Up2pay e-Transactions

REALISATION DES TESTS D'INTEGRATION

Version du 01/03/2021

REFERENCES DOCUMENTATIONS

REF.	DOCUMENT	DESCRIPTION
Ref 1	Manuel Intégration e-Transactions	Manuel d'intégration de la solution Up2pay e-Transactions
Ref 2	Manuel Intégration Conecs et CV-Connect	Manuel d'intégration spécifique pour les moyens de paiement Conecs (titres restaurant) et CV_Connect (Chèques vacances)
Ref 3	Manuel Intégration Paypal	Manuel d'intégration spécifiques pour le moyen de paiement complémentaire Paypal
Ref 4	Manuel Intégration Paylib	Manuel d'intégration spécifique pour le moyen de paiement complémentaire Paylib
Ref 5	Manuel Intégration American Express	Manuel d'intégration spécifique pour le moyen de paiement complémentaire American Express (AMEX)

AVERTISSEMENT

Les informations contenues dans ce document n'ont aucune valeur contractuelle. Elles peuvent faire l'objet de modification à tout moment. Elles sont à jour en date de rédaction au 01/03/2021.

e-Transactions est une solution d'encaissement et de gestion des paiements à distance par carte bancaire, dans un environnement sécurisé, distribuée par les Caisses régionales de Crédit Agricole. Renseignez-vous auprès de votre conseiller sur les conditions générales et tarifaires de cette solution.

Cette documentation peut être enrichie par vos commentaires. Vous pouvez nous envoyer un email à support@e-transactions.fr, en indiquant votre remarque aussi précisément que possible. Merci de préciser la référence du document ainsi que le numéro de la page.

ASSISTANCE

Pour tout renseignement ou assistance à l'installation et à l'utilisation de nos produits, nos Equipes restent à votre disposition, du lundi au vendredi (hors jours fériés) de 9H à 18H30 :

Support Technique & Fonctionnel :

Par e-mail : support@e-Transactions.fr

Téléphone : 0 810 812 810 *(1)*

(1) prix d'un appel local non surtaxé depuis un poste fixe

Pour tout contact auprès de nos services, il faut **IMPERATIVEMENT** communiquer les identifiants indiqués dans votre mail de bienvenue :

- Numéro de SITE (7 chiffres)
- Numéro de RANG (2 ou 3 chiffres)
- Numéro d'identifiant (1 à 9 chiffres)

TABLE DES MATIERES

Table des matières

1. OBJET DU DOCUMENT 2
1.1. Principe général de la Solution 2
1.2. Principe général du document 3
2. PLATEFORME DE TEST 4
2.1. Pourquoi une plateforme de test 4
2.2. URLs à appeler 4
3. REALISATION DES TESTS 5
3.1. Spécificités permettant de réaliser des tests 5
3.1.1. Simulation des cas d'erreur 5
3.1.2. Identification des environnements 5
3.1.3. Reconduction des abonnements 6
3.1.4. 3D-Secure 6
3.1.5. Clé HMAC 6
3.2. Comptes commerçants de test 6
3.2.1. Votre compte de test personnel 6
3.2.2. Comptes de test mutualisés (comptes de démonstration) 7
3.2.2.1. Tests non 3D-Secure et plusieurs moyens de paiement 7
3.2.2.2. Tests 3D-Secure avec les pages de paiement 7
3.2.2.3. Tests 3D-Secure avec les API 8
3.2.2.4. Tests non 3D-Secure avec les pages de paiement et les API 9
3.3. Cartes de test 9
3.3.1. Banque française (compatibles CB) 9
3.3.2. Cartes de paiement étrangères 10
3.3.3. E-Carte Bleue 10
3.3.4. American Express 10
3.3.5. JCB 10
3.3.6. Diners 10
3.3.7. Illicado 11
3.3.8. Paysafecard 11
3.4. Comptes clients de test 11

3.4.1. Paypal....11
3.4.2. Leetchi....11
4. ANNEXES....12
4.1. Codes de retour des pages de paiement (variable E avec PBX_RETOUR)....12
4.2. Codes réponse des APIs....13
4.3. Codes réponse du centre d'autorisation....14
4.3.1. Réseaux CB, Visa, Mastercard, American Express et Diners....14

1. OBJET DU DOCUMENT

Up2pay e-Transactions est un système sécurisé d'encaissement par cartes bancaires et/ou cartes privatives à destination des commerçants disposant d'un site e-commerce.

