque	xx		Pas de demande
	Réponse		
response_code	xx		05
complementary_code	00	99	03

Côté back-office, une transaction refusée par le serveur Sips suite à un contrôle de liste grise ne sera pas envoyée en remise en banque.

5.1.1.2 Contrôle de liste grise carte après la demande d'autorisation

Cette fonction de type "accepteur" (domaine commerçant) est effectuée par le serveur Sips **après** la demande d'autorisation acceptée de la banque pour toute nouvelle transaction de paiement effectuée par carte.

Le commerçant demande ce type de 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 liste grise carte post-autorisation :

Contrôle liste grise carte POST autorisation				
	Résultat			
Demande autorisation banque	KO	OK		
Contrôle liste grise carte		OK	KO	Problème technique
	Réponse			
response_code	xx	00		
complementary_code		00	03	99

5.1.2 Conditions d'utilisation

Si un commerçant désire opter pour le "contrôle liste grise carte" il doit en faire la demande auprès du Centre d'Assistance Technique.

Afin de gérer sa liste grise, le commerçant doit être doté de l'offre Sips Office Extranet. Un nouveau user/password n'est pas nécessaire pour gérer cette liste s'il a déjà un compte Sips Office Extranet. Il doit cependant préciser quel utilisateur sera habilité à gérer cette liste.

Le contrôle est opérationnel dès que l'option est paramétrée sur le serveur Sips suite à la demande du commerçant. Le contrôle de carte en liste grise est systématiquement effectué pour toutes les transactions de paiement par carte générées sur 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 format des journaux de fonds n'est pas modifié. La valeur du champ *complementary_code* apparaît dans le journal de fonds des transactions au format table depuis la version 5.

5.1.3 Gestion de la liste grise des cartes

Cette liste grise est mise à jour par le commerçant qui dispose d'un accès dédié avec 3 options supplémentaires sur Sips Office Extranet (Ajout, Recherche, Suppression d'une carte). Une même liste peut être utilisée par un commerçant pour plusieurs boutiques (mutualisation de liste).

5.1.3.1 Ajout d'une carte

L'ajout d'une carte en liste grise peut se faire soit à partir d'une transaction soit directement à partir du numéro de la carte.

Ajout par numéro de carte

L'utilisateur saisit le numéro de la carte à ajouter dans la liste grise et choisit un motif parmi la liste de valeurs proposées (carte perdue, carte volée, fraude suspectée, impayé, autre motif).

Contrôles effectués avant l'enregistrement en base :

- numéro de carte numérique
- longueur du numéro de carte >= 10
- existence sur carte déjà présente dans la liste grise

En cas d'erreur, un message adapté sera affiché à l'utilisateur.

Si les contrôles sont OK, le serveur enregistre la carte dans la liste grise sans étape supplémentaire de confirmation, la carte est opérationnelle immédiatement dans la liste grise.

Un message de fin d'opération «carte ajoutée dans la liste grise » est affiché à l'utilisateur.

Ajout par transaction

L'utilisateur saisit l'identifiant et la date de la transaction dont la carte est à ajouter dans la liste grise et choisit un motif parmi la liste de valeurs proposées (carte perdue, carte volée, fraude suspectée, impayé, autre motif).

Si la transaction existe encore en base, une page de confirmation d'ajout est proposée. Si l'ajout est confirmé, la présence de la carte est vérifiée dans la liste grise.

Si la carte est déjà présente dans la liste grise, un message d'erreur « carte déjà en liste grise » est affiché à l'utilisateur. Sinon un message de fin d'opération «carte ajoutée dans la liste grise » est affiché à l'utilisateur.

Quel que soit le type d'ajout, le mouvement d'ajout de carte dans la liste grise est stocké dans un historique (numéro de carte, date et heure, motif, nom de l'utilisateur).

5.1.3.2 Recherche d'une carte

La recherche d'une carte en liste grise peut se faire soit à partir d'une transaction soit directement à partir du numéro de la carte.

Recherche par numéro de carte

L'utilisateur saisit soit le numéro complet d'une carte, soit 2 numéros, complets ou partiels, définissant une plage à rechercher dans la liste grise.

Si aucune carte ne correspond aux critères de recherche saisis, un message le signalant est affiché à l'utilisateur.

Si le nombre de cartes correspondant aux critères de recherche dépasse le seuil paramétré (50), un message est affiché à l'utilisateur lui demandant d'affiner les critères.

