API Server

Guide du composant

CHECKOUT 1.03

Version AA
Août 2009

Avertissements :

- **Le fichier Version.txt précise l'environnement dans lequel le composant a été compilé et testé. L'installation du composant sur tout autre environnement n'est pas garantie.**
- **Le composant Checkout version 1.03 nécessite l'installation de l'API Server 2.04 ou supérieur.**

SOMMAIRE

1. INTRODUCTION

L'objectif de ce document est de vous aider à mettre en œuvre le composant Checkout. Pour ce faire, nous allons tout d'abord décrire le fonctionnement général du composant Checkout. Cette description va vous permettre de visualiser les différentes étapes d'une requête. Nous listerons ensuite les étapes de la mise en œuvre du composant avant de les décrire précisément.

Remarque

Ce document ne décrit pas comment vous interfacer avec votre système d'information ou votre base de données. Dans les exemples de requêtes XML fournis, les variables sont déjà renseignées, vous devrez programmer la lecture et la mise à jour des données de votre système d'information.

Pré-requis :

- Savoir programmer une connexion socket en protocole TCP/IP (des exemples en ASP, C, JAVA, PERL et PHP sont fournis avec l'API Server).
- Le compilateur ou l'interpréteur associé au langage choisi.
- L'API Server installé (cf. *LE GUIDE D'INSTALLATION*).
- Avoir des notions de XML.
- Avoir lu la *PRESENTATION GENERALE DE SIPS OFFICE SERVER*

Conventions d'écriture

Dans tout le document, les conventions d'écriture suivantes seront utilisées :

- Les renvois à d'autres documentations seront notés en majuscules et en italique.
  ex *: LE GUIDE D'INSTALLATION*
- Les champs du composant seront notés en **gras**.
  ex : **transaction_id**
- Les chemins et les noms de fichiers seront notés en *italique*.
  ex : *pathfile*

En plus de la *PRESENTATION GENERALE DE SIPS OFFICE SERVER* livrée avec le composant Office, ce document fait référence aux documentations suivantes livrées avec l'API Server.

- *LE GUIDE D'INSTALLATION* (manuel présentant les différentes étapes de l'installation de l'API Server)
- *LE GUIDE D'ADMINISTRATION* (manuel présentant les différentes fonctions d'administration de l'API Server)
- *LE GUIDE DU DEVELOPPEUR* (présentation générale de l'envoi des requêtes)
- *LA DESCRIPTION DES JOURNAUX* (manuel décrivant les différents formats des journaux de fonds)

2. FONCTIONNEMENT GENERAL DU COMPOSANT CHECKOUT

3-D Secure est un protocole de paiement sécurisé sur Internet. Il a été développé par Visa pour augmenter le niveau de sécurité des transactions, et il a été adopté par Mastercard.

Le concept de base de ce protocole est de lier le processus d'autorisation bancaire avec une authentification en ligne. Cette authentification est basée sur un modèle comportant 3 domaines (d'où le nom *3D*) qui sont:

- Le commerçant
- La banque
- Le système de carte bancaire

Lors de son authentification en ligne, l'internaute doit saisir une information personnelle sur l'ACS de sa banque (serveur de contrôle d'authentification piloté par la banque du porteur).

Dans le processus de la norme 3D-Secure, une transaction se déroule en trois étapes :

- Vérification d'enrôlement afin de savoir si la carte est enrôlée 3D-Secure ou non
- Authentification du porteur sur l'ACS de sa banque seulement dans le cas où il est enrôlé 3D-Secure
- Demande d'autorisation 3D-Secure

L'enchaînement de ces trois étapes forme un dispositif visant à réduire le risque d'impayé émis pour contestation du porteur.
Ce dispositif appelé **"liability shift"** ou **"transfert de responsabilité"** a pour principe de faire supporter le risque d'impayé émis pour contestation du porteur à la banque de celui-ci et non plus au commerçant. Si le porteur a validé son paiement en renseignant les données 3D Secure et que le commerçant a respecté les mesures de sécurité énoncées dans les conditions générales de vente de son contrat de commerce électronique, le commerçant ne subira pas la conséquence des impayés.

Le composant Checkout permet de créer des transactions 3D ou simplement contrôler si le porteur s'est bien authentifié 3D sur l'ACS de son acquéreur.
Pour plus d'informations sur la création des transactions, référez-vous à la *PRESENTATION GENERALE DE SIPS OFFICE SERVER*.

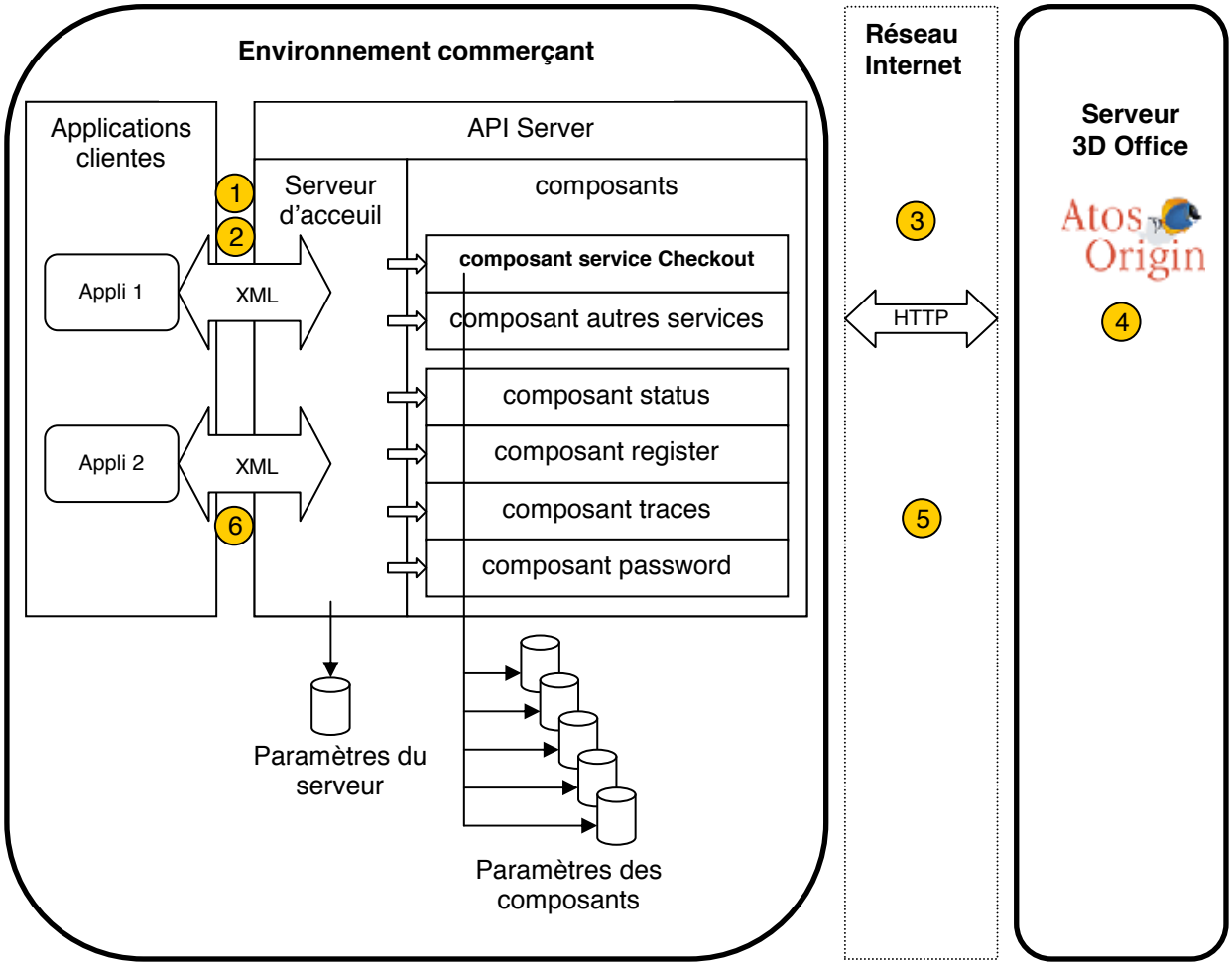


Figure 1: Shéma des connexions entre les applications clientes du commerçant et le serveur 3D Office d'Atos Origin

Pour créer une transaction 3D, le commerçant doit envoyer une requête au composant Checkout qui se connectera ensuite au serveur 3D Office d'Atos Origin. Ce processus peut se résumer en six étapes représentées sur la Figure 1 :
1/ connexion socket en protocole TCP/IP entre l'application cliente et l'API Server
2/ envoi de la requête associée à l'opération souhaitée au format XML
3/ connexion socket en protocole TCP/IP et envoi d'une requête HTTP entre le composant Checkout et le serveur 3D Office d'Atos Origin à l'adresse *office.sips-atos.com*
4/ accès à la base de données Atos Origin, demande d'autorisation vers les services bancaires si nécessaire
5/ le composant Checkout reçoit la réponse du serveur 3D Office d'Atos Origin et ferme la connexion socket
6/ l'application cliente reçoit la réponse du composant Checkout et ferme la connexion socket

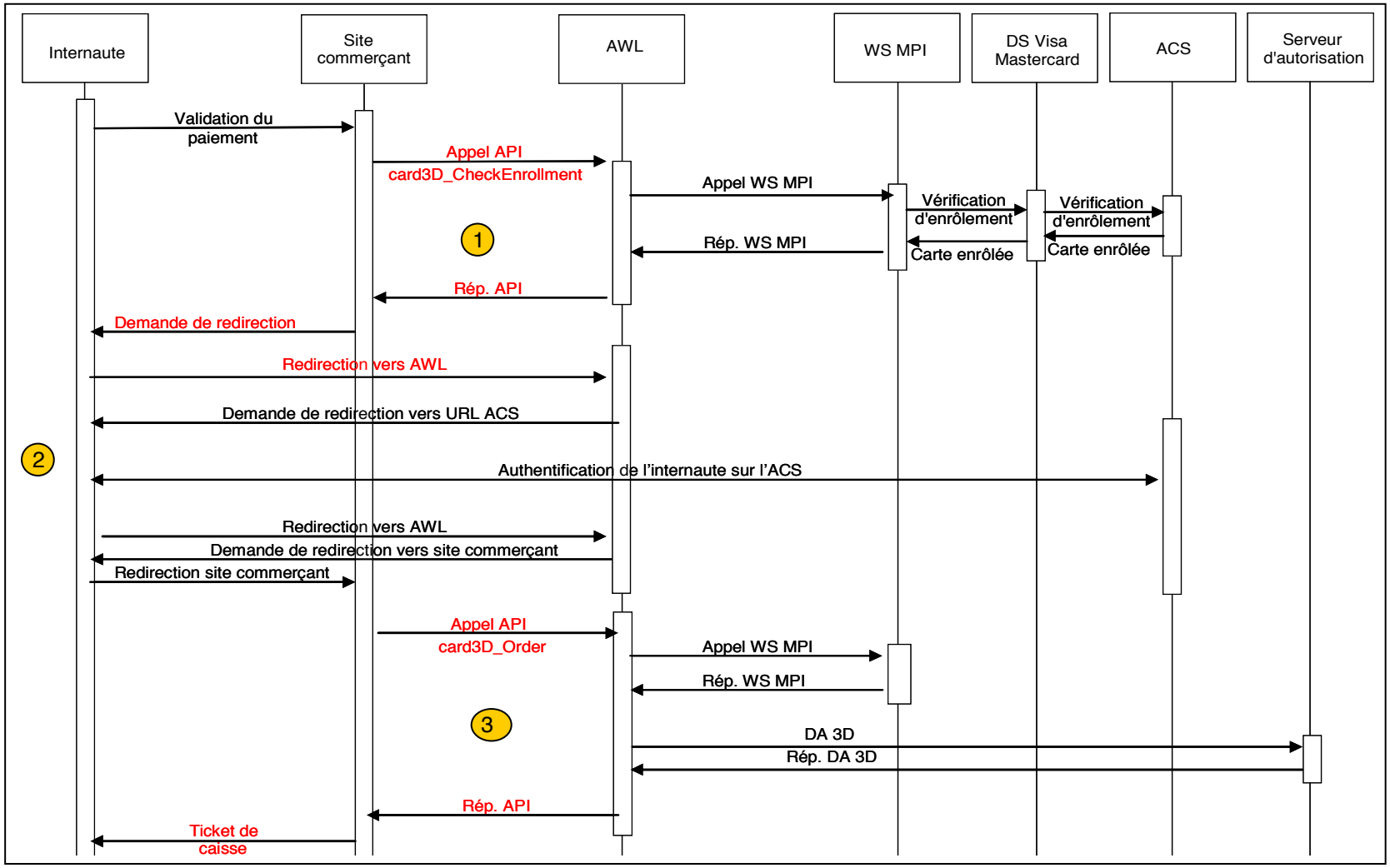


Figure 2: Shéma de la cinématique d'une transaction 3D-Secure (avec demande d'autorisation)

La création d'une transaction 3D peut se résumer en 3 étapes représentées sur la Figure 2 :
1/ **VERIFICATION D'ENROLEMENT** : Après validation du paiement par l'internaute, le site commerçant envoie une requête card3D_CheckEnrollment qui va permettre de vérifier l'enrôlement 3D du porteur. Lors de cette requête, AWL contacte le Web Service MPI (Merchant Plug-In). Ce dernier consultera les DS Visa/Mastercard (Directory Server) et l'ACS (Access Control Server) afin d'obtenir cette information.

