ANNEXE 1 LISTE DES PRODUITS PAYFIP :

LISTE DES PRODUITS	
Code produit	**Libellé**
01	EAU/ASSAINISSEMENT
02	ORDURES MENAGERES
03	CULTURE / SPORTS / LOISIRS
04	SOCIAL
05	SCOLAIRE / PERISCOLAIRE / TRANSPORT
06	TRAVAUX
07	LOCATIONS IMMEUBLES
08	PRODUITS EXCEPTIONNELS
09	PRESTATIONS EPSMS
10	PRODUITS MARCHANDISES HORS EAU-ASS
11	AUTRES PRODUITS DE GESTION
12	RECETTES D'UTILISATION DU DOMAINE
13	AUTRES PRODUITS ACTIVITES ANNEXES
14	IMPOTS ET TAXES (73)
15	AUTRES SERVICES
16	RECOLTES PDTS FOREST ET INTERMEDIAIRES
17	ETUDES
18	DOTATION PARTICIPATIONS
19	PRETS
50	RÉGIE HÔPITAL
60	PRODUITS HOSPITALIERS

ANNEXE 2

Exemples d'adaptations de sites Internet au paiement en ligne

La collectivité a le choix entre deux modalités pour récupérer les éléments nécessaires à l'identification de la dette et de l'usager :

FORMULAIRE DE SAISIE :

Exemple non contractuel, dépendant de la structure des factures émises par le régisseur, présentant au-dessus du formulaire, une facture standard et les champs où sont communiquées les références à saisir.

Sur le portail présenté en exemple, nous suggérons l'affichage simultané du formulaire de saisie et d'une facture vierge qui servira d'aide à l'usager pour la saisie des champs du formulaire.

Une autre solution consiste à faire apparaître explicitement sur les factures, les références exactes qui devront être saisis par les usagers.

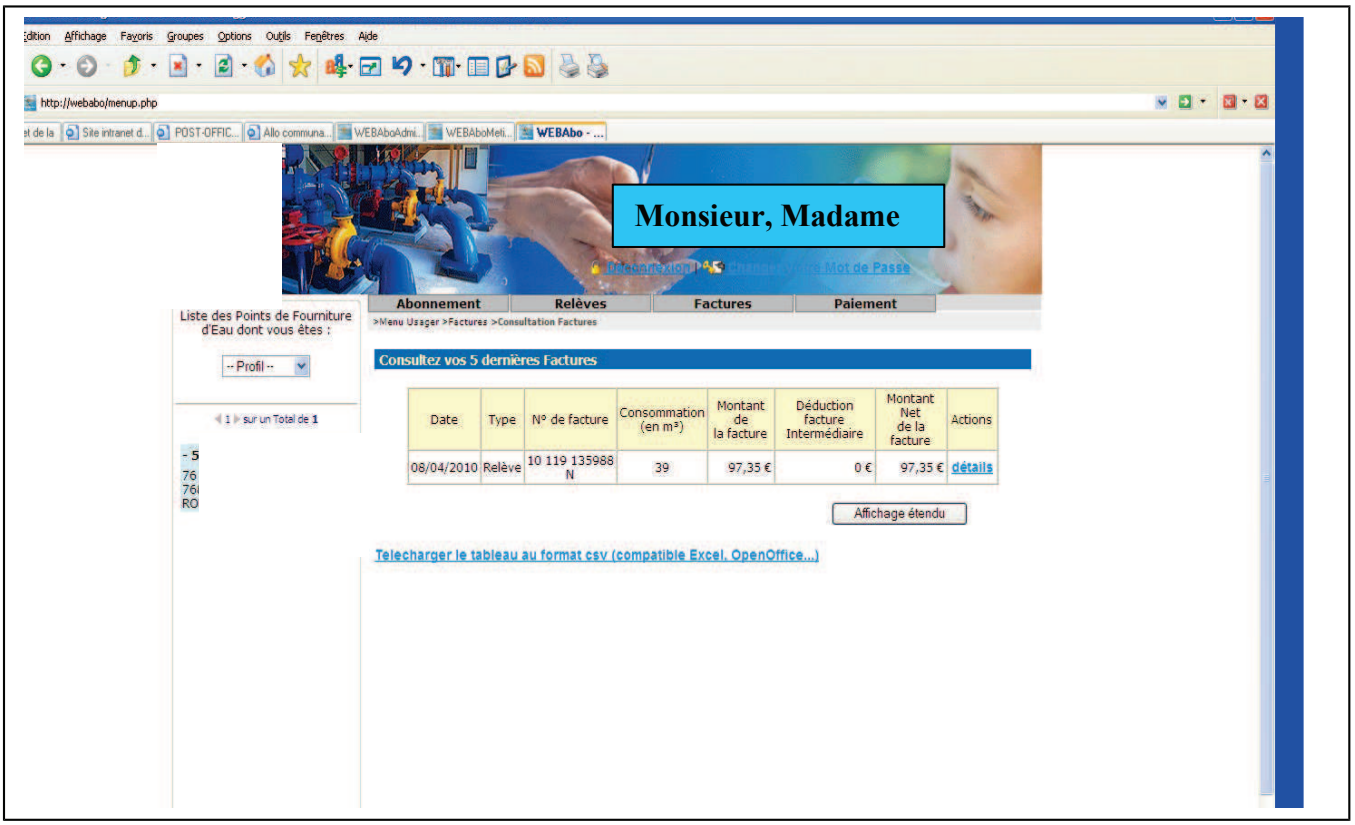
Après saisie par l'usager, et après contrôle de présence et de cohérence, la collectivité enrichit l'URL aller des informations collectées dans le formulaire de saisie. La collectivité vérifie que toutes les valeurs sont enrichies avant transmission à PayFiP. A réception, PayFiP effectue ses contrôles pour permettre à l'usager de payer sa dette par Internet.

ANNEXE 2

Compte usager :

Sur le principe des sites marchands**, l'usager après s'être identifié sur le site Web de la collectivité**, accède à son compte et visualise ses dettes restant dues et sélectionne celle qu'il souhaite payer.

Exemple non contractuel :



Après sélection d'une dette à payer et confirmation par l'usager de son choix de payer celle-ci, la collectivité enrichit des informations nécessaires l'URL aller et la transmet à. A réception, PayFiP effectue ses contrôles pour permettre à l'usager de payer sa dette par Internet.

La collectivité doit interfacer son portail avec son Système d'Information (SI) comptable afin de présenter à l'usager les dettes émises à son encontre. **Cela sous-entend l'obligation** :

- de sécuriser les accès des usagers par Identifiant et mot de passe pour accéder aux dettes restant dues,
- de traiter l'URL retour transmise par PayFiP en temps réel, en indiquant en correspondance de la dette payée via PayFiP « ***paiement CB par Internet en cours de validation*** » ou « ***paiement prélèvement par Internet en cours de validation*** » et la rendre non sélectionnable ou en la retirant, de la liste des dettes proposée à la sélection de l'usager,
- de gérer le délai de mise en ligne, qui correspond à la période pendant laquelle les factures sont payables en Régie. Dès lors que le titrage, émission des titres au comptable public, est effectué, ces factures ne doivent plus être sélectionnables par l'usager pour le paiement sur Internet.
En effet les factures ne doivent plus être payables à l'expiration de ce délai de mise en ligne. Ceci afin d'éviter le double paiement pour une même créance; d'une facture via PayFiP et d'un titre de recette pour cette même facture.

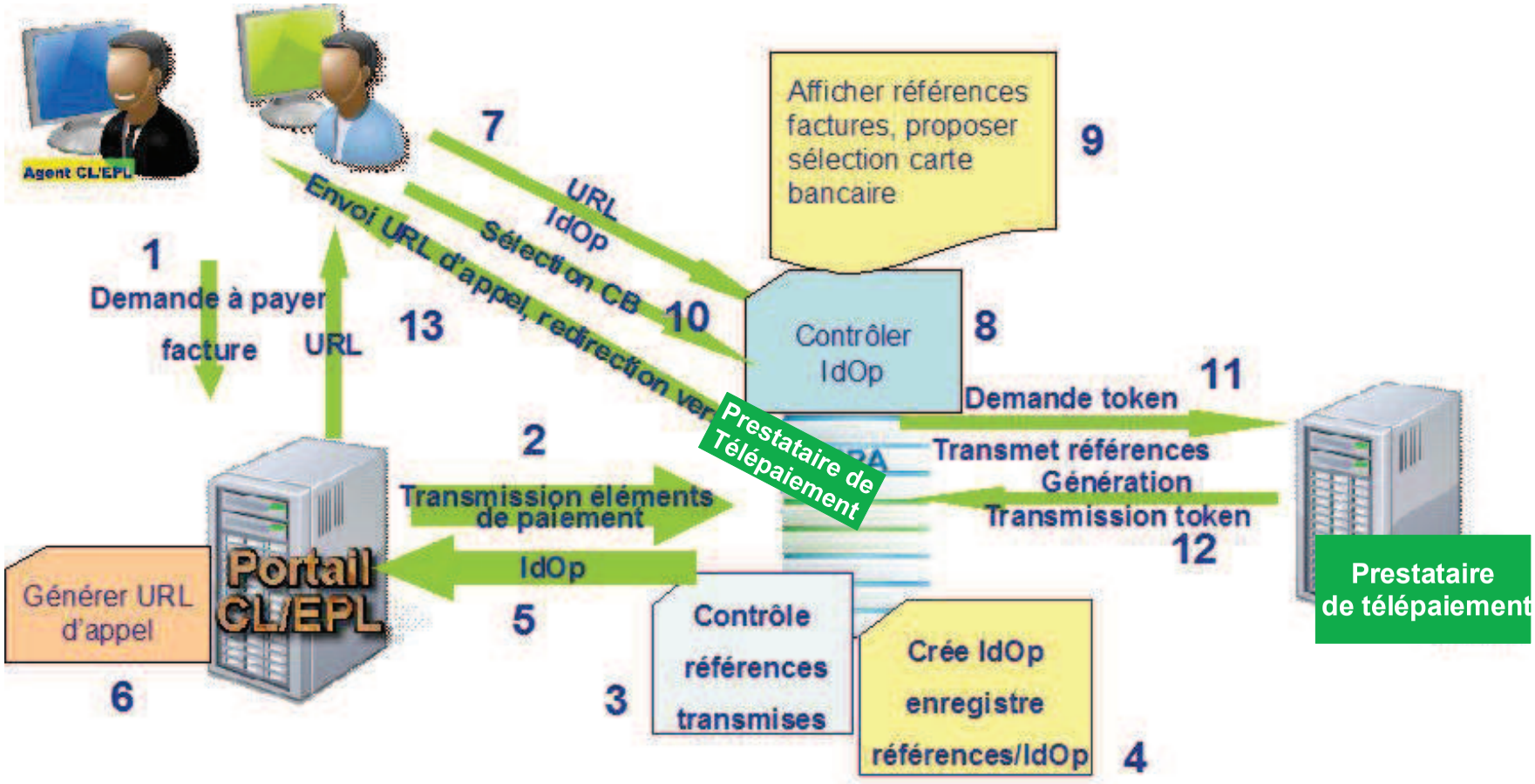
Annexe 3 : CinématiqueDetailléePaiementSécurisé

Cinématique paiement sécurisé

Comment appréhender ce document ?

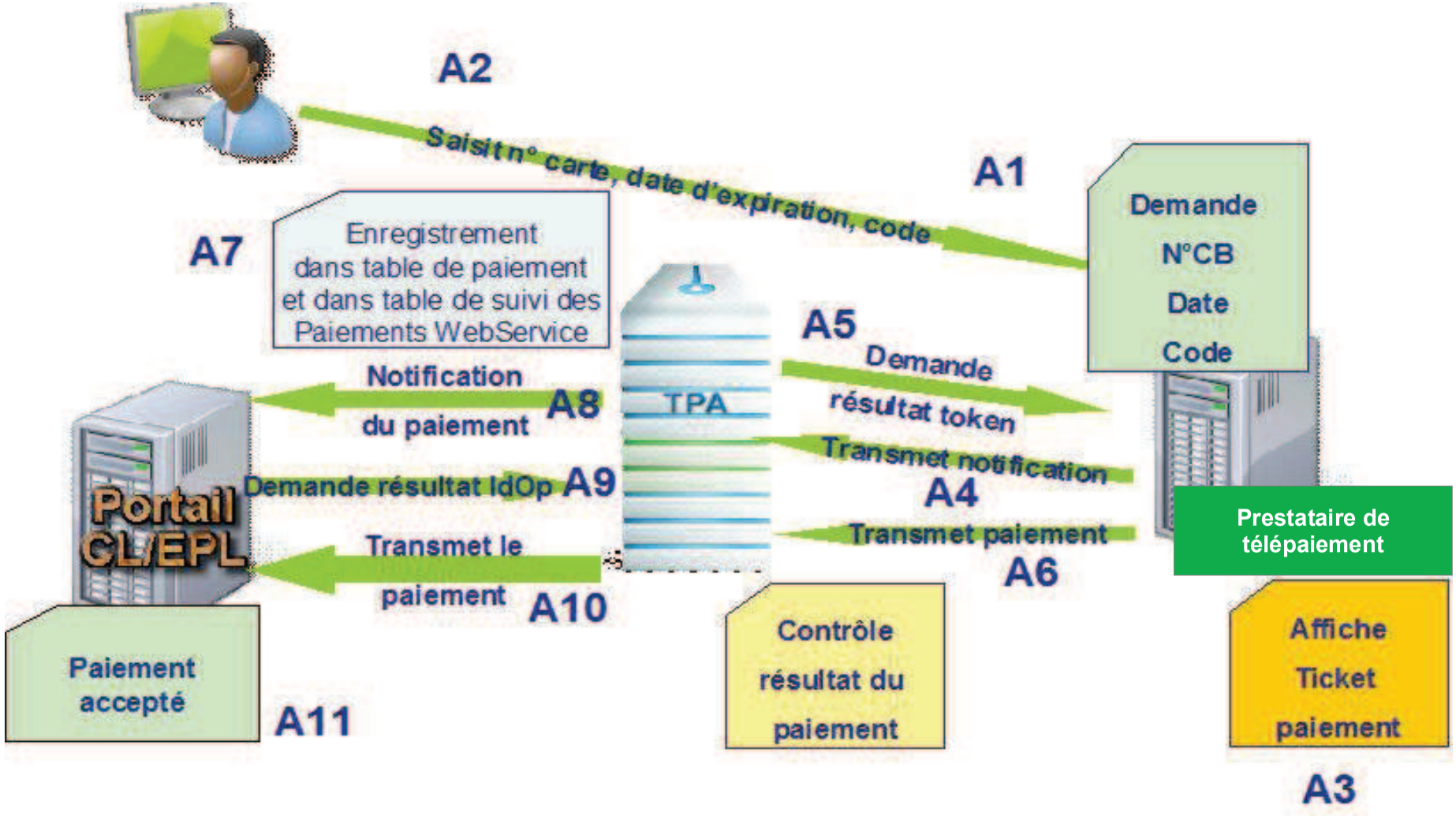
- *Il comporte un schéma des flux et systématiquement à la suite un tableau récapitulatif.*
- *Il permet de visualiser en fonctionnement nominal (sans erreur) l'enchaînement des opérations pour un paiement en prévoyant plusieurs déclinaisons :*
  - *le paiement dit «réel» qui correspond au cas standard d'un usager qui se connecte à PayFiP avec deux cas présentés (celui où l'usager achève la transaction après l'affichage du ticket commerçant – A, celui où il poursuit l'opération en cliquant sur le bouton « retour site » après cet affichage – B),*
  - *le paiement de test et le paiement d'activation qui correspondent à des procédures offertes par PayFiP pour la mise au point du dispositif avant le démarrage en production(test puis activation) ou à tout moment ensuite pour valider une évolution (test). Deux cas sont également proposés (celui où il est mis fin à la transaction après l'affichage du ticket commerçant – celui où l'opération est poursuivie en cliquant sur le bouton «retour site» après cet affichage – D),*
  - *le cas particulier d'une sollicitation de PayFiP avant qu'une opération de paiement quelle qu'elle soit (et quelle que soit sa modalité avec ou sans retour site) ne soit complètement achevée (E).*
  - *le cas particulier d'un paiement (quelque soit son type – réel, activation ou tes) refusé par le prestataire de télépaiement PayFiP (problème sur la carte utilisée, la déclaration du contrat commerçant) ou d'un abandon explicite de l'usager en cours de paiement. Deux scénarios sont également proposés (celui où l'opération est poursuivie en cliquant sur le bouton «retour site» (F), celui où il est mis directement fin à la transaction (G).*
- *Le premier schéma regroupe l'ensemble des opérations communes (tronc commun), les sept autres schémas sont des déclinaisons des possibilités de transactions évoquées ci-dessus.*