Si le nombre de cartes correspondant aux critères de recherche est inférieur au seuil paramétré (50), la liste est affichée. Associés à chaque numéro de carte, 2 boutons sont proposés pour permettre de supprimer la carte de la liste ou d'en visualiser le détail (numéro de carte, motif, date et heure d'entrée dans la liste, nom de l'utilisateur qui a effectué l'ajout).

Recherche par transaction

L'utilisateur saisit l'identifiant et la date de la transaction dont la carte est à rechercher dans la liste grise.

Si aucune transaction ne correspond aux critères de recherche saisis, un message le signalant est affiché à l'utilisateur.

Si la transaction correspondant aux critères de recherche est trouvée, une liste à un élément est affichée. Associés au numéro de carte et à la référence de transaction, 2 boutons sont proposés pour permettre de supprimer la carte de la liste ou d'en visualiser le détail (numéro de carte tronqué, référence de transaction, motif, date et heure d'entrée dans la liste, nom de l'utilisateur qui a effectué l'ajout).

5.1.3.3 Suppression d'une carte

L'utilisateur effectue une recherche selon les modalités décrites au paragraphe précédent.

Lorsque la liste s'affiche, l'utilisateur clique sur le bouton de suppression associé au numéro de carte (éventuellement associé à une référence de transaction) qu'il souhaite supprimer de la liste.

Le détail de la carte (numéro de carte, éventuellement la référence de la transaction, motif, date et heure d'entrée dans la liste, nom de l'utilisateur qui a effectué l'ajout) est affiché à l'utilisateur qui doit alors confirmer ou annuler la demande de suppression.

Si la demande est confirmée, la suppression de la carte dans la liste grise est opérationnelle immédiatement. Un message de fin d'opération "carte supprimée de la liste grise" est affiché à l'utilisateur.

Le mouvement de suppression de carte dans la liste grise est stocké dans un historique (numéro de carte, date et heure, nom de l'utilisateur).

5.1.4 Mutualisation d'une liste

Une liste grise peut être liée à une boutique ou à un ensemble de boutiques d'un même client.

Dans ce cas, il sera conseillé au client de désigner un administrateur unique pour la gestion de la liste grise des cartes.

La mutualisation d'une liste grise n'est compatible qu'avec une gestion par numéros de carte.

5.2 CONTROLE CARTES EN OPPOSITION (OPPOTOTA)

5.2.1 Fonctionnement

Cette fonction complémentaire de contrôler que la carte n'est pas en opposition avant effectuer de demande d'autorisation.

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 Cartes en opposition, le serveur Sips va interroger la liste noire nationale OPPOTOTA qui contient l'ensemble des cartes mises en opposition.

Remarque : Comme le contrôle d'opposition est effectué par le serveur de la banque lors de la demande d'autorisation il n'a aucun intérêt en mode Post-autorisation.

5.2.1.1 Contrôle cartes en opposition 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 Cartes en opposition pré-autorisation :

Contrôle Oppotota PRE autorisation			
	Résultat		
Contrôle Oppotota	Dans Oppotota	Hors Oppotota	problème technique
Demande autorisation banque	Pas de demande	xx	
	Réponse		
response_code		xx	
complementary_code	11	00	99

5.2.1.2 Contrôle cartes en opposition 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 Cartes en opposition post-autorisation :

Contrôle Oppotota POST autorisation				
	Résultat			
Demande autorisation banque	KO	OK		
Contrôle Oppotota		Hors Oppotota	Dans Oppotota	problème technique
	Réponse			
response_code	xx	00		
complementary_code		00	11	99

5.2.2 Conditions d'utilisation

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

Ce contrôle est systématiquement effectué pour toutes les transactions de paiement par carte du réseau CB (CB nationale, VISA, Mastercard) générées sur 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 format des journaux de fonds n'est pas modifié.

6. CONNAITRE LES PROPRIETES DE LA CARTE

6.1 CONTROLE E-CARTE BLEUE

6.1.1 Fonctionnement

Cette fonction complémentaire à la demande d'autorisation permet au commerçant de décider d'honorer ou non une prestation payée par un porteur de carte e-Carte Bleue.

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 e-Carte Bleue, le serveur Sips va interroger une base de données des plages e-Carte Bleue afin de déterminer si le numéro de carte appartient à une plage e-Carte Bleue.

