

## *PROTOCOL CN – CHPN*

### *CONCERT – CHèque Protocole Normalisé*

## Document N° : 041 - NATIXIS

ASSOCIATION DÉCLARÉE RÉGIE PAR LA LOI DU 1<sup>er</sup> JUILLET 1901, N°89 / 3905  
8, RUE DE CROUY - 41220 SAINT LAURENT NOUAN - TÉL : 02 54 87 06 12 - FAX : 02 54 87 06 12  
[www.concert.asso.fr](http://www.concert.asso.fr)  
[contact@concert.asso.fr](mailto:contact@concert.asso.fr)

“Le code de la propriété intellectuelle n’autorisant , aux termes des paragraphes 2 et 3 de l’article L.122.5, d’une part, que les “copies ou reproductions strictement réservées à l’usage privé du copiste et non destinées à une utilisation collective” et, d’autre part, sous réserve de la mention du nom de l’auteur et de la source que les “analyses et les courtes citations justifiées par le caractère critique, polémique, pédagogique, scientifique ou d’information” toutes représentation ou reproduction intégrale ou partielle, faite sans le consentement de l’auteur ou de ses ayants droit ou ayant cause, est illicite (article /122.4). Cette représentation ou reproduction, par quelque procédé que ce soit, constituerait donc une contrefaçon sanctionnée par les articles L335.2 et suivants du Code de la propriété intellectuelle”.

## SUIVI DES REVISIONS

Date	Libellé des modifications	Version concernée	Pages	Ajout/ Suppression/ Correction
12/2006	Cette version inclut l'aide à l'implémentation en annexe 2 Annexe 2 – Suppression de l'exigence 3, seules les exigences 1, 2 et 4 sont facultatives Champ 39 : Correction de l'utilisation 10 : Blanc. Ajout du téléparamétrage.	3.1 3.1 3.1	23	A S C
10/2008	Modification définition "Code d'accès VERIFIANCE" dans le glossaire Précision de l'utilisation de la RFC 1086 aménagée CON-CERT au lieu de RFC 1086	3.1 3.1	2 11/17	C C
La version 3.2 permet de prendre en compte deux compteurs qui viennent en complément de la réponse couleur FNCI <b>Une compatibilité ascendante est assurée entre la version 3.1 et 3.2.</b>				
13/01/2010	Modification du champ 44 (Ajout d'un commentaire)	3.2	23	A
13/01/2010	Prise en compte protocole version 3.2.	3.2	24	C
13/01/2010	Prise en compte protocole version 3.2.	3.2	34	C
13/01/2010	Prise en compte protocole version 3.2.	3.2	35	C
13/01/2010	Prise en compte protocole version 3.2.	3.2	38	C
13/01/2010	Ajout d'un sommaire pour annexe 1	3.2	42	A
13/01/2010	Modification du paragraphe A.1.1	3.2	43	C
13/01/2010	Modification du paragraphe A.1.2	3.2	43	C
13/01/2010	Modification du paragraphe A1.4	3.2	46	A
13/01/2010	Modification du paragraphe A1.4.1	3.2	46	A
13/01/2010	Modification du paragraphe A1.4.2	3.2	47	A
13/01/2010	Paragraphe A1.4.3 (Recto du chèque)	3.2	48	Remplacement
13/01/2010	Paragraphe A1.4.4 (Verso du chèque)	3.2	49	Remplacement
13/01/2010	Modification du paragraphe A1.4.5	3.2	49	A
13/01/2010	Ajout du paragraphe : A1.4.6 Les compteurs "C1, C2" et "C3, C4"	3.2	50	A
13/01/2010	Paragraphe A1.4.7 (Recto du chèque)	3.2	51	Remplacement
13/01/2010	Paragraphe A1.7.1 (Recto du chèque)	3.2	53	Remplacement
25/11/2014	Paragraphe 4.3.3 champ 44	3.3	23	Modification

25/11/2014	Annexe 1 A1.4.1 caractères 21 et 22, compteurs de consultation C5, C6	3.3	3	Modification
25/11/2014	Annexe 1 A1.4.2 caractères 21 et 22, compteurs de consultation C5, C6	3.3	5	Modification
25/11/2014	Annexe 1 A1.4.5 caractères 21 et 22, compteurs de consultation C5, C6	3.3	7	Modification
25/11/2014	Annexe 1 A1.4.6 Compteurs C5, C6	3.3	9	Modification
06/05/2015	Champs 45 : Pos 4 à 6 CN – CHPN : 330 pour le CN-CHPN V3.3	3.3	25	Modification
06/05/2015	Numéro de version protocolaire : PI06 : Ajout valeur : x « 33 » correspond à la version du protocole CN – CHPN : V3.3	3.3	39	Modification

## GLOSSAIRE

Libellé	Définition
APDU	Application Protocole Data Unit. Élément de protocole de niveau applicatif transportant les messages applicatifs (message 9100, 9110, 9300, 9310)
API standard ouverte	API (Application Programming Interface) dont les spécifications sont publiques et standardisées (Par exemple, XFS).
Applications métier	Ensemble d'applications nécessaires au point d'encaissement : acceptation " CB ", encaissement, traitement chèque, applications privatives, fidélité
CBCom	Protocole émis par le GIE Cartes Bancaires décrivant le niveau pseudo session.
Chiffrement fort	Algorithme symétrique garantissant une force au moins égale à celle du TDES avec clés de longueur double de 112 bits utiles. Algorithme asymétrique garantissant une force au moins égale à celle du RSA avec clés de longueur 1024 bits. Ces définitions pourront être revues en fonction des évolutions technologiques ou cryptographiques.
Chiffrement par domaine	Méthode de chiffrement utilisée pour protéger les données à l'intérieur d'un domaine ; N'est pas nécessairement celle qui est utilisée dans un domaine différent. Il est de la responsabilité des acteurs d'effectuer déchiffrement et chiffrement dans des enceintes cryptographiques.
CHPN	CHèque Protocole Normalisé
CHPR	CHèque PProtocole de traitement des images
CMC7	Caractère Magnétique Codé à 7 éléments : Norme de représentation de caractères (64 possibilités), utilisé principalement sur les chèques bancaires.
Code d'accès	Le terme « Code d'accès » désigne, dans ce document, l'identification de l'abonné (ou IDCF, identification du client final) (ou encore numéro d'abonné) se trouvant dans le champ 42 du protocole CN - CHPN.
Code d'Accès VÉRIFIANCE	Code délivré lors de la souscription à un contrat Vérifiance et permettant l'accès au service de consultation du Fichier National des Chèques irréguliers (FNCI).
CONCERT	COMité de Normalisation et de CERTification des Terminaux monétiques CONCERT : Siège Social et Secrétariat : 8, rue de Crouy 41220 ST LAURENT NOUAN – Tél/Fax. : 02 54 87 06 12 - <a href="http://www.concert.asso.fr">www.concert.asso.fr</a> - <a href="mailto:contact@concert.asso.fr">con-tact@concert.asso.fr</a>
Chèque de démonstration	Formule ressemblant à un chèque mais permettant de se connecter à l'environnement de démonstration de Vérifiance.
CV	Circuit Virtuel.
DCB	Décimal Codé Binaire (Binary Coded Decimal ou BCD en anglais). Méthode de codification dans laquelle chaque chiffre est représenté sur 4 bits (1/2 octet).
EBCDIC	Extended Binary Coded Decimal Interchange Code. Jeu de caractères utilisé sur certains ordinateurs.
ELC	Editeur Lecteur de Chèques
FNCI	Fichier National des Chèques Irréguliers
IDC	Identifiant Du Centre (Informatique)
IDCF	Identifiant du Client Final (ou numéro d'abonné)
Interface réseaux multiples	Systèmes d'acceptation équipés d'interfaces réseaux multiples qui disposent de plus d'une connexion réseau. Il s'agit par exemple de systèmes d'acceptation connectés avec deux adresses IP ou encore de systèmes d'acceptation possédant à la fois une connexion IP et une connexion X25.

Internet	Ensemble de réseaux de toutes tailles interconnectés entre eux. Ce réseau global est basé sur des protocoles de communication de type TCP/IP.
IPDU	Intermédiaire Protocole Data Unit Élément de protocole de niveau pseudo-session (intermédiaire)
ISO	International Standards Organization
LRMC	Voir RLMC
Maintenance monétique	Toute intervention permettant de modifier les caractéristiques, données ou application utilisées dans une opération monétique. Ces interventions nécessitent la présence ou l'assistance d'une personne qualifiée et habilitée à intervenir sur la partie monétique du point de vente.
Mandataire	Le terme « mandataire » désigne toute société qui reçoit mandat de bénéficiaires de chèques de vérifier, pour leur compte, la régularité de l'émission des chèques qui leur sont présentés en paiement. Le Mandataire propose, dans le cadre d'une offre qui apporte une valeur ajoutée spécifique, un service technique d'accès au fichier. Le Mandataire est enregistré par la BANQUE DE France après signature de « La Charte du Mandataire » (document contractuel régissant ses droits et obligations). On compte actuellement trois types de Mandataires : Les SSII qui vendent des prestations de traitements monétiques ; les sociétés de garantie de chèques, qui proposent une assurance sur l'encaissement des chèques et certains réseaux bancaires.
Mantis	Société qui exploite le FNCI (Fichier National des Chèques Irréguliers) pour le compte de la Banque de France et en assure la promotion sous le nom de marque RESIST (jusqu'au 31/12/06) ou Vérifiance (A partir du 01/01/07) Société MANTIS SA, 24, rue des Jeûneurs 75002 PARIS – Tél. : 01 44 76 90 90 – Fax : 01 42 36 32 16.
NAS	Network Access Server
PAD	Packet Assembler Disassembler (Assembleur Désassembleur de Paquets)
Point d'accès	C'est le correspondant Transpac appelé. C'est le point d'accès au système serveur chèque.
Prestataire de service de routage	Acteur utilisant les données applicatives monétiques de la transaction pour fournir un service à valeur ajoutée à l'acquéreur et/ou à l'accepteur
Protocole de communication ouvert	Tout type de protocole standardisé et ouvert permettant d'interconnecter des réseaux hétérogènes. Cette dénomination vise ici en particulier l'ensemble des protocoles applicatifs et réseaux de la famille TCP/IP
Réseau sans fil	Tout type de réseau basé sur la transmission d'ondes radio. Il s'agit : <ul style="list-style-type: none"> <li>- Du réseau GSM / GPRS</li> <li>- Tous les réseaux de la famille 802.11 (ex : WiFi).</li> <li>- Des réseaux Bluetooth</li> <li>- Etc...</li> </ul> Cette liste pourra être révisée.
RLMC	Recomposition de la Ligne Magnétique du Chèque
RTC	Réseau Téléphonique Commuté
RUF	Réservé Usage Future
Serveur	Le terme « Serveur » désigne, dans ce document, tout Fournisseur de Services qui met à disposition d'utilisateurs de solutions monétiques, des moyens d'accès télématiques permettant la transmission et la réception d'informations concernant les chèques reçus en paiement.
Solution monétique	Le terme « solution monétique » définit toute installation faisant intervenir un concentrateur et/ou un TPE/TPV et/ou lecteur de chèques.
SSL	Secure Socket Layer. Protocole développé par Netscape (en collaboration avec Mastercard, Bank on America, MCI et Silicon Graphics) pour la transmission cryptée sur les réseaux TCP/IP. Il met en place un lien entre deux parties opérationnelles au moyen de n'importe quel protocole d'application.

TCP/IP	Transmission Control Protocol / Internet Protocol
Téléchargement	Transfert du noyau ou de l'application vers un système d'acceptation
Téléparamétrage	Transfert de données de paramétrage vers un système d'acceptation
TGR	Temporisation de garantie de réponse
TIE	Temporisation de surveillance d'activité de l'équipement par le point d'accès
TNR	Temporisation de non réponse
TPE	Terminal de Paiement Électronique
TRANSPAC	Réseau français de transmission, par paquets à haut débit
Vérifiance	Appelation du service de consultation du FNCI à partir du 1 <sup>er</sup> janvier 2007 : Vérifiance-FNCI-Banque de France
X25	Norme de télécommunication pour le réseau public de commutation de paquets.

## **REFERENCES EXTERNES**

Libellé	Référence	Version
RFC 1035	<a href="http://www.ietf.org/rfc/rfc1035.txt?number=1035">http://www.ietf.org/rfc/rfc1035.txt?number=1035</a> )	
RFC 1086	<a href="http://www.ietf.org/rfc/rfc1086.txt?number=1086">http://www.ietf.org/rfc/rfc1086.txt?number=1086</a> )	
Aide à l'implémentation		
Norme : “ Formule de chèques payable en France ”	NF K11-111	2.2.
Exigences sécuritaires Groupement des Cartes Bancaires		1.5
ISO 8583		1993
Norme ISO 4217	Codes ISO numériques	

## **HISTORIQUE DES VERSIONS**

<b>Version</b>	<b>Nombre de pages</b>	<b>Date de diffusion</b>
1.0	52 pages	06/10/1993
2.0	47 pages	19/06/1997
2.1	24 pages	Octobre 1998
2.2	26 pages	Octobre 2005
3.0	56 pages	Octobre 2006
3.1	62 pages	12/12/2006
3.1	62 pages	14/10/2008
3.1.	62 pages	20/05/2009
3.2.	64 pages	01/04/2010
3.3.	64 pages	25/11/2014



## SOMMAIRE

<b>1.</b>	<b>INTRODUCTION.....</b>	<b>10</b>
<b>2.</b>	<b>PARAMÈTRES CHÈQUES.....</b>	<b>12</b>
<b>3.</b>	<b>CONNEXION .....</b>	<b>15</b>
3.1.	MODE D'ACCES AU CENTRE .....	15
3.2.	CARACTERISTIQUES PHYSIQUES DE LA TRANSMISSION .....	16
3.3.	CARACTERISTIQUES DES CONVERSIONS IP/X25 OU X25/IP .....	16
3.3.1.	Généralités .....	16
3.3.2.	Conversion X25/IP .....	16
3.3.3.	Conversion IP/X25 .....	16
<b>4.</b>	<b>PROTOCOLE APPLICATIF CN - CHPN (CONSULTATION ET GARANTIE CHEQUES) .....</b>	<b>16</b>
4.1.	INTRODUCTION .....	16
4.2.	TERMINOLOGIE .....	16
4.2.1.	Activité 16 .....	
4.3.	NIVEAU APPLICATION .....	17
4.3.1.	Structure des messages .....	17
4.3.2.	Règle de codage et formatage des données.....	18
4.3.3.	Dictionnaire des données .....	18
4.3.4.	Activité de demande de consultation FNCI et de garantie .....	30
4.3.5.	Traitement des erreurs .....	32
4.4.	NIVEAU PSEUDO-SESSION .....	33
4.4.1.	Présentation .....	33
4.4.2.	Gestion des temporisations .....	33
4.4.3.	Spécifications des échanges.....	35
4.4.4.	Personnalisation de la description issue de CBCom .....	37
<b>5.</b>	<b>OPÉRATIONS AYANT TRAIT AU LECTEUR.....</b>	<b>41</b>

## **1. INTRODUCTION**

La version 3.0 du protocole CN – CHPN a été élaborée en septembre 2006 pour répondre aux demandes suivantes :

- Possibilité de faire du TCP/IP
  - . Ajout de précisions (et d'un schéma) dans les modes de connexion aux serveurs
  - . Précisions sur l'utilisation du standard RFC 1086 aménagée CONCERT
  - . Ajout du champ 46
  - . Précisions quant à la gestion des longueurs en IP et X25 vis-à-vis de CBCom
  - . Ajout de l'annexe 2
- Notion de référence des matériels par Vérifiance
  - . Ajout de nouvelles valeurs dans le champ 39
  - . Ajout du champ 45
- Incorporation de l'aide à l'implémentation (annexe 1).
- Corrections ou adaptations d'usage
  - . Compléments apportés au glossaire
  - . Remplacement de Resist par Vérifiance
  - . Modification du tableau des paramètres chèque
  - . Suppression des références au franc (remplacées par des références à l'euro) – champ 04 et 49
  - . Précision sur les valeurs du champ 22
  - . Précision sur les valeurs du champ 32
  - . Précision sur les valeurs du champ 35
  - . Précision sur les valeurs du champ 43
  - . Précision sur les valeurs du champ 44
  - . Mise à jour du tableau de description des messages
  - . Suppression de l'utilisation du PI05 (néanmoins conservé pour comptabilité)
  - . Ajout du PI04 (version CBCom)
  - . Précision sur la valeur du PI06
  - . Mises à jour du tableau d'utilisation des différents PI en CBCom
- Réintégration du téléparamétrage
  - . Ajout du champ 47
  - . Ajout du champ 48.