2/ **AUTHENTIFICATION DU PORTEUR SUR L'ACS** : En retour de la requête card3D_CheckEnrollment, le site commerçant redirigera le flux vers AWL à l'aide d'une URL obtenue en réponse de la requête. Cela va provoquer la redirection de l'internaute sur son ACS afin qu'il puisse s'authentifier.

3/ **DEMANDE D'AUTORISATION 3D** : Après la phase d'authentification, le site commerçant envoie une requête card3D_Order qui va permettre de vérifier si l'internaute s'est bien authentifié sur son ACS (par le biais d'un appel au Web Service MPI) puis d'effectuer une demande d'autorisation 3D.

Ou

3'/ **VERIFICATION D'AUTHENTIFICATION 3D** : Après la phase d'authentification, le site commerçant envoie une requête card3D_Authenticate qui va SEULEMENT permettre de vérifier si l'internaute s'est bien authentifié sur son ACS. Il est à noter qu'aucune demande d'autorisation ne sera effectuée avec cette requête.

3. MISE EN ŒUVRE DU COMPOSANT

La mise en place complète du composant se déroule en quatre phases:

- installation et paramétrage du composant
- premiers tests sur le serveur de démonstration Office avec les fichiers d'exemple fournis dans le répertoire *examples* du répertoire principal de l'API Server et les exemples de requête XML présentés dans ce document
- le développement de vos applications clientes pour l'envoi de requête vers l'API Server
- les tests sur le serveur de production

Toutes ces étapes seront décrites plus précisément dans la suite de ce guide.

4. INSTALLATION ET PARAMETRAGE DU COMPOSANT

4.1. INSTALLATION

4.1.1. Liste des objets livrés

Le composant Checkout est livré sous la forme d'un fichier *composant_checkout_100.tar* contenant les fichiers suivants :

Fichier *Version.txt*	Fichier précisant l'environnement dans lequel le composant a été compilé et testé.
Répertoire checkout/*param*	
certif.fr.011223344553334	Certificat de la boutique de démonstration
pathfile	Fichier des informations proxy et du chemin d'accès au certificat
Répertoire *server/components/service*	
checkout.*jar*	archive du composant Checkout

4.1.2. Copie des fichiers

Vous devez tout d'abord décompresser le fichier *composant_checkout_100.tar*.

Pour un OS de type Unix :
Utiliser la commande suivante : tar –xvf *composant_checkout_100.tar*

Pour Windows :
Utiliser un logiciel de décompression qui accepte les fichiers d'extension « .tar ».

Après avoir décompressé le fichier *composant_checkout_100.tar*, vous devez copier le répertoire *checkout* et tout ce qu'il contient dans le répertoire principal de l'API Server. Le répertoire principal de l'API Server contient également les répertoires associés aux autres composants que vous utilisez, ainsi que le répertoire *server*.
Vous devez également copier le fichier *checkout.jar* dans le répertoire *server/components/service* du répertoire principal de l'API Server.

4.2. CONFIGURATION

4.2.1. Les paramètres du proxy

Si vous utilisez un proxy pour vous connecter à Internet, vous devez le paramétrer dans le fichier *pathfile* copié précédemment dans le répertoire *checkout/param*. Ce paramétrage permettra au composant Checkout de contacter le serveur Office d'Atos Origin via l'Internet (cf. étape 3 de la Figure 1).

Si vous n'utilisez pas de proxy pour vous connecter à Internet, vous ne devez rien indiquer dans les champs suivants :

PROXY_HOST : adresse IP ou nom du proxy.
PROXY_PORT : le numéro de port du proxy.

En cas de doute, votre administrateur réseau pourra vous indiquer les valeurs à renseigner.

Exemple :
Si vous passez par le proxy d'adresse IP 111.11.11.11 et de port 7878 vous devez paramétrer les champs :
PROXY_HOST!111.11.11.11!
PROXY_PORT!7878!

4.2.2. Configuration du chemin vers les fichiers certificats

Le chemin vers les fichiers certificat est localisé dans le fichier *pathfile* copié précédemment dans le répertoire *checkout/param*. Ce chemin doit être renseigné dans le champ F_CERTIFICATE et est unique pour tous les certificats du composant Checkout. Tous les fichiers certificats que vous utiliserez avec le composant Checkout devront donc être localisés dans un même répertoire.

Remarque

Les extensions du fichier certificat ne doivent en aucun cas être indiquées dans le champ F_CERTIFICATE. En effet, ces extensions correspondent aux paramètres **merchant_country** et **merchant_id** transmis dans les requêtes associées aux différentes opérations. Ils seront donc ajoutés par le composant au paramètre F_CERTIFICATE pour obtenir le chemin complet du certificat souhaité.

Exemple Windows :
Si le fichier *certif.fr.011223344553334* est localisé dans le répertoire *C:\API_Server\checkout\param*, vous devez renseigner le champ F_CERTIFICATE comme suit :

F_CERTIFICATE!C:\API_Server\checkout\param\certif!

Exemple autres OS :
Si le fichier *certif.fr.011223344553334* est localisé dans le répertoire */home/API_Server/checkout/param/*, vous devez renseigner le champ F_CERTIFICATE comme suit :

F_CERTIFICATE!/home/API_Server/checkout/param/certif!

4.2.3. Configuration du chemin vers le fichier pathfile

Vous devez paramétrer dans le fichier *config.xml* le chemin vers le fichier *pathfile* du composant Checkout. Le fichier *config.xml* est localisé dans le répertoire *server/config/* de l'API Server.

Vous trouverez ci-dessous le paragraphe concerné dans le fichier *config.xml* :

```
<components>
<pathfile id="example" path="chemin_du_fichier_pathfile" />
</components>
```

Vous devez ajouter la ligne suivante entre les balises <components> et </components> :

<pathfile id="checkout" path="chemin_absolu_vers_le_fichier_pathfile" />

avec :
id : l'identifiant du composant (ici checkout).
path : le chemin absolu vers le fichier *pathfile*.

Remarque

Le nom indiqué dans le champ « id » doit être identique au nom de l'archive sans l'extension « .jar » (cf. paragraphe 4.1.1)

Exemple Windows :
Si le fichier *pathfile* est localisé dans le répertoire *C:\API_Server\checkout\param*, vous devez renseigner la ligne comme suit :

<pathfile id="checkout" path="C:\API_Server\checkout\param\pathfile" />

Exemple autres OS :
Si le fichier *pathfile* est localisé dans le répertoire */home/API_Server/checkout/param*, vous devez renseigner la ligne comme suit :

<pathfile id="checkout" path="/home/API_Server/checkout/param/pathfile" />

4.2.4. Configuration des traces

Vous devez paramétrer dans le fichier *config.xml* le chemin des fichiers de traces du composant Checkout. Le fichier *config.xml* est localisé dans le répertoire *server/config/* de l'API Server.

Vous trouverez ci-dessous le paragraphe concerné dans le fichier *config.xml* :

```
<watchdog>
  <pollingTimer>6000</pollingTimer>
  <survPort>7183</survPort>
  <trace level="0" sizeLimit="1000" unit="Line"
path="C:\chemin_racine\server\trace" prefix="APIServer" />
<!--  <alternateTrace id="example" path="C:\chemin_racine\server\trace"
prefix="example" />     -->
  <alternateTrace id="" path="./" prefix="" />
</watchdog>
```

Vous devez ajouter la ligne suivante au-dessus du tag « </watchdog> » (la ligne avec l'identifiant example est en commentaire).

<alternateTrace id="checkout" path="chemin_absolu_vers_le_répertoire_traces"
prefix="checkout" />

avec :
id : l'identifiant du composant (ici checkout).
path : le chemin absolu vers le répertoire des traces. Vous pouvez utiliser pour vos traces le répertoire *server/traces* du répertoire principal de l'application ou tout autre répertoire de votre choix.

prefix : préfixe du fichier de traces du composant. Dans l'exemple ci-dessus, le nom du composant est utilisé, mais tout autre préfixe est également valable.

Remarque

- le nom indiqué dans le champ « id » doit être identique au nom de l'archive sans l'extension « .jar » (cf. paragraphe 4.1.1).
- La ligne « <alternateTrace id="" path="./" prefix="" />" est nécessaire au démarrage de l'API Server dans le cas ou aucun composant n'est installé, il est donc important de ne pas la modifier.

Exemple Windows :
Si le chemin du répertoire trace est *C:\API_Server\server\traces*, vous devez renseigner la ligne comme suit :

<alternateTrace id="checkout" path="C:\API_Server\server\traces" prefix="checkout" />

Exemple autres OS :
Si le chemin du répertoire trace est */home/API_Server/server/traces*, vous devez renseigner la ligne comme suit :

<alternateTrace id="checkout" path="/home/API_Server/server/traces" prefix="checkout" />

4.2.5. Adresse IP pour la configuration de votre firewall

Si vous utilisez un firewall pour vous connecter au réseau Internet, vous devez paramétrer au niveau de celui-ci l'adresse IP et le port du serveur Office d'Atos Origin. Pour communiquer avec le serveur Office d'Atos Origin votre firewall doit vous permettre une connexion socket en protocole TCP/IP vers l'adresse IP 193.56.46.110 port 2001.

4.3. ENREGISTREMENT DU COMPOSANT

Vous devez enfin enregistrer votre composant pour qu'il soit connu de l'API Server.
Pour enregistrer votre composant et lister les composants enregistrés, référez-vous respectivement au chapitre **la commande « ENREGISTRER UN NOUVEAU COMPOSANT »** et au chapitre **la commande « LISTER LES COMPOSANTS »** du *GUIDE D'ADMINISTRATION*.

5. TESTS

5.1. VERIFICATION DE L'INSTALLATION DU COMPOSANT CHECKOUT

La première étape consiste à vérifier le paramétrage et l'enregistrement du composant. Vous devez, tout d'abord, créer une connexion socket en protocole TCP/IP entre votre application cliente et l'API Server. Pour ce faire, vous pouvez vous baser sur les fichiers d'exemples livrés avec l'API Server (répertoire *examples* du répertoire principal de l'API Server) et décrits dans le *GUIDE DU DEVELOPPEUR*. Vous devez ensuite envoyer une requête XML de vérification (cf. paragraphe 7.2). Suite à cette requête XML l'API Server ne tente pas de se connecter au serveur Office d'Atos Origin, mais il vérifie la présence des fichiers *pathfile* et *certificat*, et renvoie une réponse à votre application cliente.