Tronc commun



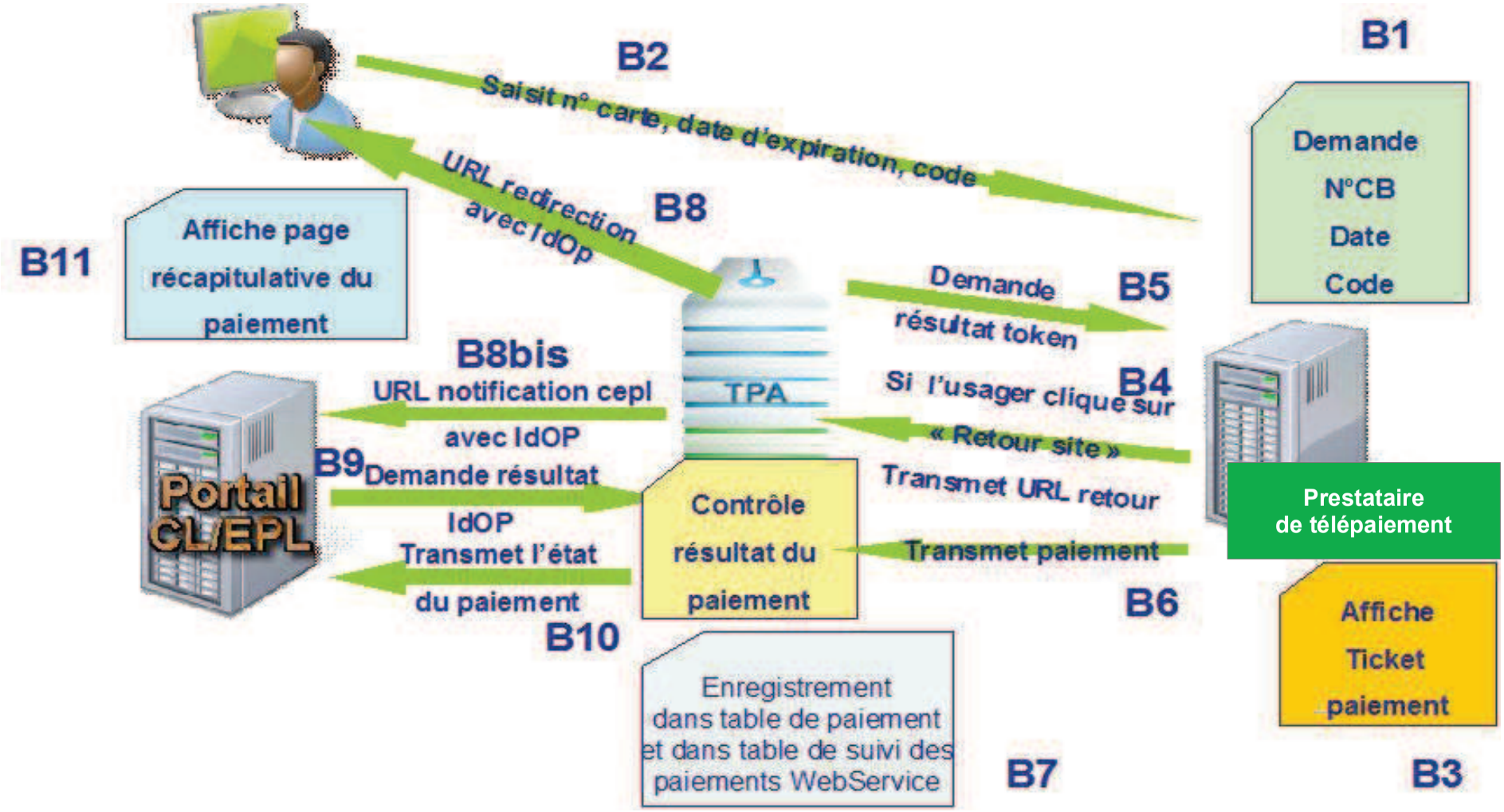
Tronc commun			
USAGER	**PORTAIL CL/EPL**	**TPA**	**Prestataire de télépaiement**
1- Demande à payer facture.			
	2- Transmission des éléments de paiement (cf. documentation technique pour les paramètres d'appel).		
		3- Contrôle les références transmises.	
		4- Crée IdOP, enregistre références/IdOp.	
		5- Envoie l'IdOp.	
	6- Génère URL d'appel.		
7- Appel de PayFiP à partir de l'URL tipi.budget.gour.fr avec en paramètre l'IdOp			
		8- Contrôle IdOp.	
		9- Affiche références factures, propose de sélectionner un type de carte bancaire.	
10- Sélectionne un type de carte bancaire.			
		11- Une fois la carte sélectionnée, demande du token au prestataire de télépaiement avec transmission de toutes les références nécessaires au paiement.	
			12- Génération transmission token.
		13- Envoie l'URL d'appel, redirection vers le prestataire de télépaiement.	

A- Paiement réel, l'usager abandonne la transaction après l'affichage du ticket.



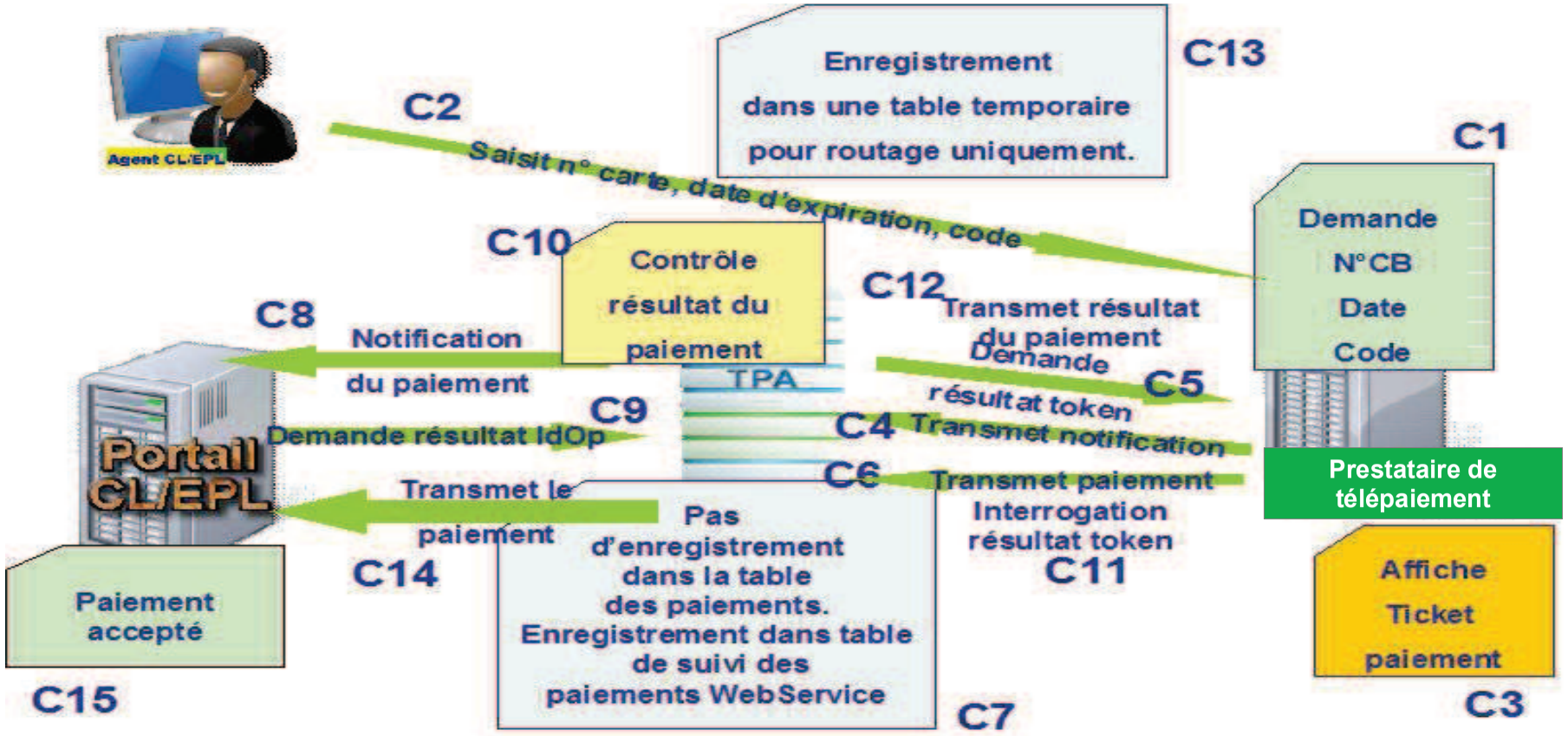
A- Paiement réel, l'usager abandonne la transaction après l'affichage du ticket.			
USAGER	**PORTAIL CL/EPL**	**TPA**	**Prestataire de télépaiement**
			A1- Demande n° de carte, date d'expiration, code.
A2- Entre n° de carte, date d'expiration, code.			
			A3- Gère la transaction de paiement et si tout est conforme, affiche ticket de paiement.
			A4- Transmet une notification dans un délai inférieur à 2 heures maximun (en général dans les 10 min)
		A5- Demande résultat token.	
			A6- Transmet les caractéristiques du paiement.
		A7- Enregistrement dans table de paiement et dans table de suivi des paiements WebService.	
		A8- Notification du paiement.	
	A9- Demande résultat avec l'IdOp.		
		A10- Contrôle le résultat du paiement et transmet le résultat.	
	A11- Paiement accepté.		

B- Paiement réel, l'usager clique sur « Retour site ».



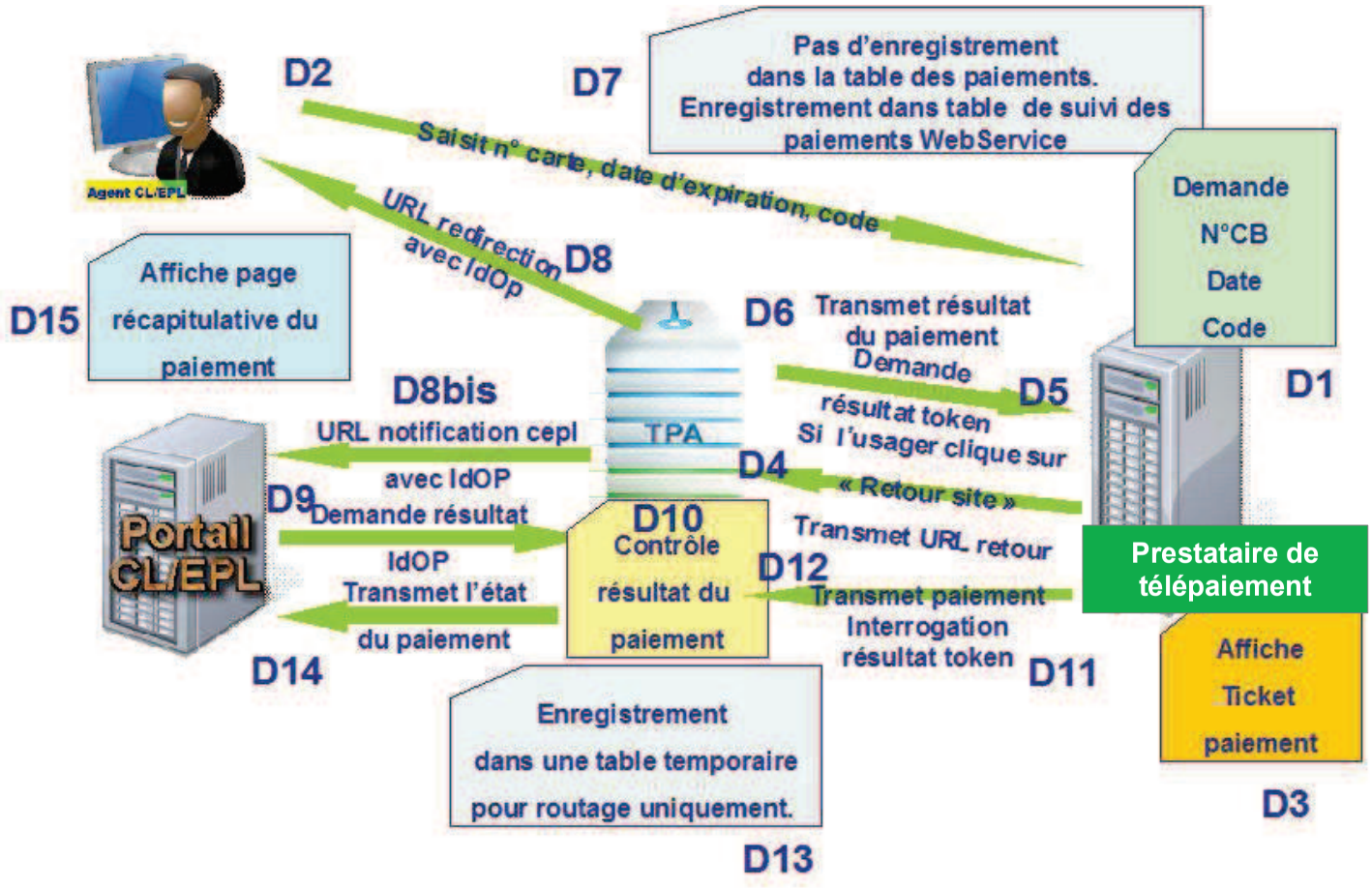
B- Paiement réel, l'usager clique sur « Retour site ».			
USAGER	**PORTAIL CL/EPL**	**TPA**	**Prestataire de télépaiement**
			B1- Demande n° de carte, date d'expiration, code.
B2- Entre n° de carte, date d'expiration, code.			
			B3- Gère la transaction de paiement et si tout est conforme, affiche ticket de paiement.
			B4- Si l'usager clique sur « Retour site » transmet URL retour.
		B5- Demande résultat token.	
			B6- Transmet les caractéristiques du paiement.
		B7- Enregistrement dans table de paiement et dans table de suivi des paiements WebService.	
		B8- Envoie à l'usager URL redirection avec IdOp.	
		B8bis- Envoie au portail CL/EPL URL notification avec IdOp.	
	B9- Demande résultat avec l'IdOp.		
		B10- Contrôle le résultat du paiement et transmet le résultat.	
	B11- Affiche page récapitulative du paiement.		

C- Paiement de test et activation puis abandon après l'affichage du ticket



C- Paiement de test et activation puis abandon après l'affichage du ticket			
USAGER	**PORTAIL CL/EPL**	**TPA**	**Prestataire de télépaiement**
			C1- Demande n° de carte, date d'expiration, code.
C2- Entre n° de carte, date d'expiration, code.			
			C3- Gère la transaction de paiement et si tout est conforme, affiche ticket de paiement.
			C4- Transmet une notification dans un délai inférieur à 2 heures maximum (en général dans les 10 min)
		C5- Demande résultat token.	
			C6- Transmet les caractéristiques du paiement.
		C7- Pas d'enregistrement dans la table des paiements. Enregistrement dans table de suivi des paiements WebService	
		C8- Notification du paiement.	
	C9- Demande résultat avec l'IdOp.		
		C10- Contrôle résultat du paiement.	
		C11- Interrogation résultat token.	
			C12- Transmet les caractéristiques du paiement.
		C13- Enregistrement dans une table temporaire pour routage uniquement.	
		C14- Transmet le résultat du paiement.	
	C15- Paiement accepté.		

