Guide d’implémentation de la solution de paiement CITELIS

Version 2H

PAGE DES EVOLUTIONS

Le tableau ci-dessous liste les dernières modifications effectuées sur ce document.

Date	Version	Modifications
04/10/07	1.0	Livraison version initiale
13/11/07	1.1	Ajout de la description des fonctions de l'API web service
10/01/08	1.2	Ajout des fonctions de paiement multiple : paiement par portefeuille client, paiement par abonnement et paiement en N fois
10/04/08	1.3	Ajout du moyen de paiement PAYPAL et des fonctions de création et modification d'un portefeuille client par l'interface web
09/07/08	1.4	Ajout des fonctions de recherche et récupération du détail d'une transaction de paiement Ajout des codes retour pour le module de détection de fraude (LCLF) Ajout de la carte privilège Ajout des fonctions et cinématiques de paiement 3DSecure
09/02/09	1.5	Ajout de la fonction doDebit
15/04/09	1.6	Mise à jour de l'objet AUTHENTIFICATION_3DSECURE Mise à jour des services Web createWallet et updateWallet pouvant implémenter l'authentification 3DSecure
26/10/09	1.7	Ajout du moyen de paiement IDEAL Ajout de la fonction doReset Ajout des acteurs visés par les messages d'erreur
23/11/09	1.8	Liste des langues
29/12/09	1.8	Complément sur l'ajout du paiement iDEAL
03/03/10	2. A	Refonte de la documentation
02/06/10	2.B	Publication de la documentation
11/10/10	2.C	Ajout des nouvelles fonctionnalités : chapitre 2.3.1 Scoring cheque Autre moyen de paiement Inclus dans la version V4 .23
09/03/11	2.D	Ajout des fonctionnalités de la version V4.24
28/06/2011	2 .E	Ajout de futures fonctionnalités
07/09/2011	2.F	V4.26
16/02/2012	2.G	Ajout des nouveaux moyens de paiement Ajout des nouvelles traductions
05/11/2012	2.H	Ajout des nouveaux moyens de paiements Ajout des nouveaux modules e-commerce

TABLE DES MATIERES

1. INTRODUCTION

1.1 Objet du document

Ce document décrit la procédure d'intégration de la solution de paiement sécurisé en ligne CITELIS dans votre site commerçant.

1.2 Liste des documents de référence

Nos documents sont disponibles sur notre site internet :
http://www.citelis.fr/installation/citelis-payline/solutions-techniques

1.3 Contacts

Pour toute question liée à la mise en place de la solution Payline, vous pouvez joindre notre assistance technique du lundi au vendredi de 09h00 à 18h00 :

- par mail : citelis@payline.com
- par téléphone : 09 69 39 04 48 (choix 1-2)

2 PRINCIPE GENERAL

2.1 Cinématique des échanges

La cinématique d'échange dans le cas le plus courant est la suivante :

1) Une fois la commande de l'internaute complète, le site marchand redirige celui-ci vers la solution de paiement CITELIS. Cette redirection prendra la forme d'un formulaire HTTP POST en HTTPS contenant des paramètres décrits dans le chapitre suivant.

2) La plateforme de paiement, après vérification des paramètres et de leur signature, présentera une page de sélection du moyen de paiement.

3) La solution de paiement affichera une page de saisie de numéro de carte, date d'expiration et cryptogramme visuel. En cas de validation, une demande d'autorisation sera effectuée auprès de l'acquéreur concerné, en plus des contrôles de fraude internes de la plateforme de paiement. Dans le cas de l'utilisation de l'option 3DSecure, une redirection vers un ACS 3D-Secure aura lieu avant la demande d'autorisation.

4) Le paiement effectué, il est possible de présenter un ticket acheteur, un bouton de retour vers le site marchand et d'envoyer un e-mail de confirmation de transaction à l'acheteur et/ou au commerçant.

2.2 Les pages web de paiement :

Sélection du type de carte :

Sélection des informations de la carte :

2.3 Fonctionnalités et moyens de paiement disponible

2.3.1 Fonctionnalités disponibles

Paiement immédiat : est un paiement dit comptant, vous réaliser soit une autorisation + validation, soit une autorisation et la validation est faite soit en automatique par la solution de paiement CITELIS, soit par le commerçant , en utilisant les appels « webservice » ou via notre outil de back office « centre administration CITELIS ».

Paiement différé : est un paiement dit différé, le commerçant fait une demande d'autorisation et la validation du paiement est faite par exemple lors de l'expédition du produit. Une demande d'autorisation est valable pendant 7 jours.
Cette validation peut être réalisée soit en automatique via CITELIS, soit par le commerçant en utilisant soit la fonctionnalité interface batch, soit en appelant le webservice « do capture », soit via le centre administration.

Paiement en n fois, par abonnement, par échéance : cette fonctionnalité est possible en utilisant un portefeuille virtuel « WALLET », pour de plus ample renseignement veuillez contacter l'équipe support CITELIS, qui vous communiquera la documentation associée.

Remboursement : une demande de remboursement d'un paiement validé et remis en banque, donc le client a été débité et le commerçant a été crédité.
Le délai de remboursement est de 6 mois.

Annulation : l'annulation d'une transaction est possible uniquement si la transaction a été validée et non remise en banque, donc le client n'a pas été débité sur son compte bancaire.