5.2. TEST DE CONNEXION VERS LE SERVER OFFICE DE DEMO D'ATOS ORIGIN

Cette étape va vous permettre de tester la connexion entre l'API Server et le serveur de démo Office d'Atos Origin. Vous pouvez transmettre tous les types de requêtes existants (vérification d'enrôlement 3D, demande d'autorisation 3D et vérification d'authentification 3D). Les serveurs de démo et de production Office d'Atos Origin ne sont pas localisés sur la même machine. Par conséquent, si vos requêtes passent par un proxy et/ou un firewall, vous aurez sans doute à le configurer pour laisser passer les requêtes de démo ET de production. Pour la démo l'url du serveur office est http://rcet-office.sips-atos.com:2001, en production l'url du serveur office est http://office.sips-atos.com:2001

Pour effectuer votre test de connexion, vous devez, tout d'abord, créer une connexion socket en protocole TCP/IP entre votre application cliente et l'API Server en vous basant sur les fichiers d'exemples livrés avec l'API Server (répertoire *examples* du répertoire principal de l'API Server) et décrits dans le *GUIDE DU DEVELOPPEUR*. Vous devez ensuite envoyer une requête XML de vérification d'enrôlement vers le serveur de démonstration Office d'Atos Origin (cf. paragraphe 7.3). Dans cette requête XML, vous devrez paramétrer le **merchant_id** à « 011223344553334 » et le **merchant_country** à « fr ». Le composant Checkout utilisera alors le certificat certif.fr.011223344553334 livré avec le composant Checkout (cf. paragraphe 4.1.1).

5.3. COMMENT PASSER SUR LE SERVEUR DE PRODUCTION ?

La dernière phase est le passage en mode « pré-production » (cf. paragraphe ***Comment en profiter*** de la *PRESENTATION GENERALE DE SIPS OFFICE SERVER*). A partir de ce moment les demandes d'autorisation 3D ne sont plus simulées comme sur le serveur de démonstration, mais elles empruntent le circuit complet du réseau bancaire. Cette phase va permettre de contrôler la bonne inscription de votre contrat bancaire.

Le passage en « pré-production » se fait par l'activation du certificat du commerçant qui va remplacer le certificat de démonstration (certif.fr.011223344553334).

1. Copier le certificat de « production », qui vous a été transmis sur disquette ou par mail, dans le même répertoire que le certificat de « démonstration » et renommer ce certificat en certif.fr.<my_merchant_id>, où <my_merchant_id> est votre numéro de boutique.

2. Remplacer le numéro de la boutique de démonstration (011223344553334) par votre numéro de boutique (champ **merchant_id**) dans vos requêtes vers l'API Server.

3. Vous devez faire au minimum un test de demande d'autorisation 3D acceptée. Pour ce test, vous devez utiliser un numéro de carte réelle. Tant que vous êtes en phase de pré-production, les demandes d'autorisation 3D ne sont pas débitées.

4. Pour le passage en « production », voir le document de *PRESENTATION GENERALE* paragraphe ***Comment en profiter***.

5.4. TESTS EN PRE-PRODUCTION

La phase de pré-production sert à valider la bonne inscription de votre boutique.

Nous vous invitons à valider l'ouverture de votre contrat VAD 3D-Secure en transmettant des requêtes de demande d'autorisation 3D avec un vrai numéro de carte. Vous devez recevoir un accord (response_code = 00). Ces transactions ne sont pas enregistrées dans notre base de données et ne sont pas envoyées en banque.

6. DESINSTALLATION DU COMPOSANT

Pour désinstaller le composant Checkout, vous devez :

1) Arrêter votre API Server (cf. chapitre **la commande « ARRETER LE SERVEUR »** du *GUIDE D'ADMINISTRATION*)
2) Supprimer le répertoire *checkout* du répertoire principal de l'API Server
3) Supprimer le fichier *checkout.jar* du répertoire *server/components/service* du répertoire principal de l'API Server.
4) Supprimer du fichier *config.xml* localisé dans le répertoire *server/config/* de l'API Server les lignes suivantes :

<pathfile id="*checkout*" path="chemin_absolu_vers_le_fichier_pathfile" />
<alternateTrace id="*checkout*" path="chemin_absolu_vers_le_répertoire_traces" prefix="*checkout*" />

5) Supprimer les fichiers de traces du composant Checkout
6) Supprimer des listes d'accès (cf. paragraphe **Configuration des listes d'accès** du *GUIDE D'INSTALLATION*) les adresses des machines qui ne doivent plus accéder à l'API Server
7) Supprimer l'autorisation de connexion au serveur Office d'Atos Origin de votre firewall si aucun des composants restants ne l'utilisent.

Au cours du redémarrage de l'API Serveur, la liste des composants restants sera remise à jour.

7. DESCRIPTION DETAILLEE DU COMPOSANT

Ce chapitre décrit les opérations disponibles avec le composant Checkout. Pour chacune de ces opérations, des exemples de requête et de réponse au format XML sont fournis, ainsi que les listes des paramètres de la requête et de la réponse avec des liens vers le dictionnaire des données.

Avant de décrire les fonctions disponibles, nous allons préciser les aspects de la sécurisation du transfert des informations entre le composant Checkout et le serveur Office d'Atos Origin.

Remarques

- Afin d'alléger le code des requêtes, les entêtes standard XML ne sont pas nécessaires, mais sont ajoutées par l'API Server pour vérification lors du parsing XML (utilisation d'un DTD). Par contre, lors des réponses de l'API Server, vers l'application cliente, aucune référence à un DTD n'est incluse dans le message. Il est donc important de désactiver la validation lors du parsing, afin de ne pas déclencher des erreurs durant cette phase.

- Pour des raisons de lisibilité, toutes les requêtes décrites dans ce chapitre sont présentées sur plusieurs lignes. Toutefois, lors de l'appel à l'API Server, elles doivent être codées sans retours chariot.

7.1. SECURISATION DU TRANSFERT DES INFORMATIONS

Voir chapitre **La sécurité des paiements en ligne avec SIPS Office Server** de la *PRESENTATION GENERALE DE SIPS OFFICE SERVER*.

7.2. REQUETE DE VERIFICATION VERS LE COMPOSANT CHECKOUT: CHECKCHECKOUT

7.2.1. Objet

Cette fonction permet de tester :

- la communication entre l'application cliente que vous développez et l'API Server
- le bon fonctionnement de l'API Server
- la configuration du composant Checkout
  - l'accès au fichier *pathfile*
  - l'accès au fichier certificat

7.2.2. Paramètres de la requête et de la réponse

Dans le tableau ci-dessous sont décrits tous les champs de la requête de vérification.

nom du champ	Facultatif/ Obligatoire	Utilisation
component	O	nom du composant appelé
name	O	nom de la fonction appelée
merchant_country	O	code pays du commerçant
merchant_id	O	identifiant du commerçant

Dans le tableau ci-dessous sont décrits tous les champs de la réponse de la vérification.

nom du champ	valeur
pathfile	renseigné à OK si le fichier *pathfile* a bien été trouvé
certificate	renseigné à OK si le fichier *certif.<merchant_country>.<merchant_id>* a bien été trouvé
message	renseigné si le fichier *pathfile* ou *certificat* n'a pu être lu

7.2.3. Exemple de requête et de réponse XML

Ci-dessous est présenté un exemple de requête XML de vérification. La signification des champs **merchant_country** et **merchant_id** est fournie au chapitre 8. Ces champs correspondent respectivement à la première et la deuxième extension du fichier certificat (exemple : le fichier *certif.fr.011223344553334* correspond à **merchant_country**=fr et **merchant_id**=011223344553334).

```
<service component="checkout" name="checkCheckout">
<checkCheckout merchant_id="011223344553334" merchant_country="fr"/>
</service>
```

Lors de la vérification, le composant Checkout va contrôler l'accès en lecture au fichier *pathfile* paramétré dans le fichier *config.xml*, puis l'accès en lecture au fichier certificat (*certif.<merchant_country>.<merchant_id>*) dont le chemin générique est indiqué dans le fichier *pathfile*. Si ces accès sont corrects, la réponse suivante sera envoyée :

```
<response pathfile="OK" certificate="OK" />
```

Si ces accès ne sont pas corrects, la réponse suivante sera envoyée :

```
<Error message="message d'erreur"/>
```

La liste des messages d'erreur est précisée dans le tableau ci-dessous.

Messages d'erreur	Cause	solution
C:\API_Server\checkout\pam\pathfile (Le chemin d'accès spécifié est introuvable)	le fichier *pathfile* configuré dans le fichier *config.xml* n'est pas accessible en lecture	Vérifier les droits d'accès du fichier *pathfile* et corriger le chemin du fichier *pathfile* si nécessaire (cf. paragraphe 4.2.3).
Cannot open certificat. (C:\API_Server\checkout\pam\certif.fr.011223344553334)	le fichier certif.fr.011223344553334 n'est pas accessible en lecture	Vérifier les droits d'accès du fichier certificat *certif.fr.011223344553334* et corriger le chemin génériques des fichiers certificats si nécessaire (cf. paragraphe 4.2.2).

7.3. REQUETE DE VERIFICATION D'ENROLEMENT 3D : CARD3D_CHECKENROLLMENT

7.3.1. Objet

Cette fonction permet au commerçant de vérifier l'enrôlement 3D d'un porteur.

En démonstration (avec le certificat certif.fr.011223344553334), le processus de vérification d'enrôlement 3D est simulé. Il est donc possible de renseigner n'importe quel numéro de carte sans aucune conséquence.

Le code réponse (**3d_response_code**) de la transaction simulée est donné par les 11 et 12ème chiffres du numéro de carte bancaire .

Exemple :

Numéros de carte	Decription du test
4970 xxxx xx00 xxxx	Porteur enrôlé 3D-Secure
4970 xxxx xx01 xxxx	Porteur non enrôlé 3D-Secure
4970 xxxx xx10 xxxx	Impossible de déterminer si le porteur est enrôlé 3D ou non
4970 xxxx xx81 xxxx	Erreur interne sur le MPI
4970 xxxx xx85 xxxx	MPI injoignable
4970 xxxx xx94 xxxx	Erreur technique au cours de l'authentification sur le Directory Server
4970 xxxx xx12 xxxx	Paramètres transmis au MPI invalides
4970 xxxx xx98 xxxx	Problème réseau lors de la tentative d'accès aux Directory Server

7.3.2. Paramètres de la requête et de la réponse

Dans le tableau ci-dessous sont décrits tous les champs de la requête de la vérification d'enrôlement 3D.

nom du champ	Facultatif/ Obligatoire	Utilisation
component	O	nom du composant appelé
name	O	nom de la fonction appelée
amount	O	montant de la transaction
card_number	O	numéro de la carte
card_type	O	type de carte utilisée
card_validity	O	date de validité de la carte
cvv_key	F	cryptogramme visuel
cvv_flag	F	indique la présence ou non du cryptogramme visuel
currency_code	O	code de la monnaie utilisée
merchant_country	O	code pays du commerçant
merchant_id	O	identifiant du commerçant
origin	F	permet d'identifier le programme à l'origine de la demande d'autorisation
transaction_id	O	numéro de la nouvelle transaction
merchant_name	O	nom du commerçant affiché sur l'ACS

merchant_url	**O**	URL du commerçant affichée sur l'ACS
merchant_url_return	**O**	URL de retour vers le site commerçant après l'authentification du porteur sur son ACS
transmission_date	**O***	date de la requête
version	**O***	version du composant

** renseigné par le composant*

Dans le tableau ci-dessous sont décrits tous les champs de la réponse de la vérification d'enrôlement.

nom du champ	origine de la valeur	description
o3d_response_code	renseigné par le serveur 3D Office	Code réponse du serveur 3D Office
o3d_office_url_acs	renseigné par le serveur 3D Office	URL de redirection vers Atos
o3d_session_id	renseigné par le serveur 3D Office	Identifiant de session de la transaction 3D

7.3.3. Exemple de requête et de réponse XML

Ci-dessous est présenté un exemple de requête XML de vérification d'enrôlement 3D.

```
<service component="checkout" name="card3D_CheckEnrollment">
<card3D_CheckEnrollment origin="Batch"
merchant_id="011223344553334"
merchant_country="fr"
transaction_id="130685"
amount="12300"
currency_code="978"
card_number="4970651231011232"
card_validity="201211"
card_type="VISA"
merchant_name=”Commercant_test”
merchant_url=”http://www.commercant_test.com"
merchant_url_return=”http://www.retourACS.com"
cvv_key=”600”
cvv_flag=”1”
/></service>
```

Pour connaître la signification de ces différents champs référez-vous au chapitre 8.

