

3DSV2 - Interface Directe - Paiements récurrents



Contenu

- Généralités
- Valorisation de la demande de paiement de la commande (CIT)
 - Valeurs communes aux demandes d'authentification et d'autorisation
 - Spécificités autorisation
- Stockage des données de paiement dans un wallet Payline.
- Valorisation des demandes de paiement subséquentes (MIT)
- Montant authentifié
- Grand fathering
- Changement et renouvellement de carte
- Pages associées

Cette page précise les paramètres à utiliser pour l'authentification et l'autorisation des paiements

- récurrents avec des échéances en nombre défini et de même montant;
- autres récurrents, c'est à dire paiements récurrents de montants variables et/ou de durée indéterminée. Par exemple, paiement de facture d'abonnement de montant variant en fonction de la consommation et/ou sans date de fin
- échelonnés, aussi appelés NX ou installments.

Généralités

Ces paiements s'effectuent en deux phases:

1. une phase de commande associée au paiement de la première échéance, initiée par l'acheteur sur les pages de l'e-commerçant appelée CIT, Customer Initiated Transaction;
2. une seconde constituée des demandes de paiement des échéances suivantes initiées par le marchand hors la présence de l'acheteur appelée MIT Merchant Initiated Transaction.

La demande de paiement de la première échéance doit **obligatoirement** être authentifiée avec un challenge.

Le numéro de carte peut être saisi par l'acheteur ou récupéré d'un card on file créé précédemment.

Les suivantes sont transmises:

- sans demande d'authentification préalable;
- en référant la première autorisation.

Valorisation de la demande de paiement de la commande (CIT)

Nous donnons dans les tableaux ci-dessous les valeurs des champs caractéristiques des différents objets de l'interface web service (cf. [traitement authentification + autorisation](#) pour l'enchaînement des web services).

Dans un premier temps les valeurs communes aux demandes d'authentification et d'autorisation puis les spécificités de l'autorisation.

Valeurs communes aux demandes d'authentification et d'autorisation

Les tableaux ci-dessous donnent les valeurs et la présence des différents champs pour le cas spécifiques des paiements NX et récurrents

Paramètre	Présence	Commentaire
version	O	La version doit être supérieure ou égale à 28
Objet Payment		

amount	F	Montant de la première échéance.
action	O	122 : autorisation pour un paiement récurrent de montant constant et de durée fixée 123: autorisation + validation pour un paiement récurrent de montant constant et de durée fixée 124: autorisation pour un paiement échelonné, NX, ou installment 125: autorisation + validation pour un paiement échelonné, NX, ou installment 128: autorisation pour les autres paiements récurrents 129: autorisation + validation pour les autres paiements récurrents
mode	O	CPT
cumulatedAmount	O	0
Objet Order		
amount	O	Contient le montant à authentifier, dépend du cas de paiement .
Objet Recurring		
firstAmount	C	Montant de la première échéance (prime sur payment.amount) Obligatoire pour les codes action (122, 123, 124, 125) Facultatif pour les codes action (128, 129)
amount	C	Montant des échéances suivantes Obligatoire pour les codes action (122, 123, 124, 125) Vide pour les codes action (128, 129)
billingCycle	C	Récurrence, par exemple 40 pour une récurrence mensuelle Obligatoire pour les codes action (122, 123, 124, 125) Vide pour les codes action (128, 129)
billingLeft	C	Nombre d'échéances total (3 pour paiement 3 fois, ...) Obligatoire pour les codes action (122, 123, 124, 125) Vide pour les codes action (128, 129)
billingRank	C	1 pour la 1 ^{ère} échéance Obligatoire pour les codes action (122, 123, 124, 125) Facultatif pour les codes action (128, 129)
endDate	C	date de la dernière échéance (prendre une marge qui inclut le temps nécessaire pour répéter la demande de paiement de la dernière échéance en cas d'incident) Obligatoire pour les codes action (122, 123, 124, 125) Vide pour les codes action (128, 129)
Objet Buyer		
ip	C	Doit être valorisé quand l'acheteur utilise un navigateur web
Objet ThreeDSinfo		
ChallengeInd	F	'04' Monext force la demande de challenge à cette valeur dans la demande envoyée à l'ACS. Il s'agit d'un aspect réglementaire. Le commerçant n'est pas obligé de remplir ce champ.
browser	C	Doit être valorisé quand l'acheteur utilise un navigateur web.

sdk	C	Doit être valorisé quand l'acheteur est connecté via une application mobile utilisant un sdk.
-----	---	---

Spécificités autorisation

L'autorisation peut être effectuée avec un

- doAuthorization;
- doImmediateWalletPayment;

Paramètre	Présence	Commentaire
authentication3DSecure.md	O	
authentication3DSecure.pares	O	

Stockage des données de paiement dans un wallet Payline.

Cette étape facultative permet de stocker les données de paiement dans un wallet Payline.

Il faut faire appel au web service createWallet en précisant:

1. le numéro de contrat
2. l'identifiant de wallet
3. l'identifiant de transaction Payline donné en réponse du doAuthorization.