Débit suite à un appel phonie : c'est un débit forcé le commerçant a contacté sa banque et la banque lui fournit un numéro d'autorisation, et ce dernier lui permet de réaliser une demande de débit sur la carte bancaire de son client.

Re autorisation : une demande d'autorisation est valable pendant 7 jours, au-delà dès 7 jours si vous n'avez pas pu la valider et donc votre client n'a pas été encore débité, il est tout à fait possible d'utiliser l'option re-autorisation, qui fait une autorisation sans présence du cryptogramme puis une validation. Le commerçant doit pouvoir avec son contrat de vente à distance effectuer des paiements dit « récurrent ».

Portefeuille virtuel électronique « WALLET » : Un portefeuille virtuel est destiné à conserver les informations de votre client en vue de le fidéliser et de lui éviter lors d'une prochaine commande une nouvelle saisie de ses informations. Un Wallet sert donc à stocker les données monétiques et éventuellement les données privées du titulaire. Veuillez contacter l'équipe support CITELIS, qui vous communiquera la documentation associée.

Interface batch : cette fonctionnalité permet de traiter des transactions par lots en mode off line, il est possible de réaliser des validations, des remboursements, des annulations, pour de plus ample renseignement veuillez contacter l'équipe support CITELIS, qui vous communiquera la documentation associée.

Notification par sms : cette fonctionnalité permet à vos acheteurs de recevoir une confirmation par sms du paiement effectué. Pour de plus ample renseignement veuillez contacter l'équipe support CITELIS, qui vous communiquera la documentation associée.

Les modules de gestions des risques : la solution de paiement en ligne CITELIS met à disposition de ces commerçants des contrôles afin de limiter les risques engendrés par le commerce par internet. Pour de plus ample renseignement veuillez contacter l'équipe support CITELIS, qui vous communiquera la documentation associée.

Reporting : deux Reporting peuvent être mise à disposition aux commerçant : Journal des transactions et le fichier image de remise, ces deux Reporting peuvent être mise à disposition sur le SI Commerçant. Ces deux rapports permettent aux commerçants de les aider à réaliser leur réconciliation bancaire. Pour de plus ample renseignement veuillez contacter l'équipe support CITELIS, qui vous communiquera la documentation associée

Terminal de Paiement Electronique Virtuel : Le TPEV, Terminal de Paiement Electronique Virtuel est comme son nom l'indique, une application de paiement électronique sur le web. Elle est destinée aux commerçants qui souhaitent enregistrer des paiements dans le cadre de ses activités au travers d'une interface web sécurisée. Pour de plus ample renseignement veuillez contacter l'équipe support CITELIS, qui vous communiquera la documentation associée.

Centre Administration CITELIS : est un outil de back office, il vous permet de visualiser la configuration du commerçant, d'avoir une vue synthétique et/ ou détaillée de votre activité. . Pour de plus ample renseignement veuillez contacter l'équipe support CITELIS, qui vous communiquera la documentation associée.

Personnalisation des pages web de paiement : le commerçant en utilisant les pages web de paiement CITELIS, peut les utiliser et les personnaliser « ajout de logo, stylet… », . Pour de plus ample renseignement veuillez contacter l'équipe support CITELIS, qui vous communiquera la documentation associée.

Scoring cheque : cette fonctionnalité permet au commerçant, de vérifier que le chèque déposé par son client ne fait pas partie du Fichier National des Chèques Irréguliers.

Option autre moyen de paiement : cette fonctionnalité permet au commerçant, en cas de refus bancaire, de proposer à ses clients de pouvoir payer avec un autre moyen de paiement.

2.3.2 Moyens de paiement disponibles

Carte Crédit et débit	Nom de carte	Description
CB	Carte Bleu / VISA / Mastercard	VISA / Mastercard
VISA (Commerçant hors France)	Visa	VISA
MASTERCARD (Commerçant hors France)	Mastercard	Mastercard
AMEX	Carte American Express	American Express
SOFINCO	Carte Sofinco	Sofinco
DINERS	Carte Diners Club	Diners Club
AURORE	Carte Aurore	CETELEM
PASS	Carte Carrefour PASS	CETELEM
CBPASS	Carte Carrefour VISA PASS	CETELEM
CPU	Carte Pass Universel MC	CETELEM
COFINOGA	Carte Cofinoga	Cofinoga
CDGP	Carte privilège	COFINOGA
PRINTEMPS	Carte Printemps	FINAREF
KANGOUROU	Carte Kangourou	FINAREF
SURCOUF	Carte Surcouf	FINAREF
CYRILLUS	Carte Cyrillus	FINAREF
FNAC	Carte FNAC	FINAREF
JCB	Carte JCB	japanese card bank
MAESTRO	Carte Maestro	MASTERCARD

Autres moyens de paiement	Description
PAYPAL	Ce moyen de paiement est un portefeuille virtuel, il permet de payer en un clic.
IDEAL	Ce moyen de paiement permet d'effectuerdes virements d'un acheteur vers un commerçant. L'acheteur et le commerçant doivent être membre d'une des banques à l'initiative d'iDEAL : ING Bank N.V., Rabobank Nederland et Fortis Bank.
NEO SURF	Est une carte prépayée, le règlement est de 10 à 100 euros. Le commerçant devra souscrire auprès de la société NEO Surf ainsi qu'auprès de Payline afin de pouvoir utiliser ce moyen de paiement. => implémentation dans les prochains mois