Ci-dessous est présentée la réponse XML de la vérification d'enrôlement 3D précédente.

```
<response component="checkout" name=" card3D_CheckEnrollment">
<card3D_CheckEnrollment
o3d_response_code="00"
o3d_office_url_acs= “https://vre16:29567/3doffice/prod/call_acs;jsessionid=ERF56GD..."
o3d_session_id="3D8B9C023BBDD10EA45294AEC9C2C922.jvm1" />
</response>
```

Pour connaître la signification de ces différents champs référez-vous au chapitre 8.

7.4. REDIRECTION VERS L'ACS ET AUTHENTIFICATION 3DS

Dans le cas où le porteur est enrôlé 3D, il est nécessaire d'effectuer la redirection vers l'ACS afin que celui-ci puisse s'authentifier.

Pour cela, il faut extraire le champ **o3d_office_url_acs** de la réponse à card3D_CheckEnrollment et rediriger le navigateur de l'internaute vers cette URL. Pour tous les cas (erreur ou porteur non enrôlé), ce champ sera vide.

Le navigateur de l'internaute sera ensuite redirigé vers l'ACS de sa banque afin qu'il puisse effectuer son authentification 3D.

En phase de test (demo), l'ACS correspondra au screenshot suivant :

Cette page permet seulement de simuler le passage par un ACS. La saisie d'un mot de passe n'est pas obligatoire et n'aura aucune conséquence sur la suite de la cinématique.

Une fois cette page validée, le navigateur sera alors redirigé vers l'URL initialement présente dans le champ **merchant_url_return** de la requête card3D_CheckEnrollment.

Il est à noter qu'aucun paramètre n'est à récupérer lors de cette redirection chez le commerçant. Cela permet simplement au commerçant de reprendre la main afin d'effectuer une nouvelle requête.

Le site commerçant enverra enfin la dernière requête choisie :

- card3D_Order pour effectuer la vérification de l'authentification 3D et la demande d'autorisation 3D
- card3D_Authenticate pour seulement effectuer la vérification de l'authentification 3D.

7.5. REQUETE DE DEMANDE D'AUTORISATION 3D : CARD3D_ORDER

7.5.1. Objet

Cette fonction permet au commerçant disposant des coordonnées bancaires de ses clients d'effectuer lui-même les demandes d'autorisation 3D (cf. *PRESENTATION GENERALE DE SIPS OFFICE SERVER*).

En démonstration (avec le certificat certif.fr.011223344553334), le processus d'autorisation est simulé. Il est donc possible de renseigner n'importe quel numéro de carte sans aucune conséquence.

Le code réponse (**o3d_response_code**) de l'authentification du porteur sur l'ACS est donné par les 13 et 14ème chiffres du numéro de carte bancaire.
Le code réponse (**response_code**) de la transaction simulée est donné par les deux derniers chiffres du numéro de la carte bancaire.

Exemple :

Numéros de carte	Decription du test
4970 xxxx xxxx 0000	Porteur authentifié et autorisation acceptée
4970 xxxx xxxx 0005	Porteur authentifié et refus de la demande d'autorisation
4970 xxxx xxxx 5575	Porteur non authentifié et refus de la demande d'autorisation pour suspicion de fraude
4970 xxxx xxxx 6200	By-pass du porteur sur l'ACS et autorisation acceptée

Pour les cartes VISA, MASTERCARD et CB, le cryptogramme visuel peut être renseigné (cf. Annexe B). Les cryptogrammes se terminant par 00 ou 40 sont considérés valides, les autres sont considérés invalides.

7.5.2. Paramètres de la requête et de la réponse

Dans le tableau ci-dessous sont décrits tous les champs de la requête de demande d'autorisation 3D.

Remarque

Si une carte ne possède pas de date de validité, le champ **card_validity** doit être présent dans la requête et non renseigné.

Bien que les champs **cvv_key** et **cvv_flag** soient tous les deux facultatifs il doit y avoir une cohérence entre eux. Si le champ **cvv_key** est renseigné, le champ **cvv_flag** doit obligatoirement contenir la valeur 1 (cf. Annexe B).

nom du champ	Facultatif/ Obligatoire	Utilisation
component	**O**	nom du composant appelé
name	**O**	nom de la fonction appelée
amount	**O**	montant de la transaction
capture_day	**F**	délai d'envoi en banque
capture_mode	**F**	mode d'envoi en banque
customer_ip_address	**F**	adresse IP de l'internaute
data	**F**	paramétrage particulier
merchant_country	**O**	code pays du commerçant
merchant_id	**O**	identifiant du commerçant
order_id	**F**	numéro de commande du commerçant
order_validity	**F**	non utilisé
origin	**F**	permet d'identifier le programme à l'origine de la demande d'autorisation
return_context	**F**	contexte de la transaction
transaction_id	**O**	numéro de la nouvelle transaction
o3d_session_id	**O**	Identifiant de session reçu en retour de l'appel à card3D_CheckEnrollment
transmission_date	**O***	date de la requête
version	**O***	version du composant

** renseigné par le composant*

Dans le tableau ci-dessous sont décrits tous les champs de la réponse d'une demande d'autorisation 3D.

nom du champ	origine de la valeur	description
o3d_response_code	Renseigné par le serveur 3D Office	Code réponse de l'authentification 3D
authorisation_id	renseigné par le serveur bancaire (si transaction autorisée)	Identifiant d'autorisation retourné par la banque
bank_response_code	renseigné par le serveur bancaire	Code réponse du serveur d'autorisation bancaire ou privatif
complementary_code	renseigné par le serveur Office	Code réponse complémentaire du serveur
complementary_info	renseigné par le serveur Office	Information sur le code réponse complémentaire
currency_code	identique à la requête	Code de la devise
cvv_response_code	renseigné par le serveur bancaire (si demande d'autorisation avec cryptogramme effectuée)	Champ renvoyé dans le cas d'une demande d'autorisation avec cryptogramme visuel
avs_response_code	renseigné par le serveur Office (si demande d'autorisation avec vérification d'adresse effectuée)	Champ renvoyé dans le cas d'une demande d'autorisation d'un porteur britannique
data	identique à la requête	Champ privé
status	renseigné par le serveur Office	l'état de la transaction après une opération
response_code	renseigné par le serveur Office ou le serveur 3DOffice	Code réponse de la demande d'autorisation
transaction_date	renseigné par le serveur Office	date et heure GMT

transaction_time	renseigné par le serveur Office	heure locale du serveur Office
transaction_certificate	renseigné par le serveur Office (si transaction acceptée)	Champ certifiant que la transaction a été traitée par le serveur Office

Remarque

Le **transaction_id** et l'**amount**, déjà transmis lors de la requête card3D_CheckEnrollment, sont une nouvelle fois des champs obligatoires lors de la requête card3D_Order ou card3D_Authenticate. Il est obligatoirede transmettre un **transaction_id** et un **amount** identiques que ceux envoyés dans la première requête.

Le **transaction_id** de la requête card3D_Order sera inscrit en base de données alors que celui de la requête card3D_CheckEnrollment est utilisé pour le cryptage des messages échangés.Quant à l'**amount**, celui de la requête card3D_Order est inscrit en base puis remisé en banque alors que celui de la requête card3D_CheckEnrollment est seulement affiché sur l'ACS.

Remarque

Lorsque la carte de paiement n'est pas enrôlé 3D-Secure, la demande de paiement s'effectue tout de même avec la requête card3D_Order du composant Checkout et non plus avec la fonction author() du composant Office.

7.5.3. Exemple de requête et de réponse XML

Ci-dessous est présenté un exemple de requête XML de demande d'autorisation 3D.

```
<service component="checkout" name="card3D_Order">
<card3D_Order origin="Batch"
merchant_id="011223344553334"
merchant_country="fr"
transaction_id="130685"
amount="12300"
return_context="context"
order_id="OI_131100_8744"
capture_mode="VALIDATION"
capture_day="2"
data=""
order_validity=""
o3d_session_id=" 71B78471DAC1B849421690AF2C418931.sips_3doffice-1"
/></service>
```

Pour connaître la signification de ces différents champs référez-vous au chapitre 8.

Ci-dessous est présentée la réponse XML de la demande d'autorisation 3D précédente.

<response component="checkout" name="card3D_Order">
<card3D_Order response_code="00"
o3d_response_code="00"
transaction_time="114147"
transaction_date="20030801"
transaction_certificate="1059730907"
authorisation_id="1059"
status="TO_VALIDATE"
currency_code="978"
data=""
avs_response_code=""
cvv_response_code="4D"
bank_response_code="00"
complementary_code=""
complementary_info="" />
</response>

Pour connaître la signification de ces différents champs référez-vous au chapitre 8.

7.6. REQUETE DE DEMANDE D'AUTHENTIFICATION 3D : CARD3D_AUTHENTICATE

7.6.1. Objet

Cette fonction permet au commerçant de contrôler l'authentification 3D d'un porteur sans effectuer de demande d'autorisation.

En démonstration (avec le certificat certif.fr.011223344553334), le processus d'authentification 3D est simulé. Il est donc possible de renseigner n'importe quel numéro de carte sans aucune conséquence.

Le code réponse (**o3d_response_code**) de l'authentification du porteur sur l'ACS est donné par les 13 et 14ème chiffres du numéro de carte bancaire.

Exemple :

Numéros de carte	Decription du test
4970 xxxx xxxx 00xx	Porteur authentifié
4970 xxxx xxxx 55xx	Porteur non authentifié
4970 xxxx xxxx 62xx	By-pass du porteur sur l'ACS

7.6.2. Paramètres de la requête et de la réponse

Dans le tableau ci-dessous sont décrits tous les champs de la requête de demande d'authentification 3D.

nom du champ	Facultatif/ Obligatoire	Utilisation
component	O	nom du composant appelé
name	O	nom de la fonction appelée
amount	O	montant de la transaction
merchant_country	O	code pays du commerçant

merchant_id	**O**	identifiant du commerçant
origin	**F**	permet d'identifier le programme à l'origine de la demande d'autorisation
transaction_id	**O**	numéro de la nouvelle transaction
o3d_session_id	**O**	Identifiant de session reçu en retour de l'appel à card3D_CheckEnrollment
data	**F**	Paramètre particulier
transmission_date	**O***	date de la requête
version	**O***	version du composant

** renseigné par le composant*

Dans le tableau ci-dessous sont décrits tous les champs de la réponse de la demande d'authentification 3D.

nom du champ	origine de la valeur	description
o3d_response_code	renseigné par le serveur 3D Office	Code réponse de l'authentification 3D

7.6.3. Exemple de requête et de réponse XML

Ci-dessous est présenté un exemple de requête XML de demande d'authentification 3D.

```
<service component="checkout" name="card3D_Authenticate">
<card3D_Authenticate origin="API SERVER"
merchant_id="011223344553334"
merchant_country="fr"
transaction_id="130685"
data=""
amount="3200"
o3d_session_id=”3D8B9C023BBDD10EA45294AEC9C2C922.jvm1”
</service>
```

Pour connaître la signification de ces différents champs référez-vous au chapitre 8.