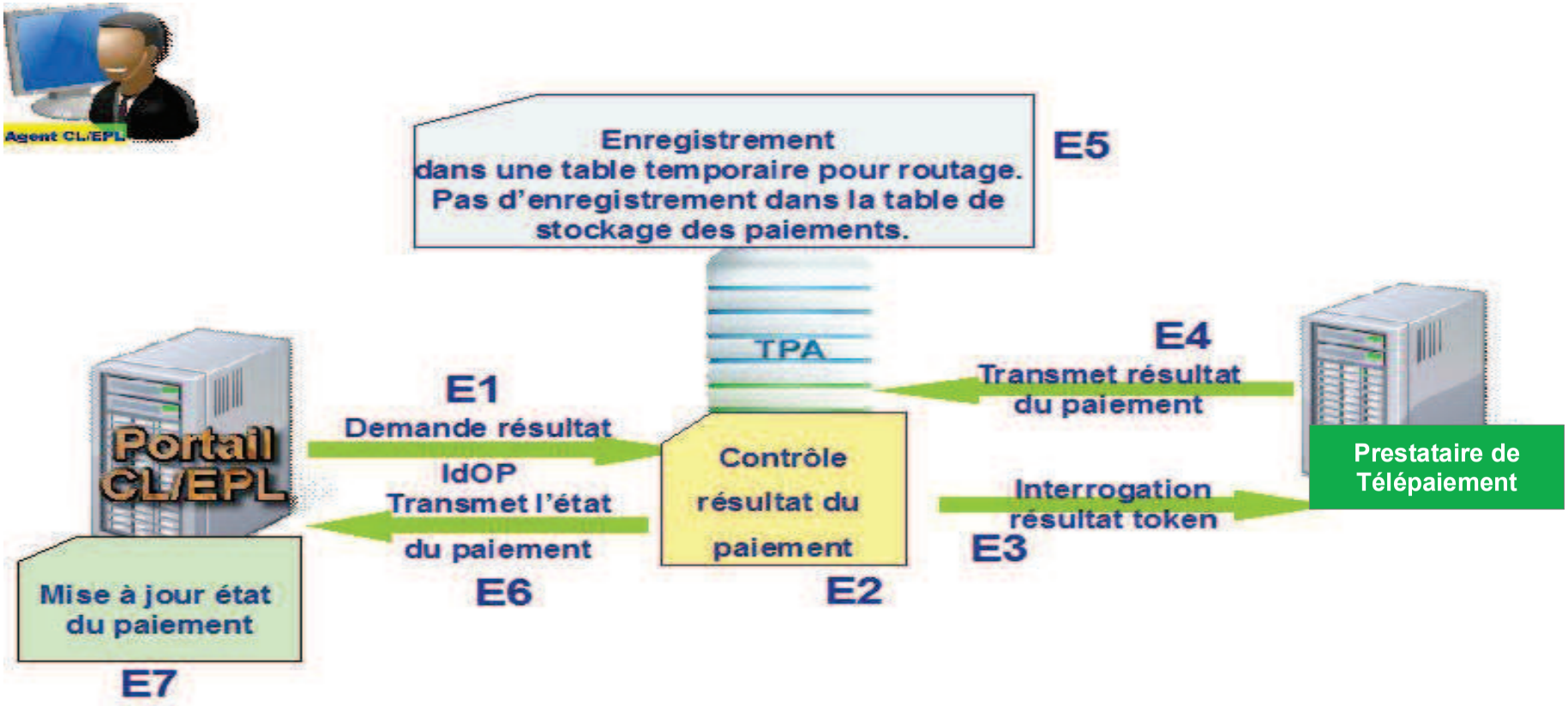
D- Paiement d'activation et de test avec «Retour site».



D- Paiement d'activation et de test avec « Retour site ».			
USAGER	**PORTAIL CL/EPL**	**TPA**	**Prestataire de télépaiement**
			D1- Demande n° de carte, date d'expiration, code.
D2- Entre n° de carte, date d'expiration, code.			
			D3- Gère la transaction de paiement et si tout est conforme, affiche ticket de paiement.
			D4- Si l'usager clique sur «Retour site» transmet URL retour.
		D5- Demande résultat token.	
			D6- Transmet les caractéristiques du paiement.
		D7- Pas d'enregistrement dans la table des paiements. Enregistrement dans table de suivi des paiements WebService.	
		D8- Envoie à l'usager URL redirection avec IdOp.	
		D8bis- Envoie au portail CL/EPL URL notification avec IdOp.	
	D9- Demande résultat avec l'IdOp.		
		D10- Contrôle le résultat du paiement.	
		D11- Interrogation résultat token.	
			D12- Transmet les caractéristiques du paiement.
		D13- Enregistrement dans une table temporaire pour routage uniquement.	
		D14- Transmet l'état du paiement.	

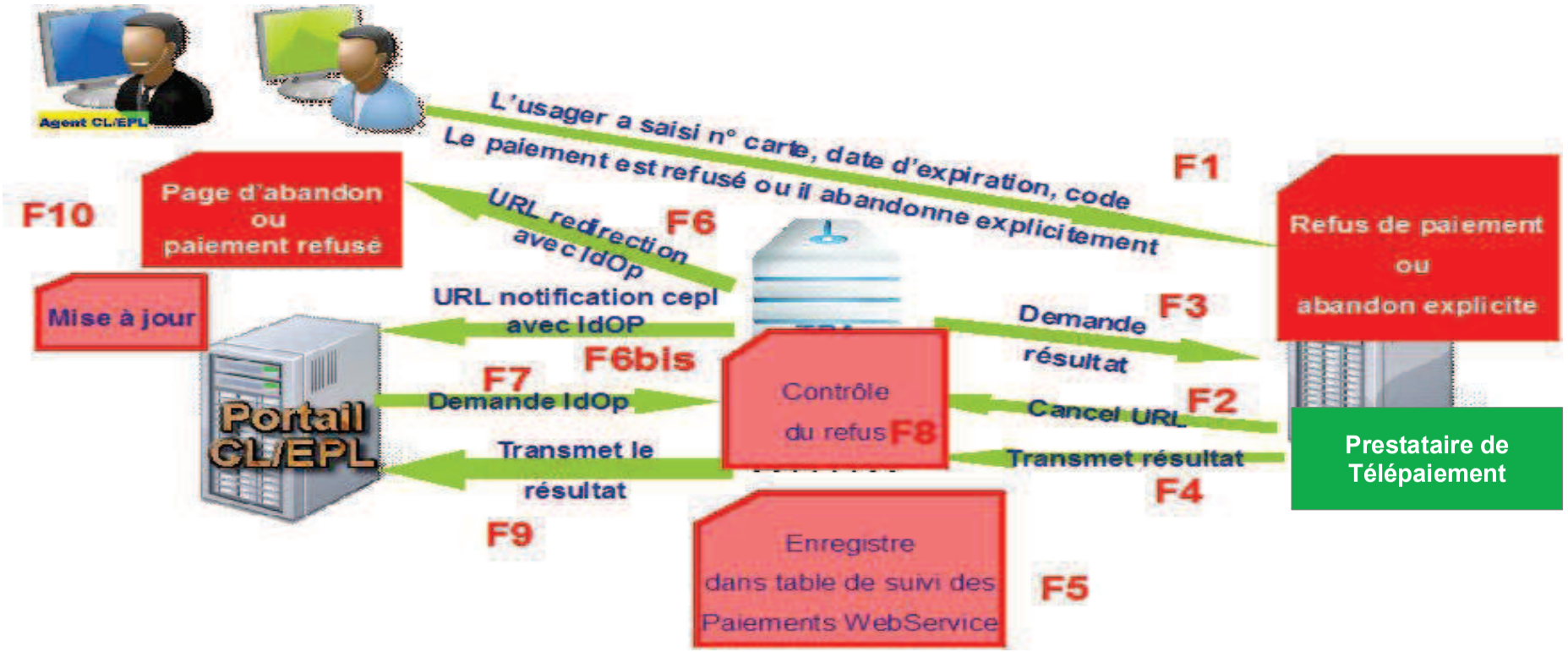
D- Paiement d’activation et de test avec « Retour site ».			
	D15- Affiche page récapitulative du paiement.		

E- Sollicitation de PayFiP par la collectivité avant notification ou redirection (activation – test – paiement réel)



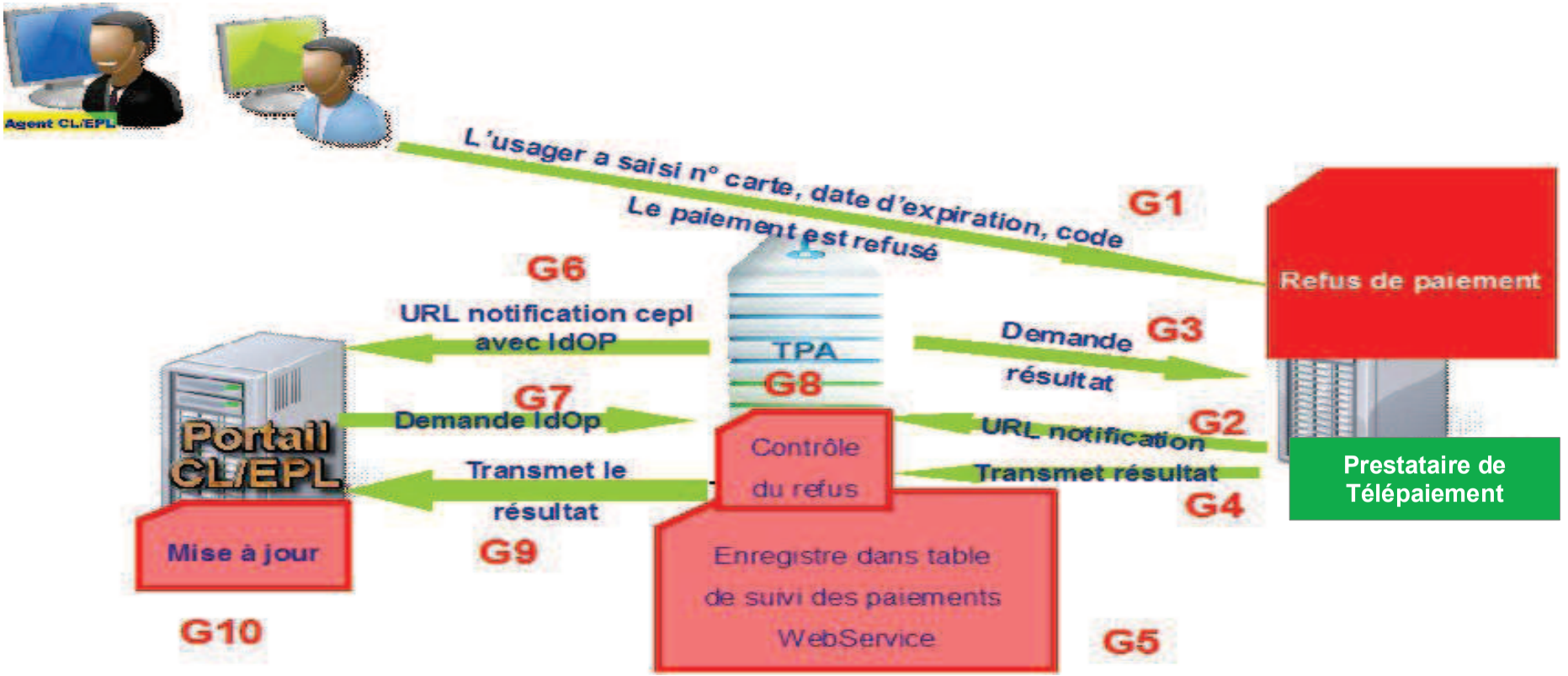
E- Sollicitation de PayFiP par la collectivité avant notification ou redirection (activation – test – paiement réel)			
USAGER	**PORTAIL CL/EPL**	**TPA**	**Prestataire de télépaiement**
	E1- Demande résultat avec l'IdOp		
		E2- Contrôle le résultat du paiement.	
		E3- Interrogation token.	
			E4- Transmet le résultat du paiement.
		E5- Enregistrement dans une table temporaire pour routage. Pas d'enregistrement dans la table de stockage des paiements.	
		E6- Transmet l'état du paiement.	
	E7- Mise à jour de l'état du paiement.		

F- Paiement réel, d'activation, de test : abandon explicite ou paiement refusé par le prestataire de télépaiement avec choix du retour site.



F- Paiement réel, d'activation, de test : abandon explicite ou paiement refusé par le prestataire de télépaiement avec choix du retour site.			
USAGER	**PORTAIL CL/EPL**	**TPA**	**Prestataire de télépaiement**
F1- L'usager a saisi n° carte, date d'expiration, code L'usager abandonne explicitement.			F1 - **Ou** le paiement est refusé suite aux contrôles effectués
			F2- Transmet l'URL d'annulation.
		F3- Demande de résultat.	
			F4- Transmet le résultat.
		F5- Enregistre dans table de suivi des paiements WebService.	
		F6- Envoie à l'usager URL redirection avec IdOp.	
		F6bis- Envoie au portail CL/EPL URL notification avec IdOp.	
	F7- Demande résultat avec l'IdOp.		
		F8- Contrôle du refus.	
		F9- Transmet le résultat	
	F10- Mise à jour, affiche page d'abandon ou de paiement refusé.		

G- Paiement réel, d'activation, de test : paiement refusé par le prestataire de télépaiement sans retour site.



G- Paiement réel, d'activation, de test : paiement refusé par le prestataire de télépaiement sans retour site.			
USAGER	**PORTAIL CL/EPL**	**TPA**	**Prestataire de télépaiement**
G1- L'usager a saisi n° carte, date d'expiration, code L'usager abandonne explicitement.			G1 - **Ou** le paiement est refusé suite aux contrôles effectués
			G2- Transmet une notification dans un délai inférieur à 2 heures maximun (en général dans les 10 min).
		G3- Demande de résultat.	
			G4- Transmet le résultat.
		G5- Enregistre dans table de suivi des paiements WebService.	
		G6- Envoi l'URL de notification CEPL avec IdOp.	
	G7- Demande résultat avec l'IdOp.		
		G8- Contrôle le refus.	
		G9- Transmet le résultat.	
	G10- Mise à jour.		

FIN DU DOCUMENT

DIRECTION GÉNÉRALE DES FINANCES PUBLIQUES	**DESCRITIF WS PayFiP**	SERVICE DES COLLECTIVITÉS LOCALES

DESCRIPTIF DES APPELS WEB SERVICE DANS LE CADRE DU DISPOSITIF PayFiP

HISTORIQUE DES VERSIONS DU DOCUMENT				
Version	**Date**	**Rédacteur**	**Commentaire**	**Statut**
1.0	17/09/2013-30/09/2013	MC. REY/ L. KORCHIA /L.OUVRAT	Version initiale constituée à partir du descriptif des traitements WS	Validé

Sommaire :

Le présent document est une annexe technique décrivant le contenu des appels web service et les résultats de ces appels.

Il vient en complément des fichiers techniques qui doivent être utilisés pour générer le client web service qui effectuera les appels vers PayFiP.

Ces fichiers techniques sont contenus dans l'archive constituant l'annexe 11.

1. Appel de PayFiP pour initier un paiement (CreerPaiementSecurise)

Une fois que l'usager a sélectionné sa facture ou saisit les informations de sa dette sur le formulaire proposé, le site partenaire doit appeler la méthode CreerPaiementSecurise exposée par l'offre web service PayFiP dénommée contrat_paiement_securise pour transférer les données utiles au paiement.

L'appel est réalisé à partir de l'url suivante :

https://tipi.budget.gouv.fr/tpa/services/mas_securite/contrat_paiement_securise/PaiementSecuriseService

1.1. *Paramètres en entrée : l'objet creerPaiementSecuriseRequest*

L'objet creerPaiementSecuriseRequest en paramètre de la méthode CreerPaiementSecurise contient l'ensemble des informations qui permettent d'initialiser un paiement.

creerPaiementSecuriseRequest	
exer	String
mel	String
montant	String
numcli	String
objet	String
refdet	String
saisie	String
urlnotif	String
urlredirect	String

Pour le détail de chaque attribut, il convient de se reporter au tableau descriptif contenu dans le cahier des charges.

1.2. Contrôles et Codes anomalie en cas d'erreur

Si les contrôles de cohérence prévus ne sont pas satisfaits, un code erreur est retourné.

La liste des contrôles et des codes erreur correspondants est à consulter dans l'annexe 8 : Anomalies ws-AppelCreerPaiementsecurisé.pdf

Principe : un seul code anomalie est retourné dans la réponse, les traitements de contrôle sont arrêtés à la première erreur détectée.

1.3. Attribution de l'idOp

L'idOp est déterminé de manière non prédictive à partir d'un service de générateur aléatoire sécurisé d'UUID.