INTERNET PLUS	L'acheteur paye chez son fournisseur d'accès internet et le commerçant reçoit une reversions des achats qui ont été réglés par internet +, le commerçant doit souscrire auprès des 3 téléopérateurs et auprès de wha, afin de pouvoir utiliser ce moyen de paiement.
ELV	Ce moyen de paiement permet d'effectuer des prélèvements « direct debit »d'un acheteur vers un commerçant. L'acheteur et le commerçant doivent être membre d'une des banques allemande
BUYSTER	Ce moyen de paiement permet de payez sur Internet avec un mobile
1EURO.COM	Paiement en plusieurs fois associé à un paiement de crédit
Moneybooker	Moneybooker est un portefeuille virtuel. Il permet de payer en ligne sans saisi des coordonnées de carte bancaire Le commerçant doit souscrire à un compte client auprès de Moneybooker => => implémentation dans les prochains mois
TicketSurf	Ticket Surf est un moyen de paiement de type carte prépayée vendu dans des points de vente physiques. L'acheteur de la carte l'utilise pour le paiement en ligne en renseignant le numéro inscrit sur la carte dans l'interface appelée par le commerçant. Le commerçant doit souscrire à un compte client chez TicketSurf pour pouvoir accepter les paiements. => implémentation dans les prochains mois
Paysafecard	PaySafeCard est un moyen de paiement de type carte prépayée vendu dans des points de vente physiques. L'acheteur de la carte l'utilise pour le paiement en ligne en renseignant le numéro inscrit sur la carte dans l'interface appelée par le commerçant. Le commerçant doit souscrire à un compte client chez PaySafeCard pour pouvoir accepter les paiements. => implémentation dans les prochains mois
Payfair	Carte de paiement européenne
MAXICHEQUE	Ce moyen de paiement est un cheque cadeau, envoyé par mail au bénéficiaire
WEXPAY	Ce moyen de paiement permet d'effectuer des paiements en espèces en achetant un moyen de paiement de type carte prépayée vendu dans des points de vente physiques.
Ukash	Ukash est un système international de paiement en espèces pour ceux qui souhaitent acheter, payer et jouer sur internet

2.3.3 Traduction

En utilisant les pages web de paiement CITELIS :

- Français (fr / fra / fre)
- Anglais (en / eng)
- Espagnol (es / spa)
- Portugais (por / pt)
- Allemand (ger / deu / de)
- Finnois (fin / fi)
- Italien (it / ita)
- Danois (da)
- Tchèque (cs)
- Néerlandais (dut / nl / nld)
- Polonais (pl)
- Hongrois (hu)
- Norvégien (no)
- Grec (el)
- Estonien (et)
- Slovaque (sk)
- Suédois (sv)

En utilisant le TPEV de CITELIS :

- Français
- Anglais
- Espagnol
- Portugais
- Allemand
- Polonais
- Néerlandais

En utilisant le Centre Administration de CITELIS :

- Français
- Anglais
- Espagnol
- Portugais

2.3.4 Trois solutions d'intégration pour utiliser la solution de paiement CITELIS :

2.3.4.1 Suite e-commerce : une utilisation immédiate

Utilisez une suite e-commerce certifiée CITELIS Payline et n'ayez aucune intégration à effectuer :

- OScommerce,
- VirtueMart,
- Zencart,
- Joomla,
- Magento,
- OpenCart,
- EShop ,
- Plici,
- Prestashop,
- TomatoCart,
- UberCart,

2.3.4.2 Kit d'intégration : une installation facilitée

Intégrez CITELIS à l'aide d'un kit. Vous devez avoir des connaissances du langage HTML et d'un langage de scripts tels que PHP, C# et Java pour l'utilisation du kit d'intégration sélectionné.

Rendez-vous sur le site http://www.citelis.fr/installation/citelis-payline/solutions-techniques afin de télécharger les kits et la documentation associée.

2.3.4.3 API SOAP : une intégration complète

Intégrez CITELIS à l'aide de l'API SOAP. Vous devez maitriser le développement d'interface client avec des services standards web sécurisés.

2.4 Sécurité

CITELIS est conforme aux normes de sécurité et a obtenu la certification PCI DSS en 2008 et obtient son renouvellement de certification chaque année.

Dans la communication entre la solution de paiement CITELIS et le site marchand, deux mécanismes de sécurité sont mis en place selon la souscription du pack choisi : Echange de clef d'accès et Echange de certificat

En fonction de votre environnement, vous pouvez être amené à ajouter dans votre « **magasin de sécurité** » (keystore) la clé publique du certificat « root » de CITELIS. Il s'agit du certificat délivré par l'autorité de certification *VeriSign, inc*. Cela permet à votre serveur d'authentifier les serveurs CITELIS et donc d'assurer une communication de serveur à serveur fortement sécurisée.

2.4.1 Pré requis sécurité

Dans l'objectif de conserver vos communications avec CITELIS sécurisées, veuillez respecter les règles décrites ci-dessous.

Vous devez obligatoirement utiliser une connexion HTTPS sécurisé par SSL V3 (SSL V2 n'est pas autorisé).