Il regroupe la version 1.0, réf. 035 du 6/10/93, et l'additif pour prendre en charge l'euro d'octobre 1998. Il constitue la synthèse des travaux menés par le CONCERT dans le domaine du chèque bancaire.

Les différentes possibilités de prise en compte du chèque, avec une exploitation automatisée sont abordées :

- consultation FNCI (Fichier National des Chèques Irréguliers),
- garantie chèque

Dans ce document sont présentés les protocoles utilisés pour le dialogue entre les terminaux associés et les centres de consultation FNCI et les centres de garantie chèques.

Le terme "TPE" (Terminal de Paiement Électronique) sera employé pour désigner indifféremment un terminal autonome, des terminaux grappés ou un concentrateur (mono ou multi-commerces) de terminaux.

Le TPE, avec le lecteur de chèque associé, a toujours l'initiative de l'appel quelle que soit la nature de cet appel.

Il peut demander les fonctions suivantes :

- en liaison avec le FNCI, la consultation du fichier des chèques irréguliers pour connaître s'il y a présence du chèque.
- en liaison avec le centre de garantie chèques, la demande de garantie du chèque.

Il est à noter que dans ce document, ces deux fonctions primordiales ont été considérées comme indépendantes l'une de l'autre et bien évidemment indépendantes de la partie carte bancaire.

En effet, la banque du commerçant ou/et le commerçant peuvent être intéressés par une ou deux de ces fonctions.

De plus, le commerçant aura pour les fonctions

- consultation FNCI,
- garantie chèques

la possibilité de choisir à chaque chèque s'il désire ou non accéder à ces services.

Le TPE s'appuiera pour échanger les informations avec les centres serveurs chèques sur ce protocole CN - CHPN (CHèque Protocole Normalisé) pour la consultation FNCI et la garantie de chèques.

Le lecteur de chèque (LC) peut avoir les trois fonctions suivantes

- lecture de la piste CMC7,
- écriture d'endos (recto ou verso) de une ou plusieurs lignes,
- postmarquage du montant CMC7

Les deux dernières fonctions sont locales et ne sont pas concernées par ce document.

L'application chèques est constituée de 3 fonctions indépendantes qui sont :

- la télécollecte des images chèques (non décrite dans ce document),
- la demande de consultation FNCI,
- la demande de garantie.

Suivant le paramétrage local du terminal, ces fonctions peuvent ou non être activées.

Chacune de ces fonctions peut faire appel à un serveur spécifique. Il convient donc d'associer des paramètres propres à chacun des serveurs associés aux fonctions présentes sur le terminal.

Lors de la première initialisation, le paramétrage du terminal sera effectué localement.

Des mécanismes similaires à ce qui peut déjà exister sur le Système Monétique (par exemple CB) ont été privilégiés en terme d'implémentation : paramétrage, exigences sécuritaires ...

## **2. PARAMÈTRES CHÈQUES**

Pour le commerçant, le choix doit être limité à chaque fois qu'il passe un chèque dans son lecteur, soit il ne fait rien, soit il fait de la consultation, soit il fait de la garantie.

Il est à noter que le "garantisser" peut tout à fait accéder au FNCI : ceci implique que le choix entre consultation ou garantie doit être exclusif dans le cas d'une transaction.

Le fait de passer le chèque permet d'enregistrer celui-ci dans la mémoire de la machine. Cette mémoire peut, éventuellement, être utilisée pour la partie télécollecte (si le terminal dispose de cette fonction).

Les paramètres internes, rentrés à la main lors de l'initialisation de la machine, sont les suivants :

- consultation: OUI/NON.
- garantie: OUI/NON,

Les paramètres relatifs aux chèques sont insérés dans la phase initialisation du terminal de paiement électronique off-line.

PARAMETRES				
	GENERAUX	CONSULTATION DU FNCI	GARANTIE CHEQUE	TELECOLLECTE CHEQUE(*)
Nom du bénéficiaire		I	I	A
Lieu de paiement		I	I	A
Numéro compte commerçant		I	I	A
Texte à éditer sur le bordereau		I	I	A
Postmarquage n° cpte sur bordereau		I	I	A
Postmarquage chèque		I	I	A
Rejet chèque mal lu		I (1)	I	C
Top Consultation FNCI		B	I	I
Top Garantie		I	B	I
Code d'accès Vérifiance		A	I	I
Code d'accès garantisseur		I	A	I
<b>Paramètres d'accès au site nominal du service de téléchargement</b>				
Type d'adressage réseau – site nominal		A	A	A
Adresse réseau du service – site nominal		A	A	A
Adresse réseau du DNS – site nominal		A	A	A
Nom de domaine – site nominal		A	A	A
Numéro de téléphone d'accès au réseau – site nominal		A	A	A
Nature du PAD – site nominal		A	A	A
Nombre maximum d'essais d'appel		A	A	A
Délai d'attente entre deux appels (en secondes)		A	A	A
Heure locale d'appel automatique (hhmm)		A	A	A
Date locale d'appel automatique (AAMMJJ)		A	A	A
Nombre maximum de reprises		A	A	A
Eléments de contrôle d'accès au système de téléchargement		A	A	A
Référence du logiciel à télécharger		A	A	A
Les données d'appel utilisateur (sans le séparateur D)		A	A	A
<b>Paramètres d'accès aux sites de secours du service de téléchargement</b>		A	A	A
Type d'adressage réseau – sites de secours		D	D	D
Adresse réseau du service – sites de secours		D	D	D
Adresse réseau du DNS – sites de secours		D	D	D
Nom de domaine – sites de secours		D	D	D
Numéro de téléphone d'accès au réseau – sites de secours		D	D	D
Nature du PAD – sites de secours		D	D	D
Nombre maximum d'essais d'appel		D	D	D
Délai d'attente entre deux appels (en secondes)		D	D	D

PARAMETRES				
	GENERAUX	CONSULTATION DU FNCI	GARANTIE CHEQUE	TELECOLLECTE CHEQUE(*)
Heure locale d'appel automatique (hhmm)		D	D	D
Date locale d'appel automatique (AAMMJJ)		D	D	D
Nombre maximum de reprises		D	D	D
Eléments de contrôle d'accès au système de téléchargement		D	D	D
Référence du logiciel à télécharger		D	D	D
Données d'appel utilisateur (sans le séparateur D)		D	D	D
<b>Paramètres d'accès au site nominal de garantie ou de consultation FNCI</b>				
Type d'adressage réseau – site nominal		A	A	A
Adresse réseau du service – site nominal		A	A	A
Adresse réseau du DNS – site nominal		A	A	A
Nom de domaine – site nominal		A	A	A
Numéro de téléphone d'accès au réseau – site nominal		A	A	A
Nature du PAD – site nominal		A	A	A
Les données d'appel utilisateur (sans le séparateur D)		A	A	A
<b>Paramètres d'accès aux sites de secours de garantie ou de consultation FNCI</b>		A	A	A
Type d'adressage réseau – sites de secours		D	D	D
Adresse réseau du service – sites de secours		D	D	D
Adresse réseau du DNS – sites de secours		D	D	D
Nom de domaine – sites de secours		D	D	D
Numéro de téléphone d'accès au réseau – sites de secours		D	D	D
Nature du PAD – sites de secours		D	D	D
Données d'appel utilisateur (sans le séparateur D)		D	D	D
Seuil d'appel		A	A	I
N° de terminal		B	B	B
Mise à l'heure		A	A	A
Code banque	B			

Remarque générale :

- Les 3 applications " Consultation FNCI " (protocole CHPN), " Garantie chèque " (protocole CHPN) et " Télécollecte Chèque " (protocole CHPR) gèrent leurs paramètres indépendamment les uns des autres. Ceci reste vrai par rapport aux éventuelles applications CB (protocole CB2A) qui seraient présentes sur le même terminal.

(A) : Paramètres saisis localement et susceptibles d'être modifiés par le téléparamétrage de l'application

(B) : Paramètres saisis localement et non modifiables par téléparamétrage

(C) : Paramètres saisis localement et modifiables par l'application de télécollecte chèque (CHPR)

(D) : Paramètres non saisis localement et susceptibles d'être modifiés par le téléparamétrage de l'application

(I) : Paramètre inexistant pour cette application

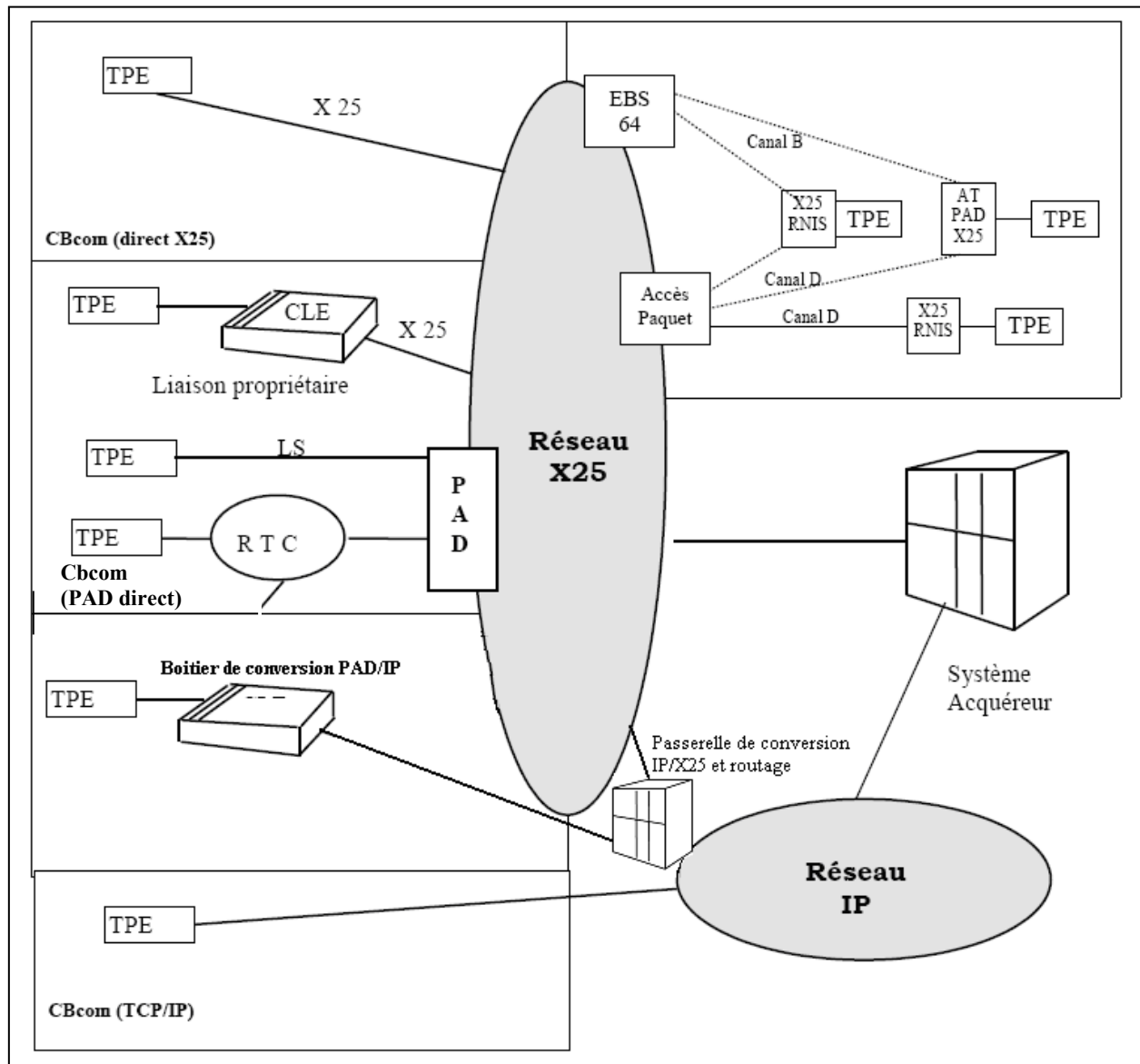
(\*) : Pour information, par rapport à ce qui existe à ce jour. La liste exhaustive des paramètres CHPR est à consulter dans la dernière version du protocole CN – CHPR.

(1) : Au moindre caractère remplacé par un A (caractère mal lu), le serveur Vérifiance répondra "blanc" (voir champ 39).

### 3. CONNEXION

#### 3.1. Mode d'accès au centre

Les modes d'accès possibles aux centres serveurs chèques sont, à ce jour, RTC et TRANSPAC via un PAD, TRANSPAC, lignes spécialisées, IP.



Remarque : Le GPRS est considéré comme un accès IP.

### **3.2. Caractéristiques physiques de la transmission**

Dans le cas d'un raccordement via un PAD TRANSPAC, les caractéristiques physiques de la connexion sont identiques à celles décrites dans le protocole CBCOM V1.3. du GIE CB.

### **3.3. Caractéristiques des conversions IP/X25 ou X25/IP**

#### **3.3.1. Généralités**

Lorsqu'une conversion est nécessaire, il existe alors une passerelle qui va servir de convertisseur entre les 2 mondes X25 et IP. Le protocole de dialogue avec cette passerelle est basé sur l'utilisation de la RFC 1086 aménagée CONCERT.