UUID est l'abréviation du terme anglais Universally Unique IDentifier (identifiant universel unique, ou IDUU).
Cet identifiant unique est codé sur 128 bits et est produit en utilisant des composantes pseudo-aléatoires ainsi que les caractéristiques d'un ordinateur (numéro de disque dur, adresse MAC, etc.).
Un UUID se présente habituellement sous cette forme :
`xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx`

Exemples d'idOp fournis par PayFiP :
`4b0eb5b0-b335-11e2-9219-001fe256bdfe`
`d2fa2170-b336-11e2-9476-001fe256bdfe`
`6475fa10-b338-11e2-a082-001fe256bdfe`

1.4. Cycle de vie de l'idOp

L'IdOp transmis doit être utilisé pour rediriger l'usager vers PayFiP dans les 15 minutes qui suivent sa génération. Au-delà, il est périmé.

Il ne peut servir que pour un seul appel de redirection.

1.5. Communication de l'idOp dans l'objet réponse creerPaiementSecuriseResponse ou d'une erreur

L'objet retourné en réponse, lorsque les contrôles sont satisfaits et l'enregistrement par PayFiP des données effectué, est creerPaiementSecuriseResponse.

Il contient l'idOp attribué à la transaction.

creerPaiementSecuriseResponse	
idOp	String

En cas d'anomalie fonctionnelle détectée lors du contrôle des informations transmises dans l'objet creerPaiementSecuriseRequest, un objet FonctionnelleErreur est retourné (liste des codes et libellés au paragraphe 1.2).

Les attributs code et libellé sont servis en fonction de l'anomalie détectée. L'attribut sévérité est valorisé systématiquement à 2. Les autres attributs ne sont pas servis.

FonctionelleErreur	
code	String
descriptif	String
libelle	String
message	String
severite	int

En cas d'erreur autre que fonctionnelle, l'erreur TechDysfonctionnementErreur est retournée. Elle comporte le code 999 et le libellé et le message contiendront le détail de l'erreur générée. La sévérité est celle de l'exception levée.

TechDysfonctionnementErreur	
code	String
descriptif	String
libelle	String
message	String
severite	int

2. *Appel de PayFiP sur la base de l'IdOp pour récupérer le résultat du paiement (recupererDetailPaiementSecurise)*

Suite à la réception de l'url de notification ou de l'url de redirection ou à n'importe quel moment, le partenaire peut appeler la méthode recupererDetailPaiementSecurise exposée par l'offre web service PayFiP dénommée contrat_paiement_securise pour récupérer le résultat de la transaction de paiement correspondante à un IdOp.

L'appel du WS est réalisé à partir de l'url suivante :
https://tipi.budget.gouv.fr/tpa/services/mas_securite/contrat_paiement_securise/PaiementSecuriseService

2.1. Paramètres en entrée : l'objet RecupererDetailPaiementSecuriseRequest

L'objet recupererDetailPaiementSecuriseRequest en paramètre de la méthode recupererDetailPaiementSecurise contient l'idOp identifiant la transaction de paiement.

recupererDetailPaiementSecuriseRequest
idOp String

2.2. Code anomalie en cas d'erreur

Principe : Si les contrôles portant sur l'identifiant d'opération ne sont pas satisfaits, un code anomalie est retourné dans la réponse.

La liste des contrôles et des codes erreur correspondants est à consulter dans l'annexe 9 : Anomalies ws-AppelrecupererDetailPaiementSecurise.pdf

Compte tenu des cas particuliers pouvant être rencontrés, plusieurs situations sont détaillées ci-après :

2.2.1. Code erreur notifié dans le cas d'un paiement en cours.

Lorsque l'usager n'a pas encore validé la page de choix de la carte bancaire, si le site partenaire fait un appel à PayFiP de son initiative pour récupérer le résultat du paiement (aucune notification ou redirection ne sont intervenues), le jeton (token) du prestataire de télépaiement n'existe pas encore. PayFiP retournera alors une FonctionnelleErreur (Code P5).

Il en est de même lorsque l'usager est sur l'écran de saisie des références de la carte bancaire. En effet, si le site partenaire fait un appel à PayFiP de son initiative pour récupérer le résultat du paiement, PayFiP effectue un appel web service auprès du prestataire de télépaiement qui lui retourne un code de paiement en cours. PayFiP retournera alors une FonctionnelleErreur (Code P5).

2.2.2. Code erreur notifié dans le cas où l'usager ferme son navigateur sur le site PayFiP

Lorsque l'usager n'a pas encore validé la page de choix de la carte bancaire et qu'il ferme son navigateur, si le site partenaire fait un appel à PayFiP de son initiative pour récupérer le résultat du paiement (aucune notification ou redirection ne sont intervenues), comme précédemment le jeton du prestataire de télépaiement n'existe pas encore. PayFiP retournera alors une FonctionnelleErreur (Code P5).

Ce code sera retourné jusqu'au passage dans la nuit du batch de purge PayFiP qui supprimera l'enregistrement correspondant aux IdOp n'ayant pas de jeton associé.
Un nouvel appel web service se traduira par une réponse contenant une FonctionelleErreur (Code P1).

2.2.3. Code erreur notifié dans le cas où l'usager ferme son navigateur sur le site du prestataire

Lorsque l'usager est sur l'écran de saisie des références de la carte bancaire et qu'il ferme le navigateur, le prestataire de télépaiement ne transmet pas de retour.

En l'absence d'appel du site partenaire, les jetons du prestataire ne font l'objet d'aucun traitement jusqu'à ce qu'ils soient supprimés par le batch de rattrapage exécutés par PayFiP dans la nuit (traitement des jetons en instance ayant été attribués depuis plus de 2 heures).

Le traitement de ces jetons, qui correspondent à des idOp, donnera lieu à des notifications.
Lors des appels du site partenaire sur la base de ces idOp, des résultats de paiement « abandonné » seront retournés.

En revanche, si le site partenaire fait un appel de son initiative :

- dans les 10 premières minutes, le code paiement en cours sera retourné par le prestataire suite à l'interrogation de PayFiP. PayFiP retournera alors une FonctionnelleErreur (code anomalie P5).
- après 10 minutes, un autre code indiquant qu'il n'y a pas de transaction pour le jeton sera retourné lors de l'appel qu'effectuera PayFiP auprès du prestataire de télépaiement. PayFiP retournera alors un résultat de paiement « abandonné ».

2.3. Communication du paiement dans l'objet recupererDetailPaiementSecuriseResponse

L'objet retourné en réponse, lorsque le résultat de la transaction identifiée par l'idOp passé en paramètre a été trouvé, est recupererDetailPaiementSecuriseResponse.

Pour le détail de chaque attribut, il convient de se reporter au tableau descriptif contenu dans le cahier des charges.

L'attribut « resultrans » sera à analyser pour déterminer le résultat du paiement. Pour rappel, il est valorisé à :

- « P » si le paiement est effectif.
- « A » en cas d'abandon du paiement
- « R » dans tous les autres cas (i.e. pour les paiements refusés).

recupererDetailPaiementSecuriseResponse	
numcli	String
exer	String
refdet	String
objet	String
montant	String
mel	String
saisie	String
resultrans	String
numauto	String
dattrans	String
heurtrans	String
idOp	String

En cas d'anomalie fonctionnelle détectée (absence des données paiement pour cet idOp, absence de jeton transmis par le prestataire de télépaiement), un objet FonctionnelleErreur est retourné (Liste des codes et libellés au paragraphe 2.2).

Les attributs code et libellé sont servis en fonction de l'anomalie détectée. L'attribut sévérité est valorisé systématiquement à 2. Les autres attributs ne sont pas servis.

FonctionelleErreur	
code	String
descriptif	String
libelle	String
message	String
severite	int

En cas d'erreur autre que fonctionnelle, l'erreur TechDysfonctionnementErreur est retournée. Elle comporte le code 999 et le libellé et le message contiendront le détail de l'erreur générée. La sévérité est celle de l'exception levée.

TechDysfonctionnementErreur	
code	String
descriptif	String
libelle	String
message	String
severite	int

Annexe 5

EXEMPLES FICHIERS DE REMISE

Fichier de remise CB :

	A	B	C	D	E
1					
2					
3	PAIEMENTS TRANSMIS A LA BDF LE XX/XX/XXXX (1) POUR LE CONTRAT nnnnn(2) (LIBELLE RÉGIE(3))				
4					
5		Code collectivité : XXX(4)			
6		Code budget : XX(5)			
7					
8	**Date de transaction**	**Référence dette**	**Montant brut**	**Montant des commissions**	**Montant net**
9	jj/mm/aaaa hh:mm:ss				
10					
11					
12		**TOTAUX**	SOMME(C9:C11)	SOMME(D9:D11)	SOMME(E9:E11)
13					
14		**Nombre total de paiements**	X		
15					
16	(1) correspond à la CAPTURE DATE présente sur le fichier PayZen				
17	(2) correspond au numéro de contrat commerçant				
18	(3) correspond au libellé de la régie (LIBELLEREGIE de TPI_CLIENT)				
19	(4) correspond au code collectivité (CODECOLLECTIVITE de TPI_CLIENT)				
20	(5) correspond au code budget (CODEBUDGET de TPI_CLIENT)				

Fichier de remise Prélèvement :

	A	B	C	D	E	F	G
1							
2							
3		PAIEMENTS TRANSMIS A LA BDF LE XX/XX/XXXX (1) POUR LE CLIENT cccccc(2) (LIBELLE RÉGIE(3))					
4							
5				Code collectivité : XXX(4)			
6				Code budget : XX(5)			
7							
8	**Date de transaction**	**Date de prélèvement**	**RUM**	**Référence dette**	**Montant**		
9	jj/mm/aaaa hh:mm:ss	jj/mm/aaaa					
10							
11							
12				**TOTAUX**	SOMME(E9:E11)		
13							
14				**Nombre total de paiements**	X		
15							
16	(1) correspond à a date de remise issue du titre du fichier global de remise PayFiP –1 jour						
17	(2) correspond au numéro de client TIPI						
18	(3) correspond au libellé de la régie (LIBELLEREGIE de TPI_CLIENT)						
19	(4) correspond au code collectivité (CODECOLLECTIVITE de TPI_CLIENT)						
20	(5) correspond au code budget (CODEBUDGET de TPI_CLIENT)						

Si le client est actif CB sans paiement et qu'il y a au moins un paiement par prélèvement, le fichier CB est envoyé vide.
S'il n'y aucun paiement CB et Prélèvement le fichier n'est pas produit.

Annexe 6 : Exemples de notifications de résultat d'un paiement

---

lors d'un paiement, plusieurs cas peuvent se présenter :

- tant que PayFiP n'a pas reçu de notification de résultat de PayZen, si le partenaire interroge PayFiP le code suivant lui est retourné :

```
<ns2:FonctionnelleErreur
xmlns:ns2="http://securite.service.tpa.cp.finances.gouv.fr/services/mas_securite/contrat_paiement_securise/PaiementSecuriseService">
    <code>P5</code>
    <descriptif/>
    <libelle>Résultat de la transaction non connu.</libelle>
    <severite>2</severite>
</ns2:FonctionnelleErreur>
```

Ce code P5 ne doit pas être systématiquement considéré comme une réelle erreur mais comme l'indique le libelle, comme un "Résultat de la transaction non connu" par PayFiP (problème réseau, paiement en cours, paiement arrêté brutalement...)

- Si le paiement est annulé chez PayZen, quand le partenaire interroge le WS PayFiP le code suivant lui est retourné :

```
<ns2:recupererDetailPaiementSecuriseResponse
xmlns:ns2="http://securite.service.tpa.cp.finances.gouv.fr/services/mas_securite/contrat_paiement_securise/PaiementSecuriseService">
    <return>
      <dattrans/>
      <exer>2015</exer>
      <heurtrans/>
      <idOp>c7ba2cb0-8eda-11e5-99d5-00000a634c44</idOp>
      <mel>gerard.riviere@dgfip.finances.gouv.fr</mel>
      <montant>1500</montant>
      <numcli>006270</numcli>
      <objet>test</objet>
      <refdet>123456789</refdet>
      <resultrans>A</resultrans>
      <saisie>W</saisie>
    </return>
</ns2:recupererDetailPaiementSecuriseResponse>
```

Avec un "<resultrans>A</resultrans>" comme Annulé.

- Quand le paiement est refusé par PayZen(solde insufisant, refus de l'établissement financier ...) on a une réponse du type :

```
<ns2:recupererDetailPaiementSecuriseResponse
xmlns:ns2="http://securite.service.tpa.cp.finances.gouv.fr/services/mas_securite/contrat_paiement_securise/PaiementSecuriseService">
  <return>
    <dattrans/>
    <exer>2015</exer>
    <heurtrans/>
    <idOp>85145640-8edc-11e5-99d5-00000a634c44</idOp>
    <mel>gerard.riviere@dgfip.finances.gouv.fr</mel>
    <montant>1502</montant>
    <numcli>006270</numcli>
    <objet>test</objet>
    <refdet>123456789</refdet>
    <resultrans>R</resultrans>
    <saisie>T</saisie>
  </return>
</ns2:recupererDetailPaiementSecuriseResponse>
```

Avec un "<resultrans>R</resultrans>" comme Refusé.

- Enfin quand le paiement est bien effectué et que PayZen a eu le temps de notifier PayFiP il doit recevoir ce type de réponse :

```
<ns2:recupererDetailPaiementSecuriseResponse
xmlns:ns2="http://securite.service.tpa.cp.finances.gouv.fr/services/mas_securite/contrat_paiement_securise/PaiementSecuriseService">
  <return>
    <dattrans>19112015</dattrans>
    <exer>2015</exer>
    <heurtrans>1735</heurtrans>
    <idOp>81bdf4c0-8edb-11e5-99d5-00000a634c44</idOp>
    <mel>gerard.riviere@dgfip.finances.gouv.fr</mel>
    <montant>1500</montant>
    <numauto>A55A</numauto>
    <numcli>006270</numcli>
    <objet>test</objet>
    <refdet>123456789</refdet>
```

```
            <resultrans>P</resultrans>
            <saisie>T</saisie>
        </return>
    </ns2:recupererDetailPaiementSecuriseResponse>
```

Avec un "<resultrans>P</resultrans>" comme Payé.
Toutes autres interprétations peuvent induire des erreurs.

Auteur :	MC REY
Projet :	PAYFIP

Document	
Nom	Anomalies ws-AppelCreerPaiementsecurise.xls
Type	Spécifications techniques
Statut	Validé
Date création	11/04/2014
Date dernière mise à jour	27/01/2017

Nom des champs concernés	Nature du contrôle	Longueur du champ	Règle de gestion	Code de la fonctionelle erreur	Libellé de la fonctionelleErreur pour paiement, activation et test SAISIE="W", "X" ou "T"
Saisie	Contrôle d'existence et de valeur	1	Le champ doit avoir pour valeur "W- X ou T". "W" correspond à un paiement réel effectué par le web service. si la valeur = "T", il s'agit d'un paiement de test, si valeur ="X", il s'agit d'un paiement d'activation	**S1**	"Mode de saisie incorrect." Un reporting informera l'administrateur PayFiP.
NUMCLI	Contrôle du nombre et du format des caractères	6	Le numéro de client PayFiP doit comporter 6 caractères numériques.	**T1**	"Numéro de client incorrect." Un reporting informera l'administrateur PayFiP.
	Contrôle d'existence du NUMCLI dans le référentiels des clients PayFiP		Le N° du client doit être pré-existant dans la base PayFiP.	**T2**	"Client non autorisé." Un reporting informera l'administrateur PayFiP.
	Contrôle du statut du client PayFiP		si le champ SAISIE = "X" : <u>Si Client uniquement CB</u> et le statut du Client CB est à "Inactif CB" Si <u>Client uniquement PREL</u> et le statut du Client PREL est à "Inactif PREL" <u>Si Client CB et PREL</u> : et les Statut CB ainsi que le statut PREL sont « inactif »	**T3**	"Le client ne peut pas être réactivé." Un reporting informera l'administrateur PayFiP.
			si le champ SAISIE = "X" : <u>Si Client uniquement CB</u> et le statut du Client CB est à Actif CB ou le statut est encore "E" (Enregistré) mais une activation vient d'être effectuée (présence des références du client dans la table TPA_ACTIVATIONCLIENT) - Rappel la mise à jour du statut au niveau du client est effectuée en différé mais il est prévu un contrôle pour empêcher la réalisation successive de l'opération d'activation <u>Si Client uniquement PREL</u> et le statut du Client PREL est à « Actif PREL » ou en cours d'activation <u>Si client CB et PREL</u> et que les deux statuts sont « Actif » ou encours d'activation	**T4**	"Le client PayFiP est déjà activé. " Un reporting informera l'administrateur PayFiP
			si le champ SAISIE = "A" ou "M" ou "P" <u>Si Client uniquement CB</u> et le statut du Client CB est différent de "Actif CB", le paiement par CB est impossible <u>Si Client uniquement PREL</u> et le statut du Client PREL est différent de "Actif PREL", le paiement par prélèvement est impossible <u>Si Client CB et PREL</u> et les deux statuts du Client sont différent de "Actif » le paiement est impossible	**T5**	"Le statut du client ne permet pas le paiement." Un reporting informera l'administrateur PayFiP.
			si le champ SAISIE = "X" et le statut du Client CB est à "Nouveau CB" ou « V » Et que le statut du client PREL n'est pas « Nouveau »	**T7**	"Le statut du client ne permet pas son activation." Un reporting informera l'administrateur PayFiP.
			<u>Client CB et PREL</u> Mode de saisie activation : les deux statuts ne sont pas « actif », ni « inactif », le statut CB est différent de « Enregistré » et le statut PREL différent de « Nouveau »	**T10**	"Le statut du client ne permet pas son activation." Un reporting informera l'administrateur PayFiP.
	Contrôle de l'accès sécurisé		Le client doit être un client Régie et comporter une autorisation de paiement par mode sécurisé ou être un client ClientGenerique	**T9**	"Ce client n'a pas d'accès sécurisé" Un reporting informera l'administrateur PayFiP.
EXER	Vérification du format d' EXER si le champ est servi (donnée facultative)	4	L'exercice comporte 4 caractères numériques, l'année doit être N ou N-1 par rapport date du jour	**E1**	Aucune erreur n'est retournée avec ce code. Seul un reporting informera l'administrateur PayFiP.
REFDET	Contrôle de forme	6 à 30	REFDET doit comporter entre 6 et 30 caractères au format a z A Z 0 9 sinon le paiement est impossible	**R3**	"Le format du paramètre REFDET n'est pas conforme." Un reporting informera l'administrateur PayFiP.
OBJET	Contrôle de forme	<100	La valeur du champ doit comporter des caractères alphanumériques + l'espace	**O1**	"La valeur de l' OBJET est incorrecte." Un reporting informera l'administrateur PayFiP.