Lorsque vous réalisez des demandes de paiement à l'API CITELIS, vous devez obligatoirement présenter votre identifiant de compte commerçant (Merchand ID) et votre clé d'accès (Merchant Access Key) pour réaliser une authentification http. CITELIS n'acceptera pas vos demandes si elles ne sont pas correctement authentifiées.

Ne communiquez jamais votre clé d'accès (Merchant Access Key) à une tierce personne. CITELIS utilise votre clé d'accès pour vous identifier en tant qu'expéditeur de vos demandes de paiement. Aucun interlocuteur chez CITELIS ne la connaît et ne vous demandera cette information.

En complément, nous vous recommandons de vérifier l'authenticité du certificat serveur qui vous est présenté lors d'une connexion HTTPS avant d'envoyer vos données ou de réaliser une authentification HTTP. Cela consiste à s'assurer que : Le certificat appartient bien à CITELIS,

Le certificat est signé par une autorité de certification digne de confiance, Le certificat est toujours valide (n'est pas expiré et n'est pas révoqué).

L'utilisation d'iframe n'est pas compatible avec une utilisation optimale et sécuritaire de CITELIS.

2.4.2 Echange de clef d'accès :

Pour toute communication entre CITELIS et le site marchand, l'authentification se fait à l'aide des éléments suivant : votre identifiant commerçant, votre clef d'accès et votre numéro de contrat.

Méthodes d'authentification HTTP
CITELIS utilise le mécanisme HTTP Basic Authentification pour authentifier les commerçants abonnés. Ce paragraphe explique comment fonctionne une authentification HTTP et comment l'implémenter dans le code client des services web.

HTTP Basic Authentification
Si votre identifiant de compte commerçant est 1234567890 et votre clé d'accès est DJMESHXYou6LmjQFdH, vous devez encoder en base64 la valeur de 1234567890:DJMESHXYou6LmjQFdH. La chaîne obtenue est à ajouter à l'entête HTTP comme dans l'exemple ci-dessous :

Authorization : Basic MTIzNDU2Nzg5MdpESk1FU0hYWW91NkxtalFGZEg=

En fonction du langage informatique, l'identifiant et clé d'accès sont automatiquement encodés en base64 et ajoutés à l'entête HTTP.

Grâce à cette mécanique, vous sécurisez de façon optimale vos échanges informatiques entre vos applications et CITELIS et assurez au travers du protocole SSL V3 :
- l'authentification des interlocuteurs : vos serveurs et les serveurs CITELIS,
- l'intégrité des messages,
- le cryptage des données.

Vous devez vous assurer d'avoir les informations suivantes en contactant le service support de CITELIS

Votre identifiant commerçant : **MerchantID**
Votre clé d'accès au service Payline : **MerchantAccesskey**
Les certificats serveur Payline* : homologation et production
Votre ou vos contrats de vente à distance : **contractNumber**

Points d'accès des services web

SSL V3 avec clé d'accès :
- https://services.payline.com

2.4.3 Echange de certificat

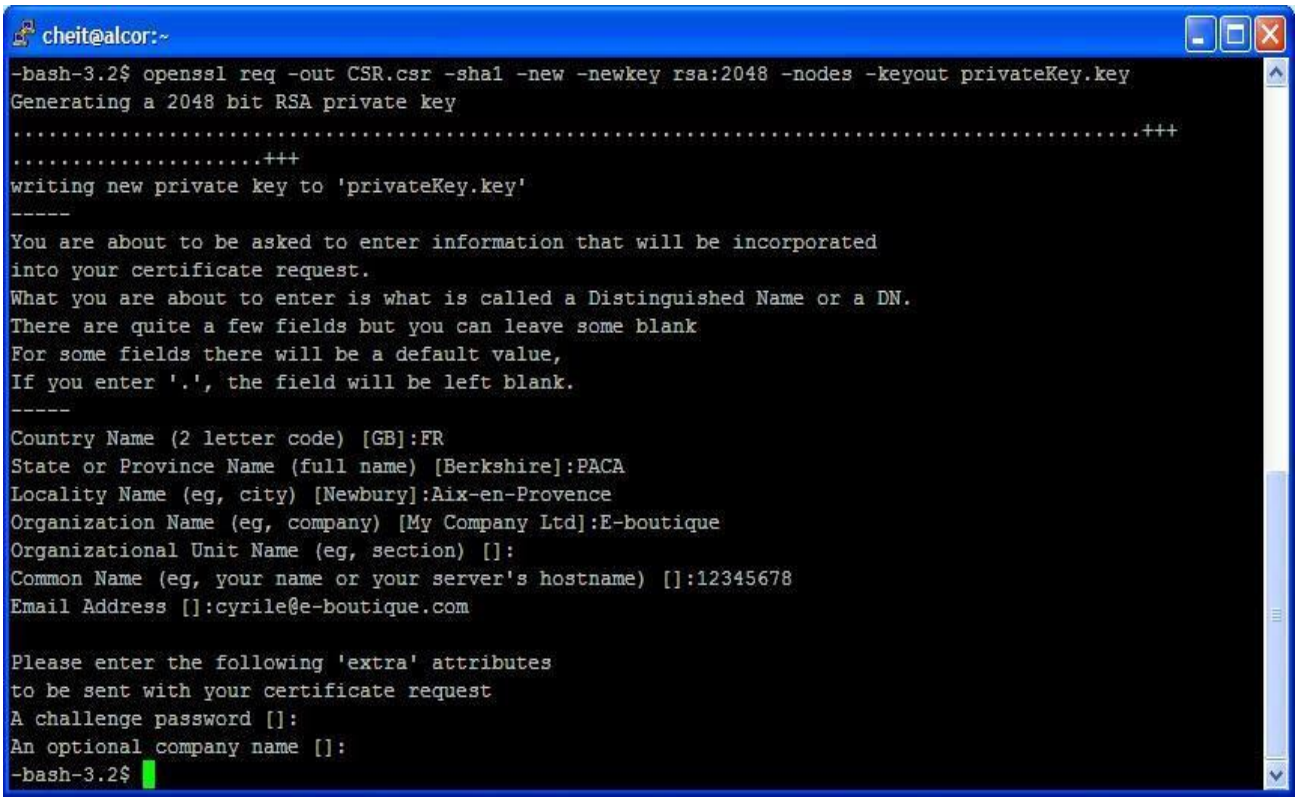
La mise en place de l'authentification par certificat de type class 3.
Le certificat utilisé pour la signature devra être présent dans le magasin des certificats pour accorder l'accès.
Le certificat client permettra de retrouver l'identifiant commerçant.
Le certificat devra prendre en compte les exigences de sécurité PCI et de la solution de paiement CITELIS : Le certificat du commerçant doit être sous un format stand PEM (base 64) et en sha-1 pour le hachage cryptographique. De plus la clef privée associée devra être supérieur ou égale à un encodage de 2048 bits (le common name doit être d'ID Marchant.)