#### **3.3.2 Conversion X25/IP**

Un boîtier de conversion PAD/IP est rajouté si le commerçant souhaite que toutes les communications issues de son système monétique passent par un réseau IP (Internet, GPRS, IPSec ....) mais que son Système Monétique ne permet pas un accès direct à un réseau IP.

#### **3.3.3 Conversion IP/X25**

Une telle conversion est nécessaire lorsque les serveurs accédés par les différentes applications présentes sur le Système Monétique ne disposent pas d'un accès IP.

## **4. PROTOCOLE APPLICATIF CN - CHPN (CONSULTATION ET GARANTIE CHEQUES)**

### **4.1. Introduction**

Le protocole CN - CHPN (Chèque Protocole Normalisé) est basé sur la norme ISO 8583.

### **4.2. Terminologie**

#### **4.2.1. Activité**

Une activité se définit comme le traitement d'une transaction dans un temps imparti, appelé temps de réponse.

Dans le cadre de ce document, seules les activités de demandes de garantie et de consultation FNCI sont traitées.

Une transaction est composée, dans le cas normal de fonctionnement, d'un message question et d'un message réponse.

Le non-respect de cette règle correspond au cas anormal où un message question n'est pas acquitté par un message réponse.

Un message (APDU) est une représentation syntaxique des données échangées entre les entités applicatives de l'équipement demandeur et du point d'accès au système serveur chèque.

Chaque message est caractérisé par un identifiant qui figure en en-tête des données le constituant.



### **4.3. Niveau application**

#### **4.3.1. Structure des messages**

##### **a) Présentation**

Les messages (APDU) ont la structure suivante

Identifiant	Bitmap	Champs de données
-------------	--------	-------------------

##### **b) Identifiant**

Il est composé de 4 digits codés DCB.

Les identifiants utilisés dans le cadre de ces spécifications sont les suivants :

9100 : Demande de garantie de chèque

9110 : Réponse à la demande de garantie

9300 : Demande de consultation FNCI

9310 : Réponse à la demande de consultation FNCI

##### **c) Champ bitmap**

Chaque bitmap est composée de 64 bits numérotés de gauche à droite. Deux bitmaps sont définies. La première est obligatoire. La deuxième est optionnelle. Le premier bit de la première bitmap spécifie la présence ou l'absence d'une seconde bitmap. Dans chaque bitmap, un bit à 1 exprime la présence du champ associé, un bit à zéro son absence.

0	0	1	...	1	0
1	2	3		63	64

##### **d) Champ de données**

La numérotation des bits s'effectue de gauche à droite. Le premier bit est réservé.

A chaque champ de données correspond un numéro.

A l'intérieur d'un message, les champs apparaissent par ordre croissant de numéro de champ.

#### 4.3.2. Règle de codage et formatage des données

ABREVIATIONS	TYPE de DONNEES	CODAGE	Longueur d'un élément de données
n	Caractères numériques	DCB	½ octet
an	Caractères alphanumériques (1)	EBCDIC	1 octet
ans	Caractères alphanumérique et spéciaux de 0x20 à 0x7F (2)	EBCDIC	1 octet
b	Données binaires		1/8 octet
ansb	Champ mixte ans et b	EBCDIC	
anA	Caractères alphanumériques (1)	ASCII	1 octet
ansA	Caractères alphanumérique et spéciaux de 0x20 à 0x7F (2)	ASCII	1 octet
ansbA	Champ mixte ans et b	ASCII	

(1) 0-9, a-z, A-Z, espace

(2) 0-9, a-z, A-Z, espace, <, >, :, %, ?, !, =, \*, \$, £, &, «, ' , +, -, .

#### 4.3.3. Dictionnaire des données

##### a) Présentation

- Chaque champ de données utilisé dans ce document est décrit sous la forme de :
  - numéro et nom
  - format
  - utilisation
  - structure
- La liste des champs présentés dans le dictionnaire est établie par ordre croissant de numéro de champ.
- Le format des champs de données est exprimé au moyen de deux principaux critères
  - le type
  - la longueur: elle exprime la longueur réelle des variables hors codage
  - ex : n6 désigne une variable numérique de longueur 6 codé en DCB sur 3 octets
- Signes particuliers :
 

AA : années	JJ : jour	mm : minute
MM : mois	hh : heure	ss : seconde
- Champ numérique (n)
 

Dans le cas d'un champ de longueur fixe, les caractères sont cadrés à droite avec un zéro en en-tête, en cas de longueur **impaire**. La position 1 est à gauche.
- Champ longueur variable (exmple : 2, 32, 35, 44, 47, 48) :
 

Devant les octets correspondant à la variable, un ou 2 octets précisent la longueur de la zone réelle. Si la longueur de champ est inférieure à 256, il y a un octet de longueur, sinon, il y a 2 octets de longueur. Si la longueur est paire dans un champ codé en DCB, le zéro de gauche est significatif. Si la longueur est impaire dans un champ codé en DCB, la variable est cadrée à droite et complétée par un zéro à gauche qui est non significatif.

Ex : variable de longueur 4, on aura: 04 xx xx  
variable de longueur 5, on aura: 05 0x xx xx

b) Liste des champs de données

Champ 1

- Définition : Extension de la bitmap
- Messages : 9100, 9110, 9300, 9310
- Format : b 64
- Longueur : 64 bits soit 8 octets

Champ 2

- Définition : Identification du tireur
- Messages : 9100, 9110, 9300, 9310
- Format : n ... 19
- Longueur : un octet binaire, puis jusqu'à 19 éléments
- Non utilisé (numéro de compte éventuel).

Champ 3

- Définition : Code de traitement
- Messages : 9100, 9110, 9300, 9310
- Format : n 6
- Longueur : 6 digits soit 3 octets
- Structure :
  - Pos 1 et 2 : spécifications de la transaction
    - 00 = achat de biens et de services
    - 01 = opération de retrait (cash advance)
  - Pos 3 et 4 : "00"
  - Pos 5 et 6 : "00"
- Exemple : demande de garantie de paiement. Champ 3 : "000000"

Champ 4

- Définition : Montant de la transaction
- Messages 9100, 9110, 9300, 9310
- Format : n 12
- Longueur 12 digits soit 6 octets
- Utilisation : Le montant est exprimé dans l'unité monétaire mineure spécifiée dans le champ 49 en centièmes d'euro si champ 49= « 978 »

Champ 7

- Définition : Date et heure du serveur
- Messages: 9110, 9310
- Format : n 10 sous la forme MMJJhhmmss
- Longueur : 10 digits soit 5 octets
- Utilisation : date et heure auxquelles le message est émis.

#### Champ 11

- Définition : Identification de la transaction
- Messages : 9100, 9110, 9300, 9310
- Format : n 6
- Longueur : 6 digits soit 3 octets
- Utilisation : ce champ, géré par l'équipement demandeur, permet de référencer de manière unique la transaction
  - Pos 1 – 2 : non utilisé (00). Cet emplacement était auparavant utilisé par le numéro logique du terminal qui se trouve maintenant dans le champ 41
  - Pos 3 – 6 : numéro séquentiel de la transaction

#### Champ 12

- Définition : Heure locale de la transaction
- Messages : 9100, 9110, 9300, 9310
- Format : n 6 sous la forme hhmmss
- Longueur : 6 digits soit 3 octets

#### Champ 13

- Définition : Date locale de la transaction
- Messages : 9100, 9110, 9300, 9310
- Format : n 4 sous la forme MMJJ
- Longueur : 4 digits soit 2 octets

#### Champ 18

- Définition : Type d'activité
- Messages : 9100, 9300
- Format : n 4
- Longueur : 4 digits soit 2 octets
- Utilisation : non utilisé, contient 9999

#### Champ 22

- Définition : Capacité de lecture
- Messages : 9100, 9300
- Format : n 3
- Longueur : 3 digits soit 2 octets
- Structure : 0a bc
  - Pos a et b : 01 = saisie manuelle de la ligne CMC7 et clé RLMC non contrôlée  
02 = saisie manuelle de la ligne CMC7 et clé RLMC contrôlée  
04 = lecture automatique de la ligne CMC7
  - Pos c : 2 = non utilisé

#### Champ 25

- Définition : Condition d'émission de la transaction
- Messages : 9100, 9300
- Format : n 2
- Longueur : 2 digits soit 1 octet
- Utilisation :
  - 00 = présence du client
  - 01 = client non présent

#### Champ 32

- Définition : Identification de l'organisme demandeur
- Messages : 9100, 9110, 9300, 9310
- Format : n ... 11
- Longueur : 1 octet binaire puis jusqu'à 11 éléments (maxi 7 octets)
- Utilisation : identifie la banque commerçant
- Structure :
  - pos 1 à 6 : valeur 0
  - pos 7 à 11 : code banque

#### Champ 35

- Définition : Piste CMC7
- Messages : 9100, 9110, 9300, 9310
- Format : n ... 35
- Longueur : un octet binaire puis jusqu'à 18 octets
- Exemples :
  - Chèque bancaire : un octet (0x23), puis 18 octets (zéro à gauche non significatif)

S1 --> B

S3 --> D

S5 --> F

Les caractères mal lus seront codés A.

Exemple de codification :

Zone 4 : numéro de chèque								Zone 3 : Codes interbancaires												Zone 2 : codes intérieurs														
S								S	1	1	1										S	1	1	1									S	
3	7	6	5	4	3	2	1	3	2	1	0	9	8	7	6	5	4	3	2	1	5	2	1	0	9	8	7	6	5	4	3	2	1	1

N.B. : la zone 1 correspond au montant, en cas de post-marquage.

#### Champ 37

- Définition : Identifiant du centre informatique
- Messages : 9100, 9300
- Format : an 12
- Longueur : 12 caractères soit 12 octets
- Utilisation : permet l'identification du centre informatique (=IDC) ou numéro d'abonné si demande directe.
- Structure :
  - pos 1 à 10 : identifiant fourni par Vérifiance
  - pos 11 et 12 : espaces

#### Champ 38

- Définition : Référence du garantisseur
- Message : 9110
- Format : an 6
- Longueur : 6 caractères soit 6 octets à gauche, complétés éventuellement par des espaces
- Utilisation : libre utilisation du garantisseur, information à éditer. Si la garantie est accordée, contient le numéro de garantie qui est imprimé sur le ticket et/ou sur le chèque.

#### Champ 39

- Définition : Code réponse du FNCI
- Messages : 9110, 9310
- Format : an 2
- Longueur : 2 caractères soit 2 octets
- Utilisation :
  - bb : Pas d'interrogation FNCI pour cette demande
  - 00 : Vert - Le chèque ne fait l'objet d'aucune interdiction
  - 01 : Orange - Alerte sur le compte
  - 02 : Rouge - Chèque irrégulier
  - 03 : Blanc - Chèque non référencé
  - 04 : Blanc - N° d'abonné incorrect (IDCF incorrect)
  - 05 : Blanc - Erreur serveur FNCI
  - 06 : Blanc - Piste CMC7 incorrecte
  - 07 : Blanc - IDC incorrect
  - 08 : Blanc - Matériel non référencé
  - 10 : Blanc - Service non disponible
  - 99 : Blanc - Transaction refusée

Dans le cas d'un message 9110 c'est la réponse indiquée dans le champ 40 qui est prioritaire sur celle du champ 39 pour définir le comportement du TPE.

#### Champ 40

- Définition : Code réponse du garantisseur
- Messages : 9110
- Format : an 3
- Longueur : 3 caractères soit 3 octets :
- Utilisation :
  - 000 : Transaction accordée
  - 001 : Transaction refusée
  - 002 : Demande non traitée de façon automatique (contre-appel)
  - 003 : Abonné inconnu (IDCF inconnu)
  - 004 : Transaction interdite
  - 005 : Service interdit pour cet abonné
  - 006 : Accord avec réserve...
  - 007 : IDC incorrect
  - 010 : Service indisponible.

#### Champ 41

- Définition : Identification du terminal
- Messages : 9100, 9110, 9300, 9310
- Format : ans 8
- Longueur : 8 caractères, soit 8 octets
- Structure :
  - pos 1, 2 et 3 : N° logique du terminal
  - pos 4 à 8 : espaces

#### Champ 42

- Définition : Identification de l'abonné (= IDCF - identifiant du client final)
- Messages : 9100, 9110, 9300, 9310
- Format : ans 15
- Longueur : 15 caractères soit 15 octets
- Utilisation : Les données sont cadrées à gauche, complétées éventuellement par des espaces
- Structure :
  - Position 1 : Type de codification:      « 0 » : SIRET (usage futur)  
  « 1 » : numéro d'abonné
  - Autres positions :
    - soit positions 2 à 15 : numéro de SIRET
    - soit positions 2 à 11 : numéro d'abonné
    - positions 12 à 15 : complétées avec des blancs

#### Champ 43

- Définition : Données complémentaires à la garantie
- Message : 9100, 9110
- Format : ans 40
- Longueur : 40 caractères soit 40 octets
- Valeurs par défaut : blancs
- Utilisation : Message de demande de garantie 9100
- \* Pos 1 à 4 : Mois année de naissance (mmaa),
- \* Pos 5 : Type de pièce d'identité :

1	Carte Nationale d'Identité
2	Permis de Conduire
3	Passeport
4	Carte de Résident
5	Carte de Séjour
6	Carte Européenne d'Identité
7	Permis de Conduire Européen
8	Passeport Union Européenne
9	Autre

- \* Pos 6 à 9 : Mois année de la pièce d'identité (mmaa)
- \* Pos 10 : Type de chèque  
(0 = chèque personne, 1 = chèque société)
- \* Pos 11 à 40 : Non utilisé - Blanc par défaut

Message de réponse à la garantie dans la 9110

- \* Pos 1 à 16 : Message en clair pour affichage sur la visu
- \* Pos 17 à 40 : Blancs

#### Champ 44

- Définition : Données complémentaires de réponse FNCI (\*)
- Message : 9110, 9310
- Format : ans20...25
- Longueur : un octet binaire puis jusqu'à 25 octets
- Structure :
  - pos 1 à 16 = message FNCI en clair pour affichage sur la visu
  - pos 17 à 20 = signature FNCI qui peut être imprimée sur le chèque
  - pos 21 - 22 = Compteur de consultation sur les X derniers jours.
  - pos 23 - 25 = Libre

(\*) Les réponses FNCI sont détaillées dans l'annexe 1 de ce document au § A1.4.1



#### Champ 45

- Définition : Identification du matériel (nécessaire au référencement Vérifiance)
- Messages : 9100, 9110, 9300, 9310
- Format : n15
- Longueur : 15 digits soit 8 octets
- Structure :
  - Pos 1 à 3 : code constructeur. La liste des codes constructeurs est maintenue à jour par Vérifiance.
  - Pos 4 à 6 : version du protocole exemple : CN - CHPN : 330 pour le CN - CHPN V3.3
  - Pos 7 à 12 : type de matériel (codification propre à chaque constructeur, qui en garantit l'unicité et s'engage à fournir les différentes valeurs possibles à Vérifiance)
  - Pos 13 à 15 : version logiciel (codification propre à chaque constructeur, qui en garantit l'unicité et s'engage à fournir les différentes valeurs possibles à Vérifiance)