MONTANT	Contrôle du nombre et du format des caractères	6	Si le nombre de chiffres du montant est supérieur à 7 caractères numériques ou s'il comporte une virgule, l'activation, le test et le paiement sont impossibles.	**M1**	"Le format du montant n'est pas correct (présence de caractères non autorisés ou seuil de paiement sur Internet dépassé)." Un reporting informera l'administrateur PayFiP.
	Contrôle de la valeur du champ MONTANT		Si la valeur est supérieure à 9 999,99 euros, le paiement est impossible	**M2**	Le contrôle est effectué mais ne donnera lieu à aucune anomalie car la vérification du nombre maximum de caratères (M1) est fait en premier. (10 000,00 fait plus de 7 caractères) "Le format du montant n'est pas correct (présence de caractères non autorisés ou seuil de paiement sur Internet dépassé)."
			Si la valeur est inférieure à 1 € le paiement est impossible	**M3**	" Montant inférieur au seuil minimum accepté." Un reporting informera l'administrateur PayFiP.
			Les montants sont libres en activation et en test mais il sera vérifié qu'ils ne correspondent pas à un montant interdit (Liste fourni par le prestataire de télépaiement - Cf. cahier des charges).	**M5**	"Montant non autorisé pour le paiement de test ou d'activation." Un reporting informera l'administrateur PayFiP.
MEL	Contrôle du nombre et du format des caractères	6 à 80	L'adresse MEL du débiteur doit être servie sinon le paiement est impossible	**A1**	"Adresse mèl non renseignée." Un reporting informera l'administrateur PayFiP.
			L'adresse MEL du débiteur doit comporter entre 6 et 80 caractères maximum ainsi que les caractères "@" et "." sinon le paiement est impossible	**A2**	"Adresse mél est incorrecte." Un reporting informera l'administrateur PayFiP.
URLNOTIF	Contrôle du nombre et du format des caractères	<250	Ce champ doit être servi obligatoirement et doit être au format http://..... ou https://.....; 250 caractères maximum sans indication de port sinon l'activation, le test et le paiement sont impossibles.	**N1**	"Url de notification non valide ou comportant des ports non autorisés." un reporting informera l'administrateur PayFiP
URLREDIRECT	Contrôle du nombre et du format des caractères	<250	Ce champ doit être servi obligatoirement et doit être au format http://..... ou https://.....; 250 caractères maximum sans indication de port sinon l'activation, le test et le paiement sont impossibles	**D1**	"Url de redirection non valide ou comportant des ports non autorisés." Un reporting informera l'administrateur PayFiP.

ANNEXE 8 – Anomalies ws-AppelCreerPaiementsecurisé

Acteur :	:
Projet :	PAYFIP

Document	
Nom	Anomalies ws-AppelCreerPaiementsecurisé.xls
Type	Spécifications techniques
Statut	Validé
Date création	10/04/2013
Date dernière mise à jour	18/03/2016

Nom des champs concernés	Nature du contrôle	Longueur du champ	Règle de gestion	Code de la fonctionelle erreur	Libellé de la fonctionelleErreur pour paiement, activation et test SAISIE="W", "X" ou "T"
Saisie	Contrôle d'existence et de valeur	1	Le champ doit avoir pour valeur "W- X ou T". "W" correspond à un paiement réel effectué par le web service. si la valeur = "T", il s'agit d'un paiement de test, si valeur ="X", il s'agit d'un paiement d'activation	**S1**	"Mode de saisie incorrect." Un reporting informera l'administrateur TIPI.
NUMCLI	Contrôle du nombre et du format des caractères	6	Le numéro de client TIPI doit comporter 6 caractères numériques.	**T1**	"Numéro de client incorrect." Un reporting informera l'administrateur TIPI.
	Contrôle d'existence du NUMCLI dans le référentiels des clients TIPI		Le N° du client doit être pré-existant dans la base TIPI.	**T2**	"Client non autorisé." Un reporting informera l'administrateur TIPI.
	Contrôle du statut du client TIPI		Si le champ SAISIE = "X" et le statut du Client est à "I" (inactif)	**T3**	"Le client ne peut pas être réactivé." Un reporting informera l'administrateur TIPI.
			Si le champ SAISIE = "X" et le statut du Client est à "A" (actif) ou le statut est encore "E" (Enregistré) mais une activation vient d'être effectuée (présence des références du client dans la table TPA_ACTIVATIONCLIENT) -	**T4**	"Le client TIPI est déjà activé. " Un reporting informera l'administrateur TIPI
			Si le champ SAISIE = "W" et le statut du Client est différent de "A" (actif) le paiement est impossible	**T5**	"Le statut du client ne permet pas le paiement." Un reporting informera l'administrateur TIPI.
			Si le champ SAISIE = "X" et le statut du Client est à "N" (Nouveau)	**T7**	"Le statut du client ne permet pas son activation." Un reporting informera l'administrateur TIPI.
	Contrôle de l'accès sécurisé		Le client doit être un client Régie et comporter une autorisation de paiement par mode sécurisé ou être un client ClientGenerique	**T9**	"Ce client n'a pas d'accès sécurisé" Un reporting informera l'administrateur TIPI.
EXER	Vérification du format d' EXER si le champ est servi (donnée facultative)	4	L'exercice comporte 4 caractères numériques, l'année doit être N ou N-1 par rapport date du jour	**E1**	Aucune erreur n'est retournée avec ce code. Seul un reporting informera l'administrateur TIPI.
REFDET	Contrôle de forme	6 à 30	REFDET doit comporter entre 6 et 30 caractères au format a z A Z 0 9 sinon le paiement est impossible	**R3**	"Le format du paramètre REFDET n'est pas conforme." Un reporting informera l'administrateur TIPI.
OBJET	Contrôle de forme	<100	La valeur du champ doit comporter des caractères alphanumériques + l'espace	**O1**	"La valeur de l' OBJET est incorrecte." Un reporting informera l'administrateur TIPI.
MONTANT	Contrôle du nombre et du format des caractères	6	Si le nombre de chiffres du montant est supérieur à 7 caractères numériques ou s'il comporte une virgule, l'activation, le test et le paiement sont impossibles.	**M1**	"Le format du montant n'est pas correct (présence de caractères non autorisés ou seuil de paiement sur Internet dépassé)." Un reporting informera l'administrateur TIPI.
	Contrôle de la valeur du champ MONTANT		Si la valeur est supérieure à 99 999,99 euros, le paiement est impossible	**M2**	Le contrôle est effectué mais ne donnera lieu à aucune anomalie car la vérification du nombre maximum de caratères (M1) est fait en premier. (100 000,00 fait plus de 7 caractères) "Le format du montant n'est pas correct (présence de caractères non autorisés ou seuil de paiement sur Internet dépassé)."
			Si la valeur est inférieure à 1 € le paiement est impossible	**M3**	" Montant inférieur au seuil minimum accepté." Un reporting informera l'administrateur TIPI.
			Les montants sont libres en activation et en test mais il sera vérifié qu'ils ne correspondent pas à un montant interdit (Liste fourni par le prestataire de télépaiement - Cf. cahier des charges).	**M5**	"Montant non autorisé pour le paiement de test ou d'activation." Un reporting informera l'administrateur TIPI.
MEL	Contrôle du nombre et du format des caractères	6 à 80	L'adresse MEL du débiteur doit être servie sinon le paiement est impossible	**A1**	"Adresse mèl non renseignée." Un reporting informera l'administrateur TIPI.
			L'adresse MEL du débiteur doit comporter entre 6 et 80 caractères maximum ainsi que les caractères "@" et "." sinon le paiement est impossible	**A2**	"Adresse mél est incorrecte." Un reporting informera l'administrateur TIPI.
URLNOTIF	Contrôle du nombre et du format des caractères	<250	Ce champ doit être servi obligatoirement et doit être au format http://..... ou https://.....; 250 caractères maximum sans indication de port sinon l'activation, le test et le paiement sont impossibles.	**N1**	"Url de notification non valide ou comportant des ports non autorisés." un reporting informera l'administrateur TIPI
URLREDIRECT	Contrôle du nombre et du format des caractères	<250	Ce champ doit être servi obligatoirement et doit être au format http://..... ou https://.....; 250 caractères maximum sans indication de port sinon l'activation, le test et le paiement sont impossibles	**D1**	"Url de redirection non valide ou comportant des ports non autorisés." Un reporting informera l'administrateur TIPI.

Auteur :	MC REY
Projet :	TIPI

Document	
Nom	Anomalies ws-AppelCreerPaiementsecurisé.xls
Type	Spécifications techniques
Statut	Validé
Date création	11/04/2014
Date dernière mise à jour	30/04/2014

Nom des champs concernés	Nature du contrôle	Longueur du champ	Règle de gestion	Code de la fonctionelle erreur	Libellé de la fonctionelleErreur pour paiement, activation et test SAISIE="W", "X" ou "T"
Saisie	Contrôle d'existence et de valeur	1	Le champ doit avoir pour valeur "W- X ou T". "W" correspond à un paiement réel effectué par le web service. si la valeur = "T", il s'agit d'un paiement de test, si valeur ="X", il s'agit d'un paiement d'activation	**S1**	"Mode de saisie incorrect." Un reporting informera l'administrateur TIPI.
NUMCLI	Contrôle du nombre et du format des caractères	6	Le numéro de client TIPI doit comporter 6 caractères numériques.	**T1**	"Numéro de client incorrect." Un reporting informera l'administrateur TIPI.
	Contrôle d'existence du NUMCLI dans le référentiels des clients TIPI		Le N° du client doit être pré-existant dans la base TIPI.	**T2**	"Client non autorisé." Un reporting informera l'administrateur TIPI.
	Contrôle du statut du client TIPI		Si le champ SAISIE = "X" et le statut du Client est à "I" (inactif)	**T3**	"Le client ne peut pas être réactivé." Un reporting informera l'administrateur TIPI.
			Si le champ SAISIE = "X" et le statut du Client est à "A" (actif) ou le statut est encore "E" (Enregistré) mais une activation vient d'être effectuée (présence des références du client dans la table TPA_ACTIVATIONCLIENT) -	**T4**	"Le client TIPI est déjà activé. " Un reporting informera l'administrateur TIPI
			Si le champ SAISIE = "W" et le statut du Client est différent de "A" (actif) le paiement est impossible	**T5**	"Le statut du client ne permet pas le paiement." Un reporting informera l'administrateur TIPI.
			Si le champ SAISIE = "X" et le statut du Client est à "N" (Nouveau)	**T7**	"Le statut du client ne permet pas son activation." Un reporting informera l'administrateur TIPI.
	Contrôle de l'accès sécurisé		Le client doit être un client Régie et comporter une autorisation de paiement par mode sécurisé ou être un client ClientGenerique	**T9**	"Ce client n'a pas d'accès sécurisé" Un reporting informera l'administrateur TIPI.
EXER	Vérification du format d' EXER si le champ est servi (donnée facultative)	4	L'exercice comporte 4 caractères numériques, l'année doit être N ou N-1 par rapport date du jour	**E1**	Aucune erreur n'est retournée avec ce code. Seul un reporting informera l'administrateur TIPI.
REFDET	Contrôle de forme	6 à 30	REFDET doit comporter entre 6 et 30 caractères au format a z A Z 0 9 sinon le paiement est impossible	**R3**	"Le format du paramètre REFDET n'est pas conforme." Un reporting informera l'administrateur TIPI.
OBJET	Contrôle de forme	<100	La valeur du champ doit comporter des caractères alphanumériques + l'espace	**O1**	"La valeur de l' OBJET est incorrecte." Un reporting informera l'administrateur TIPI.
MONTANT	Contrôle du nombre et du format des caractères	6	Si le nombre de chiffres du montant est supérieur à 6 caractères numériques ou s'il comporte une virgule, l'activation, le test et le paiement sont impossibles.	**M1**	"Le format du montant n'est pas correct (présence de caractères non autorisés ou seuil de paiement sur Internet dépassé)." Un reporting informera l'administrateur TIPI.
	Contrôle de la valeur du champ MONTANT		Si la valeur est supérieure à 9999,99 euros, le paiement est impossible	**M2**	Le contrôle est effectué mais ne donnera lieu à aucune anomalie car la vérification du nombre maximum de caratères (M1) est fait en premier. (10000,00 fait plus de 6 caractères) "Le format du montant n'est pas correct (présence de caractères non autorisés ou seuil de paiement sur Internet dépassé)."
			Si la valeur est inférieure à 1 € le paiement est impossible	**M3**	" Montant inférieur au seuil minimum accepté." Un reporting informera l'administrateur TIPI.
			Les montants sont libres en activation et en test mais il sera vérifié qu'ils ne correspondent pas à un montant interdit (Liste fourni par le prestataire de télépaiement - Cf. cahier des charges).	**M5**	"Montant non autorisé pour le paiement de test ou d'activation." Un reporting informera l'administrateur TIPI.
MEL	Contrôle du nombre et du format des caractères	6 à 80	L'adresse MEL du débiteur doit être servie sinon le paiement est impossible	**A1**	"Adresse mèl non renseignée." Un reporting informera l'administrateur TIPI.
			L'adresse MEL du débiteur doit comporter entre 6 et 80 caractères maximum ainsi que les caractères "@" et "." sinon le paiement est impossible	**A2**	"Adresse mél est incorrecte." Un reporting informera l'administrateur TIPI.
URLNOTIF	Contrôle du nombre et du format des caractères	<250	Ce champ doit être servi obligatoirement et doit être au format http://.....; 250 caractères maximum sans indication de port sinon l'activation, le test et le paiement sont impossibles.	**N1**	"Url de notification non valide ou comportant des ports non autorisés." un reporting informera l'administrateur TIPI
URLREDIRECT	Contrôle du nombre et du format des caractères	<250	Ce champ doit être servi obligatoirement et doit être au format http://.....; 250 caractères maximum sans indication de port sinon l'activation, le test et le paiement sont impossibles	**D1**	"Url de redirection non valide ou comportant des ports non autorisés." Un reporting informera l'administrateur TIPI.