Le certificat CSR fournit par le commerçant sera signé par MONEXT, et ce certificat CSR signé sera déposé avec la clef privé généré lors de la création du csr sur le keystore du commerçant et il sera utilisé lors de chaque appels web services vers la solution de paiement CITELIS.

Dans le cas où vous utilisez openSSL :
La commande à exécuter pour générer la clef privée et le certificat csr :

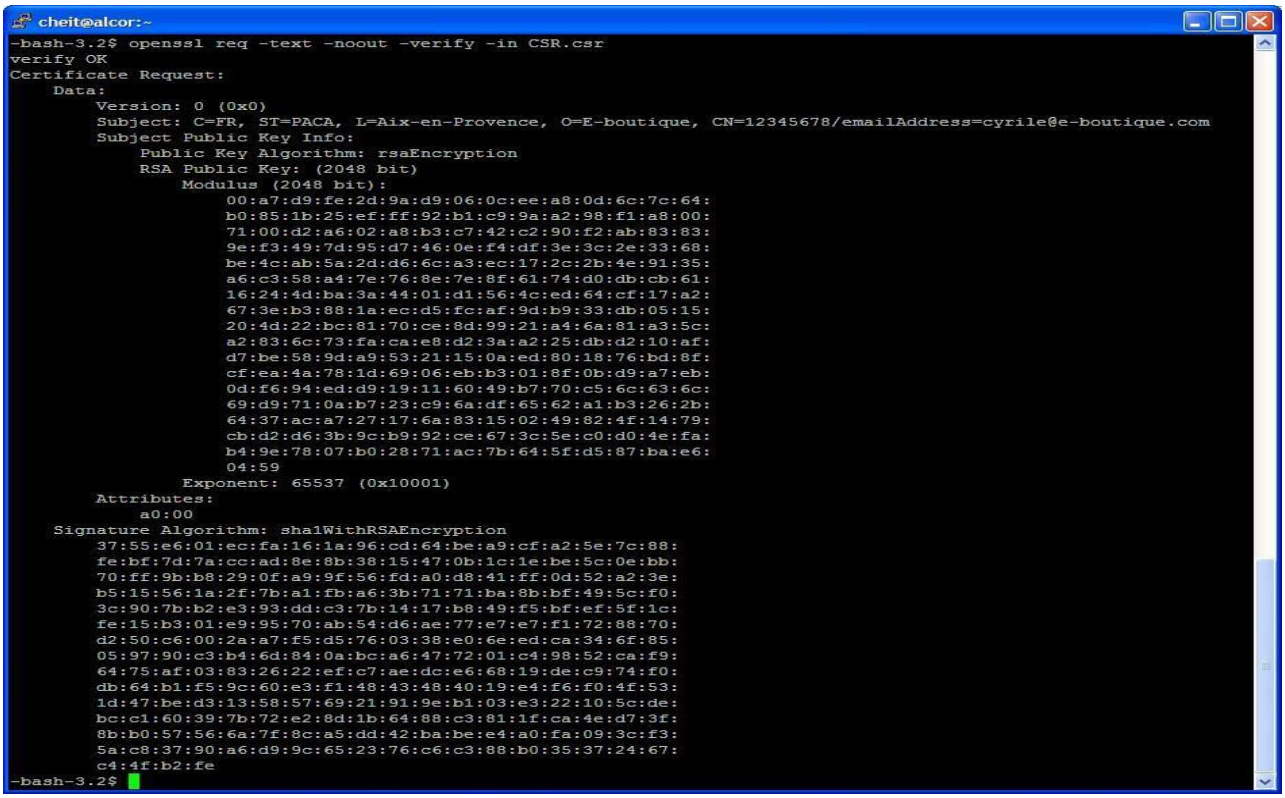
```
openssl req -out CSR.csr -sha1 -new -newkey rsa:2048 -nodes -keyout privateKey.key
```