#### Champ 46

- Définition : Capacité du système d'acceptation
- Messages : 9100, 9300
- Format : n4
- Longueur : 4 digits soit 2 octets
- Structure :
  - Pos 1 et 2 : capacité de raccordement du système d'acceptation

00	Inconnue
01	IP v4
02	DNS IP v4
03	DNS et IP
04	X25
05	X25 et IP v4
06	X25 et DNS
07	X25 et DNS et IP v4

- Pos 3 : Indique si le Système d'Acceptation sait faire du téléchargement (et donc prendre en compte le champ 47)

0	Ne sait pas faire du téléchargement
1	Sait faire du téléchargement

- Pos 4 : Indique si le Système d'Acceptation sait faire du téléparamétrage (et donc prendre en compte le champ 48)

0	Ne sait pas faire du téléparamétrage
1	Sait faire du téléparamètre

#### Champ 47

- Définition : Liste des paramètres dédiés au téléchargement
- Messages : 9310, 9110,
- Format : ansbA...65535
- Longueur : 2 octets binaires puis jusqu'à 65535 octets
- Utilisation : ce champ est transmis à l'initiative du serveur, qui envoie les paramètres permettant de réaliser un téléchargement sous la forme :
  - . Type (2 octets ansA)
  - . Longueur (2 octets ansA)
  - . Valeur (n octets ansbA)
- Structure :

Type	Longueur maximale	Codage	Libellé	Présence dans les messages	
				9110 (Garantie)	9310 (FNCI)
T1	61	ansbA	Paramètres de télécommunication vers le site nominal de téléchargement.	X	X
	1	anA	Type d'adressage réseau : <ul style="list-style-type: none"> <li>- 0 : IP v4</li> <li>- 1 : DNS (IP v4)</li> <li>- 2 : X25</li> </ul>		
	20	b	Adresse réseau du service ou du DNS Une adresse IP V4 est codée en binaire sur 4 octets. Un port TCP est codé en binaire sur 2 octets. Dans ce cas, ces informations sont cadrées à gauche, complétées à droite par des 0 binaires. Si le port n'est pas mentionné (valeur 0x00) alors le port par défaut 21000 sera utilisé. Dans le cas d'accès au réseau via un point de présence ou un PAD, le numéro de téléphone désignant ce point de présence sera fourni par ailleurs. Dans le cas de l'accès à l'acquéreur par l'intermédiaire d'un DNS, l'adresse IP indiquée dans cette donnée est l'adresse du serveur DNS. Le numéro de port est valorisé à 53 (cf. RFC 1035). Si des adresses de serveurs DNS sont configurées par le fournisseur d'accès, les adresses fournies par l'acquéreur dans le paramétrage sont prioritaires. Si aucune adresse de DNS n'est fournie par paramétrage, elles devront obligatoirement être données par le fournisseur d'accès (DHCP, etc.). Le nom de domaine désignant le serveur acquéreur sera fourni par ailleurs. Une adresse X25 est codée en DCB, complétée à droite par la valeur 0xF. Exemples : Codage de l'adresse IP 10.2.123.4 (0x0A027B04), port TCP 12453 (0x30A5) : '0A027B0430A50000'. Codage de l'adresse X25 19512457896 : '19512457896FFFFF'.		
	40	ansA	Nom de domaine Les caractères autorisés sont les caractères alphanumériques, le '.' (code ASCII 0x2E) et le '-' (code ASCII 0x2D). Le nom de domaine est immédiatement suivi du caractère '.' (code ASCII 0x3A) et du numéro de port (codé en caractères) à utiliser pour accéder à l'acquéreur une fois la résolution de nom réalisée. Si le port n'est pas fourni alors le port par défaut 21000 sera utilisé. Il est paddé à blanc (caractère 0x20) Présent uniquement pour un adressage réseau via DNS. Présent et non significatif si l'accès au réseau est réalisé via un accès téléphonique et l'adressage réseau réalisé via une adresse IP. Exemple : "Vérifiance.bdf.org:21000" donne "76 65 72 69 66 69 61 6E 63 65 2E 62 64 66 2E 6F 72 67 3A 32 31 30 30 30".		

Type	Longueur maximale	Codage	Libellé	Présence dans les messages	
				9110 (Garantie)	9310 (FNCI)
	15	anA	Numéro de téléphone d'accès au réseau Contient le numéro de téléphone du PAD pour l'accès à un réseau X25 ou d'un point de présence pour l'accès à un réseau IP. Présent uniquement si l'accès au réseau est réalisé par un modem téléphonique.		
	1	anA	Nature du PAD : Présent uniquement si l'accès au réseau est réalisé par un modem téléphonique. - 0 : non significatif - 1 : EMA - 2 : EBAM		
	10	anA	Données d'appel utilisateur de l'accès secondaire (sans le séparateur D)	X	X
T2	61	ansbA	Paramètres de télécommunication vers le 1er site de secours : Contient les informations relatives aux télécommunications avec le service de téléchargement Son découpage est identique à celui du paramètre T1.	X	X
T3	61	ansbA	Paramètres de télécommunication vers le 2ème site de secours : Contient les informations relatives aux télécommunications avec le service de téléchargement. Son découpage est identique à celui du paramètre T1.	X	X
T4	61	ansbA	Paramètres de télécommunication vers le 3ème site de secours : Contient les informations relatives aux télécommunications avec le service de téléchargement. Son découpage est identique à celui du paramètre T1.	X	X
PA	18		Paramètres d'appel : Ce paramètre complète les paramètres T1 et/ou T2 et/ou T3 et/ou T4	X	X
	2	anA	Nombre maximum d'essais d'appel.		
	4	anA	Délai d'attente entre deux appels (en secondes)		
	4	anA	Heure locale d'appel automatique (hhmm)		
	6	anA	Date locale d'appel automatique (AAMMJJ)		
	2	anA	Nombre maximum de reprises		
CA	20	ansA	Eléments de contrôle d'accès au système de téléchargement	X	X
RL	20	ansA	Référence du logiciel à télécharger	X	X

#### Champ 48

- Définition : Liste des téléparamètres génériques
- Messages : 9310, 9110,
- Format : ansbA...65535
- Longueur : 2 octets binaires puis jusqu'à 65535 octets
- Utilisation : ce champ est transmis à l'initiative du serveur, qui envoie les paramètres permettant de réaliser un téléchargement sous la forme :
  - . Type (2 octets ansA)
  - . Longueur (2 octets ansA)
  - . Valeur (n octets ansbA)
- Structure :

Type	Longueur maximale	Codage	Libellé	Présence dans les messages	
				9110 (Garantie)	9310 (FNCI)
T1	61	ansbA	Paramètres de télécommunication vers le site nominal : Contient les informations relatives aux télécommunications avec le service de garantie ou d'accès au FNCI, pour une application :	X	X
	1	anA	Type d'adressage réseau : <ul style="list-style-type: none"> <li>- 0 : IP v4</li> <li>- 1 : DNS (IP v4)</li> <li>- 2 : X25</li> </ul>		
	20	b	<p>Adresse réseau du service ou du DNS</p> <p>Une adresse IP V4 est codée binaire sur 4 octets. Un port TCP est codé binaire sur 2 octets. Dans ce cas, ces informations sont cadrées à gauche, complétées à droite par des 0 binaires. Si le port n'est pas mentionné (valeur 0x00) alors le port par défaut 21000 sera utilisé.</p> <p>Dans le cas d'accès au réseau via un point de présence ou un PAD, le numéro de téléphone désignant ce point de présence sera fourni par ailleurs.</p> <p>Dans le cas de l'accès à l'acquéreur par l'intermédiaire d'un DNS, l'adresse IP indiquée dans cette donnée est l'adresse du serveur DNS. Le numéro de port est valorisé à 53 (cf. RFC 1035). Si des adresses de serveurs DNS sont configurées par le fournisseur d'accès, les adresses fournies par l'acquéreur dans le paramétrage sont prioritaires. Si aucune adresse de DNS n'est fournie par paramétrage, elles devront obligatoirement être données par le fournisseur d'accès (DHCP, etc.). Le nom de domaine désignant le serveur acquéreur sera fourni par ailleurs.</p> <p>Une adresse X25 est codée en DCB, complétée à droite par la valeur 0xF.</p> <p>Exemples :</p> <p>Codage de l'adresse IP 10.2.123.4 (0x0A027B04), port TCP 12453 (0x30A5) : '0A027B0430A50000'.</p> <p>Codage de l'adresse X25 19512457896 : '19512457896FFFFF'.</p>		

Type	Longueur maximale	Codage	Libellé	Présence dans les messages	
				9110 (Garantie)	9310 (FNCI)
	40	ansA	<p>Nom de domaine</p> <p>Les caractères autorisés sont les caractères alphanumériques, le '.' (code ASCII 0x2E) et le '-' (code ASCII 0x2D). Le nom de domaine est immédiatement suivi du caractère '.' (code ASCII 0x3A) et du numéro de port (codé en caractères) à utiliser pour accéder à l'acquéreur une fois la résolution de nom réalisée. Si le port n'est pas fourni alors le port par défaut 21000 sera utilisé.</p> <p>Il est paddé à blanc (caractère 0x20)</p> <p>Présent uniquement pour un adressage réseau via DNS. Présent et non significatif si l'accès au réseau est réalisé via un accès téléphonique et l'adressage réseau réalisé via une adresse IP.</p> <p>Exemple : "Vérifiance.bdf.org:21000" donne "76 65 72 69 66 69 61 6E 63 65 2E 62 64 66 2E 6F 72 67 3A 32 31 30 30 30".</p>		
	15	anA	<p>Numéro de téléphone d'accès au réseau</p> <p>Contient le numéro de téléphone du PAD pour l'accès à un réseau X25 ou d'un point de présence pour l'accès à un réseau IP.</p> <p>Présent uniquement si l'accès au réseau est réalisé par un modem téléphonique.</p>		
	1	anA	<p>Nature du PAD :</p> <p>Présent uniquement si l'accès au réseau est réalisé par un modem téléphonique.</p> <ul style="list-style-type: none"> <li>- 0 : non significatif</li> <li>- 1 : EMA</li> <li>- 2 : EBAM</li> </ul>		
	10	ansA	Données d'appel utilisateur de l'accès secondaire (sans le séparateur D)	X	X
T2	61	ansbA	<p>Paramètres de télécommunication vers 1er site de secours. Contient les informations relatives aux télécommunications avec le service de garantie ou d'accès au FNCI.</p> <p>Son découpage est identique à celui du paramètre T1.</p>	X	X
T3	61	ansbA	<p>Paramètres de télécommunication vers 2ème site de secours. Contient les informations relatives aux télécommunications avec le service de garantie ou d'accès au FNCI.</p> <p>Son découpage est identique à celui du paramètre T1.</p>	X	X
T4	61	ansbA	<p>Paramètres de télécommunication vers 3ème site de secours. Contient les informations relatives aux télécommunications avec le service de garantie ou d'accès au FNCI.</p> <p>Son découpage est identique à celui du paramètre T1.</p>	X	X
SP	12	anA	Seuil minimum d'appel dans l'unité monétaire mineure spécifiée dans le champ 49	X	X
CF	10	ansA	Client final à téléparamétrer (cf. description champ 42)		X

#### Champ 49

- Définition : Identification de la monnaie
- Messages : 9100, 9110, 9300, 9310
- Format : n 3
- Longueur : 3 digits soit 2 octets (le premier digit est à 0)
- Utilisation : valeur « 978 » : Euro (norme ISO 4217 : codes ISO numériques)

#### 4.3.4. Activité de demande de consultation FNCI et de garantie

##### a) Fonction

- 9100 : Demande de garantie de chèque
- 9110 : Réponse à la demande de garantie
- 9300 : Demande de consultation FNCI
- 9310 : Réponse à la demande de consultation FNCI

La demande est relative à un montant exprimé dans une monnaie dont l'unité est précisée dans son contenu. Elle contient l'ensemble des informations nécessaires à son traitement.

La réponse à la demande reprend des champs de la demande qui constitue la référence de la transaction. En cas d'accord, celui-ci concerne toujours le montant spécifié dans la demande et repris dans la réponse.

## b) Description des messages

Le tableau ci-après décrit la composition d'une demande de garantie, de consultation FNCI et sa réponse.

N°	CHAMP	FORMAT	GARANTIE		FNCI	
			9100	9110	9300	9310
1	Extension bitmap	b64	(1)	(1)	(1)	(1)
2	Identification du tireur	n...19	O	O=	O	O=
3	Code traitement	n6	O	O=	O	O=
4	Montant de la transaction	n12	R	R=	R	R=
7	Date et heure du serveur	n10	-	R	-	R
11	Identification de la transaction	n6	O	O=	O	O=
12	Heure locale de la transaction	n6	O	O=	O	O=
13	Date locale de la transaction	n4	O	O=	O	O=
18	Type d'activité	n4	O	-	O	-
22	Capacité lecture	n3	R	-	R	-
25	Conditions d'émission	n2	O	-	O	-
32	Identification de l'organisme demandeur	n..11	O	O=	O	O=
35	Piste CMC7	n...35	R	R=	R	R=
37	Identification du centre informatique	an12	R	-	R	-
38	Référence du garantisseur	an6	-	R	-	-
39	Code réponse FNCI	an2	-	R	-	R
40	Code réponse du garantisseur	an3	-	R	-	-
41	Identification du terminal	ans8	O	O=	O	O=
42	identification de l'abonné	ans15	R	R=	R	R=
43	Données complémentaires à la garantie	ans40	O	R	-	-
44	Données complémentaires de réponse FNCI	ans20...25	-	R	-	R
45	Identification du matériel	n15	O	O=	R	R=
46	Capacité du système d'acceptation	n4	R	O=	R	O=
47	Liste des paramètres dédiés au téléchargement	ansbA...65535	-	O	-	O
48	Liste des téléparamètres génériques	ansbA...65535	-	O	-	O
49	Identification de la monnaie	n3	R	R=	R	R=

O Optionnel

R Requis

- Non présent

= Valeur identique à la valeur de la demande

(1) La présence d'une 2ème bitmap à zéro doit être supportée en réception par l'équipement

#### c) Règles d'utilisation des champs dans les messages

- *Champs définis dans le protocole*  
L'équipement doit être capable de recevoir des champs non requis dans le message de réponse. Dans ce cas, ces champs doivent être ignorés.
- *Champs non définis par le protocole*  
Les champs non définis par le protocole sont considérés comme devant être absents dans les messages échangés. Le serveur ou le TPE considère alors la requête comme étant non conforme (code 34)

#### 4.3.5. Traitement des erreurs

Ce chapitre traite des incidents détectés par l'équipement lors de l'émission de la demande vers le système d'autorisation.