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

6.1.1.1 Contrôle e-Carte Bleue 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 e-Carte Bleue pré-autorisation :

Contrôle e-Carte Bleue PRE autorisation			
	Résultat		
Contrôle Contrôle e-Carte Bleue	OK	problème technique	KO (eCB)
Demande autorisation banque	xx		Pas de demande
	Réponse		
response_code	xx		05
complementary_code	00	99	07

6.1.1.2 Contrôle e-Carte Bleue 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 e-Carte Bleue post-autorisation :

Contrôle e-Carte Bleue POST autorisation				
	Résultat			
Demande autorisation banque	KO	OK		
Contrôle e-Carte Bleue		OK	KO (eCB)	problème technique
	Réponse			
response_code	xx	00		
complementary_code		00	07	99

6.1.2 Conditions d'utilisation

Si un commerçant Sips désire opter pour le "contrôle e-Carte Bleue", il doit en faire la demande auprès du Centre d'Assistance Technique.

La restitution de cette information est opérationnelle dès que l'option est paramétrée sur le serveur Sips suite à la demande du commerçant.

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 format des journaux de fonds n'est pas modifié.

6.2 CONTROLE DES CARTES A AUTORISATION SYSTEMATIQUE

6.2.1 Fonctionnement

Cette fonction complémentaire à la demande d'autorisation permet au commerçant de décider d'honorer ou non une prestation payée par un porteur dont la carte nécessite une demande d'autorisation systématique. Ces cartes sont entre autres les cartes Electron, les cartes Maestro, les cartes Cadeaux, etc….

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 des cartes à autorisation systématique, le serveur Sips va interroger une base de données des plages porteurs afin de déterminer si le numéro de carte appartient à une plage de carte à autorisation systématique.

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

6.2.1.1 Contrôle des cartes à autorisation systématique 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 des cartes à autorisation systématique en mode pré-autorisation :

Contrôle des cartes à autorisation systématique en mode PRE autorisation				
	Résultat			
Contrôle des cartes à autorisation systématique	OK	Problème technique	KO	BIN inconnu
Demande autorisation banque	xx		Pas de demande	
	Réponse			
response_code	xx		05	
complementary_code	00	99	14	15

6.2.1.2 Contrôle des cartes à autorisation systématique 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 des cartes à autorisation systématique en mode post-autorisation :

Contrôle des cartes à autorisation systématique en mode POST autorisation					
	Résultat				
Demande autorisation banque	KO	OK			
Contrôle des cartes à autorisation systématique		OK	KO	BIN inconnu	problème technique
	Réponse				
response_code	xx	00			
complementary_code		00	14	15	99

6.2.2 Conditions d'utilisation

Si un commerçant Sips désire opter pour le "contrôle des cartes à autorisation systématique", il doit en faire la demande auprès du Centre d'Assistance Technique.

La restitution de cette information est opérationnelle dès que l'option est paramétrée sur le serveur Sips suite à la demande du commerçant.

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 format des journaux de fonds n'est pas modifié.

6.3 INFORMATION CARTE BANCAIRE

6.3.1 Fonctionnement

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
- le code pays de la banque émettrice (code iso alphabétique 3166, cf. annexe)
- le code produit (cf. ***8.3. Annexe 3 : liste des codes produits***
-)

Cette information est calculée avant même l'engagement dans un premier contrôle complémentaire. L'information est retournée dans le champ complementary_info des API Sips Payment Web et Sips Office Server avec la structure suivante :

<CARD_INFOS BDOM=<nom de la banque émettrice> COUNTRY=<pays de la banque émettrice> PRODUCTCODE=<code produit> />

ou en cas d'erreur

<CARD_INFOS BDOM=ERROR />

ou en cas de carte non CB :

<CARD_INFOS BDOM=UNKNOWN />

ou en cas de plage non trouvée :

<CARD_INFOS BDOM=NOTFOUND />

6.3.2 Conditions d'utilisation

Si un commerçant Sips désire opter pour *la restitution des informations carte*, il doit en faire la demande auprès du Centre d'Assistance Technique.

La restitution de cette information est opérationnelle dès que l'option est paramétrée sur le serveur Sips suite à la demande du commerçant.

6.4 CONTROLE CARTE COMMERCIALE

6.4.1 Fonctionnement

Ce contrôle complémentaire à la demande d'autorisation permet au commerçant de décider d'honorer ou non une prestation payée par un porteur de carte commerciale. Cette contrôle ne sera activée que pour les transactions de paiement par carte du réseau CB (CB nationale, VISA, Mastercard). Le contrôle ne sera pas activé lors d'un paiement par carte de type privatif ou hors réseau CB (Amex, Cetelem, Solo, Switch…).