Ci-dessous est présentée la réponse XML de la demande d'authentification 3D précédente.

```
<response component="checkout" name="card3D_Authenticate">
< card3D_Authenticate o3d_response_code="00"
/></response>
```

Pour connaître la signification de ces différents champs référez-vous au chapitre 8

7.7. ABSENCE DE REPONSE ET MESSAGES D'ERREUR

Si vous ne recevez pas de réponse, vous devez vérifier les points suivants :

- L'API Server est-il bien démarré ? (cf. chapitre **Lancement du serveur** du *GUIDE D'INSTALLATION*)
- N'y a-t-il pas un firewall entre le client et l'API Server qui pourrait empêcher l'accès au serveur ?
- Est-ce que l'adresse de la machine cliente est paramétrée dans les listes d'accès de l'API Server ? (cf. paragraphe **Configuration des listes d'accès** du GUIDE D'INSTALLATION)
- L'adresse IP de l'API Server que vous utilisez pour votre connexion socket est-elle correcte ?

- Le port de l'API Server que vous utilisez pour votre connexion socket est-il identique à celui configuré dans le fichier config.xml (cf. paragraphe **Configuration des paramètres de service** du GUIDE D'INSTALLATION)
- Avez-vous enregistré le composant Checkout (cf. paragraphe **La commande « ENREGISTRER UN NOUVEAU COMPOSANT »** du GUIDE D'ADMINISTRATION)

Si vous obtenez un message d'erreur tel que celui présenté ci-dessous :

<Error message=" message d'erreur "/>

cela signifie que la requête a bien été reçue par l'API Server, mais elle comporte une erreur. Vous trouverez dans le tableau ci-dessous les principaux messages renvoyés par le composant ainsi que leur origine.

Exemple de messages	Cause	solution
(Le chemin d'accès spécifié est introuvable)	il y a une erreur au niveau du paramètre « id="checkout" » du sous-attribut pathfile dans le fichier *config.xml*	Corriger la configuration en vous référant au paragraphe 4.2.3.
Element "service" does not allow "toto" here.	toto n'est pas un nom d'opération correct dans la requête XML.	Corriger le nom de l'opération en vous référant aux exemples des paragraphes 7.3 à 7.6.
Attribute "toto" is not declared for element "checkCheckout".	Vous utilisez un nom d'attribut inconnu dans la requête XML.	Vérifier le nom des attributs en vous référant aux exemples des paragraphes 7.3 à 7.6.
Root element type is "service", but was declared to be "command".	Vous utilisez le port de commande de l'API Server au lieu du port de service	Utiliser le port de service configuré dans le fichier *config.xml* pour votre connexion socket à l'API Server (cf. (cf. GUIDE D'ADMINISTRATION).
Autres messages		Contacter le Centre d'Assistance Technique

8. DICTIONNAIRE DES DONNEES DU COMPOSANT

Ce chapitre décrit toutes les caractéristiques des champs présents dans le composant Checkout. Nous allons tout d'abord présenter les conventions d'écriture utilisées dans la description des champs ainsi que les caractères qui ne doivent pas être renseignés dans certains de ces champs.

8.1. CONVENTIONS D'ECRITURE

Afin d'accéder le plus rapidement possible aux informations nécessaires à l'utilisation d'un champ du composant Checkout, toutes les caractéristiques des champs sont décrites suivant le même modèle.

Champ : **Nom du champ dans les structures de requête et de réponse**

Format : Type de caractères acceptés dans ce champ. Le type est spécifié par la combinaison des lettres a, n et s correspondant à :

- **a** : caractère alphabétique.
- **n** : caractère numérique.
- **s** : caractère spécial.

Un champ de format **an** acceptera donc des caractères alphanumériques.

Taille : Deux possibilités pour la taille du champ :
Jusqu'à X caractères : champs de taille variable
X caractères : champs de taille fixe

Description : Description de la fonctionnalité du champ

8.2. CARACTERES INTERDITS

Les caractères « | », « ; » et « : » sont interdits dans les champs suivants : order_id, origin et return_context.

Si ces caractères sont utilisés, ils sont remplacés par des blancs par le serveur Office. Dans le journal des transactions et le journal des opérations, ces champs contiendront donc des blancs à la place des caractères interdits.

8.3. DESCRIPTION DES CHAMPS

Champ :	**amount**
Format :	n
Taille :	jusqu'à 12 caractères (minimum 3 caractères)
Description :	Contient le montant de l'opération. Le montant doit être transmis dans la plus petite unité de la devise. Exemple pour l'Euro : un montant de 10,50 Euros doit être transmis sous la forme 1050 et un montant de 0,50 Euros doit être transmis sous la forme 050. Pour les autres devises voir tableau annexe A.

Champ :	**authorisation_id**
Format :	an
Taille :	jusqu'à 32 caractères
Description :	Pour toute opération conduisant à une demande d'autorisation, ce champ contient l'identifiant d'autorisation retourné par la banque si la demande a été acceptée.

Champ :	**avs_response_code**
Format :	n
Taille :	2 caractères
Description :	Champ renvoyé dans la réponse dans le cas d'une demande d'autorisation d'un porteur britannique chez un commerçant britannique. Pour connaître la composition et la signification de ce champ, veuillez vous référer à l'annexe K.

Champ :	**bank_response_code**
Format :	n
Taille :	2 caractères
Description :	Champ renvoyé dans la réponse et contenant le code de la réponse du serveur d'autorisation bancaire ou privatif. Pour connaître la valeur des différents codes et leur signification, référez-vous à l'annexe F.

Champ :	**capture_day**
Format :	n
Taille :	jusqu'à 2 caractères
Description :	Contient le nombre de jours avant l'envoi en banque de la transaction. Pour plus d'informations, vous devez vous référer au chapitre 9 traitant de la capture différée.

Champ :	**capture_mode**
Format :	as
Taille :	jusqu'à 20 caractères
Description :	Contient le mode d'envoi en banque de la transaction. Pour plus d'informations, vous devez vous référer au chapitre 9 traitant de la capture différée.

Champ :	**card_number**
Format :	n
Taille :	jusqu'à 21 caractères
Description :	Contient le numéro de carte bancaire pour une opération de demande d'autorisation.

Champ :	**card_type**
Format :	a
Taille :	20 caractères
Description :	Contient le type de carte pour une opération de demande d'autorisation. Pour connaître la liste des cartes acceptées, vous devez vous référer à l'annexe E.

Champ :	**card_validity**
Format :	n (aaaamm)
Taille :	6 caractères
Description :	Contient la date de validité de la carte bancaire pour une opération de demande d'autorisation. Si la carte ne possède pas de date de validité, ce champ doit être vide.

Champ :	**complementary_code**
Parmcom :	non présent
Format :	n
Taille :	2 caractères
Description :	Champ renvoyé dans la réponse et contenant le code réponse complémentaire du serveur.Pour en savoir plus, adressez-vous au Centre d'assistance Technique.

Champ :	**complementary_info**
Parmcom :	non présent
Format :	an
Taille :	jusqu'à 255 caractères
Description :	Champ renvoyé dans la réponse et contenant une information sur le code réponse complémentaire du serveur Pour en savoir plus, adressez-vous au Centre d'assistance Technique.

Champ :	**currency_code**
Format :	n
Taille :	3 caractères
Description :	**Pour une demande d'autorisation :** Contient le code de la devise de la nouvelle transaction. Ce code est compatible ISO 4217. La liste des codes devises acceptés par le serveur Office est précisée en annexe A.

Champ :	**customer_ip_address**
Format :	an
Taille :	15 caractères
Description :	Contient l'adresse IP du provider de l'internaute.

Champ :	**cvv_flag**
Format :	n
Taille :	1 caractère
Description :	Dans le cas d'une demande d'autorisation, ce champ contient un code précisant la présence ou non du cryptogramme visuel de la carte bancaire. Pour plus d'information sur le cryptogramme visuel et connaître la liste des cartes concernées, vous devez vous référer à l'annexe B.

Champ :	**cvv_key**
Format :	n
Taille :	3 ou 4 caractères
Description :	Dans le cas d'une demande d'autorisation, ce champ contient le cryptogramme visuel de la carte bancaire. Pour plus d'information sur le cryptogramme visuel et connaître la liste des cartes concernées, vous devez vous référer à l'annexe B.

Champ :	**cvv_response_code**
Format :	an
Taille :	2 caractères
Description :	Champ renvoyé dans la réponse dans le cas d'une demande d'autorisation avec une carte possédant un cryptogramme visuel. Les serveurs bancaires ne renseignent pas obligatoirement ce champ même si la vérification du cryptogramme visuel a été effectuée. Pour plus d'informations, vous devez vous référer à l'annexe B.

Champ :	**data**
Format :	ans
Taille :	jusqu'à 1024 caractères
Description :	**Requête d'une demande d'autorisation :** Champ privé qui permet de transmettre au serveur Office des paramètres lors du traitement des demandes d'autorisation. Si plusieurs paramètres doivent être transmis dans le champ data, ils doivent être séparés par un « ; ». Pour plus d'informations sur les paramètres transmis dans ce champ référez-vous à l'annexe E. **Requête d'une demande d'authentification 3D :** Dans le cas d'une authentification 3D-Secure, l'internaute peut passer outre la saisie de sont mot de passe sur l'ACS pour ses trois premières transactions 3DS. Il est possible de différencier ce cas d'une authentification réussie (voir annexe C) **Réponse d'une demande d'autorisation :** Champ identique au champ **data** transmis au serveur Office lors d'une demande d'autorisation.

Champ :	**merchant_country**
Format :	a
Taille :	2 caractères
Description :	Contient le code du pays du commerçant. La liste des codes pays utilisés sur le serveur Office est précisée en annexe H.

Champ :	**merchant_id**
Format :	n
Taille :	jusqu'à 15 caractères
Description :	La valeur de ce champ est fournie par Atos Origin au commerçant lors de l'inscription de sa boutique. Il permet l'identification d'une boutique. Il correspond généralement au SIRET précédé de 0.

Champ :	**merchant_name**
Format :	an
Taille :	50 caractères
Description :	Nom de la boutique du commerçant affichée sur l'ACS.

Champ :	**merchant_url**
Format :	an
Taille :	512 caractères
Description :	URL de la boutique du commerçant affichée sur l'ACS.

Champ :	**merchant_url_return**
Format :	an
Taille :	512 caractères
Description :	URL de retour vers la boutique du commerçant après le passage par l'ACS. Lors du passage sur l'ACS, le navigateur n'est pas en moyen de déterminer sur quel URL revenir après l'authentification 3D de l'internaute. Il est donc indispensable, dès la requête de vérification d'enrôlerment 3D, de prévoir ce futur retour vers la boutique.

Champ :	**new_amount**
Format :	n
Taille :	jusqu'à 12 caractères (minimum 3 caractères)
Description :	Contient le montant de la transaction à la fin d'une l'opération. Par exemple, si après avoir effectué une demande d'autorisation acceptée de 10,00 Euros, un commerçant annule 3,00 Euros, le champ **new_amount** à la fin de l'annulation sera de 7,00 Euros. Le montant est transmis dans la plus petite unité de la devise. Exemple pour l'Euro : un montant de 10,50 Euros doit être transmis sous la forme 1050. Pour les autres devises voir tableau annexe A.