- Incidents détectés par le niveau d'application  
  
Il s'agit de la réception par l'entité de niveau applicatif de l'équipement demandeur d'un message réponse incompréhensible (identifiant inconnu, bitmap erronée, erreur sur champ longueur,...). Dans ce cas, l'équipement met fin à la connexion et affiche un message « ACCÈS IMPOSSIBLE ».
- Incidents détectés par le système de communication
  - *Impossibilité d'établir une connexion*  
Dans ce cas l'équipement doit proposer à l'abonné, soit de réitérer la demande, soit de l'abandonner.
  - *La communication est établie*  
Une indication de rupture est remontée de niveau intermédiaire. Cette indication est consécutive aux événements tels que expiration du timer de non-réponse, réception d'une IPDU d'erreur, rupture de connexion...  
Dans ce cas, l'équipement met fin à la connexion et affiche un message "ACCÈS IMPOSSIBLE".



#### **4.4. Niveau pseudo-session**

##### **4.4.1. Présentation**

Le protocole de niveau pseudo-session permet d'envisager, vu du niveau applicatif, la disponibilité de services identiques indépendamment des protocoles de niveau bas utilisé. Ce protocole reprend certaines fonctionnalités de niveau Transport et Session par l'intermédiaire de champs de données particuliers dans les données utilisateur du niveau réseau.

La couche pseudo-session offre les moyens nécessaires à l'échange de données entre utilisateurs de niveau application.

Elle permet aux utilisateurs :

- d'échanger des données sur cette connexion,
- de libérer cette connexion.

Les fonctionnalités retenues sont les suivantes :

- identification du protocole de niveau pseudo-session entre l'équipement et le point d'accès,
- gestion des échanges au niveau pseudo-session,
- temporisation de non-réponse
- surveillance d'activité de l'équipement par le point d'accès,
- identification du terminal,
- indication du numéro de version applicative.

Ces fonctionnalités se traduisent sous forme de paramètres et de timer, négociés ou non, dans les éléments de protocole du niveau pseudo-session (IPDU).

##### **4.4.2. Gestion des temporisations**

###### **a) Présentation**

Deux types de temporisation assurent la supervision des échanges

Temporisation de non-réponse (TNR) et de garantie de réponse (TGR),

Temporisation de surveillance d'activité de l'équipement par le point d'accès (TIE).

b) Temporisation de non-réponse et de garantie de réponse

La surveillance de l'activité du système serveur chèque est basée sur l'utilisation d'un timer de non-réponse par l'équipement et d'un timer de garantie de réponse par le point d'accès au système serveur chèque.

L'équipement lance son timer de non-réponse (TNR) lors de l'émission d'une APDU question (message 9300 ou 9100), et le désarme lors de la réception d'une APDU réponse (message 9310 ou 9110).

En cas d'expiration, l'équipement considère que le point d'accès est indisponible et libère la connexion de niveau inférieur.

Le point d'accès lance le timer de garantie de réponse (TGR) lors de la réception d'une APDU question (9300 ou 9100) et le désarme lors de l'émission d'une APDU réponse. Son expiration entraîne l'émission d'un message réponse (9310 ou 9110) contenu dans une IPDU DE avec un code retour signifiant l'incident ("010" des champs 40 si demande 9100 et "99" des champs 39 si demande 9300).

La condition pour une gestion optimum du dialogue est la suivante

$$\boxed{\text{TNR} > \text{TGR} + \text{temps de transit maximum}}$$

Mise en œuvre du timer TNR

La valeur du timer de non-réponse est un paramètre de configuration de l'équipement. Sa valeur préconisée est de 30 secondes. Elle est négociable à l'aide du PI03 (voir page 38).

Mise en œuvre du timer TGR

La valeur du timer de garantie de réponse est un paramètre de configuration du point d'accès. Sa valeur préconisée est de 24 secondes.

c) Temporisation de surveillance d'activité de l'équipement

Un équipement autonome rompt la connexion physique entre chaque activité.

Un équipement concentrateur peut enchaîner plusieurs activités sur une même connexion de pseudo-session.

L'absence de dialogue, au niveau pseudo-session, est contrôlée par le point d'accès au moyen d'un timer TIE, dont la valeur n'est pas négociée.

A l'expiration du timer, le point d'accès transmet à l'équipement un élément de protocole de niveau pseudo-session (IPDU AB), dit de coupure, dont le code retour (paramètre PI01) prend la valeur adéquate. La valeur préconisée de TIE est de 50 secondes.

Le point d'accès ne déconnecte que sur l'échéance d'un temporisateur.

#### 4.4.3. Spécifications des échanges

##### a) Présentation

- La phase de transfert de données concerne l'échange de données entre deux utilisateurs connectés, un seul service lui est associé, le service de transfert de données
- La phase de libération de connexion concerne la libération d'une connexion préalablement établie. Un seul service lui est associé, le service de coupure utilisateur.

Le tableau ci-après présente les services de niveau pseudo-session, les éléments de protocole associés et leur utilisation par l'équipement et le point d'accès.

SERVICES	Eléments de protocole	Utilisation par équipement	Utilisation par point d'accès
Service de transfert de données	IPDU DE	X	X
Service de coupure utilisateur	IPDU AB		X

##### b) Phase de connexion

Le protocole CN – CHPN V3.2 n'utilise pas de service de connexion, et donc d'éléments de protocole IPDU CN/AC.

Ce sont des IPDU DE qui transportent les éléments de protocole de niveau supérieur (APDU question et réponse).

L'initialisation des paramètres de la connexion de pseudo-session s'effectue en même temps que la demande (APDU).

Les IPDU DE contiennent :

- Identification du protocole,
- Longueur des paramètres,
- Identification du terminal,
- Indication du numéro de version applicative (CN – CHPN).

##### Remarques :

La réception d'une IPDU AB provoque l'arrêt de la pseudo-session avec le point d'accès.

Dans le cas de dialogue normal, l'équipement demandeur n'envoie jamais d'IPDU AB, il coupe la connexion de niveau inférieur.

c) Phase de transfert de données

Le service de données permet à l'un des utilisateurs de transmettre un élément de protocole de niveau supérieur (APDU question ou réponse).

L'IPDU DE possède les informations suivantes :

- Identifiant de protocole applicatif (CN – CHPN),
- Longueur des paramètres
- Paramètres : la présence des paramètres, en fonction du protocole utilisé et de l'émetteur de l'IPDU DE, est définie au chapitre 2
- Données (APDU)

d) Phase de déconnexion

Le service de déconnexion permet au point d'accès, au niveau pseudo-session lui-même, de terminer de façon anormale une connexion de pseudo-session.

Service de coupure utilisateur

Ce service permet au point d'accès de libérer une connexion de niveau pseudo-session, et d'indiquer la raison de cette libération.

Ce service utilise l'élément de protocole IPDU AB, qui comporte les informations suivantes :

- Identifiant de protocole applicatif (CN – CHPN V3.2),
- Longueur des paramètres,
- Paramètre gestion des échanges (code retour pseudo-session).

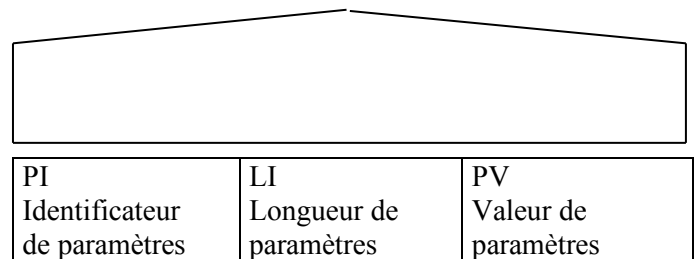
Les IPDU AB ne transportent pas d'éléments de protocole de niveau supérieur. Sur réception d'une IPDU AB, l'équipement coupe la connexion avec le point d'accès.

#### 4.4.4. Personnalisation de la description issue de CBCom

##### a) Format général

Les unités de protocole de niveau pseudo-session sont codées à partir du premier octet des données utilisateurs du niveau transport.

Longueur totale	PGI Indicateur d'IPDU	LGI Longueur des paramètres	Zone paramètres	Données APDU
-----------------	--------------------------	--------------------------------	-----------------	--------------



##### b) Règles d'utilisation

- Tout PI inconnu peut être présent et sera ignoré par le récepteur
- Tout PI défini peut être présent mais seuls ceux qui sont nécessaires seront pris en compte ;
- Un PI ne peut être présent qu'une seule fois ;
- La zone paramètre s'obtient en concaténant les blocs paramètres dans un ordre quelconque ;
- Les informations constituant les IPDU sont codées binaires sur un ou plusieurs octets.

##### c) Format

- Les longueurs LGI, et LI sont des longueurs en octets exprimées sur 1 octet ;
- PI est codé sur un octet binaire ;
- LI est codé sur un octet binaire ;
- PV est codé en binaire sur le nombre d'octets précisé par LI.

##### d) Gestion des longueurs

La longueur totale, codée sur 4 octets, précise le nombre d'octets total du message, longueur non comprise.

**Attention** : Selon la définition de CBCom 1.3, cette longueur est présente quelle que soit le mode de connexion du Système Monétique (**elle est donc aussi présente si la connexion se fait via un PAD ou en appel X25 direct**).

La longueur LGI, codée sur un octet, précise le nombre d'octets de la zone paramètres, le champ LGI n'est pas compris dans la taille précisée.

La zone paramètre s'obtient en concaténant les blocs paramètres par ordre de type croissant. Les informations constituant les IPDU sont codées binaires sur 1 ou plusieurs octets. Les longueurs LGI et LI sont des longueurs en octets.

### Valeur de l'identifiant de protocole - PGI

L'identifiant de protocole est découpé en deux 1/2 octets. Le premier indique le type de protocole, le second le type d'IPDU.

IPDU	CHPN
IPDU DE IPDU AB	X 'C1' X 'C9'

### e) Paramètres

#### Code retour de niveau pseudo-session - PI01

Code : X '01'

Longueur : 1 octet

Valeur : voir tableau

CODE (décimal)	SIGNIFICATION
0	Pas d'anomalie
2	Identifiant de PGI invalide
4	Paramètre requis manquant
7	Saturation du point d'accès
9	Rupture d'alternat
14	Service arrêté
15	Point d'accès en arrêt
17	APDU inconnue
18	APDU incorrecte (champs obligatoires manquants)
19	Longueur APDU incorrecte
24	Erreur protocole (réception message de l'équipement pendant la transaction)
25	Expiration du timer d'inactivité TIE
34	Transaction invalide (présence champ inconnu)
35	Format d'IPDU invalide
36	Échange d'IPDU incorrecte
39	Absence ou valeur de paramètre invalide

#### Valeur du timer de non-réponse acceptée - PI03

Code : x '03'

Longueur : 1 octet

Valeur : x "1E" pour représenter 30 secondes (codées en binaire)

Il s'agit d'une durée d'attente maximale du terminal pour recevoir une réponse de la part du serveur. Compte tenu de la cinématique du protocole, cette durée n'est valable que pour les demandes ultérieures. Lors de la 1ère demande, le terminal doit gérer une valeur par défaut.

#### N° de version CBCom – PI04

Code : x "04"

Longueur : 1 octet

Valeur : x "12" pour CBCom 1.2

x "13" pour CBCom 1.3

#### Identification du terminal - PI05

Code : x '05'

Longueur : 2 octets

Valeur : Ce paramètre étant conservé à des fins de compatibilité avec les versions antérieures du protocole, sa valeur peut être quelconque. Il ne sera plus contrôlé par les serveurs à partir de la version 3.0 de CN-CHPN.

#### Numéro de version protocolaire – PI06

Code : x "06"

Longueur : 1 octet

Valeur : x « 31 » correspond à la version du protocole CN - CHPN V3.1.

Valeur : x « 32 » correspond à la version du protocole CN - CHPN V3.2.

Valeur : x « 33 » correspond à la version du protocole CN – CHPN V3.3.

#### Timer de surveillance d'activité de l'équipement – PI08

Code : x "08"

Longueur : 2 octets

Valeur : 50 secondes, codée binaire.

Le serveur indique à la solution monétique qu'il utilise ce paramètre pour couper le CV au bout du temps d'inactivité indiqué par la valeur transmise.

La solution monétique recevant ce paramètre peut en tenir compte et agir en conséquence.

#### **EXPLICATIONS CONCERNANT LA VALEUR DE 50 SECONDES**

Une solution monétique établit une connexion avec le Service Vérifiance et effectue une première consultation Vérifiance. Le service Vérifiance lance une temporisation de 50 secondes dès que la connexion est établie. Si la solution monétique ne ferme pas la connexion et lance une seconde consultation avant l'expiration des 50 secondes, la temporisation redémarre à zéro pour une durée de 50 secondes. Et ainsi de suite, tant que 50 secondes ne se sont pas écoulées depuis le dernier passage de chèque en consultation Vérifiance.

f) Utilisation des paramètres

Tableau d'utilisation des paramètres

	ÉQUIPEMENT	POINT D'ACCES
PI01	-	IPDU DE, AB
PI03	-	IPDU DE
PI04	PIDU DE	
PI05	IPDU DE	
PI06	IPDU DE	
PI08		IPDU DE

Format des IPDU

*IPDU DE émise par l'équipement*

PGI	LGI	PI04	LI04	PV04	PI05	LI05	PV05	PI06	LI06	PV06	APDU Question
-----	-----	------	------	------	------	------	------	------	------	------	---------------

*IPDU DE émise par le point d'accès*

PGI	LGI	PI01	LI01	PV01	PI03	LI03	PV03	PI08	LI08	PV08	APDU Réponse
-----	-----	------	------	------	------	------	------	------	------	------	--------------

*IPDU AB émise par le point d'accès*

PGI	LGI	PI01	LI01	PV01
-----	-----	------	------	------



## **5. OPÉRATIONS AYANT TRAIT AU LECTEUR**

Lors du passage du chèque en caisse pour une transaction de paiement, les fonctions suivantes peuvent être déroulées, sachant que c'est l'équipement de l'abonné qui pilote le lecteur de chèques :

- Saisie sur le terminal de paiement du montant de la transaction et lecture de la piste CMC7 du chèque,
- Constitution et transmission d'une demande de garantie ou de consultation FNCI après choix de l'abonné,
- Réception de la réponse sur le terminal et affichage du libellé correspondant,
- Impression du contenu du chèque dans le cas des lecteurs éditeurs,
- Mise à jour du fichier de télécollecte (pour plus de détails, voir le protocole CN – CHPR).