1.1. Principe général de la Solution

Dans le domaine du e-commerce, le Crédit Agricole propose une solution de paiement sur internet appelée Up2pay **e-Transactions**, prévue pour être intégrée à votre site marchand de différentes façons en s'appuyant sur des interfaces techniques spécifiques :

- ✓ s'interface avec votre site marchand accessible depuis un navigateur web sur ordinateur, tablette et smartphone.
  Une fois votre solution de paiement intégrée à votre site marchand, vos clients peuvent effectuer des paiements en toute sécurité : ils sont redirigés vers la plateforme Up2pay **e-**Transactions suite à la réalisation d'une commande.
  Une connexion cryptée est établie avec le navigateur de vos clients, une page de paiement sécurisée et multilingue est affichée, et les invite à saisir leurs informations Carte.
  Cette page de paiement est personnalisable afin de pouvoir l'harmoniser à votre identité graphique.
  Notre solution de paiement répond aux normes de sécurité des paiements par carte en affichant une page HTTPS (sécurisée en TLS 1.2) et hébergée sur une plate-forme certifiée PCI-DSS.

- ✓ La **G**estion **A**utomatisée des **E**ncaissements (GAE dans le document), est une des fonctionnalités de l'offre, qui permet de communiquer avec la solution par API.
  Elle permet de valider directement depuis votre boutique, les transactions préalablement autorisées, d'effectuer des remboursements et des annulations.

  Elle peut également offrir un parcours de paiement confortable et simplifié pour vos clients directement sur votre site en se substituant à la page de paiement **e-**Transactions.
  Votre site collecte, via un formulaire de saisie, les informations bancaires de votre client pour les envoyer à la solution **e-**Transactions.

Dans ce cas, votre site marchand joue le rôle de collecteur des informations sensibles telle que le numéro de carte et vous devez les transmettre à notre plateforme via un dialogue sécurisé de serveur à serveur. Vous devez être certifié PCI-DSS par les autorités compétentes.

Le principe de ce fonctionnement est donc de :

- Générer un formulaire de saisie des informations bancaires
- Créer une session de communication sécurisée grâce à une trame HTTPS « question »,
- Appeler une URL présente sur nos serveurs et envoyer les éléments du formulaire,
- Récupérer dans la même session HTTPS, la trame « réponse » retournée par la plateforme après traitement de la transaction, contenant entre autres, l'information sur l'acceptation ou le refus de la transaction.

- Fermer la session HTTPS

✓ Votre site marchand peut demander à notre plateforme de conserver les données du moyen de paiement carte ou Paypal utilisé lors d'un achat. Cette solution s'interface en complément du paiement en utilisant les pages de paiement de la solution Up2pay e-Transactions ou en utilisant les API.
Ce service vous permet entre autres de gérer des abonnements ainsi que des paiements en un clic (one-click) où l'Acheteur ne ressaisie pas les données de son moyen de paiement à chaque nouvelle transaction.

Une fois les informations bancaires saisies et reçues par notre serveur, **Up2pay e-Transactions** effectue une demande d'autorisation auprès de l'émetteur associé au moyen de paiement choisi, dans le respect des normes de paiement en vigueur pour chaque paiement.
A la suite du paiement, un ticket de paiement est envoyé par e-mail à vous et à votre client.

En parallèle, les informations relatives au paiement sont envoyées à votre site pour mise à jour automatique de l'état de la commande par IPN (*Instant Payment Notification*) et votre client est en parallèle redirigé sur une page de confirmation de commande de votre site.