Champ :	**new_status**
Format :	as
Taille :	jusqu'à 20 caractères
Description :	Contient l'état de la transaction après une opération sur celle-ci. L'état d'une transaction est décrit par différents mots clés évoluant au fil des opérations qu'elle subit. Pour plus d'information sur les états possibles d'une transaction, référez-vous à l'annexe I.

Champ :	**o3d_office_url_acs**
Format :	an
Taille :	256 caractères
Description :	Contient l'URL de redirection vers AWL permettant la redirection de l'internaute sur son ACS dans le cadre d'une transaction 3D-Secure.

Champ :	**o3d_response_code**
Format :	n
Taille :	2 caractères
Description :	Champ renvoyé dans la réponse et contenant le code réponse du serveur 3D Office. Pour connaître la valeur des différents codes et leur signification, référez-vous à l'annexe C.

Champ :	**o3d_session_id**
Format :	an
Taille :	128 caractères
Description :	Identifiant de session du paiement 3D-Secure qui devra être copié dans la requête card3D_Order ou card3D_Authenticate

Champ :	**order_id**
Format :	ans
Taille :	jusqu'à 32 caractères
Description :	Ce champ peut être utilisé par le commerçant pour associer à une demande d'autorisation un numéro de commande. Ce champ est présent dans le journal des transactions et dans le journal des opérations expédiés quotidiennement au commerçant. ATTENTION : certains caractères sont interdits dans ce champ, référez-vous au paragraphe 8.2 pour en connaître la liste.

Champ :	**order_validity**
Format :	n
Taille :	2 caractères
Description :	non utilisé

Champ :	**origin**
Format :	ans
Taille :	jusqu'à 20 caractères
Description :	Ce champ peut être utilisé par le commerçant pour préciser l'origine d'une opération (ex : nom du programme). Ce champ sera présent dans le journal des opérations expédié quotidiennement au commerçant. ATTENTION : certains caractères sont interdits dans ce champ, référez-vous au paragraphe 8.2 pour en connaître la liste.

Champ :	**payment_date**
Format :	n (aaaammjj)
Taille :	8 caractères
Description :	**Réponse :** Champ renvoyé dans la réponse et contenant la date de la demande d'autorisation renseignée par le serveur Office.

Champ :	**response_code**
Format :	n
Taille :	2 caractères
Description :	Champ renvoyé dans la réponse et contenant le code réponse du serveur Office. Pour connaître la valeur des différents codes et leur signification, référez-vous à l'annexe G.

Champ :	**return_context**
Format :	ans
Taille :	jusqu'à 256 caractères
Description :	Ce champ peut être utilisé par le commerçant pour préciser le contexte d'une transaction. Ce champ sera présent dans le journal des transactions expédié quotidiennement au commerçant. ATTENTION : certains caractères sont interdits dans ce champ, référez-vous au paragraphe 8.2 pour en connaître la liste.

Champ :	**transaction_certificate**
Format :	an
Taille :	12 caractères
Description :	Champ renvoyé dans la réponse dans le cas d'une transaction acceptée. La valeur contenue dans ce champ est calculée à partir des éléments de l'opération et certifie que celle-ci a bien été traitée par le serveur Office.

Champ :	**transaction_date**
Format :	n (aaaammjj)
Taille :	8 caractères
Description :	Champ renvoyé dans la réponse et contenant la date de l'opération traitée par le serveur Office.

Champ :	**transaction_id**
Format :	n
Taille :	jusqu'à 6 caractères
Description :	**Demande d'autorisation:** Contient l'identifiant de la nouvelle transaction. Une transaction est définie à l'aide d'une clé formée de quatre valeurs : **merchant_country**, **merchant_id**, **payment_date** et **transaction_id**. Par conséquent, il suffit à un commerçant donné de fournir un **transaction_id** unique sur une journée pour chacune des transactions envoyées au serveur Office pour en assurer l'unicité. Si une demande d'autorisation a été effectuée pour un **transaction_id** donné et qu'une nouvelle transaction est tentée le même jour avec ce même **transaction_id**, le code retour 94 signifiant transaction déjà existante sera renvoyé.

Champ :	**transaction_time**
Format :	n (hhmmss)
Taille :	6 caractères
Description :	Champ renvoyé dans la réponse et contenant l'heure locale du serveur Office lors du traitement de l'opération.

Champ :	**transmission_date**
Format :	n (aaaammjjhhmmss)
Taille :	14 caractères
Description :	Champ interne renseigné par le composant Checkout contenant la date et l'heure GMT (Greenwich Mean Time) à laquelle le composant Office a été appelé.

Champ :	**version**
Format :	an
Taille :	5 caractères
Description :	Champ interne renseigné par le composant Checkout contenant le numéro de version du composant Office.

9. PARAMETRAGE DE LA CAPTURE DIFFEREE

L'envoi en banque d'une transaction, également appelé capture ou remise d'une transaction, peut être défini à l'aide de deux paramètres : capture_mode et capture_day. Le champ **capture_mode** précise le mode d'envoi en banque, tandis que le champ **capture_day** indique le délai avant l'envoi en banque.
Le champ **capture_mode** peut prendre les valeurs AUTHOR_CAPTURE ou VALIDATION, tandis que le champ **capture_day** peut varier de 0 à 99. Dans le cas d'une transaction 3D-Secure, si la valeur du capture_day est supérieur à 3, elle sera automatiquement assigné à la valeur 3. Dès lors que le **capture_day** est non nul, on parle de capture différée car l'envoi en banque ne se fait pas le même jour que la création de la transaction.

Si les champs **capture_mode** et **capture_day** ne sont pas renseignés au niveau du composant Checkout, ils sont respectivement initialisés par le serveur Office à AUTHOR_CAPTURE et 0 pour signifier une capture immédiate après l'acceptation du paiement.

Pour connaître les règles de gestion exactes de la capture différée, veuillez vous référer au document de *PRESENTATION GENERALE DE SIPS OFFICE SERVER*.

9.1. MODE AUTHOR_CAPTURE

Dans ce mode, les transactions sont automatiquement envoyées en banque par le serveur Office, aucune action n'est nécessaire au commerçant. Cependant, si le commerçant souhaite annuler tout ou partie de la transaction avant l'envoi en banque, il peut le faire à l'aide de l'opération d'annulation du composant Office.

Par exemple, si le champ **capture_mode** est vide et le champ **capture_day** a la valeur 2, le serveur Office fait une demande d'autorisation du montant réel lors de la transaction. Cette dernière est ensuite envoyée en banque 2 jours calendaires plus tard.

9.2. MODE VALIDATION

Les transactions ne sont envoyées en banque qu'après la validation du commerçant. La validation d'une transaction se fait à l'aide de l'opération validation du composant Office. Si une transaction n'est pas validée dans le délai fixé par le **capture_day**, elle expire. La transaction n'est alors jamais envoyée en banque.

Par exemple, si le champ **capture_mode** est à VALIDATION et le champ **capture_day** a la valeur 3, le serveur Office fait une demande d'autorisation du montant réel lors de la transaction. Le commerçant a 3 jours pour valider la transaction. La transaction est envoyée en banque le jour de la validation.

Le choix du mode VALIDATION ou AUTHOR_CAPTURE dépend du souhait du commerçant de contrôler ou non l'envoi en banque des transactions.

10. DESCRIPTION DES TRACES

Suite à la réception d'une requête, le composant Checkout écrit dans les fichiers de traces configurés au paragraphe 4.2.4.

10.1. SI AUCUNE ERREUR N'EST SURVENUE

Le composant inscrit dans les traces le nom de la fonction, la clé définissant la transaction créée ou modifiée (**merchant_id**, **merchant_country**, **transaction_id** et **payment_date**), le code réponse de l'opération et la réponse XML renvoyée au client de l'API Server.

Un exemple de traces pour une vérification d'enrôlement est présenté ci-dessous.

```
132:18:54:09-0-(3)-CheckoutWrapper : fonction : card3D_CheckEnrollment
132:18:54:09-0-(3)-CheckoutWrapper : merchant_id=011223344552222,
merchant_country=fr
132:18:54:10-0-(3)-CheckoutWrapper : response_code=00
132:18:54:10-0-(3)-CheckoutWrapper : response : <response
component="checkout" name="card3D_CheckEnrollment"><card3D_CheckEnrollment
merchant_country="fr" merchant_id="011223344552222" 3d_response_code="00"
3d_checkenrolled_resp="00&VISA&eJxVUdtugkAQ/RXCc2UvgKIZ1lC1qQ9eYvG5IbBBjIAu
UPTvO4uoLS875zBzZuYMTK/5yfiRqsrKwjeZRU1DFnGZZEXqm/vwY+CZUwHhQUk5/5Jxo6SAlay
qKJVGlvhmUJfVYKOyNCu+GXfYkHvMdobcMQVsg528COjVBYpbHMgDooyKD1FRC4jiy/tyLZzxiF
IKpIeQS7WcC8oY57btOK7L8QNyp6GIcilmZY4wRhWjllUNpGMhLpuiVjfBXZR7AGjUSbRta+lMK
y5zIJoB8hpk2+ioQoVrlojVMWg3YcBW4bJdH/cUX7YOU74OFz4QnQFJVEvBKR1Tl3GDeRPXmTCc
seMhynVrwbj9Rqmx2O9wtzsFZ90peP7Xa/+lAJ1WeIibGI88XOGBQF7PZSExA5s8YyCvwWef2s+
4Rovuj/azg7o2Qx8YOtoVawBEF5D+VKQ/LUb/Tv4LM+yztw==&20090512185412&01=01&http
s://rcet-3dsecure.sips-
atos.com/acs/simu/ACSServlet&26@011223344552222&www.test.com&9vGqYkS4wJc6ym
wrMDJdGVCqF+U=
" correct_card_type="VISA"
3d_office_url_acs="https://vre16:29567/3doffice/prod/call_acs"
3d_session_id="F783C00697C899CFE6E85713BD532619.sips_3doffice-
1"/></response>
132:18:54:10-0-(3)-CheckoutWrapper : ----------------------------------------
----------------------------------
```

Dans le cas de la fonction de vérification checkCheckout, les champs **transaction_id** et **payment_date** contiennent respectivement la référence de la transaction et la date de la requête de vérification.

Un exemple de traces de vérification est présenté ci-dessous.

```
132:18:53:41-0-(2)-CheckoutWrapper : fonction : checkCheckout
132:18:53:41-0-(2)-CheckoutWrapper : merchant_id=011223344552222,
merchant_country=fr
132:18:53:41-0-(2)-CheckoutWrapper : ----------------------------------------
----------------------------------
132:18:53:41-0-(2)-CheckoutWrapper : response : <response  pathfile="OK"
certificate="OK" />
132:18:53:41-0-(2)-CheckoutWrapper : ----------------------------------------
----------------------------------
```


10.2. EN CAS D'ERREUR

Le composant inscrit dans les traces le nom de la fonction appelée suivi du message d'erreur complet.

Un exemple de traces en cas d'erreur lors d'une demande d'autorisation est présenté ci-dessous.

```
238:10:43:09-2-(8)-CheckoutWrapper : fonction : checkCheckout
238:10:43:09-2-(8)-CheckoutWrapper : Error message:
C:\sips_office\API\Server\checkout\param\pathfile (Le fichier spécifié est
introuvable)
238:10:43:09-2-(8)-CheckoutWrapper : ------------------------------------
----------------------------------
```

ANNEXE A : TABLEAU DES CODES DEVISE

Afin de mieux comprendre comment renseigner le champ **amount**, le tableau ci-dessous présente, pour chaque devise acceptée par le serveur Office, un exemple de montant ainsi que la valeur à transmettre dans le champ **amount**.
L'unité fractionnaire, mentionnée dans ce tableau, correspond au nombre de décimales de la monnaie.