Auteur :	MC REY
Projet :	TIPI

Document	
Nom	Anomalies ws-AppelCreerPaiementsecurisé.xls
Type	Spécifications techniques
Statut	Validé
Date création	10/04/2013
Date dernière mise à jour	30/09/2013

Nom des champs concernés	Nature du contrôle	Longueur du champ	Règle de gestion	Code de la fonctionelle erreur	Libellé de la fonctionelleErreur pour paiement, activation et test SAISIE="W", "X" ou "T"
Saisie	Contrôle d'existence et de valeur	1	Le champ doit avoir pour valeur "W- X ou T". "W" correspond à un paiement réel effectué par le web service. si la valeur = "T", il s'agit d'un paiement de test, si valeur ="X", il s'agit d'un paiement d'activation	**S1**	"Mode de saisie incorrect." Un reporting informera l'administrateur TIPI.
NUMCLI	Contrôle du nombre et du format des caractères	6	Le numéro de client TIPI doit comporter 6 caractères numériques.	**T1**	"Numéro de client incorrect." Un reporting informera l'administrateur TIPI.
	Contrôle d'existence du NUMCLI dans le référentiels des clients TIPI		Le N° du client doit être pré-existant dans la base TIPI.	**T2**	"Client non autorisé." Un reporting informera l'administrateur TIPI.
	Contrôle du statut du client TIPI		Si le champ SAISIE = "X" et le statut du Client est à "I" (inactif)	**T3**	"Le client ne peut pas être réactivé." Un reporting informera l'administrateur TIPI.
			Si le champ SAISIE = "X" et le statut du Client est à "A" (actif) ou le statut est encore "E" (Enregistré) mais une activation vient d'être effectuée (présence des références du client dans la table TPA_ACTIVATIONCLIENT) -	**T4**	"Le client TIPI est déjà activé. " Un reporting informera l'administrateur TIPI
			Si le champ SAISIE = "W" et le statut du Client est différent de "A" (actif) le paiement est impossible	**T5**	"Le statut du client ne permet pas le paiement." Un reporting informera l'administrateur TIPI.
			Si le champ SAISIE = "X" et le statut du Client est à "N" (Nouveau)	**T7**	"Le statut du client ne permet pas son activation." Un reporting informera l'administrateur TIPI.
	Contrôle de l'accès sécurisé		Le client doit être un client Régie et comporter une autorisation de paiement par mode sécurisé	**T9**	"Ce client n'a pas d'accès sécurisé" Un reporting informera l'administrateur TIPI.
EXER	Vérification du format d' EXER si le champ est servi (donnée facultative)	4	L'exercice comporte 4 caractères numériques, l'année doit être N ou N-1 par rapport date du jour	**E1**	Aucune erreur n'est retournée avec ce code. Seul un reporting informera l'administrateur TIPI.
REFDET	Contrôle de forme	6 à 30	REFDET doit comporter entre 6 et 30 caractères au format a z A Z 0 9 sinon le paiement est impossible	**R3**	"Le format du paramètre REFDET n'est pas conforme." Un reporting informera l'administrateur TIPI.
OBJET	Contrôle de forme	<100	La valeur du champ doit comporter des caractères alphanumériques + l'espace	**O1**	"La valeur de l' OBJET est incorrecte." Un reporting informera l'administrateur TIPI.
MONTANT	Contrôle du nombre et du format des caractères	6	Si le nombre de chiffres du montant est supérieur à 6 caractères numériques ou s'il comporte une virgule, l'activation, le test et le paiement sont impossibles.	**M1**	"Le format du montant n'est pas correct (présence de caractères non autorisés ou seuil de paiement sur Internet dépassé)." Un reporting informera l'administrateur TIPI.
	Contrôle de la valeur du champ MONTANT		Si la valeur est supérieure à 9999,99 euros, le paiement est impossible	**M2**	Le contrôle est effectué mais ne donnera lieu à aucune anomalie car la vérification du nombre maximum de caratères (M1) est fait en premier. (10000,00 fait plus de 6 caractères) "Le format du montant n'est pas correct (présence de caractères non autorisés ou seuil de paiement sur Internet dépassé)."
			Si la valeur est inférieure à 1 € le paiement est impossible	**M3**	" Montant inférieur au seuil minimum accepté." Un reporting informera l'administrateur TIPI.
			Les montants sont libres en activation et en test mais il sera vérifié qu'ils ne correspondent pas à un montant interdit (Liste fourni par le prestataire de télépaiement - Cf. cahier des charges).	**M5**	"Montant non autorisé pour le paiement de test ou d'activation." Un reporting informera l'administrateur TIPI.
MEL	Contrôle du nombre et du format des caractères	6 à 80	L'adresse MEL du débiteur doit être servie sinon le paiement est impossible	**A1**	"Adresse mèl non renseignée." Un reporting informera l'administrateur TIPI.
			L'adresse MEL du débiteur doit comporter entre 6 et 80 caractères maximum ainsi que les caractères "@" et "." sinon le paiement est impossible	**A2**	"Adresse mél est incorrecte." Un reporting informera l'administrateur TIPI.
URLNOTIF	Contrôle du nombre et du format des caractères	<250	Ce champ doit être servi obligatoirement et doit être au format http://.....; 250 caractères maximum sans indication de port sinon l'activation, le test et le paiement sont impossibles.	**N1**	"Url de notification non valide ou comportant des ports non autorisés." un reporting informera l'administrateur TIPI
URLREDIRECT	Contrôle du nombre et du format des caractères	<250	Ce champ doit être servi obligatoirement et doit être au format http://.....; 250 caractères maximum sans indication de port sinon l'activation, le test et le paiement sont impossibles	**D1**	"Url de redirection non valide ou comportant des ports non autorisés." Un reporting informera l'administrateur TIPI.

Annexe 9 : Anomalies ws-AppelrecupererDetailPaiementSecurise

Auteur :	MC REY
Projet :	TIPI

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Document	
Nom	Anomalie WS-AppelrecupererDetailPaiementsecurise.xls
Type	Spécifications techniques
Statut	Validé
Date création	10/04/2013
Date dernière mise à jour	26/09/2013

Nom des champs concernés	Nature du contrôle	Longueur du champ	Règle de gestion	Code de la fonctionelle erreur	Libellé de la fonctionelleErreur pour paiement, activation et test SAISIE="W", "X" ou "T"
IDOP	Si IdOp non trouvé dans la table des données de paiement lors de la récupération du paiement sécurisé		L'IdOp doit être connu afin de récupérer le token fourni par le prestataire de télépaiement et les informations du paiement.	**P1**	"IdOp incorrect." Pas de reporting.
	Si le prestataire de télépaiement n'a pas attribué de Token ou que le paiement en cours à son niveau lors de la récupération du paiement sécurisé		La consultation d'un résultat ne peut intervenir que si la transaction est terminée et que l'on a pu récupérer un résultat auprès de Payline.	**P5**	"Résultat de la transaction non connu." Un reporting informera l'administrateur TIPI.

Annexe 9bis (Optionnel) : Anomalies ws-AppelrecupererDetailClient

Méthode **recupererDetailClient**

- **Appel Web service de Tipi pour initier l'opération de recherche sur un client (Utilisation optionnelle pour vérifier le bon paramétrage d'un client).**

Les paramètres ***en entrée*** sont décrits dans ce tableau

PARAMETRES	LONGUEUR	Format	DESCRIPTION
NUMCLI	6		LE NUMERO CLIENT ATTRIBUE A LA COLLECTIVITE PAR L'ADMINISTRATEUR TIPI

- **Si un résultat est connu pour le numéro de client transmis dans le paramètre d'appel, une réponse est retournée par TIPI avec les paramètres suivants :**

Les paramètres ***en sortie*** sont décrits dans ces tableaux

1) Pour les clients génériques (Code protocole 9)

PARAMETRES	LONGUEUR	Format	DESCRIPTION
NUMCLI	6		LE NUMERO CLIENT ATTRIBUE A LA COLLECTIVITE PAR L'ADMINISTRATEUR TIPI
libelleN1			libellé structure N1
libelleN2			libellé structure N2
libelleN3			libellé structure N3

2) Pour les régies (Code protocole 0)

PARAMETRES	LONGUEUR	Format	DESCRIPTION
NUMCLI	6		LE NUMERO CLIENT ATTRIBUE A LA COLLECTIVITE PAR L'ADMINISTRATEUR TIPI
libelleN1			libellé Régie
libelleN2			libellé Client
libelleN3			libellé Budget

- **Gestion des erreurs**

- **Cas 1** : le client dont le numéro client passé en paramètre n'existe pas dans le référentiel des clients :
code erreur : 1
libellé erreur court : Client non existant
libellé erreur long : Le client demandé n'est pas présent dans le référentiel

- **Cas 2** : Le client dont le numéro client passé en paramètres n'est pas une régie ou n'est pas un client générique
code erreur : 2
libellé erreur court : Client non générique ou non régie
libellé erreur long : Le client demande n'est pas un client générique ou une régie

- **Cas 3** : Le client dont le numéro client passé en paramètre n'est pas une régie utilisant le WebService
code erreur : 3
libellé erreur court : Régie non WebService
libellé erreur long : Le client demandé n'est pas une régie utilisant le WebService

Auteur :	MC REY
Projet :	TIPI

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Document	
Nom	Anomalie protocole simplifié.xls
Type	Spécifications techniques
Statut	Validé
Date création	04/06/2013
Date dernière mise à jour	30/09/2013

Liste des anomalies et des messages affichés à l'utilisateur

Nom des champs	nature du contrôle	Règle de gestion	Code anomalie	Message à l'utilisateur pour activation et test SAISIE="X" ou "T"	Message à l'utilisateur pour paiement réel SAISIE= "W"
IDOP	Contrôle si présence IDOP	L'Idop doit être trouvé dans le référentiel TIPI (table TPA_DONNEESPAIEMENT)	P2	"Votre transaction n'a pu aboutir, veuillez effectuer une nouvelle tentative. " Un bouton "Fermer la fenêtre" ferme la fenêtre (à confirmer). Pas de reporting.	"Votre transaction n'a pu aboutir, veuillez effectuer une nouvelle tentative. " Un bouton "Fermer la fenêtre" ferme la fenêtre (à confirmer). Pas de reporting.
		L'Idop ne doit pas avoir déjà été utilisé pour un paiement (état différent de "U")	P3	"Votre transaction n'a pu aboutir, veuillez effectuer une nouvelle tentative. " Un bouton "Fermer la fenêtre" ferme la fenêtre (à confirmer). Un reporting informera l'administrateur TIPI	"Votre transaction n'a pu aboutir, veuillez effectuer une nouvelle tentative. " Un bouton "Fermer la fenêtre" ferme la fenêtre (à confirmer). Un reporting informera l'administrateur TIPI
		L'Idop ne doit pas avoir été enregistré depuis plus de "temps paramétré dans appli.properties paramètre "nombreminutesautorisees". (actuellement 15 minutes)	P4	"Votre transaction n'a pu aboutir, veuillez effectuer une nouvelle tentative. " Un bouton "Fermer la fenêtre" ferme la fenêtre (à confirmer). Un reporting informera l'administrateur TIPI	"Votre transaction n'a pu aboutir car le délai imparti est dépassé.Veuillez effectuer une nouvelle tentative. " Un bouton "Fermer la fenêtre" ferme la fenêtre (à confirmer). Un reporting informera l'administrateur TIPI

Annexe 11 : FAQ mise en place d'une solution Web Service avec PayFiP

Ce document à pour but d'aider les nouveaux partenaires dans la mise en place et l'interfaçage de leur solution avec le Web Service fourni par PayFiP.
Pour ce faire nous avons répertorié les difficultés déjà rencontrées par les partenaires.

Table des matières

1) Puis-je tester ma solution Web Service directement vers le serveur de production de PayFiP ?

Oui, PayFiP propose un mode test ou vous pouvez réaliser vos essais en production.

Pour information, l'activation de votre client permet de débloquer les paiements réels mais ne bloque pas les paiements de test (toujours possibles après l'activation).

2) Puis-je disposer d'un environnent de test dédié pour la mise au point de ma solution ?

Oui, PayFiP vous propose sur demande, un client de test sur une plate-forme de qualification quasi identique à celle de production.(demande à faire parvenir au bureau CL1C par le biais du correspondant moyen de paiement de votre DR/DDFIP)

Même si les paiements de « type réels » sont possibles sur cette plate-forme de test (avec une carte de fictive : 4012001037141112), aucun flux financier n'est généré derrière et nous ne pouvons ainsi pas fournir de fichier des transactions journalières sur cette plate-forme(comme c'est le cas en production)

3) Je ne peux pas contacter PayFiP, comment dois-je procéder?

3.a) Vérifier l'URL d'appel utilisée

- L'url d'appel du Web Service à utiliser est la suivante:

https://www.tipi.budget.gouv.fr/tpa/services/securite

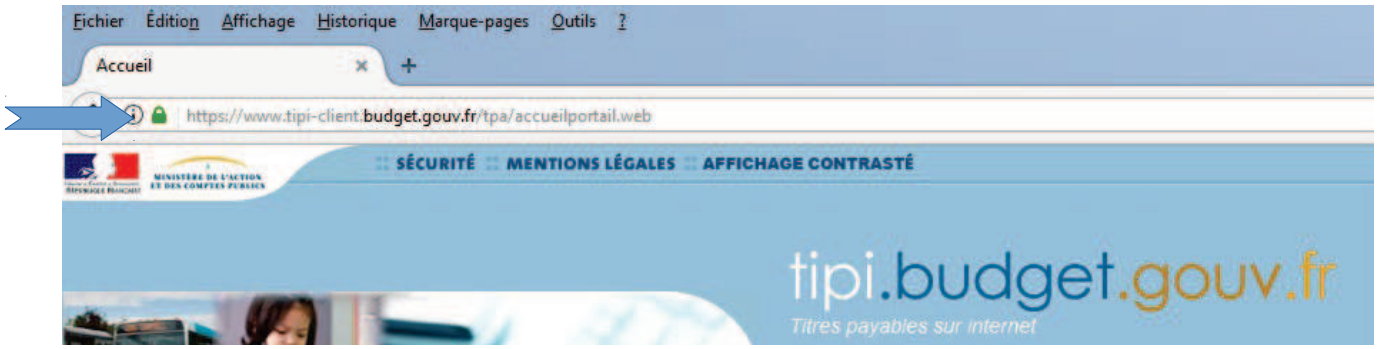
3.b) Intégrer le certificat de PayFiP dans votre base de confiance

- Pour pouvoir contacter une URL en https, tout serveur/navigateur doit avoir dans sa base de confiance le certificat du serveur destination ou du moins le certificat de l'autorité de certification dont il dépend. En l'occurrence Certigna pour PayFiP.

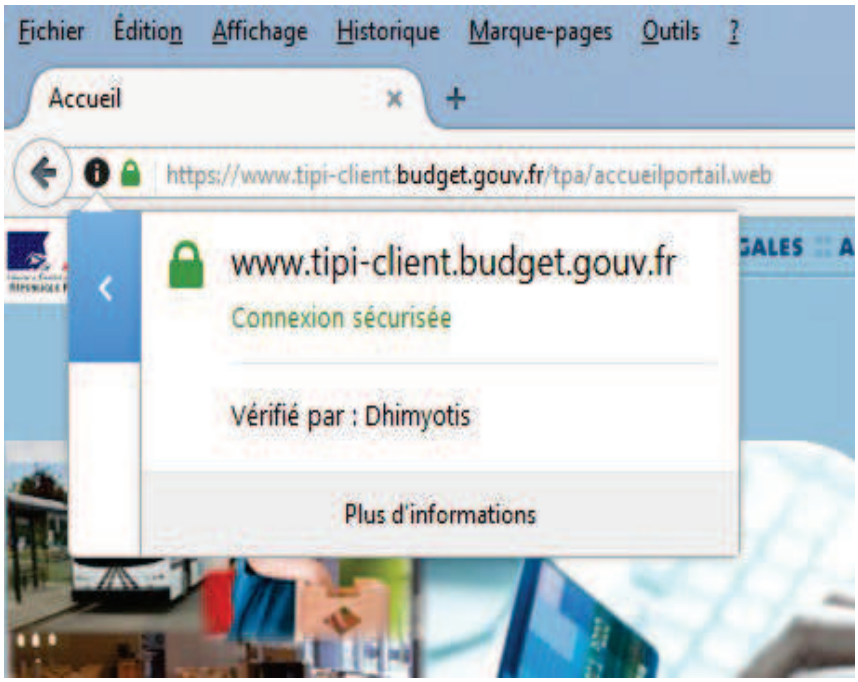
- Il se trouve que cela est invisible quand on contacte PayFiP par le biais d'un navigateur car l'ensemble des principaux navigateurs web intègrent un magasin de certificats contenant les principales autorités de certification du marché.