Dans la nuit, **Up2pay e-Transactions** réunit sous forme d'un « fichier remise » tous les paiements cartes bancaires réalisés sur votre site et les envoie au centre de télécollecte du Crédit Agricole pour traitement des transactions.
Si vous avez effectué un ou plusieurs remboursements, ces transactions de remboursement seront également réunies dans le fichier de remise.
Vous recevez quotidiennement un ticket de compte-rendu de télécollecte par e-mail, sous plusieurs formats.
Pour les autres moyens de paiements, Up2pay e-Transactions respecte les modalités des différents fournisseurs.

1.2. Principe général du document

Le présent document présente l'ensemble des éléments nécessaires à la réalisation de vos tests d'intégration de la solution Up2pay e-Transactions dans votre boutique.

Il est composé de 2 parties :
- Les éléments techniques de la plateforme de test d'Up2pay e-Transactions
- La description des spécificités de cette plateforme et les données permettant de réaliser les tests.

Il s'adresse aux personnes ayant besoin des informations nécessaire à réaliser les tests de l'intégration de la solution e-Transactions qu'ils ont réalisé sur une boutique.

2. PLATEFORME DE TEST

2.1. Pourquoi une plateforme de test

Le Crédit Agricole met à la disposition des commerçants et intégrateurs une plateforme de tests (« pré-production ») accessible librement et gratuitement.

Cet environnement permet de valider l'intégration des produits e-Transactions sans prendre de risques.

En effet, les paiements réalisés dans cet environnement ne sont pas transmis à la banque ou à l'établissement financier privatif. Vous pouvez donc procéder à de nombreux tests pour valider votre intégration sans risquer d'être débité ou facturé.

Une fois que vous avez réalisé et validé votre intégration de la solution Up2pay e-Transactions dans votre boutique avec la plateforme de test, vous pouvez « basculer » vers la plateforme de production.
Pour cela, vous devez générer une clé HMAC pour la plateforme de production tel que décrit dans le document ***Ref1 – Manuel d'intégration e-Transactions*** et remplacer, dans votre boutique, la clé HMAC de test par celle de production puis changer les URLs d'appel à la solution e-Transactions par celles de la plateforme de Production (voir ***Ref1 – Manuel d'intégration e-Transactions*** pour le détail sur les URLs à appeler en production).

2.2. URLs à appeler

Attention : ne sont listées ici que les URLs de la plateforme de test. Reportez-vous au document ***Ref1-Manuel d'intégration e-Transactions*** pour connaitre l'ensemble des URLs de la plateforme e-Transactions.

L'URL pour initier une transaction avec une page de choix de moyen de paiement (RWD – Responsive Web Design – La page s'adapte au média utilisé) :

Plateforme	URL d'accès
Recette	https://preprod-tpeweb.e-transactions.fr/php/

L'URL (sensible à la casse) pour initier une transaction directement sur la page de paiement correspondant au moyen de paiement choisi (Page RWD) :

Plateforme	URL d'accès
Recette	https://preprod-tpeweb.e-transactions.fr/cgi/FramepagepaiementRWD.cgi

PBX_TYPEPAIEMENT et PBX_TYPECARTE doivent être envoyés à ces URL, surtout si vous avez plus d'un moyen de paiement souscrit.
Vous pouvez aussi utiliser la page /php/ ci-dessus avec les champs PBX_TYPEPAIEMENT et PBX_TYPECARTE. Dans ce cas, votre client est redirigé automatiquement vers la bonne page de paiement (saut visible dans le navigateur).