Nom de la devise	Code de la devise (champ currency_code)	Unité fractionnaire	Montant	Champ amount
Euro	978	2	106,55	10655
Dollar Américain	840	2	106.55	10655
Franc Suisse	756	2	106,55	10655
Livre Sterling	826	2	106.55	10655
Dollar Canadien	124	2	106.55	10655
Yen	392	0	106	106
Peso Mexicain	484	0	106	106
Livre Turque	792	2	106.55	10655
Dollar Australien	036	2	106.55	10655
Dollar Néo-Zélandais	554	2	106.55	10655
Couronne Norvégienne	578	2	106.55	10655
Real Brésilien	986	2	106.55	10655
Peso Argentin	032	2	106.55	10655
Riel	116	2	106.55	10655
Dollar de Taïwan	901	2	106.55	10655
Couronne Suédoise	752	2	106.55	10655
Couronne Danoise	208	2	106.55	10655
Won	410	2	106.55	10655
Dollar de Singapour	702	2	106.55	10655

ANNEXE B : CRYPTOGRAMME VISUEL (CVV2,CVC2,CBN2)

Dans le but de combattre la fraude et particulièrement les générateurs de vrais-faux numéros de carte bancaire, MASTERCARD, VISA et CARTE BLEUE ont choisi d'accroître le niveau de sécurité de leurs cartes, en adjoignant un cryptogramme visuel (CVV2 pour VISA, CVC2 pour MASTERCARD et CBN2 pour CARTE BLEUE) au numéro de ces dernières.

Le cryptogramme visuel est une clé de trois chiffres, calculée par des boîtes noires à partir des données de la carte. On le trouve à la suite des 4 derniers chiffres du numéro de la carte sur le panneau signature au dos des cartes MASTERCARD, VISA et CARTE BLEUE.

Un commerçant peut renseigner le cryptogramme visuel dans ses requêtes de demande d'autorisation pour les cartes MASTERCARD, VISA et CARTE BLEUE.

Demande d'autorisation

Les informations associées au cryptogramme visuel sont véhiculées entre le serveur Office et le serveur bancaire dans deux champs :

cvv_flag : ce champ numérique indique la présence ou l'absence du cryptogramme visuel. Ce champ est renseigné dans la requête de demande d'autorisation.
Dans le tableau ci-dessous sont présentées les différentes valeurs possibles du **cvv_flag** ainsi que leur signification.

valeur	signification
0	Le cryptogramme visuel n'est pas remonté par le commerçant
1	Le cryptogramme visuel est présent
2	Le cryptogramme visuel est présent sur la carte du porteur mais illisible
9	Le porteur a informé le commerçant que le cryptogramme visuel n'était pas imprimé sur sa carte

cvv_key : ce champ de trois caractères numériques contient la valeur du cryptogramme visuel. Ce champ est renseigné dans la requête de demande d'autorisation. Il doit y avoir cohérence entre la valeur du **cvv_flag** et la présence de données ou non dans le champ **cvv_key** : Le **cvv_key** doit contenir 3 caractères numériques si le **cvv_flag** contient la valeur 1, il doit être vide dans tous les autres cas.

Codes retour

En réponse à chaque demande d'autorisation, le serveur Office renvoie trois codes retour : bank_response_code, response_code et le cvv_response_code.

Les champs **bank_response_code** et **cvv_response_code** correspondent respectivement au code réponse autorisation du serveur d'autorisation bancaire et au code réponse cryptogramme visuel du serveur bancaire.
Dans le Tableau 1 sont présentées les différentes valeurs possible du **cvv_response_code** ainsi que leur signification.

Valeur	**Signification**
4E	Cryptogramme incorrect
4D	Cryptogramme correct
50	Cryptogramme non traité
53	Le cryptogramme est absent de la demande d'autorisation
55	La banque de l'internaute n'est pas certifiée, le contrôle n'a pu être effectué.
vide	La banque de l'internaute n'a pas répondu.

*Tableau 1: valeurs possibles pour le **cvv_response_code***

ANNEXE C : CODES REPONSE SERVEUR 3D OFFICE

Vous trouverez dans le tableau ci-dessous les codes réponse renvoyés par le serveur 3D Office dans le champ **o3d_response_code**.

En retour de la* méthode *card3D_CheckEnrollment()

Codes réponse	Signification
00	Porteur enrôlé 3D
01	Porteur non enrôlé 3D
03	Commerçant inconnu
10	Impossible de déterminer si le porteur est enrôlé ou non
12	Requête invalide, vérifier les paramètres transférés dans la requête
40	Utilisation d'une fonctionnalité non supportée.
81	Erreur interne au MPI lors du 1er appel au MPI
82	Erreur interne au MPI lors du 2nd appel au MPI
85	MPI injoignable lors du 1er appel au MPI
86	MPI injoignable lors du 2nd appel au MPI
94	Erreur technique au cours de l'authentification sur le DS
97	Paramètres transmis au MPI invalides
98	Problème réseau lors de la tentative d'accès aux DS
99	Erreur technique au niveau du serveur 3D Office

En retour des méthodes card3D_Authenticate() et card3D_Order()

Codes réponse	Signification
00	Porteur authentifié
02	Problème technique sur l'ACS
03	Commerçant inconnu
12	Requête invalide, vérifier les paramètres transférés dans la requête
40	Utilisation d'une fonctionnalité non supportée.
55	Porteur non authentifié
62	By-pass du porteur sur l'ACS
81	Erreur interne au MPI lors du 1er appel au MPI
82	Erreur interne au MPI lors du 2nd appel au MPI
84	Réponse du Directory Server invalide (VERes invalid)
85	MPI injoignable lors du 1er appel au MPI
86	MPI injoignable lors du 2nd appel au MPI
88	Problème réseau
92	Erreur interne du Directory Server
93	Erreur interne de l'ACS
95	Erreur d'intégrité sur le message renvoyé par l'ACS
96	Message renvoyé par l'ACS invalide
99	Erreur technique au niveau du serveur 3D Office

Utilisation du champ **data** (seulement pour la requête card3D_Authenticate) :

Lors des trois premières transactions 3D-Secure d'un internaute, ce dernier aura le choix de passer outre l'authentification sur son ACS. Ce cas est considéré comme une authentification réussie (**o3d_response_code** = 00) du porteur (malgré le fait qu'il n'ait pas saisi son mot de passe).

Pour repérer ces cas, il suffit d'ajouter dans le champ **data** la valeur *NO_ATTEMPT* lors d'une requête card3D_Authenticate. Ainsi, ce cas de by-pass de l'ACS par le porteur sera identifié par le code 62 dans le champ **o3d_response_code**.

ANNEXE E : LISTE DES CARTES ACCEPTEES

Dans le tableau ci-dessous, vous trouverez la liste des cartes acceptées par le serveur Office, la valeur à renseigner dans le champ **card_type** et leur réseau d'appartenance. Les cartes marquées d'un astérisque (*) n'ont pas de date de fin de validité.

Carte	valeur dans le champ card_type	Réseau d'appartenance
CB	CB	CB National
VISA	VISA	CB International
MASTERCARD	MASTERCARD	CB International
AMEX	AMEX	AMEX
FINAREF (*)	FINAREF	FINAREF
FNAC	FNAC	FINAREF
CYRILLUS (*)	CYRILLUS	FINAREF
PRINTEMPS	PRINTEMPS	FINAREF
KANGOUROU (*)	KANGOUROU	FINAREF
SURCOUF (*)	SURCOUF	FINAREF
POCKETCARD (utilisé en Belgique)	POCKETCARD	FINAREF
CONFORAMA	CONFORAMA	FINAREF
NUITEA	NUITEA	CETELEM
AURORE (*)	AURORE	CETELEM
PASS (*)	PASS	CETELEM
JCB	JCB	JCB
DINERS	DINERS	DINERS
SOLO	SOLO	NATWEST
SWITCH	SWITCH	NATWEST
DELTA	DELTA	NATWEST
BANCONTACTMISTERCASH	BANCONTACTMISTERCASH	BANKSYS

Paramétrage spécifique :
Quelques cartes nécessitent des paramètres supplémentaires pour la demande d'autorisation. Dans ce cas, ces paramètres supplémentaires sont transmis dans le champ **data**. Si le formatage du champ data n'est pas respecté, le champ **response_code** sera renseigné à 12.

La carte AURORE :
Le champ **data** doit être complété par « DATE_NAISSANCE=aaaammjj, MODE_REGLEMENT=MR_CREDIT »

La carte PASS :
Le champ **data** doit être complété par « DATE_NAISSANCE=aaaammjj; MODE_REGLEMENT_PASS=COMPTANT ou CREDIT ou 3FOIS »

Les cartes SOLO et SWITCH :
Le champ **data** peut contenir les valeurs des paramètres ISSUE_NUMBER et START_DATE. Ces données sont optionnelles, elles ne sont traitées que si elles sont présentes.

Paramètre ISSUE_NUMBER
Le champ **data** doit être complété par « ISSUE_NUMBER=<value> »
avec <value> une donnée numérique à un ou deux caractères

Paramètre START_DATE
Le champ **data** doit être complété par « START_DATE=aaaamm »
avec aaaamm la date d'activation de la carte.

Si vous souhaitez renseigner dans le champ **data** les paramètres ISSUE_NUMBER et START_DATE vous devez les séparer par un point virgule (exemple ISSUE_NUMBER=9;START_DATE=200301). Il n'y a pas d'ordre particulier pour les paramètres ISSUE_NUMBER et START_DATE, le champ **data** renseigné par « ISSUE_NUMBER=9;START_DATE=200301 » aura la même signification que si il est renseigné par « START_DATE=200301;ISSUE_NUMBER=9 ».

Les cartes VISA ou MASTERCARD pour des transactions en Livres Sterling (GBP) :
Ces cartes utilisent l'AVS. Le champ **data** doit être complété comme suit :

- Écrire la balise « AVS; »
- Renseigner les champs au format « NOM_CHAMP=VALEUR; » (voir ci-dessous pour la liste des champs)
- Écrire la balise « /AVS; »

Champ	Taille max (caractères)	Obligatoire (O/N)
TITLE	20	N
FIRSTNAME	50	N
LASTNAME	50	N
LINE1	50	O(*)
LINE2	50	N
LINE3	50	N
CITY	50	N
POSTCODE	10	O(*)
COUNTRYCODE	3	N
CHECK	2	N

Le champ **CHECK** permet de préciser la politique qui sera appliquée pour la vérification. Voici les valeurs possibles pour ce champ :

- 0 – Pas de vérification ;
- 1 – Si la vérification échoue, faire échouer la transaction
- 2 – Si la vérification échoue, ne pas modifier le résultat de la transaction

(*) Le seul cas où ces éléments sont obligatoires est lorsque CHECK est fourni avec la valeur 1.

Si le champ **CHECK** n'est pas renseigné, le comportement par défaut sera d'effectuer une vérification bloquante si des données AVS sont fournies, sinon rien n'est fait. Ce comportement est présent pour assurer la compatibilité ascendante, il est conseillé de remplir le champ **CHECK**.

Si la balise « AVS; » n'est pas trouvée dans le champ **data**, il sera considéré qu'aucune donnée AVS n'est présente.

Si la balise « /AVS; » n'est pas trouvée alors que « AVS; » l'est, la transaction échouera.

Les données nominatives sont stockées en base de données si elles sont fournies.

ANNEXE F : CODES REPONSE BANCAIRE (CHAMP BANK_RESPONSE_CODE)

Vous trouverez dans les tableaux ci-dessous les principaux codes réponse renvoyés par les serveurs d'autorisations bancaires Carte Bancaire (CB, VISA, MASTERCARD), AMEX et FINAREF. Pour Natwest, Cetelem et JCB, les codes ne sont pas renvoyés.