Ensuite il faut répondre à un certain nombre de question. Le plus important est de mettre l'identifiant du commerçant dans le Common Name (pour l'exemple nous avons inséré comme exemple id marchant 12345678)



Si vous souhaitez vérifier votre CSR, vous pouvez utiliser cette commande :

openssl req -text -noout -verify -in CSR.csr



Puis vous devez utiliser la commande décrite ci-dessous, dès réception du certificat signé par Monext, ce fichier générer le pkcs12, vous permettra de configurer votre serveur lors de chaque appel webservice

openssl pkcs12 -export -in cert_client_xxx.pem -inkey clef.key -certfile ca_inter.pem -out nom_du fichier_de_sortie.p12 -name "Nom du certificat"

Pour de plus ample information, veuillez contacter notre équipe support CITELIS, citelis@payline.com

Points d'accès des services web

SSL V3 certificat client :

- https://services-cc.payline.com

2.4.4 WSDL :

Les schémas WSDL de l'API CITELIS sont accessibles aux adresses suivantes :
Les wsdl doivent être téléchargés en local sur le SI du commerçant, et ne doivent pas être sollicité à chaque demande paiement.

Schéma Production CITELIS :
http://www.payline.com/wsdl/v4_0/production/WebPaymentAPI.wsdl
http://www.payline.com/wsdl/v4_0/production/DirectPaymentAPI.wsdl
http://www.payline.com/wsdl/v4_0/production/ExtendedAPI.wsdl

2.4.5 Accès au Centre Administration CITELIS:

Interface utilisateur :

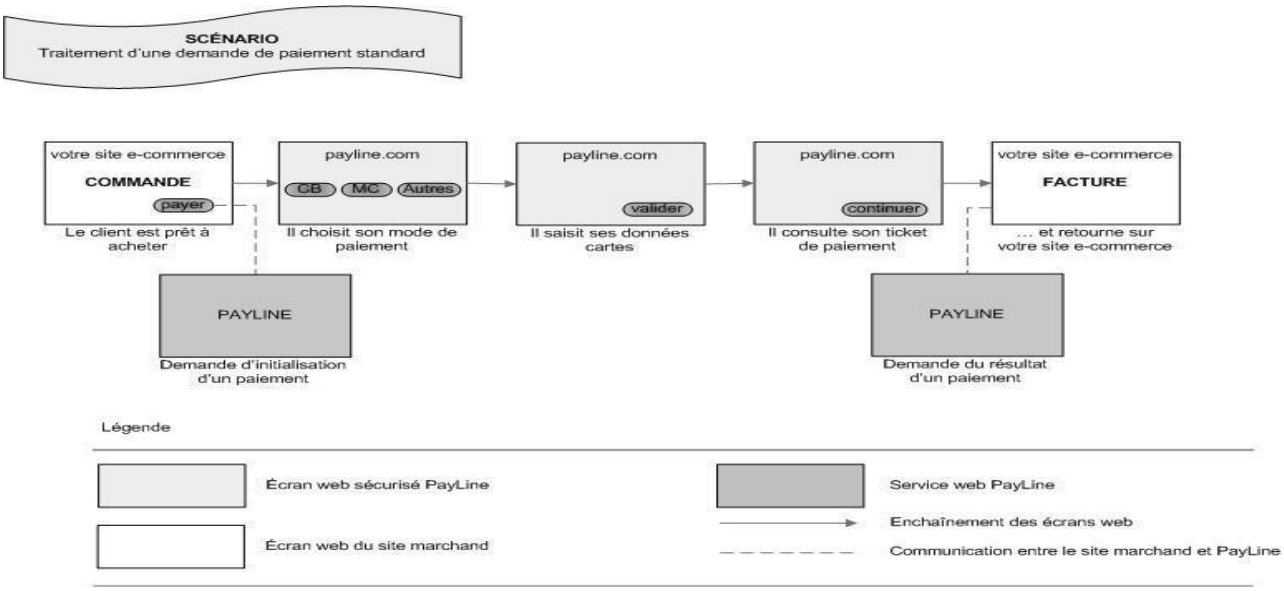
- Centre d'administration commerçant:
  https://test-adminpayment.citelis.fr/

3 INTEGRATION INTERFACE WEB

CITELIS s'interface avec votre site d'e-commerce et permet à vos clients de payer en toute simplicité. Vos clients sont redirigés automatiquement sur les pages de paiement multilingue CITELIS, personnalisables à l'image de votre site d'e-commerce. CITELIS répond aux normes de sécurité des paiements par carte sur les sites d'e-commerce.

3.1 Cinématique du processus de paiement standard

CITELIS prend en charge l'acquisition, le contrôle et le traitement monétique des informations de paiement de votre client. Deux points d'intégration suffisent à créer une demande de paiement et à récupérer le résultat de la transaction.