Pour les commerçants qui demandent le contrôle carte commerciale, le serveur Sips va interroger une base de données contenant les informations carte afin de déterminer si le numéro de carte appartient à une plage de type commerciale.

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

6.4.1.1 Contrôle carte commerciale avant la demande d'autorisation

Le commerçant demande ce contrôle en pré autorisation car il refuse les paiements effectués avec une carte commerciale (exemple : obligation des opérateurs de jeu en ligne)

Le tableau suivant résume le comportement du serveur Sips selon le résultat du contrôle carte commerciale pré-autorisation :

Contrôle carte commerciale PRE autorisation				
	Résultat			
Contrôle carte commerciale	OK	problème technique	KO (Carte commerciale)	BIN inconnu
Demande autorisation banque	xx		Pas de demande	Pas de demande
	Réponse			
response_code	xx		05	
complementary_code	00	99	18	05
complementary_info	Non renseigné			

xx = code réponse suite à demande d'autorisation

6.4.1.2 Contrôle carte commerciale 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 carte commerciale post-autorisation :

Contrôle carte commerciale POST autorisation					
	Résultat				
Demande autorisation banque	KO	OK			
Contrôle carte commerciale		OK	KO (carte commerciale)	BIN inconnu	problème technique
	Réponse				
response_code	xx	00			
complementary_code	Non renseigné	00	18	05	99
Complementary_info	Non renseigné				

xx = code refus suite à demande d'autorisation

6.4.2 Conditions d'utilisation

Si un commerçant Sips désire opter pour le "contrôle carte commerciale", il doit en faire la demande auprès du Centre d'Assistance Technique.

La restitution de cette information est opérationnelle dès que l'option est paramétrée sur le serveur Sips suite à la demande du commerçant.

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 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.

7. « DEBRAYAGE » DES CONTROLES COMPLEMENTAIRES DE LUTTE CONTRE LA FRAUDE

Un commerçant adhérant au service des contrôles complémentaires pour ses transactions de paiement a la possibilité de débrayer momentanément tout ou partie des ses contrôles.

Pour débrayer un ou plusieurs contrôles complémentaires, il suffit de notifier le mot-clef correspondant au contrôle dans le champ *DATA* de l'API de la manière suivante :

Contrôle	***Mot-clé***
Suppression du contrôle d'en-cours carte	NO_CTL_SCORING
Suppression du contrôle liste grise carte	NO_CTL_GREYCARD
Suppression du contrôle liste grise des codes postaux	NO_CTL_GREYCODE
Suppression du contrôle des BIN étrangers	NO_CTL_BIN
Suppression du retour du pays de l'adresse IP	NO_INF_IP
Suppression du retour des informations carte	NO_INF_CARD
Suppression du contrôle des e-Carte Bleue	NO_CTL_ECARD
Suppression du contrôle du pays de l'IP	NO_CTL_IP_COUNTRY
Suppression du contrôle sur la liste Oppotota	NO_CTL_OPPOTOTA
Suppression du contrôle de similitude pays carte/IP	NO_CTL_SIMILARITY
Suppression du contrôle de carte à autorisation systématique	NO_CTL_SYSTEMATIC
Suppression du contrôle de plages de BIN	NO_CTL_BIN_RANGE
Suppression du contrôle d'en-cours IP	NO_CTL_VELOCITY_IP
Suppression de tous les contrôles	NO_CTL_ALL

Les mot-clés doit être séparés d'un point-virgule.

Exemple : data= « NO_CTL_SCORING;NO_INF_IP »

8. ANNEXES

8.1 ANNEXE 1 : CHAMP COMPLEMENTARY_CODE

Le tableau suivant liste les différentes valeurs que peut prendre le champ *complementary_code.*

Champ complementary_code	
Valeur	Signification
non renseigné	Contrôle local non effectué
00	Contrôle local OK
02	En-cours carte KO
03	Liste grise carte KO
04	Liste grise codes postaux KO
05	BIN inconnu
06	BIN étranger
07	e-Carte Bleue détectée
08	Plage de BIN KO
09	Pays IP inconnu
10	Pays IP interdit
11	Carte dans Oppotota
12	Combinaison pays carte/IP interdite
13	Pays IP ou carte inconnu
14	Carte à autorisation systématique
15	BIN inconnu (sur le contrôle de carte à autorisation systématique)
16	En-cours IP KO
99	Problème technique