# ANNEXE 1

## AIDE A L'IMPLEMENTATION DU PROTOCOLE CN - CHPN V3.3

ASSOCIATION DÉCLARÉE RÉGIE PAR LA LOI DU 1<sup>er</sup> JUILLET 1901, N°89 / 3905  
8, RUE DE CROUY - 41220 SAINT LAURENT NOUAN - TÉL : 02 54 87 06 12 - FAX : 02 54 87 06 12  
[www.concert.asso.fr](http://www.concert.asso.fr)  
[contact@concert.asso.fr](mailto:contact@concert.asso.fr)

## SOMMAIRE

<b>A1.4. AFFICHAGE DE LA RÉPONSE EN FONCTION DES ENVIRONNEMENTS VÉRIFIANCE.....</b>	<b>3</b>
A1.4.1. L'ENVIRONNEMENT DE PRODUCTION .....	3
A1.4.2. L'ENVIRONNEMENT DE DEMONSTRATION.....	5
A1.4.3. PRESENTATION D'UN CHEQUE DE DEMONSTRATION VERIFIANCE .....	6
A1.4.4. PARAMETRES D'ACCES AU SERVICE DE DEMONSTRATION VERIFIANCE (DOS DU CHEQUE).....	7
A1.4.5. L'ENVIRONNEMENT DE TESTS .....	7
A1.4.6. LES COMPTEURS « C1,C2 », « C3,C4 » ET « C5,C6 » .....	9
A1.4.7. LA CLE RL MC .....	10
<b>A1.5. SIGNATURE FN CI .....</b>	<b>11</b>
<b>A1.6. RÈGLE D'AFFICHAGE DES CHAMPS RÉPONSES.....</b>	<b>11</b>
<b>A1.7. LES SPÉCIFICATIONS DU CODE DEVISE .....</b>	<b>12</b>
A1.7.1. RAPPEL SUR LA PRESENTATION D'UN CHEQUE .....	12
A1.7.2. REGLE DE GESTION DU CODE DEVISE « EURO » .....	12
A1.7.3. LES AUTRES DEVISES .....	12
<b>A1.8. LE TELEPARAMETRAGE DES DONNEES.....</b>	<b>13</b>
A1.8.1. DEFINITIONS - RAPPELS .....	13
A1.8.2. CHAMP 46.....	13
<b>A1.8.2.1 Positions 1 et 2.....</b>	<b>13</b>
<b>A1.8.2.2 Position 3.....</b>	<b>13</b>
<b>A1.8.2.3 Position 4.....</b>	<b>13</b>
A1.8.3. CHAMP 47.....	14
<b>A1.8.3.1 Paramètre T1 .....</b>	<b>15</b>
<b>A1.8.3.2 Paramètres T2, T3 et T4.....</b>	<b>15</b>
<b>A1.8.3.3 Paramètre PA.....</b>	<b>16</b>
<b>A1.8.3.4 Paramètre CA .....</b>	<b>16</b>
<b>A1.8.3.5 Paramètre RL .....</b>	<b>16</b>
A1.8.4. CHAMP 48.....	17
<b>A1.8.4.1 Paramètre T1 .....</b>	<b>18</b>
<b>A1.8.4.2 Paramètres T2, T3 et T4.....</b>	<b>18</b>
<b>A1.8.4.3 Paramètre SP.....</b>	<b>19</b>
<b>A1.8.4.4 Paramètre CF.....</b>	<b>19</b>
<b>A1.8.5 Initialisation des paramètres .....</b>	<b>20</b>

#### **A1.4. AFFICHAGE DE LA RÉPONSE EN FONCTION DES ENVIRONNEMENTS VÉRIFIANCE**

En plus du « **code-réponse du FNCI** » transmis dans le **CHAMP 39**, des données complémentaires de réponse sont fournies dans le champ 44 (données complémentaires de réponse).

Plus particulièrement, les 16 premiers caractères du champ 44 contiennent un « message FNCI à afficher sur la visu ».

**Attention:** La solution monétique effectuant un accès au service Vérifiance doit afficher ces 16 caractères en totalité sans en altérer le contenu.

Vérifiance met à disposition de tous ses utilisateurs trois environnements :

- Un environnement de production
- Un environnement de démonstration
- Un environnement de tests

Les tableaux ci-dessous présentent une liste des messages FNCI transmis dans le champ 44 selon les différents environnements

##### **A1.4.1. L'environnement de production**

16 PREMIERS CARACTERES DU CHAMP 44 DE LA REPONSE FNCI Liste non exhaustive pouvant être modifiée																17	18	19	20	21	22	23	24	25
V	E	R	T	Ø	Ø	F	N	C	I	C1	C2	C3	C4	Y1	Y2	S1	S2	S3	S4	C5	C6	Ø	Ø	Ø
O	R	A	N	G	E	F	N	C	I	C1	C2	C3	C4	Y1	Y2	S1	S2	S3	S4	C5	C6	Ø	Ø	Ø
R	O	U	G	E	Ø	F	N	C	I	C1	C2	C3	C4	Y1	Y2	S1	S2	S3	S4	C5	C6	Ø	Ø	Ø
B	L	A	N	C	Ø	F	N	C	I	C1	C2	C3	C4	Y1	Y2	S1	S2	S3	S4	C5	C6	Ø	Ø	Ø

«» = Le caractère « espace »

« C1, C2 » = Compteur de consultation sur la journée en cours. Ce compteur est sur 2 digits, et on affiche 01 et non 1.

« C3, C4 » = Compteur de consultation sur les N derniers jours. Ce compteur est sur 2 digits, et on affiche 01 et non 1.

« Y1, Y2 » = La clé RLMC calculée par le Service VÉRIFIANCE à partir des informations contenues sur la piste CMC7 reçue.

« S1, S2, S3, S4 » = La signature

« C5, C6 » = Compteur de consultation sur les X derniers jours. Ce compteur est sur 2 digits, et on affiche 01 et non 1.

#### **A1.4.2. L'environnement de démonstration**

16 PREMIERS CARACTERES DU CHAMP 44 DE LA REPONSE FNCI Liste non exhaustive pouvant être modifiée																17	18	19	20	21	22	23	24	25
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
V	E	R	T			D	E	M	O	C1	C2	C3	C4	Y1	Y2	S1	S2	S3	S4	C5	C6			
O	R	A	N	G	E	D	E	M	O	C1	C2	C3	C4	Y1	Y2	S1	S2	S3	S4	C5	C6			
R	O	U	G	E		D	E	M	O	C1	C2	C3	C4	Y1	Y2	S1	S2	S3	S4	C5	C6			
B	L	A	N	C		D	E	M	O	C1	C2	C3	C4	Y1	Y2	S1	S2	S3	S4	C5	C6			

«  » = Le caractère « espace »

« C1, C2 » = Compteur de consultation sur la journée en cours. Ce compteur est sur 2 digits, et on affiche 01 et non 1.

« C3, C4 » = Compteur de consultation sur les N derniers jours. Ce compteur est sur 2 digits, et on affiche 01 et non 1.

« Y1, Y2 » = La clé RLMC calculée par le Service VÉRIFIANCE à partir des informations contenues sur la piste CMC7 reçue.

« S1, S2, S3, S4 » = La signature

« C5, C6 » = Compteur de consultation sur les X derniers jours. Ce compteur est sur 2 digits, et on affiche 01 et non 1.

**Attention: Dans l'environnement de démonstration les couleurs, ainsi que les trois compteurs "C1, C2", "C3, C4", "C5, C6" varient en fonction des montants transmis.**

Voir les valeurs sur le dos du chèque fourni ci-après.

#### A1.4.3. Présentation d'un chèque de démonstration Vérifiance

The diagram shows a specimen check from 'Vérifiance' (FNCI - Banque de France). It includes the following elements and annotations:

- Top Left:** Logo of 'Vérifiance FNCI - Banque de France'.
- Top Right:** Text 'à rédiger exclusivement en euros' and a Euro symbol (€).
- Center:** A large white box for the amount, with a Euro symbol (€) to its left.
- Bottom Left:** A box containing the name 'MANTIS', address '24 rue des Jeûneurs CS 60205 75086 PARIS CEDEX 02', and phone number 'Tél. : 0 825 888 999 (0,150 € TTC/Min)'.
- Bottom Center:** A MICR line with the numbers '0010250 800000000909 000000000000'.
- Bottom Right:** The word 'SPÉCIMEN' in large blue letters, and the code '< 68 >'.

Annotations (arrows pointing to specific areas):

- Top Left: Les mentions « à », « A » ou « A l'ordre de » sont INTERDITES.
- Top Center: Les mentions « Payables » ou « Compensables » sont INTERDITES.
- Top Right: La mention « Chèques » est INTERDITE.
- Far Top Right: La mention « B.P.F. » est INTERDITE.
- Bottom Left: Les 2 premiers chiffres de cette zone sont OBLIGATOIREMENT « 00 ». Les 5 derniers chiffres de cette zone sont libres d'utilisation.
- Bottom Center: « 800000000909 » est OBLIGATOIRE dans cette zone pour éviter toute confusion avec une piste CMC7 authentique lors des traitements automatisés.
- Bottom Right: La Mention SPECIMEN est OBLIGATOIRE et doit être lisible.
- Far Bottom Right: La clé RLMC doit être présente (ici « 68 »).

#### A1.4.4. Paramètres d'accès au service de démonstration Vérifiance (dos du chèque)

SERVICE DE DEMONSTRATION VÉRIFIANCE				
Les informations fournies au recto et au verso de ce document ne sont pas contractuelles et peuvent être modifiées sans préavis par la société Mantis.				
Code d'accès Vérifiance (code de l'abonné) : ABCDE00A99				
Caractéristiques de l'accès de démonstration via X25 Pad public 08.36.06 24.24		Caractéristiques de l'accès de démonstration via IP	Port	DNS
Adresse du serveur	1.96.376.752	Adresse IP 1 : 193.56.46.150	<b>5457</b>	V3.CHEQUE.VERIFIANCE-FNCI.FR
Données complémentaires	V7DE ou « DV7DE »	Adresse IP 2 : 160.92.189.8	<b>5457</b>	V4.CHEQUE.VERIFIANCE-FNCI.FR

Information Multi-Chèques				
Montant	Couleurs FNCI	Cpt 1	Cpt 2	Cpt 3
10,00 EUR	Blanc	01	03	05
20,00 EUR	Orange	02	06	08
30,00 EUR	Vert	03	09	11
Autres	Rouge	04	12	14

#### A1.4.5. L'environnement de tests

Afin d'aider les constructeurs dans leurs développements, la société Mantis peut mettre à leur disposition un environnement de tests.

16 PREMIERS CARACTERES DU CHAMP 44 DE LA REPONSE FNCI Liste non exhaustive pouvant être modifiée																17	18	19	20	21	22	23	24	25
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	S1	S2	S3	S4	C5	C6	Ø	Ø	Ø
V	E	R	T	Ø	Ø	T	E	S	T	C1	C2	C3	C4	Y1	Y2	S1	S2	S3	S4	C5	C6	Ø	Ø	Ø
O	R	A	N	G	E	T	E	S	T	C1	C2	C3	C4	Y1	Y2	S1	S2	S3	S4	C5	C6	Ø	Ø	Ø
R	O	U	G	E	Ø	T	E	S	T	C1	C2	C3	C4	Y1	Y2	S1	S2	S3	S4	C5	C6	Ø	Ø	Ø
B	L	A	N	C	Ø	T	E	S	T	C1	C2	C3	C4	Y1	Y2	S1	S2	S3	S4	C5	C6	Ø	Ø	Ø



« ␣ » = Le caractère « espace »

« C1, C2 » = Compteur de consultation sur la journée en cours. Ce compteur est sur 2 digits, et on affiche 01 et non 1.

« C3, C4 » = Compteur de consultation sur les N derniers jours. Ce compteur est sur 2 digits, et on affiche 01 et non 1.

« Y1, Y2 » = La clé RLMC calculée par le Service VÉRIFIANCE à partir des informations contenues sur la piste CMC7 reçue.

« S1, S2, S3, S4 » = La signature

« C5, C6 » = Compteur de consultation sur les X derniers jours. Ce compteur est sur 2 digits, et on affiche 01 et non 1.

<p><b><u>Attention:</u> Dans l'environnement de tests les couleurs, ainsi que les trois compteurs "C1, C2", "C3, C4" et "C5, C6" varient en fonction des montants transmis</b></p>
--

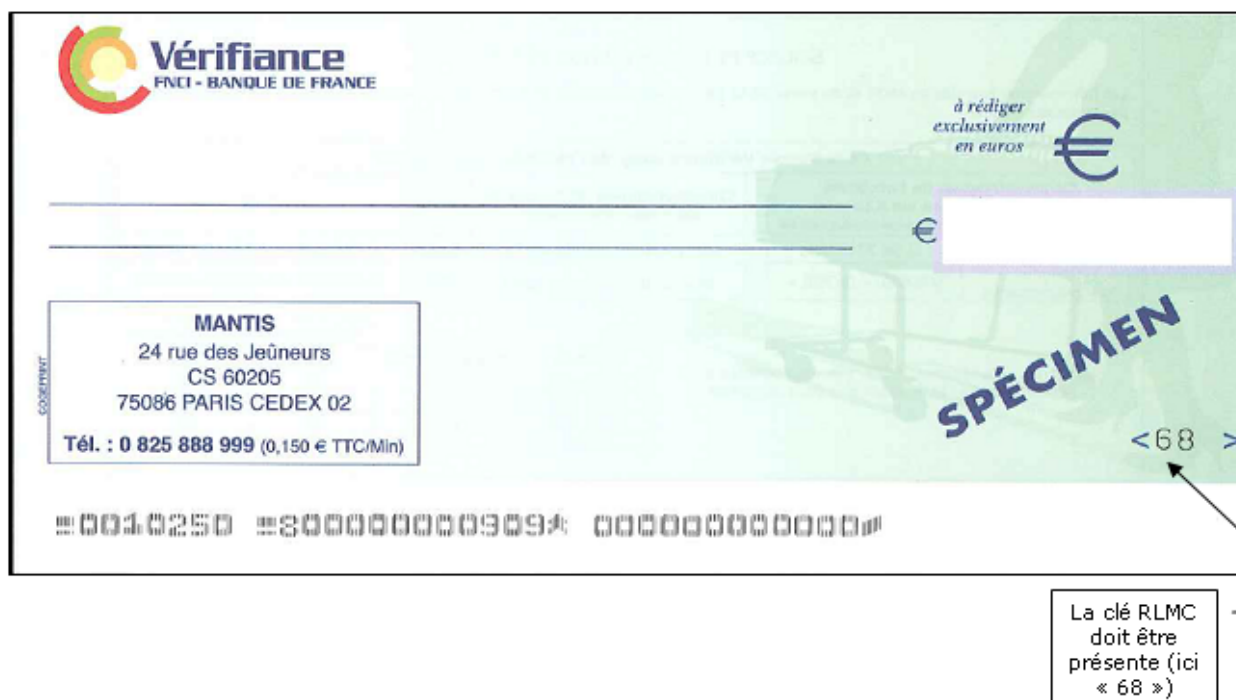
#### **A1.4.6. Les compteurs « C1,C2 », « C3,C4 » et « C5,C6 »**

Ces 3 compteurs viennent en complément de la réponse couleur FNCI et représentent :

- « C1, C2 » = Le nombre de chèques consultés sur un même compte bancaire depuis le début de la journée. (y compris le chèque en cours de consultation). Ce compteur est sur 2 digits, et on affiche 01 et non 1.
- « C3, C4 » = Le nombre de chèques consultés sur un même compte bancaire durant les N derniers jours. (y compris le chèque en cours de consultation). Ce compteur est sur 2 digits, et on affiche 01 et non 1.
- « C5, C6 » = Le nombre de chèques consultés sur un même compte bancaire durant les X derniers jours. (y compris le chèque en cours de consultation). Ce compteur est sur 2 digits, et on affiche 01 et non 1.