1. Sur votre site d'e-commerce, votre client clique sur le bouton « payer » pour procéder au paiement de sa commande.
2. Votre site contacte CITELIS (1er point d'intégration) pour effectuer une transaction. CITELIS renvoie un jeton de session et l'URL à utiliser pour le transfert de votre client vers les pages web CITELIS.
3. Votre client saisit ses données carte en toute sécurité sur CITELIS. Après validation, il consulte son justificatif de paiement.
4. CITELIS redirige votre client sur votre site d'e-commerce pour consultation de sa facture.
5. Votre site contacte CITELIS (2eme point d'intégration) pour obtenir le détail du résultat du paiement.
   A votre convenance, CITELIS peut prendre en charge l'appel d'une URL sur votre site pour déclencher la demande de résultat d'un paiement (notification automatique de paiement).

3.2 Cinématique du processus de paiement 3DSecure

La solution 3D Secure CITELIS Web prend en charge l'acquisition, le contrôle et le traitement monétique.

Aucun point d'intégration supplémentaire n'est nécessaire à la création de la demande d'autorisation et à la récupération du résultat de la transaction. Les 2 points d'intégration CITELIS standard suffisent.

1. Sur le site marchand (site e-commerce), l'acheteur clique sur le bouton « payer » pour procéder au paiement de sa commande.
2. Le site d'e-commerce contacte CITELIS (1er point d'intégration) pour effectuer une transaction. CITELIS renvoie un jeton de session et l'url à utiliser pour le transfert du client vers les écrans web CITELIS.
3. L'acheteur saisit ses données cartes sur CITELIS. Après validation, il est redirigé vers le site internet de sa banque.
4. Sur le site internet de la banque, l'acheteur s'authentifie en toute sécurité.
5. Le site internet de la banque redirige l'acheteur vers CITELIS pour consulter son justificatif de paiement.
6. CITELIS redirige votre client sur votre site d'e-commerce pour consultation de sa facture.
7. Le site marchand contacte CITELIS (2eme point d'intégration) pour obtenir le résultat du paiement. Optionnellement, CITELIS peut prendre en charge l'appel d'une URL sur le site web marchand pour l'inciter à récupérer le résultat de la transaction (notification instantanée de paiement).

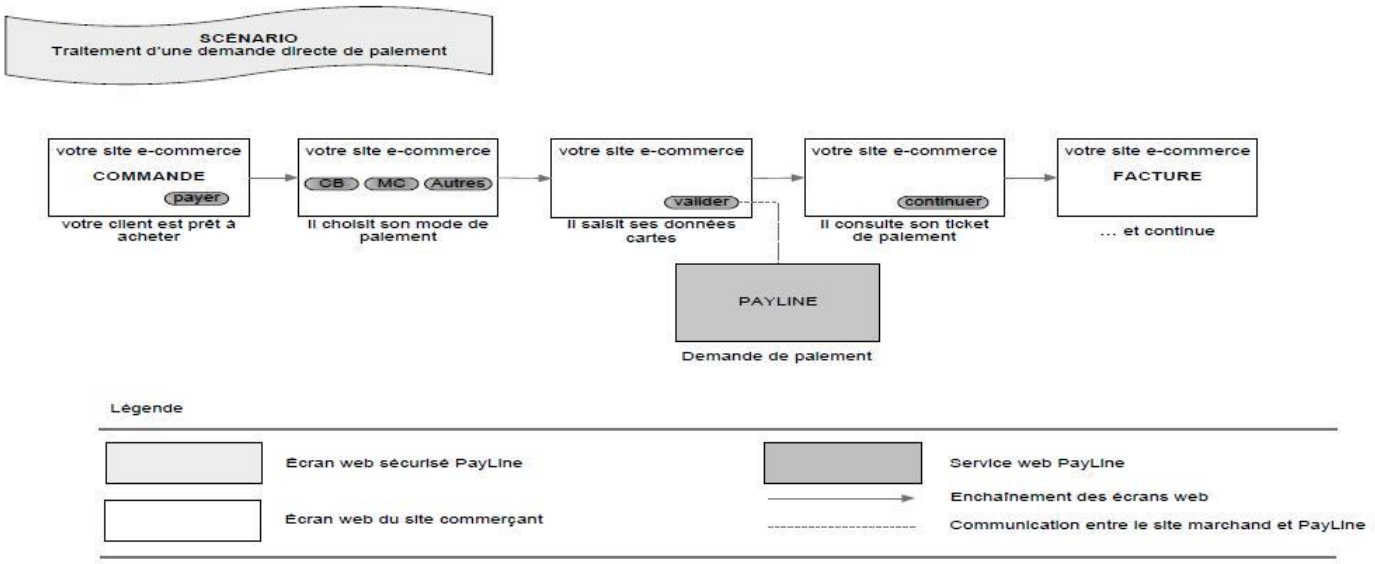
4. INTEGRATION INTERFACE DIRECT

L'interface Direct s'intègre au cœur de votre solution informatique.

La solution de paiement CITELIS agit en tant que passerelle entre votre point de vente et vos établissements financiers qui gèrent les transactions de paiement. Les données de paiement sont soumises à CITELIS pour une autorisation en temps réel via Internet ou sur un réseau privé.