- Pour ce qui est des serveurs, tomcat par exemple, le magasin de certificats ne contient pas obligatoirement les certificats des autorités de certification qui doivent y être intégrés pour pouvoir dialoguer en https avec d'autres serveurs.

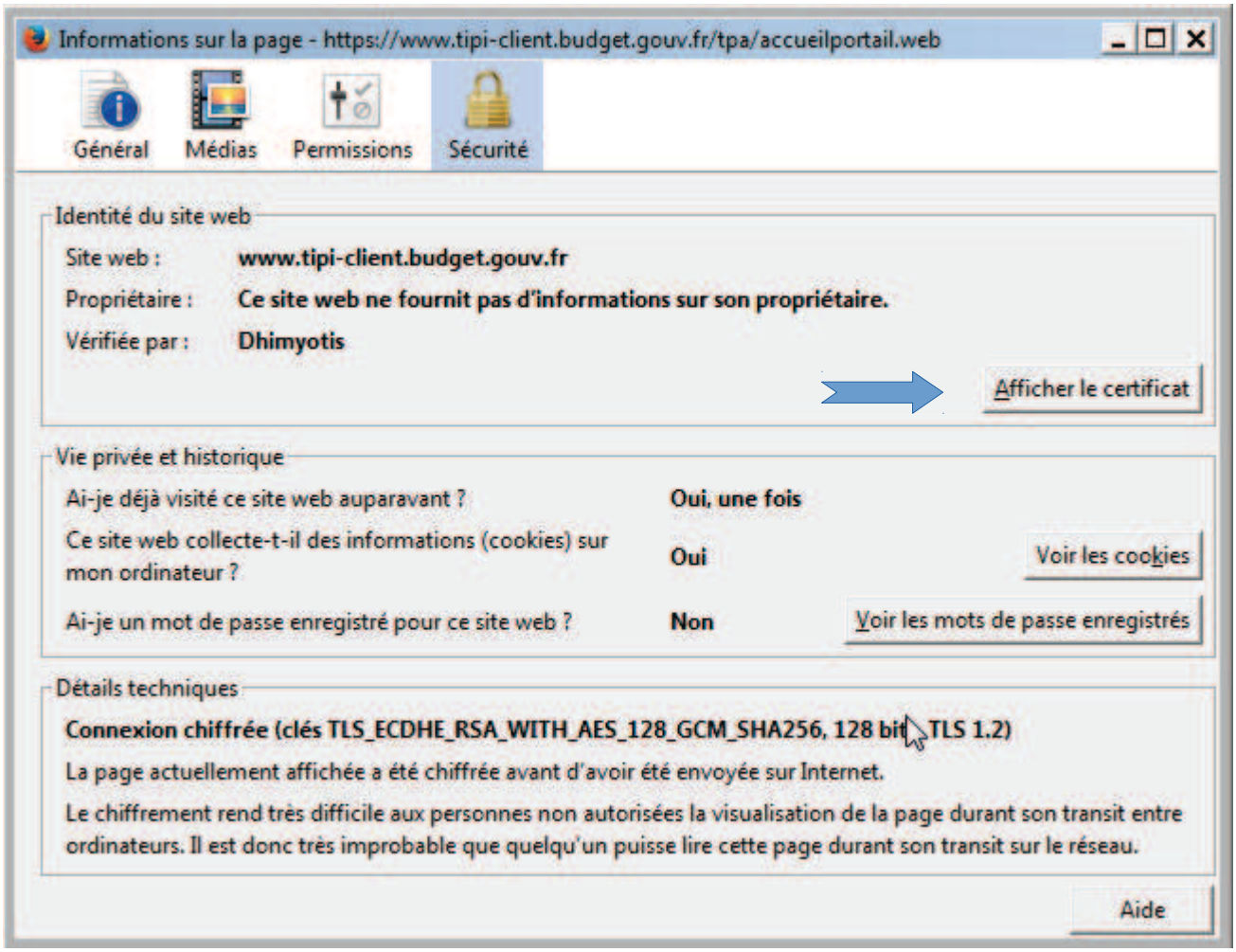
Pour information, les certificats sont téléchargeables directement dans un navigateur web (firefox par exemple), en entrant dans la barre d'adresse l'url (https://www.tipi.budget.gouv.fr/)



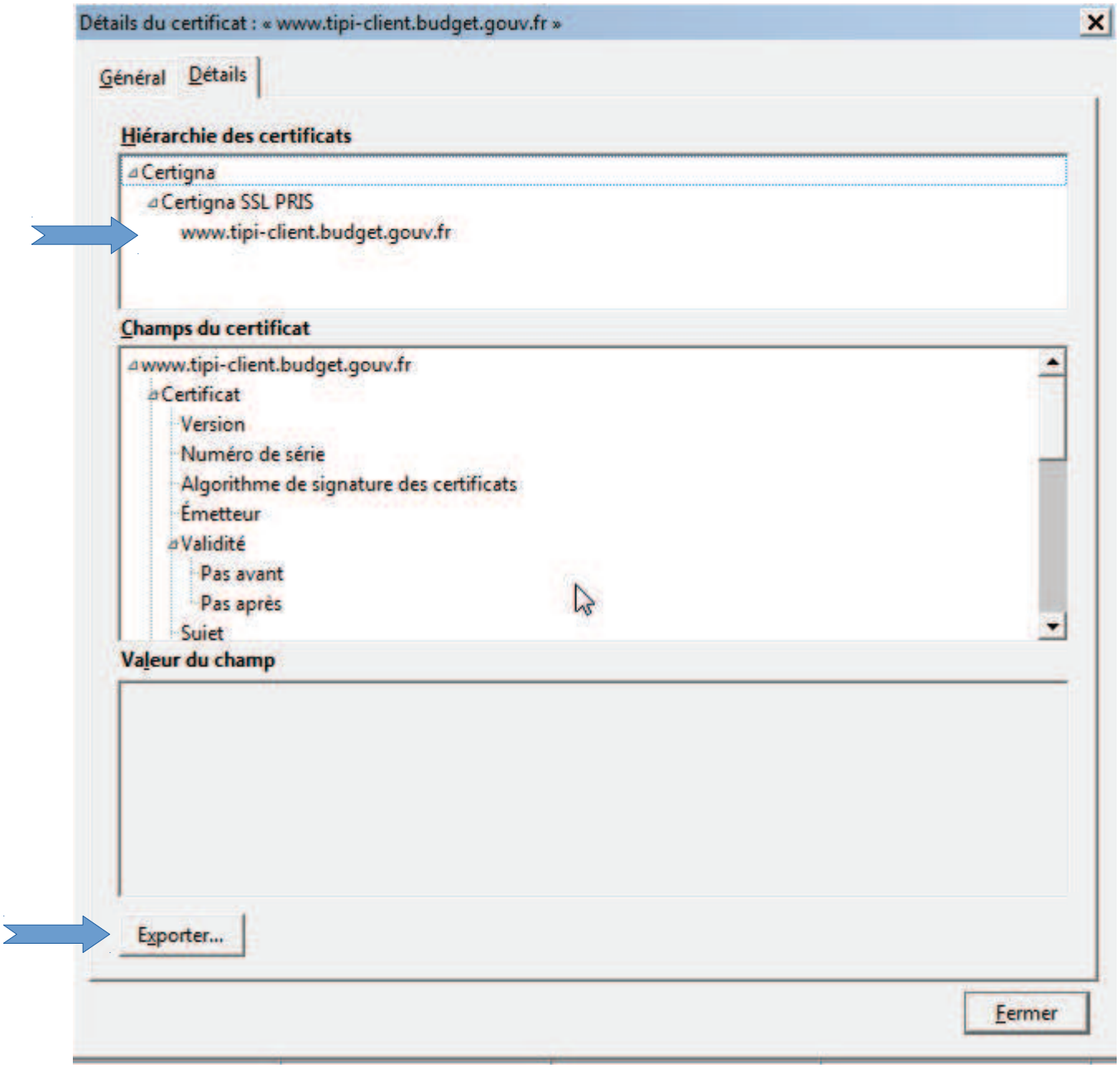
Puis en cliquant sur le petit cadenas à gauche de l'url, puis sur le bouton « Plus d'informations... »



Cliquer ensuite sur le bouton «Afficher le certificat »



Dans l'onglet « Détails » cliquer sur « www.tipi.budget.gouv.fr » puis sur le bouton exporter



Ce certificat devra être intégré dans le magasin de confiance de votre serveur.

Au vu de la grande diversité des types de serveurs, si nécessaire, il faudra vous rapprocher de l'équipe technique en charge de vos serveurs pour insérer le certificat PayFiP dans leur base de confiance.

3.c) Vous avez une erreur de type T9

Si lors de votre appel Web service vous avez une erreur de type « T9 - Ce client n'a pas d'accès sécurisé. », vérifier auprès de votre correspondant moyens de paiement de la DR/DDFiP si votre client est bien en mode Web Service.

4) Puis-je tester les appels web-service vers PayFiP sans avoir finalisé le développement de ma solution ?

Oui, vous pouvez générer l'appel par le biais d'utilitaires de génération d'appel SOAP (*Simple Object Access Protocol*)

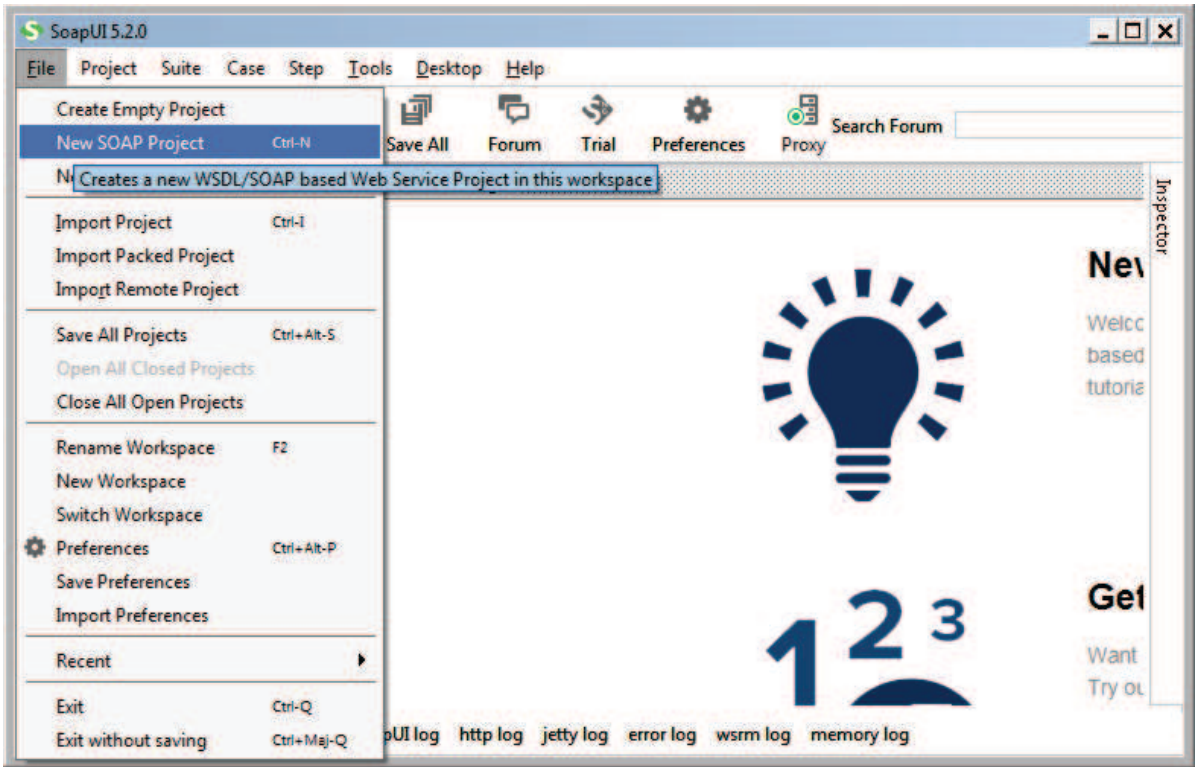
4.a) Prérequis pour tester le Web Service PayFiP (avec SoapUI version 5.2 minimum):

Disposer d' un numéro de client PayFiP Client attribué en qualification.

4.b) Télécharger SoapUI et l'installer (projet libre)

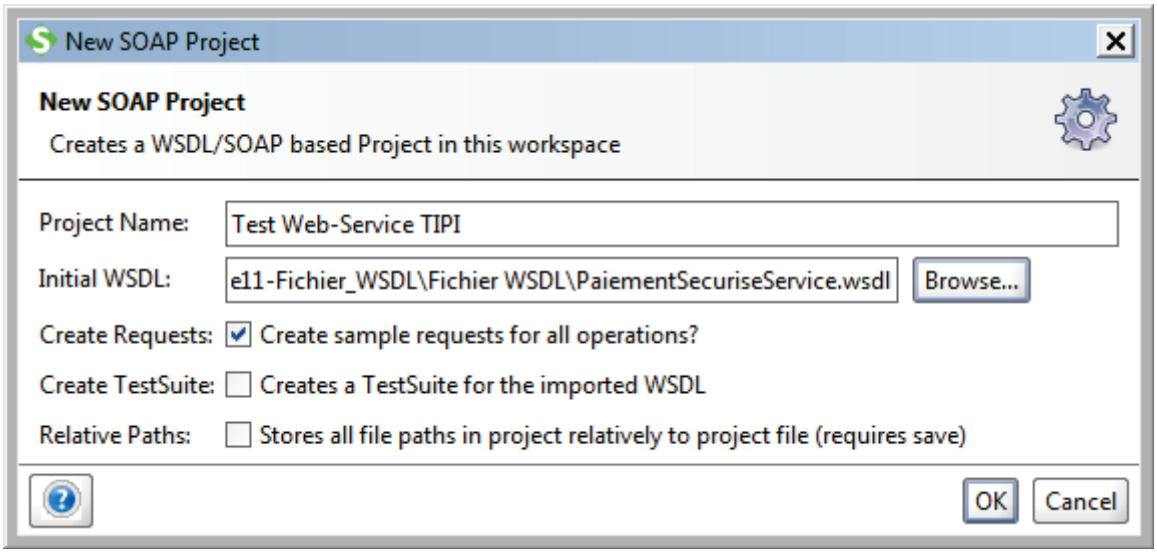
Le logiciel est disponible gratuitement à l'adresse : https://www.soapui.org

4.c) Créer un nouveau projet SOAP



4.d) Entrer un nom de projet :

Par exemple « Test Web-Service PayFiP » et choisir le fichier « PaiementSecuriseService.wsdl » fourni en annexe 11 (WSDL)