Valorisation des demandes de paiement subséquentes (MIT)

Les demandes de paiement des autres échéances sont initiées par le marchand hors la présence de l'acheteur, il n'y a pas d'authentification.

La demande de paiement peut être effectuée en utilisant:

- doAuthorization;
- doImmediateWalletPayment;
- doScheduledWalletPayment.

Les paramètres spécifiques à ces demandes sont précisés dans le tableau ci-dessous.

linkedTransactionID	C	Valeur retournée dans la réponse à la première demande d'autorisation CIT dans le paramètre 'linkedTransactionId' (dans le getWebPaymentDetails si CIT en mode web). Si l'autorisation initiale est effectuée avant la mise en application des RTS SCA se référer à la description du ' Grand fathering ' Facultatif pour actions 128/129 avec utilisation d'un doImmediateWalletPayment ou doScheduledWalletPayment si le wallet a été créé avec la transaction de la 1ere échéance (Payline utilise le linkedTransactionID stocké lors de la création du wallet). Obligatoire dans les autres cas
authentication3DSecure	C	Valeur retournée dans la réponse à la première demande d'autorisation CIT dans le paramètre 'authentication3DSecure' (dans le getWebPaymentDetails si CIT en mode web). Absent si Grand fathering, Facultatif pour actions 128/129 . Obligatoire dans les autres cas

Objet Payment		
action	O	En fonction du code utilisé pour la commande (CIT): Si 122 ou 123 alors 123 ; Si 124 ou 125 alors 125 ; Si 128 ou 129 alors 129 ;
mode	O	CPT
amount	O	Montant de l'échéance (prime sur recurring.amount)
cumulated Amount	C	Somme des montants déjà autorisés. Absent pour 'autres paiements récurrents'
Objet Recurring		
billingRank	C	2 pour la 2 ^e échéance, 3 pour la 3 ^e , etc ... Obligatoire pour les codes action (122, 123, 124, 125) Facultatif pour les codes action (128, 129), valeur strictement supérieure à 1
autres champs		Mêmes valeurs que dans les appels précédents Facultatif pour les codes 128 et 129 Obligatoires dans les autres cas.

O : Obligatoire ; F: Facultatif ; C : Conditionnel

Montant authentifié

Le tableau ci-dessous précise le montant à fournir à la demande d'authentification en fonction du paiement

Paiement	Payment code	Montant authentifié
récurrents avec des échéances en nombre défini et de même montant	122 ou 123	Montant total: somme du montant des échéances
autres récurrents Paiement d'abonnement à un bien ou un service par prélèvements sur une carte enregistrée par le commerçant <ul style="list-style-type: none"> ▪ de montant fixe, variable, révisable; ▪ sans date de fin, tacite reconduction. 	128 ou 129	Montant de la première échéance. Quand le montant est variable ou ne peut être déterminé à l'avance indiquer un montant à 0.
échelonnés, NX, installments	124 ou 125	Montant total: somme du montant des échéances

Grand fathering

Ce paragraphe traite des paiements récurrents et Nx initiés avant l'application de la dsp2 et n'ayant pas pu récupérer auprès du serveur d'autorisation la référence d'autorisation initiale.

Le traitement de la première MIT sans identifiant de regroupement est spécifique.

Le marchand pour cette échéance :

- envoie la demande de paiement en utilisant comme identifiant de regroupement la valeur '*Pv4-999999999999'
- récupère l'identifiant de regroupement présent dans la réponse,
- si cet identifiant est différent de '*Pv4-999999999999', le mémorise et l'utilise comme identifiant de regroupement dans les MIT ultérieures.

Le paramètre authentication3DSecure n'est jamais envoyé.

Changement et renouvellement de carte

Ce paragraphe traite du cas du changement de carte pour un paiement récurrent ou n fois en cours.

Le changement est effectué par l'acheteur sur les pages du commerçant.

Le commerçant propose à son acheteur de venir modifier ses données de paiement.

Il lui présente une demande de paiement récurrent de montant variable de durée indéterminée (code 128).

Il récupère l'identifiant de regroupement (linkedTransactionId) et le paramètre authentication3DSecure .

Il peut ensuite reprendre le recouvrement des échéances en utilisant le nouvel identifiant de regroupement et le nouveau paramètre authentication3DSecure .

Pages associées

- [3D Secure 2.0 - Comply with DSP2](#)
- [3DSv2 - Acquirer exemption](#)
- [3DSV2 - Direct Interface](#)
- [3DSV2 - Direct Interface - Authentication and Authorization](#)
- [3DSV2 - Direct Interface - JSON container format](#)
- [3DSV2 - Direct Interface - Recurring payments](#)
- [3DSV2 - Direct Interface - SDK Mobile partner](#)
- [3DSV2 - Functionalities](#)
- [3DSv2 - Increase frictionless](#)
- [3DSV2 - La liste des impacts Codes retour](#)
- [3DSV2 - Mail Order / Telephon Order \(MO /TO\) Payments](#)
- [3DSv2 - Webpage Interface](#)
- [Codes - ChallengeCancelInd](#)
- [Codes - ChallengeInd](#)
- [Codes - threeDSReqPriorAuthMethod](#)