4.1 Cinématique du processus de paiement standard

Votre application de vente soumet à CITELIS les informations de paiement de votre client. CITELIS assure le transfert sécurisé et le traitement monétique de ces données. Un seul point d'intégration suffit à réaliser une demande de paiement et à récupérer le résultat de la transaction.



Sur votre application de vente, votre client saisit ses données cartes pour procéder au paiement de sa commande.
Votre application contacte CITELIS (point d'intégration) pour effectuer une transaction de paiement.
CITELIS réalise la transaction de paiement et retourne le résultat (réponse synchrone). Les données carte sont enregistrées sur votre application. Votre client termine son paiement et consulte sa facture.

4.2 Cinématique du processus de paiement 3DSecure en mode Direct

La solution 3D Secure CITELIS Direct assure le transfert sécurisé des données sensibles et traite les demandes d'authentification, d'autorisation. Deux points d'intégration supplémentaires (***verifyEnrollment*** et ***doAuthorization)*** sont nécessaires pour assurer l'authentification, en plus du point d'intégration réalisant l'autorisation et récupérant le résultat de la transaction.
Veuillez contacter l'équipe support CITELIS citelis@arkea.com , afin qu'il vous délivre la documentation associée à la mise en place de 3DSecure en mode interface direct.

5. API

L'API CITELIS fournit l'accès aux différentes fonctionnalités de la solution de paiement CITELIS. Elle est basée sur des composants « Web Service » standards, qui incluent le protocole SOAP et les langages de définition WSDL et XSD. Ces standards sont supportés par une large gamme d'outils de développement sur des plateformes multiples.
L'utilisation du client Java Axis2 avec XMLBeans est très fortement préconisé car il permet de garantir une continuité de service en cas d'évolution des Web Services. L'utilisation d'un client Java Axis2 est déconseillée avec ADB.

Le détail des « webservice » est fournit dans la documentation qui vous sera fourni par notre équipe support citelis@arkea.com , manuel utilisateur des « webservice »

L'API CITELIS recouvre les fonctions suivantes :

5.1Interface web de CITELIS

Méthode	Description
doWebPayment	Initialisation d'une transaction de paiement web
getWebPaymentDetails	Récupère le résultat d'une transaction de paiement web
createWebWallet	Création d'un portefeuille client au travers de pages web
updateWebWallet	Modification d'un portefeuille client au travers de pages web
getWebWallet	Récupère les informations d'un portefeuille virtuel crée via l'interface web.

Préconisation : à chaque appel webservice, il est impératif de réaliser un getWebPaymentDetails ou getWebWallet

5.2 Interface direct de CITELIS

Méthode	Description
doAuthorization	Réalise une demande d'autorisation de paiement
doCapture	Valide une demande d'autorisation acceptée
doRefund	Rembourse un paiement à partir d'un n° d'autorisation acceptée
doCredit	Recrédite une carte de paiement à partir du compte commerçant
doDebit	Réalise une transaction de paiement
doReset	Annule une transaction à partir d'une transaction autorisée et validée mais non remise en banque.
createWallet	Création d'un portefeuille client.
updateWallet	Mise à jour d'un portefeuille client
getWallet	Récupère les informations qui constituent un portefeuille client
disableWallet	Désactive un portefeuille client
enableWallet	Réactive un portefeuille client
doImmediateWalletPayment	Réalise une demande de paiement à partir d'un portefeuille client
doScheduledWalletPayment	Planifie une demande de paiement à un jour fixé
doRecurrentWalletPayment	Programme une demande de paiement d'un montant fixe (abonnement)
getPaymentRecord	Récupère un dossier de paiement
disablePaymentRecord	Désactive un dossier de paiement
getTransactionDetails	Permet d'obtenir le détail d'une transaction de paiement quelque soit son état.
verifyEnrollment	Vérifie que la carte de l'acheteur est 3DSecure.

6. INTEGRATION PAS A PAS

Intégrez dans votre application

Vous pouvez maintenant choisir votre façon d'intégrer la solution de paiement CITELIS dans votre application.

Il existe trois solutions pour utiliser CITELIS :

Suite e-commerce : une utilisation immédiate

Utilisez *une suite e-commerce* certifiée CITELIS et n'ayez aucune intégration à effectuer. La liste des *suites d'e-commerce* qui propose la solution de paiement CITELIS est disponible sur demande auprès de notre assistance technique CITELIS.

Kit d'intégration : une installation facilitée

Intégrez CITELIS à l'aide d'un kit. Vous devez avoir des connaissances du langage HTML et d'un langage de scripts tels que PHP, C# et Java pour l'utilisation du kit d'intégration sélectionné.

API SOAP : une intégration complète

Intégrez CITELIS à l'aide de l'API SOAP. Vous devez maitriser le développement d'interface client avec des services standards web sécurisés.

Validez votre intégration

Cette étape vous permet de contrôler que votre intégration est correcte.

- Lors de votre inscription, vous avez du recevoir de notre équipe support, un PV de Recette qui vous décrit les tests à réaliser.
- Consultez le centre d'administration commerçant et validez le bon enregistrement de vos transactions de paiement.

Demandez l'activation de votre compte en production

Lorsque vous avez validé l'intégration de CITELIS dans votre application, activez votre compte en production en suivant les indications suivantes :

- Transmettez le PV de recette signé au service support CITELIS par email : citelis@arkea.com