8.2 ANNEXE 2 : CODES PAYS ALPHABETIQUE ISO 3166

ABW	Aruba	AFG	Afghanistan	AGO	Angola
AIA	Anguilla	ALB	Albanie	AND	Andorre
ANT	Antilles Néerlandaises	ARE	Emirats arabes unis	ARG	Argentine
ARM	Arménie	ASM	Samoa américaines	ATA	Antarctique
ATF	Terres australes françaises	ATG	Antigua et Barbuda	AUS	Australie
AUT	Autriche	AZE	Azerbaïdjan	BDI	Burundi
BEL	Belgique	BEN	Bénin	BFA	Burkina faso
BGD	Bangladesh	BGR	Bulgarie	BHR	Bahreïn
BHS	Bahamas	BIH	Bosnie Herzégovine	BLR	Bélarus
BLZ	Belize	BMU	Bermudes	BOL	Bolivie
BRA	Brésil	BRB	Barbade	BRN	Brunéi Darussalam
BTN	Bhoutan	BVT	Bouvet, île	BWA	Botswana
CAF	Centrafricaine, République	CAN	Canada	CCK	Cocos (Keeling), îles
CHE	Suisse	CHL	Chili	CHN	Chine
CIV	Côte d'Ivoire	CMR	Cameroun	COG	Congo
COK	Cook, îles	COL	Colombie	COM	Comores
CPV	Cap-Vert	CRI	Costa rica	CUB	Cuba
CXR	Christmas, îles	CYM	Caïmanes, îles	CYP	Chypre
CZE	Tchèque, république	DEU	Allemagne	DJI	Djibouti
DMA	Dominique	DNK	Danemark	DOM	Dominicaine, république
DZA	Algérie	ECU	Equateur	EGY	Egypte
ERI	Erythrée	ESH	Sahara occidental	ESP	Espagne
EST	Estonie	ETH	Ethiopie	FIN	Finlande
FJI	Fidji	FLK	Falkland, îles (Malvinas)	FRA	France
FRO	Féroé, îles	FSM	Micronésie, Etats fédérés de	GAB	Gabon
GBR	Royaume-uni	GEO	Géorgie	GHA	Ghana
GIB	Gibraltar	GIN	Guinée	GLP	Guadeloupe
GMB	Gambie	GNB	Guinée-Bissau	GNQ	Guinée équatoriale
GRC	Grèce	GRD	Grenade	GRL	Groenland
GTM	Guatemala	GUF	Guyane française	GUM	Guam
GUY	Guyana	HKG	Hong-kong	HMD	Heard, île et McDonald, îles
HND	Honduras	HRV	Croatie (nom local: Hrvatska)	HTI	Haïti
HUN	Hongrie	IDN	Indonésie	IND	Inde
IOT	Océan indien, Territoire britannique de l'	IRL	Irlande	IRN	Iran, république islamique d'
IRQ	Iraq	ISL	Islande	ISR	Israël
ITA	Italie	JAM	Jamaïque	JOR	Jordanie
JPN	Japon	KAZ	Kazakhstan	KEN	Kenya
KGZ	Kirghizistan	KHM	Cambodge	KIR	Kiribati
KNA	Saint Kitts and Nevis	KOR	Corée, République de	KWT	Koweït
LAO	Lao, République démocratique populaire	LBN	Liban	LBR	Libéria
LBY	Libyenne, Jamahiriya arabe	LCA	Saint Lucia	LIE	Liechtenstein
LKA	Sri Lanka	LSO	Lesotho	LTU	Lituanie
LUX	Luxembourg	LVA	Lettonie	MAC	Macao
MAR	Maroc	MCO	Monaco	MDA	Moldova, République de