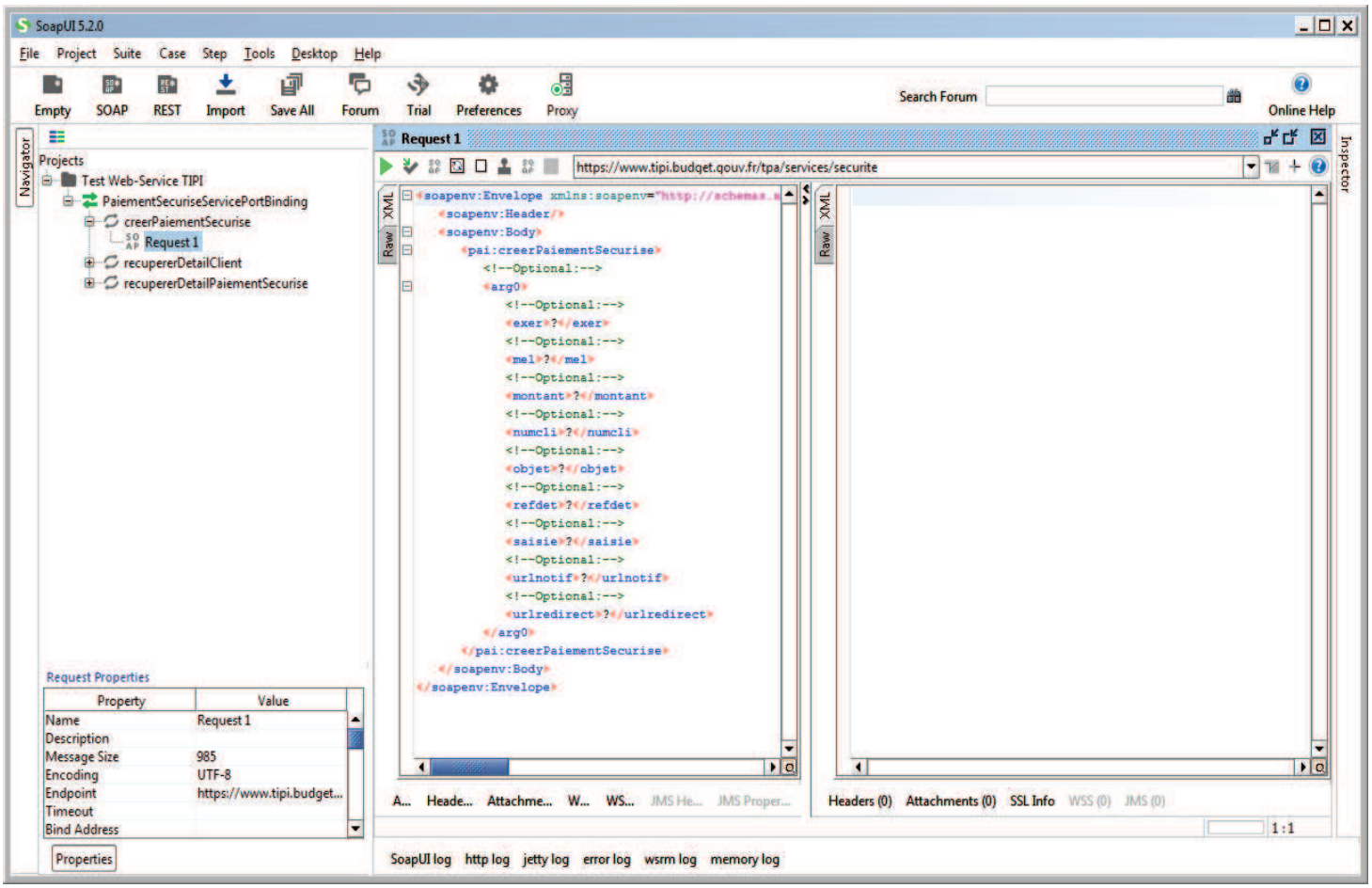


Un nouveau projet est alors créé avec les appels suivants :

- creerPaiementSecurise
- recupererDetailClient
- recupererDetailPaiementSecurise

4.e) Procédure de test

- Choisissez dans la méthode « creerPaiementSecurise » et la «Request 1 » :

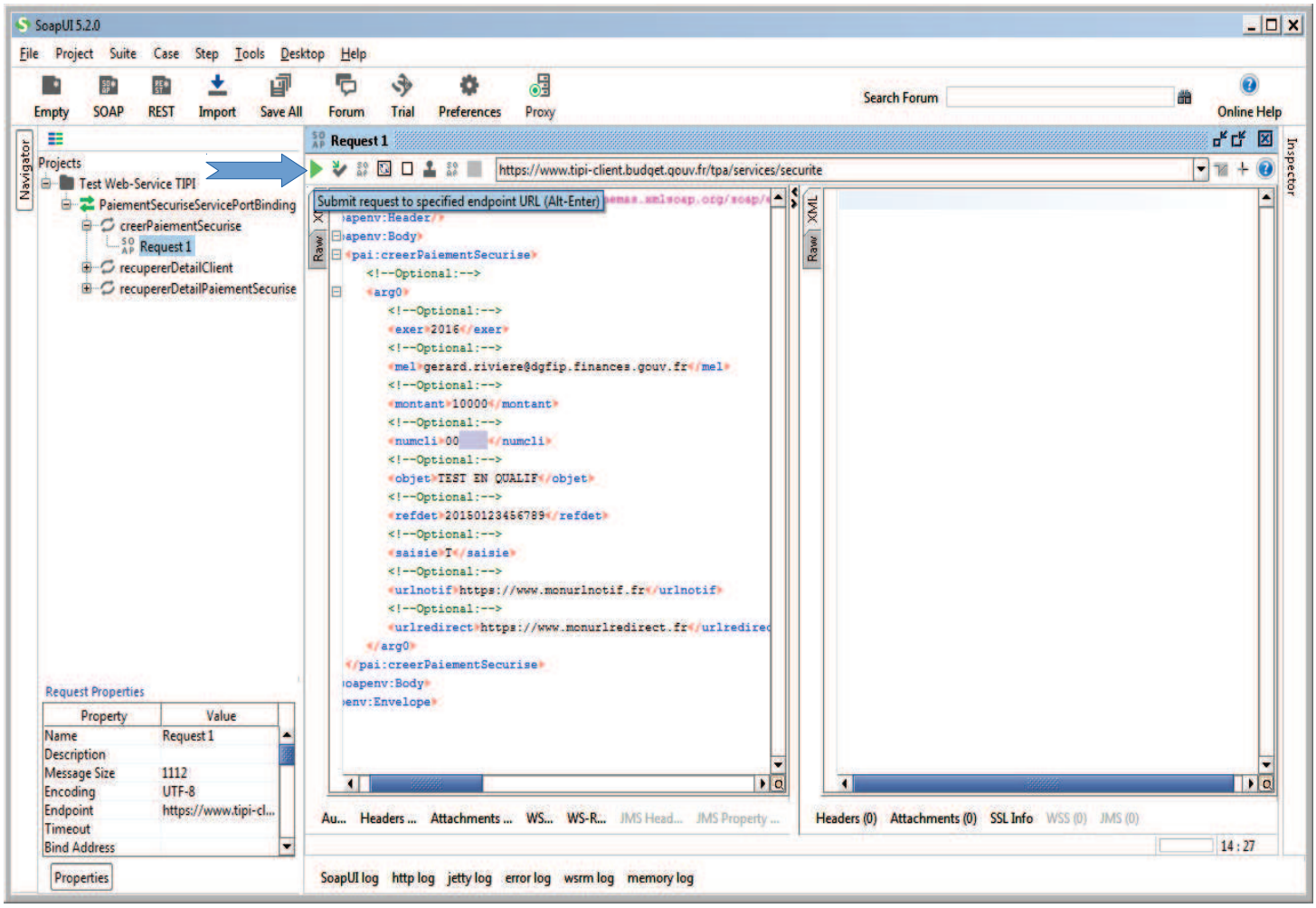


L'url d'appel renseignée par défaut est celle de production :
https://www.tipi.budget.gouv.fr/tpa/services/securite

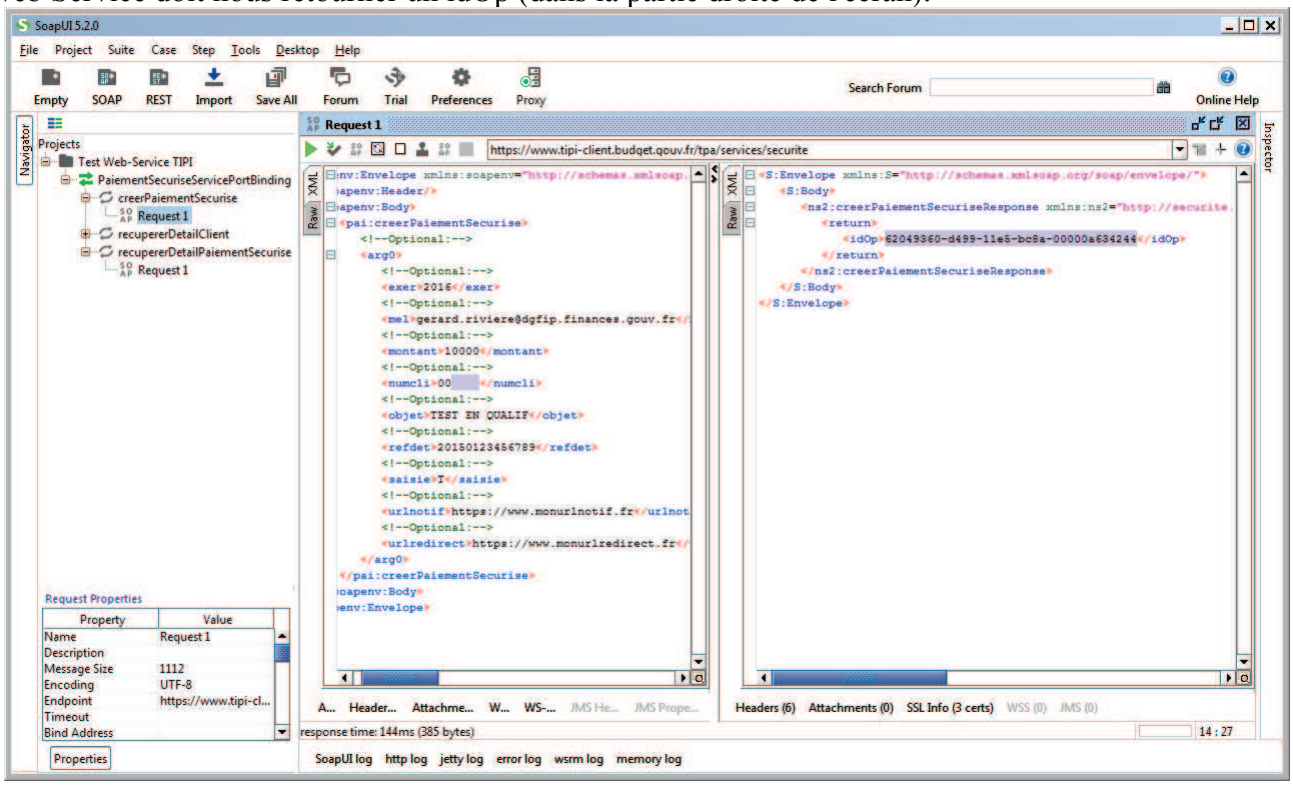
Pour le client sur la qualification il faudra mettre l'url suivante :
https://www.tipi-client.budget.gouv.fr/tpa/services/securite

Renseigner les champs suivant selon les spécifications détaillés dans le cahier des charges Web Service : <exer>, <mel>, <montant>, <numcli>(fourni par le CMP ou sur demande en qualif à CL1C), <objet>, <refdet>, <saisie>(T pour test, W en mode réel),<urlnotif> et <urlredirect>

Puis cliquer sur le triangle en haut à gauche de la fenêtre « Request 1 »



Le Web Service doit nous retourner un idOp (dans la partie droite de l'écran):

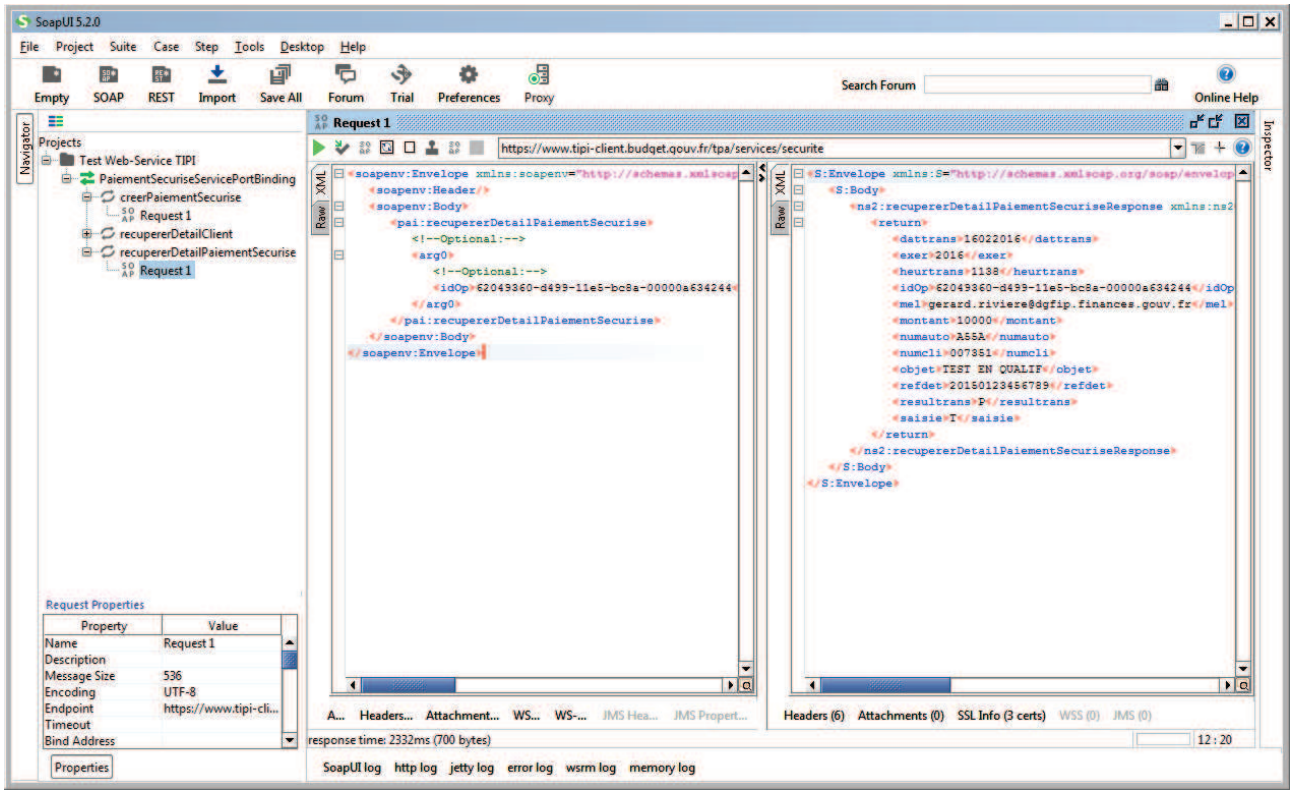


Déjà ici nous avons un appel au Web Service PayFiP qui a fonctionné.
Si l'on veut aller plus loin et faire un paiement de test on peut utiliser l'url suivante dans un navigateur :

https://www.tipi.budget.gouv.fr/tpa/paiementws.web?idop=

Il convient d'insérer à la suite de cette url, l'idOp récupéré lors de l'appel Web Service ci-dessus et effectuer le paiement jusqu'au bout.

Une fois le paiement effectué sur le navigateur, il faut appeler dans soapUI la méthode « recupererDetailPaiementSecurise » en indiquant l'idOp initial pour récupérer le résultat du paiement :



Nous avons ainsi reproduit la procédure associée à un paiement.

5) Je ne reçois pas de notification de la part de PayFiP suite à mes paiements, comment dois-je procéder?

5.a) Utilisation d'une URL joignable depuis internet.

Vérifier que vous utilisez bien une URL associée à une adresse IP publique et non privée.
PayFiP ne pourra jamais vous notifier sur une URL accessible depuis votre intranet uniquement, encore moins sur une URL de type *http://localhost :8080/retour_tipi*
Vous devez impérativement utiliser pour les paramètres URLNOTIF et URLREDIRECT , des URL accessibles depuis internet.

5.b) Utilisation d'une URLNOTIF en HTTPS

Comme indiqué dans le cahier des charges, au chapitre 2 « Conditions requises pour adhérer à PayFiP », si

vous souhaitez recevoir les notifications en https, vous devez communiquer à l'administrateur local PayFiP (correspondant moyens de paiement de la DR/DDFiP) le certificat utilisé ainsi que l'url de notification associée.
Les certificats sont intégrés à la base de confiance des serveurs PayFiP chaque premier jeudi du mois.

5.c) Récupération des paramètres envoyés lors de la notification

Lors de la notification, PayFiP envoie le paramètre (idop) et la valeur associées en mode POST et non en mode GET.

Exemple :

POST http://domaine.fr/recup_notif HTTP/1.1
User-Agent: Jakarta Commons-HttpClient/3.1
Host: domaine.fr
Proxy-Connection: Keep-Alive
Content-Length: 41
Content-Type: application/x-www-form-urlencoded

idop=4b12b6a0-b4aa-11e7-b2ed-01234e12345f

6) Puis-je limiter les notifications entrantes uniquement aux serveurs de PayFiP?

Oui, vous pouvez autoriser sur votre architecture, uniquement les notifications en provenance du serveur PayFiP de production dont l'adresse ip publique est la suivante : 145.242.11.3