L'URL pour initier des transactions avec une page de paiement intégrée dans votre boutique (iFrame) :

Plateforme	URL d'accès
Recette	https://preprod-tpeweb.e-transactions.fr/cgi/MYframepagepaiement_ip.cgi

L'URL pour utiliser les API de la solution (**G**estion **A**utomatisée des **E**ncaissements):

Plateforme	URL d'accès
Recette	https://preprod-ppps.e-transactions.fr/PPPS.php

L'URL pour utiliser réaliser l'authentification 3D-Secure pour les paiements effectués par API (services **e-Transactions Remote MPI)** :

Plateforme	URL d'accès
Recette	https://preprod-tpeweb.e-transactions.fr/cgi/RemoteMPI.cgi

Pour accéder au Back-office Vision de test, choisissez l'environnement « Recette » en ouvrant votre logiciel Back-office Vision Air.

3. REALISATION DES TESTS

3.1. Spécificités permettant de réaliser des tests

3.1.1. Simulation des cas d'erreur

Au-delà de simuler un retour « PAIEMENT ACCEPTE », e-Transactions vous permet de simuler des paiements refusés. Vous pouvez aussi bien simuler des erreurs retournées par la plateforme, que des codes associés à des refus d'autorisation bancaire.

Pour obtenir un code erreur volontairement, il faut renseigner la variable ERRORCODETEST (PBX_ERRORCODETEST pour e-Transactions). Cette variable est ignorée sur la plateforme de production.

L'ensemble des codes retour disponibles (présentés en annexe) sont ainsi simulables, vous permettant d'anticiper le traitement ad hoc au sein de votre application.

3.1.2. Identification des environnements

Dans le cadre de vos tests, en cas de paiement accepté, le numéro d'autorisation retourné par la plateforme sera toujours « XXXXXX ».

L'enseigne affichée sur la page de paiement **e-Transactions** est préfixée par "***TEST*** vous permettant ainsi de savoir que vous utilisez l'environnement de test (recette) ou de production.

3.1.3. Reconduction des abonnements

Les échéances des abonnements ne sont pas exécutées. Pour vérifier la bonne prise en compte de la demande de création d'abonnement, il faut vérifier la présence du numéro d'abonné dans la réponse de la plateforme Up2pay e-Transactions (variable B de *PBX_RETOUR*). ***(voir document Ref1 – Manuel d'intégration e-Transactions)***

3.1.4. 3D-Secure

Le système d'authentification 3D-Secure est simulé sur la plateforme de test. Vous êtes par conséquent toujours redirigé sur une page de test qui valide systématiquement l'authentification 3D-Secure du client.

3.1.5. Clé HMAC

Votre clé HMAC de la plateforme de test est indépendante de votre clé HMAC de production.

Vous devez donc générer une clé spécifique à l'environnement de test depuis l'onglet Paramètres du back-office Vision commerçant (voir document ***Ref1 – Manuel d'intégration e-Transactions*** pour plus de détails).

Attention : Lorsque vous avez terminé vos tests et que vous passez votre intégration en mode production, vous devez changer à la fois les URL d'appel à la solution et la clé HMAC pour correspondre à celle générée pour la production dans votre Back-office Vision.

Pour les comptes de test mutualisés (comptes de démonstration) et fournis par le support e-Transactions, la clé est prédéfinie et n'est pas modifiable. Elle est fournie au niveau dans l'onglet [Paramètres] du Back-office Vision de ces comptes de démonstration.

3.2. Comptes commerçants de test

3.2.1. Votre compte de test personnel

A l'ouverture des services Up2pay e-Transactions, un compte vous est simultanément créé sur l'environnement de production et sur l'environnement de test, avec les mêmes services et options.

Par conséquent, si vous êtes déjà client et que vos services sont ouverts (tel précisé dans votre mail de bienvenue), il est conseillé d'utiliser votre propre compte personnel pour valider que votre intégration correspond bien aux services souscrits.

3.2.2. Comptes de test mutualisés (comptes de démonstration)

Dans le cas où vous n'êtes pas encore client, Le Crédit Agricole met à votre disposition des comptes de tests mutualisés, utilisables par tout le monde, et simulant différentes configurations.

Pour tous les comptes de démonstration décrits ci-dessous, les données SITE, RANG, et IDENTIFIANT sont utiles pour réaliser des paiements. Les données LOGIN et MOT DE PASSE permettent, eux, l'accès à l'interface Back-office Vision e-Transactions.