**Attention** : Les informations apportées par les compteurs ne sauraient être invoquées pour fonder, à elles seules, un refus de chèque. Elles ne devront servir au commerçant qu'à engager, le cas échéant, un contrôle accru du contexte de la transaction lorsque le chèque donnera lieu par ailleurs à une réponse verte du FNCI. Ce contrôle approfondi pourra porter sur la pièce d'identité produite, les mentions de la formule de chèque utilisée, la conformité de la signature portée sur le chèque avec celle de la pièce d'identité, les surcharges ou ratures portées sur le chèque, les raisons de l'utilisation du chéquier, etc. Chaque Utilisateur devra définir les critères à partir desquels il considérera être en présence d'un chèque présumé 'à risque'. Il veillera en particulier à adapter les critères en fonction des périodes de l'année, des produits vendus, de la zone de chalandise, de sa connaissance de la clientèle, etc. Il conviendra également de veiller que le message diffusé au personnel de caisse soit suffisamment explicite pour lui permettre de justifier la mise en œuvre des vérifications complémentaires susmentionnées, à l'exclusion de toute incitation au rejet systématique du chèque.

#### A1.4.7. La clé RLMC



**Vérifiance**  
 FNCI - BANQUE DE FRANCE

à rédiger  
 exclusivement  
 en euros €

€

**SPÉCIMEN**

< 68 >

La clé RLMC  
 doit être  
 présente (ici  
 « 68 »)

MANTIS  
 24 rue des Jeûneurs  
 CS 60205  
 75086 PARIS CEDEX 02  
 Tél. : 0 825 888 999 (0,150 € TTC/Min)

00010250 8000000000309 000000000000

Vérifiance ajoute à sa réponse couleur, le calcul de la clé RLMC (Recomposition de la Ligne Magnétique du Chèque). Ce nombre, toujours composé de 2 digits, est le résultat du calcul de l'algorithme des chiffres composant la piste CMC7 située en bas du chèque dans la partie blanche. Lors du contrôle d'un chèque, Vérifiance recalcule cet algorithme et bien évidemment, le nombre qui apparaît dans la réponse Vérifiance doit être identique à celui indiqué entre < > ou ( ) sur le chèque.

En cas de différence, il s'agit vraisemblablement d'un chèque contrefait qui est susceptible de ne pas être payé.

Exemple d'une réponse Vérifiance au point d'encaissement :

Couleur FNCI		"C1, C2"	"C3, C4"	Clé RLMC
VERT	FNCI	01	03	35

#### **A1.5. SIGNATURE FNCI**

La signature est la confirmation pour le commerçant qu'une interrogation FNCI a été correctement réalisée.

Les octets 17 à 20 (4 caractères) du champ 44 sont affectés à la signature FNCI transmise par le service Vérifiance.

La solution monétique peut imprimer les 4 caractères alphanumériques de cette signature FNCI sur le chèque passé en consultation Vérifiance.

En revanche, à part l'édition sur le chèque, la signature FNCI ne doit, en aucun cas, être conservée par le commerçant sur quelque support que ce soit, en référence à l'article 5 du décret (abrogé et remplacé par l'article R-131-9 du code monétaire et financier), sous peine des sanctions prévues par l'article 226-21 du code pénal).

#### **A1.6. RÈGLE D'AFFICHAGE DES CHAMPS RÉPONSES**

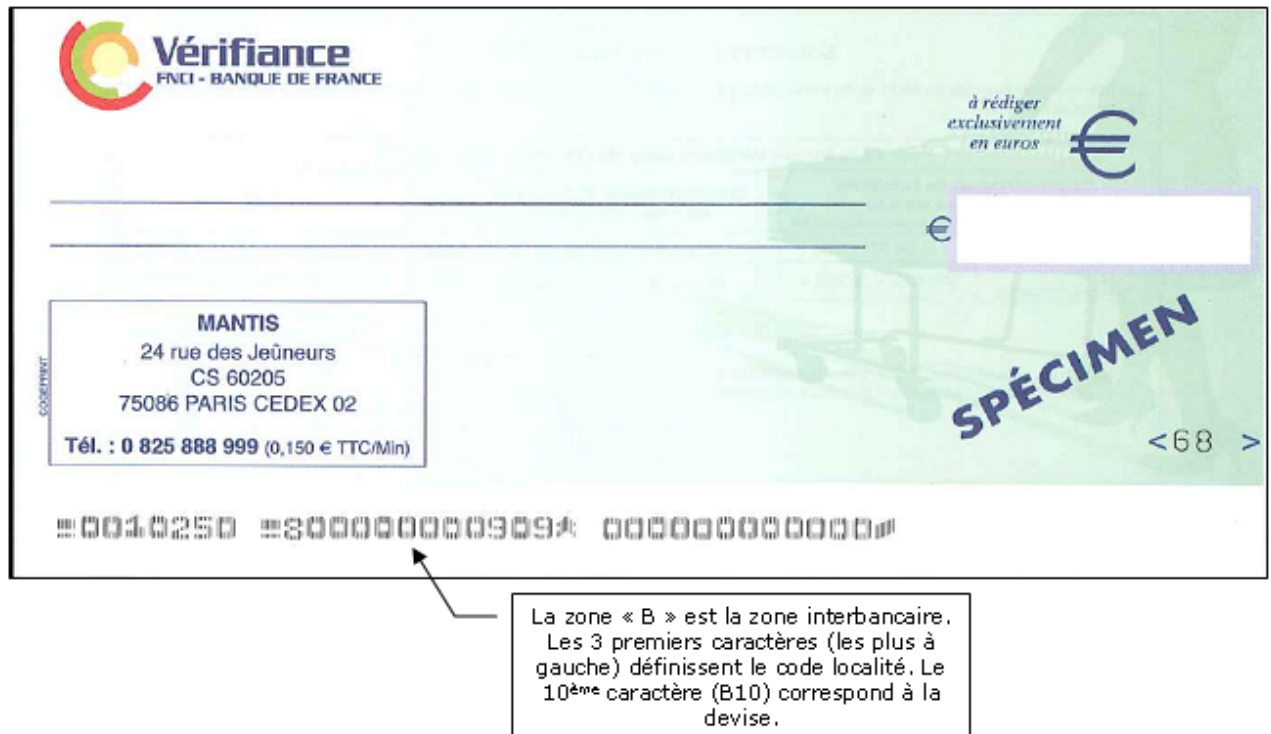
**ATTENTION** : Les garantisateurs qui utilisent le service Vérifiance pour leurs clients, doivent afficher clairement la réponse fournie par Vérifiance, sans l'occulter ni la déformer, avant d'afficher leurs propres réponses.

Le mandataire s'engage dans tous les cas à restituer sans délai et en l'état à son client la réponse Vérifiance selon la forme définie ci-dessus au paragraphe A1.4.1 (l'environnement de production).

Toute autre information que le mandataire aurait à communiquer à son mandant dans le cadre d'une prestation contractuelle distincte de Vérifiance devrait être adjointe à la réponse visée ci-dessus, sans l'occulter ni la déformer.

## A1.7. LES SPÉCIFICATIONS DU CODE DEVISE

### A1.7.1. Rappel sur la présentation d'un chèque



### A1.7.2. Règle de gestion du code devise « Euro »

Les vignettes " EURO " sont identifiables grâce au dixième caractère (en partant de la gauche) de la zone inter-bancaire de la ligne magnétique CMC7 qui prend la valeur " 9 " pour l'Euro (voir l'exemple ci-dessus).

La consultation FNCI entraîne une réponse de couleur Vérifiance.

### A1.7.3. Les autres devises

Si B10= 8 il s'agit d'un chèque en devise : La consultation FNCI entraîne une réponse de couleur Vérifiance.

Si B10= 0 ou autres (1-2-3-4-5-6-7) et si le code localité B1-B2-B3 (position 1, 2, 3 dans la zone interbancaire) est égal à:

- 984 Polynésie française ;
- 985 Nouvelle Calédonie ;
- 986 Wallis et Futuna

Alors on est face à un chèque libellé en Franc Pacifique (FCFP) : La consultation FNCI entraîne une réponse de couleur Vérifiance

Sinon la réponse du FNCI sera " BLANC "

## **A1.8. LE TELEPARAMETRAGE DES DONNEES**

### **A1.8.1 Définitions - rappels**

Le téléparamétrage permet de transmettre des données d'un Serveur vers une solution monétique, dans le but de renseigner ou modifier certains paramètres de celle-ci. Il peut être effectué soit à l'initiative du serveur soit manuellement sur la solution monétique.

Le téléchargement quant à lui consiste à transférer un (ou plusieurs) module(s) logiciel d'un serveur (de téléchargement) vers une solution monétique. Pour que le téléchargement se déclenche de façon automatique, il est nécessaire que certains paramètres spécifiques aient été transmis à la solution monétique au préalable.

Différents champs sont utilisés spécifiquement pour mettre en œuvre le téléparamétrage :

- Champ 46 : permet à la solution monétique d'indiquer au serveur ce qu'elle sait faire,
- Champ 47 : permet au serveur de fournir les paramètres permettant à la solution monétique d'appeler un serveur de téléchargement,
- Champ 48 : permet au serveur de fournir les paramètres permettant à la solution monétique de fonctionner.

Chacun de ces paramètres va être détaillé par la suite.

### **A1.8.2 CHAMP 46**

Le champ 46 permet donc à la solution monétique d'indiquer au serveur ce qu'elle sait faire.

#### **A1.8.2.1 Positions 1 et 2**

Elles permettent de préciser la capacité de raccordement. Cette information ne peut être qu'une combinaison entre ce que la solution monétique sait faire (d'un point de vue logiciel) et la réalité des infrastructures réseau auxquels elle est connecté.

Ainsi, ce n'est pas parce que la solution monétique sait gérer l'IP quelle peut se connecter à un réseau IP : si le commerçant ne dispose pas d'un abonnement à un FAI, la solution monétique ne saura jamais quoi faire avec une adresse IP.

Inversement, si le commerçant a résilié son abonnement téléphonique, il est inutile de transmettre un numéro de PAD malgré que la solution monétique sache gérer les PADs X25.

#### **A1.8.2.2 Position 3**

Elle permet à la solution monétique d'indiquer si elle peut déclencher un téléchargement de manière automatique, c'est à dire si elle sait traiter un champ 47.

#### **A1.8.2.3 Position 4**

Elle permet à la solution monétique d'indiquer si elle peut faire du téléparamétrage, c'est à dire si elle sait traiter un champ 48.

### **A1.8.3 CHAMP 47**

Ce champ permet au serveur de fournir les paramètres permettant à la solution monétique de se connecter à un serveur de téléchargement.

Il est intégré dans un message réponse FNCI 9310 utilisé par le Service Vérifiance ou dans un message réponse Garantisseur 9110 utilisé par les mandataires.

**ATTENTION** : Si la solution monétique a indiqué qu'elle ne gèrait pas le téléchargement automatique (position 3 du champ 46 valorisée à 0), elle doit ignorer ce champ s'il est malgré tout envoyé par le serveur.

Il a une longueur variable qui peut aller jusqu'à 65 535 caractères. De ce fait, il est précédé de 2 octets qui permettent de préciser sa longueur exacte.

Les paramètres fournis dans ce champ sont de la forme TYPE - LONGUEUR - VALEUR. De ce fait, ils peuvent apparaître dans n'importe quel ordre ou encore, être absents. Même s'ils ne sont pas dans l'ordre, ils doivent être acceptés par la solution monétique.

Le type est codé sur 2 caractères alphanumériques codés en ASCII.

La longueur est codé sur 2 caractères alphanumériques codés en ASCII (chaque caractère a donc une valeur hexadécimale comprise entre 0x30 et 0x39).

Les valeurs des paramètres (et leurs règles d'alimentation et d'utilisation) sont détaillées ci-après.

Un paramètre ne peut être accepté par la solution monétique (et donc être utilisé par la suite) que s'il est correctement formaté (valeurs possibles, caractères utilisés, longueur). Si ce n'est pas le cas, il n'est pas remplacé et ne sera donc pas utilisé.

A chaque changement de paramètre, une information peut être fournie à l'utilisateur (soit de façon temporaire via la visu soit de façon définitive via un ticket spécifique).

Un paramètre non connu de la solution monétique doit être ignoré. Par contre, cela ne signifie pas qu'il faut ignorer tout ce qui suit dans le champ 47 : la codification des différents paramètres permet tout à fait de passer au paramètre suivant, sans erreur.

Les paramètres transmis ne peuvent être utilisés que lors de la connexion suivante.

Le TPE doit accepter un message comportant des paramètres dans un ordre quelconque ou des paramètres non prévus à ce jour. Si un paramètre, indentifié par son type, est absent ou incorrect, le paramètre correspondant en mémoire dans le TPE ne doit pas être modifié.

**Exemple** : si le type d'adressage réseau dans T1 est incorrect c'est tout le paramètre T1 qui doit être ignoré.

**Remarque** : Pour supprimer l'un des paramètres T2, T3 ou T4, il convient de le transmettre avec une longueur nulle.

#### A1.8.3.1 Paramètre T1

Il permet de préciser les paramètres de télécommunication vers le site nominal de téléchargement.

Le type d'adressage réseau permet de savoir quelles informations sont présentes par la suite :

Valeur du type d'adressage réseau	Informations présentes	R = Requis O = Optionel	Taille maximale (en octets)
0 (IP v4)	Adresse réseau du service ou du DNS : il s'agit de l'adresse IP du serveur Vérifiance	R	10
	Numéro de téléphone d'accès au réseau : N° accès au NAS IP	O	15
	<b>Total</b>		<b>25</b>
1 (DNS IP v4)	Adresse réseau du service ou du DNS : il s'agit de l'adresse IP du DNS du serveur Vérifiance	R	10
	Nom de domaine	R	40
	Numéro de téléphone d'accès au réseau : N° accès au NAS IP	O	15
	<b>Total</b>		<b>65</b>
2 (X25)	Adresse réseau du service ou du DNS : il s'agit de l'adresse X25 du serveur Vérifiance	R	10
	Numéro de téléphone d'accès au réseau : N° de PAD	R	15
	Nature du PAD	R	1
	Données d'appel utilisateur*	R	10
	<b>Total</b>		<b>36</b>

\*Les données d'appel utilisateurs saisies lors de l'installation ne contiennent pas le caractère " D " qui sera rajouté automatiquement par la Solution Monétique. Il en va de même pour le champ "données d'appel utilisateur", qui ne contient pas de "D" en 1ère position.