Code	Signification
00	Transaction approuvée ou traitée avec succès
02	Contacter l'émetteur de carte
03	Accepteur invalide
04	Conserver la carte
05	Ne pas honorer
07	Conserver la carte, conditions spéciales
08	Approuver après identification
12	Transaction invalide
13	Montant invalide
14	Numéro de porteur invalide
15	Emetteur de carte inconnu
30	Erreur de format
31	Identifiant de l'organisme acquéreur inconnu
33	Date de validité de la carte dépassée
34	Suspicion de fraude
41	Carte perdue
43	Carte volée
51	Provision insuffisante ou crédit dépassé
54	Date de validité de la carte dépassée
56	Carte absente du fichier
57	Transaction non permise à ce porteur
58	Transaction interdite au terminal
59	Suspicion de fraude
60	L'accepteur de carte doit contacter l'acquéreur
61	Dépasse la limite du montant de retrait
63	Règles de sécurité non respectées
68	Réponse non parvenue ou reçue trop tard
90	Arrêt momentané du système
91	Emetteur de cartes inaccessible
96	Mauvais fonctionnement du système
97	Échéance de la temporisation de surveillance globale
98	Serveur indisponible routage réseau demandé à nouveau
99	Incident domaine initiateur

Tableau 2 : Codes réponse serveur Carte Bancaire (CB, VISA, MASTERCARD), d'après le protocole CB2A 1.1

Code	Signification
00	Transaction approuvée ou traitée avec succès
02	Dépassement de plafond
04	Conserver la carte
05	Ne pas honorer
97	Échéance de la temporisation de surveillance globale

Tableau 3 : Codes réponse serveur AMEX

Code	Signification
00	Transaction approuvée
03	Commerçant inconnu Identifiant de commerçant incorrect
05	Compte / Porteur avec statut bloqué ou invalide
11	Compte / porteur inconnu
16	Provision insuffisante
20	Commerçant invalide Code monnaie incorrect Opération commerciale inconnue Opération commerciale invalide
80	Transaction approuvée avec dépassement
81	Transaction approuvée avec augmentation capital
82	Transaction approuvée NPAI
83	Compte / porteur invalide

Tableau 4 : Codes réponse serveur FINAREF

ANNEXE G : CODES REPONSE SERVEUR OFFICE

Vous trouverez dans le tableau ci-dessous les codes réponse renvoyés par le serveur Office dans le champ **response_code**.

Codes réponse	Signification
00	Autorisation acceptée
02	demande d'autorisation par téléphone à la banque à cause d'un dépassement du plafond d'autorisation sur la carte
03	Contrat de vente à distance inexistant, contacter votre banque.
05	Refus simple
12	Transaction invalide, vérifier les paramètres transférés dans la requête.
14	coordonnées bancaires ou cryptogramme visuel invalides.
24	Opération impossible. L'opération que vous souhaitez réaliser n'est pas compatible avec l'état de la transaction.
25	Transaction non trouvée dans la base de données d'Atos Origin.
30	Erreur de format
34	Suspicion de fraude
40	Fonction non supportée : l'opération que vous souhaitez réaliser ne fait pas partie de la liste des opérations auxquelles vous êtes autorisé sur le serveur Office. Contactez le Centre d'assistance Technique.
63	Règles de sécurité non respectées, transaction arrêtée
75	Porteur non authentifié 3D-Secure
90	Problème temporaire au niveau du serveur bancaire
94	Transaction dupliquée : pour une journée donnée, le **transaction_id** a déjà été utilisé.
99	Problème temporaire au niveau du serveur Office.

Si un autre code que ceux mentionnés dans le tableau ci-dessus est renvoyé par un serveur bancaire, le serveur Office le transforme systématiquement en code 05. Ceci permet de simplifier le traitement des codes réponse car le commerçant n'est pas obligé de gérer tous les codes possibles.

Le champ **response_code** est le résultat de la combinaison du **bank_response_code** et du **cvv_response_code**. C'est donc ce code qu'il faut analyser pour vérifier que le paiement est accepté ou pas.

Dans le cas d'une autorisation refusée (code 05), vous pouvez vous référer aux champs **bank_response_code** (cf. Annexe F) ou cvv_response_code (cf. Annexe B) pour connaître la raison du refus bancaire.

ANNEXE H : LISTE DES CODES PAYS

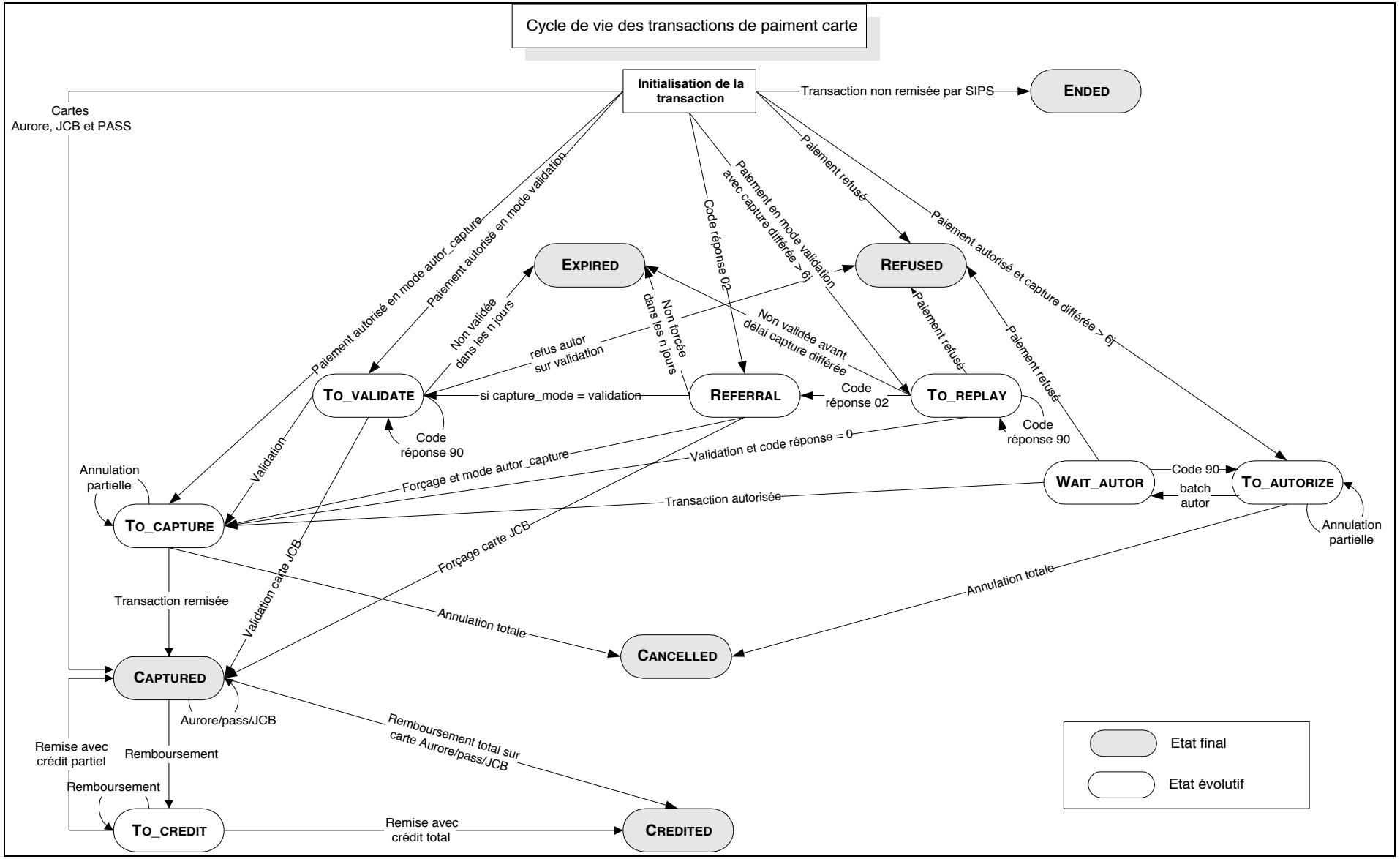
Dans le tableau ci-dessous, vous trouverez la liste des principaux codes pays, utilisés dans l'API Server et leur signification.

Code	Pays
be	Belgique
fr	France
de	Allemagne
it	Italie
en	Grande Bretagne
es	Espagne

ANNEXE I : CYCLE DE VIE D'UNE TRANSACTION

Une transaction peut subir un certain nombre de modifications via le composant Office (cf . *PRESENTATION GENERALE DE SIPS OFFICE SERVER*) ou le service Office client (cf. *PRESENTATION GENERALE DE SIPS PAYMENT*). Les modifications qu'elle peut subir dépendent de son paramétrage d'origine (mode et délai de remise en banque) et des opérations qu'elle a déjà subies. Pour définir, à chaque instant, les futures modifications qu'elle pourra subir, un état est associé à chaque transaction. La transition d'un état à un autre est définie par le diagramme des états présenté page suivante.
Ci-dessous est précisée la signification des différents états présents dans le diagramme des états.

Nom de l'état	Signification
CANCELLED	Transaction totalement annulée
CAPTURED	Transaction envoyée en banque
CREDITED	Transaction totalement remboursée
ENDED	Transaction terminée
EXPIRED	Transaction expirée
REFERRAL	Transaction en attente de forçage
REFUSED	Transaction refusée
TO_AUTHORIZE	Transaction en attente de demande d'autorisation
TO_CAPTURE	Transaction à envoyer en banque pour débiter l'internaute
TO_CREDIT	Transaction à envoyer en banque pour créditer l'internaute
TO_REPLAY	Transaction en attente d'une validation avec demande d'autorisation
TO_VALIDATE	Transaction en attente de validation
WAITING_AUTHOR	Transaction extraite par les serveurs d'Atos Origin pour réaliser une demande d'autorisation automatique à la fin du délai de capture différée



ANNEXE K : AVS

L'Address Verification System – AVS – est un outil de prévention de la fraude mis en place notamment au Royaume Uni. Il s'appuie sur les données numériques de l'adresse du porteur de la carte en prenant en compte séparément ceux du code postal de ceux du reste de l'adresse.

Lorsqu'un porteur de carte désire se servir de sa carte de crédit, on lui demande l'adresse de facturation associée. Elle est alors transmise avec la demande d'autorisation pour que la banque du porteur puisse vérifier la concordance entre l'adresse saisie et celle associée à la carte.

Dans la demande d'autorisation, l'adresse est encodée en supplément des données présentes dans le champ **data**. Pour plus de détails au sujet de comment remplir ce champ, reportez-vous à l'annexe E.

Le champ **avs_response_code** dans la réponse à la demande d'autorisation

Lors de la réponse du serveur SIPS, le champ **avs_response_code** est renseigné comme suit :

- Le champ est rempli sur 2 chiffres. Le premier chiffre renseigne le résultat de la vérification pour les numériques de l'adresse. Le second chiffre renseigne le résultat de la vérification pour les numériques du code postal.
- Les valeurs employées pour coder ce champ sont les suivantes :
    - 0 – Aucune donnée n'avait été fournie ;
    - 1 – Aucune vérification n'a été effectuée ;
    - 2 – La vérification a réussi ;
    - 4 – La vérification a échoué ;
    - 8 – La vérification n'a réussi que partiellement.
- Par exemple, un code 28 signifie que les données de l'adresse sont correctes mais que celles du code postal ne le sont que partiellement.

CONTACTS

Pour toute information complémentaire, contactez le Centre d'Assistance Technique :

e-mail : sips@atosorigin.com
tel : 02.54.44.70.33
fax : 02.54.44.70.96

Pour toute demande de renseignements, veuillez fournir votre numéro commerçant et la phase d'installation (recette, pré-production ou production) de votre boutique. Ces paramètres nous permettront de vous identifier rapidement, et ainsi répondre à votre demande dans les meilleurs délais.