3.2.2.1. Tests non 3D-Secure et plusieurs moyens de paiement

SITE + IDENTIFIANT	RANG	LOGIN	MOT DE PASSE
1999887 Identifiant : 215	32	integration@e-Transactions.fr (Vision)	CAtest1999887 (Vision)
CLE HMAC			
0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF			
SERVICES		**MOYENS DE PAIEMENT**	
• Pack e-Transactions Premium • Appels en API (GAE) • Back-office Vision		 …	

Note : Ce compte permet principalement le test des pages de paiement avec la disponibilité de nombreux moyens de paiement.

3.2.2.2. Tests 3D-Secure avec les pages de paiement

SITE + IDENTIFIANT	RANG	LOGIN	MOT DE PASSE
1999887 Identifiant : 221	43	integration@e-Transactions.fr (Vision)	CAtest1999887 (Vision)

CLE HMAC
0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF

SERVICES	MOYENS DE PAIEMENT
• Pack e-Transactions Premium • Appels en API (GAE) • Back-office Vision	

Attention : Ce compte permet l'utilisation des API pour l'utilisation des abonnés et les opérations de caisse (remboursement, capture, …). Par contre, il n'est pas possible d'initier un paiement 3D-Secure sur ce compte. Pour cela, il faut utiliser le compte suivant.

3.2.2.3. Tests 3D-Secure avec les API

SITE + IDENTIFIANT	RANG	LOGIN	MOT DE PASSE
1999887 Identifiant : 222	63	integration@e-Transactions.fr (Vision)	CAtest1999887 (Vision)

CLE HMAC
0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF

SERVICES	MOYENS DE PAIEMENT
• Appels en API (GAE) • API RemoteMPI pour authentification 3DS • Back-office Vision	

Note : Ce compte permet la réalisation de transactions 3D-Secure en utilisant les API et via l'utilisation du module RemoteMPI.

3.2.2.4. Tests non 3D-Secure avec les pages de paiement et les API

SITE + IDENTIFIANT	RANG	LOGIN	MOT DE PASSE
1999887 Identifiant : 218	85	integration@e-Transactions.fr (Vision)	CAtest1999887 (Vision)
CLE HMAC			
0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF			
SERVICES		**MOYENS DE PAIEMENT**	
• Pack e-Transactions Premium • Appels en API (GAE) • Back-office Vision			

Note : Ce compte permet la réalisation de transactions non 3D-Secure avec les pages de paiement et les appels aux API.

3.3. Cartes de test

Ces cartes de test sont valables sur la plateforme de test (recette) pour les comptes commerçants de test mutualisés (démonstration) et pour votre compte de test personnel.

Note : Les valeurs « Date de fin de validité » et « CVV » ne sont pas contrôlées sur la plateforme de tests. N'importe quelle valeur est donc possible.

3.3.1. Banque française (compatibles CB)

Vous pouvez également utiliser votre carte personnelle CB/VISA/Mastercard sur la plateforme de tests : **celle-ci ne sera jamais débitée**.

DESCRIPTION	CARTE	VALIDITE*	CVV*
Numéro de carte de test	1111 2222 3333 4444	12/24	123
Carte participant au programme 3D-Secure (enrôlée)	4012 0010 3714 1112	12/24	123

Carte hors programme 3D-Secure (non enrôlée)	4012 0010 3844 3335	12/24	123

3.3.2. Cartes de paiement étrangères

DESCRIPTION	CARTE	VALIDITE*	CVV*
Carte Visa belge	4236 8615 8842 3130	12/24	123
Carte Mastercard belge	5476 8520 5684 3079	04/24	922
Carte Maestro belge	6703 1111 2222 3334	12/24	N/A

3.3.3. E-Carte Bleue

DESCRIPTION	CARTE	VALIDITE*	CVV*
e-CB LCL	4150 5500 0000 0004	12/24	123
PayWebCard Crédit Mutuel	4972 6400 0000 0009	12/24	123