Ce paramètre doit être systématiquement présent si l'on veut que la solution monétique puisse partir en téléchargement de manière automatique.

#### A1.8.3.2 Paramètres T2, T3 et T4

Ils permettent de préciser les paramètres de télécommunication vers les sites de secours de téléchargement.

La présence de 4 paramètres de télécommunication est rendue nécessaire pour permettre un adressage réseau nominal et une adresse réseau de secours, chacun de ces adressage ayant une adresse nominale et une adresse de secours.



Ainsi, pour permettre un accès nominal en IP avec un secours sur X25, un serveur peut fournir une adresse IP nominale et une adresse IP de secours puis une adresse X25 nominale et une adresse X25 de secours, ce qui fait donc 4 adresses différentes.

Toutefois, si le serveur ne souhaite fournir que 2 adresses différentes (par exemple un accès nominal en IP sur une adresse et un accès de secours en X25 sur une adresse), il utilisera uniquement les paramètres T1 et T2.

En conséquence, la solution monétique doit utiliser, à chaque connexion, les paramètres dans l'ordre : d'abord T1 puis, si la connexion ne fonctionne pas, elle utilise T2 (s'il a été transmis) puis, si la connexion ne fonctionne pas, elle utilise T3 (s'il a été transmis) puis, si la connexion ne fonctionne pas, elle utilise T4 (s'il a été transmis). Ce n'est qu'à ce moment qu'elle peut indiquer à l'utilisateur qu'elle ne peut se connecter au serveur.

#### A1.8.3.3 Paramètre PA

Ce paramètre permet de compléter tous les paramètres Ti (pour i compris entre 1 et 4) transmis dans le même champ.

Il peut être situé avant ou après les paramètres Ti, sans que cela n'ait un impact sur le traitement des différents paramètres.

**ATTENTION** : En cas d'absence du paramètre PA, on considère que les différents paramètres Ti sont incorrects et ne doivent pas être pris en compte.

La date et l'heure qui sont transmises dans ce paramètre sont bien locales à la solution monétique et non au serveur. Ceci peut donc avoir un impact sur la valeur à transmettre à une solution monétique située dans un autre fuseau horaire que le serveur qu'elle doit appeler.

#### A1.8.3.4 Paramètre CA

Ce paramètre permet à la solution monétique de s'identifier auprès du serveur de téléchargement. Sa valorisation ne peut être fournie que par l'entité responsable du téléchargeur (constructeur et/ou mainteneur).

#### A1.8.3.5 Paramètre RL

Ce paramètre permet à la solution monétique de demander le bon logiciel au serveur de téléchargement. Sa valorisation ne peut être fournie que par l'entité responsable du téléchargeur (constructeur et/ou mainteneur).

#### **A1.8.4 CHAMP 48**

Ce champ permet au serveur de fournir ses propres paramètres d'accès (ou les paramètres permettant d'accéder à un nouveau serveur : cas des migrations).

Il est intégré dans un message réponse FNCI 9310 utilisé par le Service VÉRIFIANCE ou dans un message réponse Garantisseur 9110 utilisé par les mandataires.

**ATTENTION** : Si la solution monétique a indiqué qu'elle ne gèrait pas le téléparamétrage automatique (position 3 du champ 46 valorisée à 0), elle doit ignorer ce champ s'il est malgré tout envoyé par le serveur.

Il a une longueur variable qui peut aller jusqu'à 65 535 caractères. De ce fait, il est précédé de 2 octets qui permettent de préciser sa longueur exacte.

Les paramètres fournis dans ce champ sont de la forme TYPE - LONGUEUR - VALEUR. De ce fait, ils peuvent apparaître dans n'importe quel ordre ou encore, être absents. Même s'ils ne sont pas dans l'ordre, ils doivent être acceptés par la solution monétique.

Le type est codé sur 2 caractères alphanumériques codés en ASCII

La longueur est codé sur 2 caractères alphanumériques codés en ASCII (chaque caractère a donc une valeur hexadécimale comprise entre 0x30 et 0x39)

Les valeurs des paramètres (et leurs règles d'alimentation et d'utilisation) sont détaillées ci-après.

Une "campagne " de téléparamétrage de données peut avoir lieu sans que l'utilisateur ne soit prévenu : il s'agit, pour le serveur, de pouvoir mettre à jour rapidement les données indiquées ci-après. La solution monétique recevant les données ainsi transmises doit les prendre en compte pour mettre à jour ses paramètres locaux.

Un paramètre ne peut être accepté par la solution monétique (et donc être utilisé par la suite) que s'il est correctement formaté (valeurs possibles, caractères utilisés, longueur). Si ce n'est pas le cas, il n'est pas remplacé et ne sera donc pas utilisé.

A chaque changement de paramètre, une information peut être fournie à l'utilisateur (soit de façon temporaire via la visu soit de façon définitive via un ticket spécifique).

Un paramètre non connu de la solution monétique doit être ignoré. Par contre, cela ne signifie pas qu'il faut ignorer tout ce qui suit dans le champ 48 : la codification des différents paramètres permet tout à fait de passer au paramètre suivant, sans erreur.

Les paramètres transmis ne peuvent être utilisés que lors de la connexion suivante.

Le TPE doit accepter un message comportant des paramètres dans un ordre quelconque ou des paramètres non prévus à ce jour. Si un paramètre, indentifié par son type, est absent ou incorrect, le paramètre correspondant en mémoire dans le TPE ne doit pas être modifié.

**Exemple** : si le type d'adressage réseau dans T1 est incorrect c'est tout le paramètre T1 qui doit être ignoré.

**Remarque** : Pour supprimer l'un des paramètres T2, T3 ou T4, il convient de le transmettre avec une longueur nulle.

#### A1.8.4.1 Paramètre T1

Il permet de préciser les paramètres de télécommunication vers le site nominal de consultation FNCI ou de garantie.

Le type d'adressage réseau permet de savoir quelles informations sont présentes par la suite :

Valeur du type d'adressage réseau	Informations présentes	R = Requis O = Optionel	Taille maximale (en octets)
0 (IP v4)	Adresse réseau du service ou du DNS : il s'agit de l'adresse IP du serveur Vérification	R	10
	Numéro de téléphone d'accès au réseau : N° accès au NAS IP	O	15
	<b>Total</b>		<b>25</b>
1 (DNS IP v4)	Adresse réseau du service ou du DNS : il s'agit de l'adresse IP du DNS du serveur Vérification	R	10
	Nom de domaine	R	40
	Numéro de téléphone d'accès au réseau : N° accès au NAS IP	O	15
	<b>Total</b>		<b>65</b>
2 (X25)	Adresse réseau du service ou du DNS : il s'agit de l'adresse X25 du serveur Vérification	R	10
	Numéro de téléphone d'accès au réseau : N° de PAD	R	15
	Nature du PAD	R	1
	Données d'appel utilisateur*	R	10
	<b>Total</b>		<b>36</b>

\*Les données d'appel utilisateurs saisies lors de l'installation ne contiennent pas le caractère " D " qui sera rajouté automatiquement par la Solution Monétique. Il en va de même pour le champ "données d'appel utilisateur", qui ne contient pas de "D" en 1ère position.

#### A1.8.4.2 Paramètres T2, T3 et T4

Ils permettent de préciser les paramètres de télécommunication vers les sites de secours de consultation FNCI ou de garantie.

La présence de 4 paramètres de télécommunication est rendue nécessaire pour permettre un adressage réseau nominal et un adresse réseau de secours, chacun de ces adressage ayant une adresse nominale et une adresse de secours.

Ainsi, pour permettre un accès nominal en IP avec un secours sur X25, un serveur peut fournir une adresse IP nominale et une adresse IP de secours puis une adresse X25 nominale et une adresse X25 de secours, ce qui fait donc 4 adresses différentes.

Toutefois, si le serveur ne souhaite fournir que 2 adresses différentes (par exemple un accès nominal en IP sur une adresse et un accès de secours en X25 sur une adresse), il utilisera uniquement les paramètres T1 et T2.

En conséquence, la solution monétique doit utiliser, à chaque connexion, les paramètres dans l'ordre : d'abord T1 puis, si la connexion ne fonctionne pas, elle utilise T2 (s'il a été transmis) puis, si la connexion ne fonctionne pas, elle utilise T3 (s'il a été transmis) puis, si la connexion ne fonctionne pas, elle utilise T4 (s'il a été transmis). Ce n'est qu'à ce moment qu'elle peut indiquer à l'utilisateur qu'elle ne peut se connecter au serveur.

#### A1.8.4.3 Paramètre SP

Ce paramètre permet au serveur d'indiquer à la solution monétique à partir de quel montant elle doit appeler son serveur.

Si ce paramètre est fourni dans un message FNCI 9310, avec une valeur VA alors la solution monétique n'appellera le service VÉRIFIANCE que si le montant de la transaction (champ 4) est supérieur ou égal à VA.

Si ce paramètre est fourni dans un message Garantisseur 9110, avec une valeur VB alors la solution monétique n'appellera le garantisseur que si le montant de la transaction (champ 4) est supérieur ou égal à VB.

**REMARQUE** : Si la solution monétique dispose des 2 applications (Vérifiance et Garantie) et si le montant de la transaction est supérieur à VA et à VB alors le constructeur de la solution monétique doit avoir traité ce cas de manière explicite afin d'éviter d'avoir deux appels.

Par défaut, ce paramètre vaut 0 € ou peut être initialisé à l'installation.

#### A1.8.4.4 Paramètre CF

Ce paramètre n'est utilisé que par le service Vérifiance. Il permet de remplacer le code d'accès Vérifiance présent dans la solution monétique.

Le code d'accès est formé de 10 caractères alphanumériques qui se décomposent de la façon suivante :

- Une racine comportant 7 caractères qui ne sont modifiés que lorsque des problèmes sont détectés sur l'utilisation du code d'accès.
- Un suffixe de 3 caractères qui est mis à jour (au moins) une fois par an, à la date anniversaire de l'abonnement.

Les 10 caractères doivent donc être modifiables.

Dans le cas du téléparamétrage, même si les 7 premiers caractères restent identiques, le service Vérifiance transmet les 10 caractères du code d'accès.

Lorsqu'un commerçant renouvelle (annuellement) son abonnement Vérifiance, la racine du nouveau code d'accès reste identique mais un nouveau suffixe est attribué.

Pendant un mois, le service Vérifiance accepte donc les codes d'accès comportant, soit l'ancien, soit le nouveau suffixe.

De plus, dans le cas d'un renouvellement complet du code d'accès Vérifiance, le nouveau code remplace immédiatement l'ancien (il doit donc être utilisé lors de la connexion suivante).

Lors d'une première ou de toute autre connexion, la solution monétique accédant au service Vérifiance doit utiliser, un code d'accès valide.

#### A1.8.5 Initialisation des paramètres

Lors de l'installation de la solution monétique, certains paramètres seront déjà valorisés par défaut et d'autres devront être initialisés par l'installateur. Le tableau ci-dessous précise le mode d'alimentation des différentes données :

Donnée		Paramètre concerné	Valeur par défaut	Saisie ou calcul obligatoire ?
Capacité de raccordement du Système d'Acceptation		Champ 46 - Positions 1 et 2	00 (Inconnue)	OUI
Gestion du téléchargement		Champ 46 - Position 3	Logiciel	NON
Gestion du téléparamétrage		Champ 46 - Position 4	Logiciel	NON
Site nominal de téléchargement	Type d'adressage réseau	Champ 47 - Paramètre T1	Non	NON
	Adresse réseau du service	Champ 47 - Paramètre T1	Non	NON
	Adresse réseau du DNS	Champ 47 - Paramètre T1	Non	NON
	Nom de domaine	Champ 47 - Paramètre T1	Non	NON
	Numéro de téléphone d'accès au réseau	Champ 47 - Paramètre T1	Non	NON
	Nature du PAD	Champ 47 - Paramètre T1	Non	NON
Site nominal de téléparamétrage	Type d'adressage réseau	Champ 48 - Paramètre T1	Non	OUI
	Adresse réseau du service	Champ 48 - Paramètre T1	Non	OUI (1)
	Adresse réseau du DNS	Champ 48 - Paramètre T1	Non	OUI (1)
	Nom de domaine	Champ 48 - Paramètre T1	Non	OUI (1)
	Numéro de téléphone d'accès au réseau	Champ 48 - Paramètre T1	Non	OUI (1)
	Nature du PAD	Champ 48 - Paramètre T1	Non	OUI (1)

Remarque (1) : la saisie de ces données est fonction de la valeur du type d'adressage réseau : on ne demande pas la saisie d'un PAD si l'adresse est de type IP.

## **ANNEXE 2**

<p><b>Exigences sécuritaires liées aux communications avec les systèmes d'acceptation</b></p>
---

ASSOCIATION DÉCLARÉE RÉGIE PAR LA LOI DU 1<sup>er</sup> JUILLET 1901, N°89 / 3905  
8, RUE DE CROUY - 41220 SAINT LAURENT NOUAN - TÉL : 02 54 87 06 12 - FAX : 02 54 87 06 12

[www.concert.asso.fr](http://www.concert.asso.fr)  
[contact@concert.asso.fr](mailto:contact@concert.asso.fr)

## **SOMMAIRE**

<b>A2.1. CONTEXTE.....</b>	<b>3</b>
----------------------------	----------

### **A2.1. CONTEXTE**

L'arrivée de nouveaux moyens de communications, de nouveaux terminaux et de nouvelles offres tarifaires modifient considérablement le schéma d'acheminement de la transaction.

L'ensemble des exigences sécuritaires est destiné à ajuster le niveau de sécurité pour tenir compte des nouveaux risques liés aux évolutions des communications avec les équipements qui utilisent un réseau IP pour se connecter au serveur FNCI ou à un serveur de garantie de chèque.

Le Groupe de Travail CONCERT s'est appuyé sur le document « Exigences Sécuritaires liées aux communications avec les systèmes d'acceptation paiement » (Version 1.5 de novembre 2005). Ce document est publié par le Groupement des Cartes Bancaires qui en assure la diffusion, sous la référence CEF/IS/HP/03.018.

Les principales évolutions par rapport au document original concernent les points suivants :

- La suppression du référencement à PCI DSS
- Les exigences 1, 2 et 4 sont facultatives
- Les autorités de certifications seront fournies par Vérifiance pour les accès FNCI et par les garantisseurs pour les demandes de garanties.

Nota Bene : Lors de la rédaction de cette version du document, il existait au sein du CONCERT un groupe de travail chargé de l'uniformisation de la gestion des certificats. Il sera bon de tenir compte des travaux de ce groupe de travail.