MDG	Madagascar	MDV	Maldives	MEX	Mexique
MHL	Marshall, îles	MKD	Macédoine, l'ex-république yougoslave de	MLI	Mali
MLT	Malte	MMR	Myanmar	MNG	Mongolie
MNP	Mariannes du nord, îles	MOZ	Mozambique	MRT	Mauritanie
MSR	Montserrat	MTQ	Martinique	MUS	Maurice
MWI	Malawi	MYS	Malaisie	MYT	Mayotte
NAM	Namibie	NCL	Nouvelle-Calédonie	NER	Niger
NFK	Norfolk, île	NGA	Nigéria	NIC	Nicaragua
NIU	Niué	NLD	Pays-bas	NOR	Norvège
NPL	Népal	NRU	Nauru	NZL	Nouvelle-Zélande
OMN	Oman	PAK	Pakistan	PAN	Panama
PCN	Pitcairn	PER	Pérou	PHL	Philippines
PLW	Palaos	PNG	Papouasie-Nouvelle-Guinée	POL	Pologne
PRI	Porto Rico	PRK	Corée, République populaire démocratique de	PRT	Portugal
PRY	Paraguay	PYF	Polynésie française	QAT	Qatar
REU	Réunion	ROM	Roumanie	RUS	Russie, Fédération de
RWA	Rwanda	SAU	Arabie saoudite	SDN	Soudan
SEN	Sénégal	SGP	Singapour	SGS	Géorgie du sud et les îles Sandwich du sud
SHN	Sainte-Hélène	SJM	Svalbard et île Jan Mayen	SLB	Salomon, îles
SLE	Sierra leone	SLV	El Salvador	SMR	Saint-Marin
SOM	Somalie	SPM	Saint-Pierre-et-Miquelon	STP	Sao Tomé-et-Principe
SUR	Suriname	SVK	Slovaquie	SVN	Slovénie
SWE	Suède	SWZ	Swaziland	SYC	Seychelles
SYR	Syrienne, république arabe	TCA	Turks et Caïques, îles	TCD	Tchad
TGO	Togo	THA	Thaïlande	TJK	Tadjikistan
TKL	Tokelau	TKM	Turkménistan	TMP	Timor-Leste
TON	Tonga	TTO	Trinité-et-Tobago	TUN	Tunisie
TUR	Turquie	TUV	Tuvalu	TWN	Taïwan, Province de Chine
TZA	Tanzanie, République-unie de	UGA	Ouganda	UKR	Ukraine
UMI	Iles mineures éloignées des Etats-Unis	URY	Uruguay	USA	Etats-Unis
UZB	Ouzbékistan	VAT	Saint-Siège (Etat de la cité du Vatican)	VCT	Saint Vincent et les Grenadines
VEN	Vénézuéla	VGB	Iles Vierges britanniques	VIR	Iles Vierges des Etats-Unis
VNM	Viet Nam	VUT	Vanuatu	WLF	Wallis et Futuna
WSM	Samoa	YEM	Yémen	YUG	Yougoslavie
ZAF	Afrique du Sud	ZAR	Zaïre	ZMB	Zambia
ZWE	Zimbabwe				

8.3 ANNEXE 3 : LISTE DES CODES PRODUITS

Produit CB

Code	Libellé ou commentaires
1	Carte nationale de retrait
2	Carte nationale de retrait et de paiement
3	Carte nationale de paiement
4	Carte nationale de paiement et de retrait à autorisation systématique
5	Carte nationale de paiement à autorisation systématique

Produit VISA

Code	Libellé ou commentaires
A	ATM
B	Business Card
C	Classic
E	Electron
G	Visa Travel Money
H	Super Premium / Infinite
J	Platinium
K	Signature
P	Gold/Premier
R	Corporate
S	Purchasing Card

Produit EPI/MCI

Code	Libellé ou commentaires
1	Standard
2	Corporate Purchasing
3	Corporate Business
4	Corporate Fleet card
5	Gold
6	Debit gold
7	Debit
8	World
9	Platinium class
A	Mastercard Corporate Card
B	Private Label generic service
C	Eurocard Master
D	Proprietary
E	Cirrus
F	Eurocheque pictogram
G	Maestro
H	Mastercard Electronic Card
J	Mastercard debit
K	Mastercard debit other
L	Mastercard debit Platinum
M	Mastercard Debit Brokerage
N	Mastercard Debit Pre-Paid

8.4 ANNEXE 4 : LISTES PREETABLIES DES CODES PAYS

Clé	Commentaire
	Valeurs
#FRJEL	Liste des pays autorisés pour les jeux en ligne français
	AUT,BEL,BGR,CYP,CZE,DEU,DNK,ESP,EST,FIN,FRA,GBR,GRC,HUN,IRL,ISL,ITA,LTU,LUX, LVA,MLT,NLD,NOR,POL,PRT,ROM,SVK,SVN,SWE