3.3.4. American Express

DESCRIPTION	CARTE	VALIDITE*	CVV*
Carte American Express	3749 0740 3001 005	12/24	1234

3.3.5. JCB

DESCRIPTION	CARTE	VALIDITE*	CVV*
Carte JCB	3569 9900 1200 0112	12/24	123

3.3.6. Diners

DESCRIPTION	CARTE	VALIDITE*
Carte Diners	3613 3990 076 017	06/24

3.3.7. Illicado

DESCRIPTION	CARTE	CVV*
Carte illicado	9250 0041 0000 0127 783	649

3.3.8. Paysafecard

DESCRIPTION	CARTE
Carte Paysafecard	0000 0000 0990 3985

3.4. Comptes clients de test

3.4.1. Paypal

Il n'est pas possible de tester Paypal sur les comptes de test mutualisés (démonstration), mais uniquement sur votre compte de test personnel.

Une fois votre compte Paypal créé et les informations fournies au Support e-Transactions, connectez-vous à l'espace Développeur Paypal avec votre compte Paypal :
https://developer.paypal.com/

Cliquez ensuite sur « Applications », puis sur « Sandbox accounts ».
A partir de cet emplacement, vous pouvez créer des comptes clients de test (Account type : Personal).

3.4.2. Leetchi

Vous devez demander un compte client de test directement aux équipes de Leetchi.

Contact : sales@leetchi.com – http://www.leetchi-partners.com

4. ANNEXES

4.1. Codes de retour des pages de paiement (variable E avec PBX_RETOUR)

CODE	DESCRIPTION
00000	Opération réussie.
00001	La connexion au centre d'autorisation a échoué ou une erreur interne est survenue. Dans ce cas, il est souhaitable de faire une tentative sur l'autre site: tpeweb.e-transactions.fr ou tpeweb1.e-transactions.fr en fonction de celui que vous utilisez.
001xx	Paiement refusé par le centre d'autorisation [voir *4.3-Codes réponse du centre d'autorisation*]. En cas d'autorisation de la transaction par le centre d'autorisation de la banque ou de l'établissement financier privatif, le code erreur "00100" est remplacé directement par "00000".
00003	Erreur de la plateforme. Dans ce cas, il est souhaitable de faire une tentative sur l'autre site tpeweb.e-transactions.fr ou tpeweb1. e-transactions.fr en fonction de celui que vous utilisez.
00004	Numéro de porteur ou cryptogramme visuel invalide.
00006	Accès refusé ou site/rang/identifiant incorrect. Veuillez vérifier votre paramétrage ou le calcul de la signature HMAC (PBX_HMAC).
00008	Date de fin de validité incorrecte.
00009	Erreur de création d'un abonnement.
00010	Devise inconnue.
00011	Montant incorrect.
00015	Paiement déjà effectué.
00016	Abonné déjà existant (inscription nouvel abonné). Valeur 'U' de la variable PBX_RETOUR
00021	Carte non autorisée.
00029	Carte non conforme. Code erreur renvoyé lors de la documentation de la variable « PBX_EMPREINTE ».
00030	Temps d'attente > 15 mn par l'internaute/acheteur au niveau de la page de paiements.
00031	Réservé
00032	Réservé
00033	Code pays de l'adresse IP du navigateur de votre client non autorisé.
00040	Opération sans authentification 3D-Secure, bloquée par le filtre.
99999	Opération en attente de validation par l'émetteur du moyen de paiement.

Tableau 1 : Codes réponse de la donnée (E) PBX_RETOUR

4.2. Codes réponse des APIs

CODE	DESCRIPTION
00000	Opération réussie.
00001	La connexion au centre d'autorisation a échoué ou une erreur interne est survenue.
001xx	Paiement refusé par le centre d'autorisation. [voir *4.3-Codes réponse du centre d'autorisation*]. En cas d'autorisation de la transaction par le centre d'autorisation de la banque, le résultat "00100" sera en fait remplacé directement par "00000".
00201	Le paiement est réalisé sans authentification 3D-Secure qui est requise par le centre d'autorisation de votre client. Vous devez réaliser une demande d'authentification avec le composant RemoteMPI. [voir document ***Ref1-Manuel d'intégration e-Transactions***]
00002	Une erreur de cohérence est survenue.
00003	Erreur Plateforme.
00004	Numéro de porteur invalide.
00005	Numéro de question invalide.
00006	Accès refusé ou site / rang incorrect.
00007	Date invalide.
00008	Date de fin de validité incorrecte.
00009	Type d'opération invalide.
00010	Devise inconnue.
00011	Montant incorrect.
00012	Référence commande invalide.
00013	Cette version n'est plus soutenue.
00014	Trame reçue incohérente.
00015	Erreur d'accès aux données précédemment référencées.
00016	Abonné déjà existant (inscription nouvel abonné).
00017	Abonné inexistant.
00018	Transaction non trouvée (question du type 11).
00019	Réservé.
00020	Cryptogramme visuel non présent.
00021	Carte non autorisée.
00022	Plafond atteint
00023	Porteur déjà passé aujourd'hui
00024	Code pays filtré pour ce commerçant
00037	HMAC invalide
00097	Timeout de connexion atteint.
00098	Erreur de connexion interne.
00099	Incohérence entre la question et la réponse. Refaire une nouvelle tentative ultérieurement.

Tableau 2 : Codes réponse des APIs

4.3. Codes réponse du centre d'autorisation

Cette information est transmise dans les informations de retour en fin de transaction.

Concernant le paiement avec les pages de paiement, si la donnée « **E** » est demandée lors de l'appel dans la variable **PBX_RETOUR** (voir ***Ref1-Manuel d'intégration e-Transactions***), vous retrouvez ces valeurs dans les 2 derniers chiffres du code d'erreur retourné si sa valeur est de la forme **001xx** *(où xx représentent les codes réponse du centre d'autorisation)*.

Concernant les opérations de paiement par API, vous retrouvez ces valeurs dans les 2 derniers chiffres du code d'erreur retourné (CODEREPONSE) si sa valeur est de la forme **001xx** *(où xx représentent les codes réponse du centre d'autorisation)*.

4.3.1. Réseaux CB, Visa, Mastercard, American Express et Diners

CODE	SIGNIFICATION CODE REPONSE DU CENTRE D'AUTORISATION
00	Transaction approuvée ou traitée avec succès
01	Contacter l'émetteur de carte
02	Contacter l'émetteur de carte
03	Commerçant invalide
04	Conserver la carte
05	Ne pas honorer
07	Conserver la carte, conditions spéciales
08	Approuver après identification du porteur
12	Transaction invalide
13	Montant invalide
14	Numéro de porteur invalide
15	Emetteur de carte inconnu
17	Annulation client
19	Répéter la transaction ultérieurement
20	Réponse erronée (erreur dans le domaine serveur)
24	Mise à jour de fichier non supportée
25	Impossible de localiser l'enregistrement dans le fichier
26	Enregistrement dupliqué, ancien enregistrement remplacé
27	Erreur en « edit » sur champ de mise à jour fichier
28	Accès interdit au fichier
29	Mise à jour de fichier impossible
30	Erreur de format
33	Carte expirée
38	Nombre d'essais code confidentiel dépassé
41	Carte perdue
43	Carte volée

51	Provision insuffisante ou crédit dépassé
54	Date de validité de la carte dépassée
55	Code confidentiel erroné
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
75	Nombre d'essais code confidentiel dépassé
76	Porteur déjà en opposition, ancien enregistrement conservé
89	Echec de l'authentification
90	Arrêt momentané du système
91	Emetteur de cartes inaccessible
94	Demande dupliquée
96	Mauvais fonctionnement du système
97	Echéance de la temporisation de surveillance globale

Tableau 3 : Codes réponses du centre d'auto CB