

LECTEUR CALYPSO "VOJJ"

Manuel d'intégration

Siège, Europe

SpringCard
13 voie la Cardon
Parc Gutenberg
91120 Palaiseau
FRANCE

Tel : +33 (0) 164 53 20 10
Fax : +33 (0) 164 53 20 18

Amériques

SpringCard
964 Fifth Avenue
Suite 235
San Diego, CA 92101
USA

Tel : +1 (619) 544 1450
Fax : +1 (619) 573 6867

www.springcard.com

IDENTIFICATION DU DOCUMENT

Catégorie : Manuels d'intégration
Famille : Contrôle d'accès / Calypso
Référence : PMD9328
Version : AC
Etat : DRAFT

Mots clés :

Résumé :

pmd9328-ac.doc
enregistré le 21/08/09 – imprimé le 21/08/09

HISTORIQUE DES VERSIONS

Ver.	Date	Auteur	Validation		Approb.	Détails :
			Tech.	Qual.		
AB	17/08/09	JDA				Première version diffusée
AC	21/08/09	JDA		ECL		Mise à jour protocole de test RCTIF

TABLE DES MATIERES

1.	INTRODUCTION.....	4
1.1.	CONTEXTE	4
1.2.	PRESENTATION DU PRODUIT	4
1.3.	IDENTIFICATION DU DOCUMENT	4
1.4.	DOCUMENTS APPLICABLES	4
2.	PROTOCOLE DE COMMUNICATION.....	6
2.1.	ASPECTS PHYSIQUES	6
2.2.	PROTOCOLE SIMPLIFIE POINT A POINT.....	6
2.3.	PROTOCOLE MULTIPOINT	7
3.	JEU DE COMMANDES	9
3.1.	COMMANDES D'ETAT.....	9
3.2.	COMMANDES DE PARAMETRAGE	14
3.3.	COMMANDES DE LECTURE.....	18
3.4.	ACQUITTEMENT ET MESSAGES D'ERREURS	21
4.	DONNEES DES CARTES	22
4.1.	PRINCIPES	22
4.2.	TYPE DE CARTE	22
4.3.	NUMERO DE SERIE	23
4.4.	RESULTAT DU TRAITEMENT.....	23
4.5.	INFORMATIONS COMPLEMENTAIRES.....	27
5.	REGISTRES DE CONFIGURATION.....	28
5.1.	LISTE DES REGISTRES DE CONFIGURATION	28
5.2.	REGISTRES GENERAUX	29
5.3.	REGISTRES POUR LE PROTOCOLE CALYPSO	32
5.4.	REGISTRES POUR LE TRAITEMENT CALYPSO	34
5.5.	PARAMETRES DE COMMUNICATION.....	37
6.	PROTOCOLE DE TEST RCTIF	38
6.1.	ACCEDER AU MODE TEST	38
6.2.	JEU DE COMMANDES POUR LES TESTS	39
6.3.	SUITE DE TESTS DU RCTIF 3.4	42
6.4.	SUITE DE TESTS DU RCTIF 4.0	43
6.5.	AUTRES COMMANDES POUVANT ETRE UTILISEES POUR LES TESTS.....	44

1. INTRODUCTION

1.1. CONTEXTE

L'équipement de parcs relais (P+R) en région Ile-de-France nécessite la l'installation de lecteurs :

- pouvant lire les cartes Calypso,
- conformes aux spécifications du STIF,
- capables de valider et d'authentifier les cartes (à l'aide SAM), pour décharger les systèmes de traitement de cette tâche.

Pro Active, bureau d'étude de SpringCard, propose un firmware pour ses produits OEM qui répond à ces 3 exigences.

1.2. PRESENTATION DU PRODUIT

Le produit fourni par Pro Active reprend la plateforme matérielle du **SpringCard CrazyWriter**, mais dispose d'un firmware (logiciel embarqué) spécifique, qui assure notamment les fonctionnalités suivantes :

- Communication avec le serveur via un protocole multi point (compatible avec une mise en œuvre en bus RS-485),
- La lecture et l'authentification des cartes Calypso en respectant les particularités du réseau Ile-de-France (« Navigo »),
- Lecture possible d'autres types de cartes (dont Mifare) pour les badges abonnés hors Navigo.

1.3. IDENTIFICATION DU DOCUMENT

Le présent document constitue le manuel d'intégration du lecteur. Il ne contient que les éléments spécifiques à ce firmware.

Pour les éléments non-spécifiques (spécifications du matériel, installation du pilote USB, utilisation des cartes de configuration, ...) se reporter aux documents du **SpringCard CrazyWriter**.

Le chapitre 6 détaille les fonctionnalités implémentées pour faciliter la mise en œuvre du programme de tests RCTIF.

1.4. DOCUMENTS APPLICABLES

1.4.1. Standard internationaux

- ISO/IEC 14443-2 2001
- ISO/IEC 14443-3 2001
- ISO/IEC 14443-4 2001

1.4.2. Spécification Calypso

- Validator Batteryless Tag Protocol v. 3.2
- Portable Object Application Revision 3
- Calypso Technical Note #003 27/12/2002
- Calypso Technical Note #012 17/01/2005
- Calypso Technical Note #014 29/08/2006

1.4.3. Spécifications STIF

- RCTIF 3.4B
- RCTIF 4.0
- Définition des données sur les cartes, 1^{ère} phase
- Définition des données sur les cartes, 2^{ème} phase
- Traitement des données sur la carte - Contrôle d'accès aux Parcs Relais

2. PROTOCOLE DE COMMUNICATION

2.1. ASPECTS PHYSIQUES

Le lecteur communique en liaison série à 38400bps¹, 8 bits de données, 1 bit de stop, pas de parité, pas de contrôle de flux.

La liaison physique utilise généralement un RX/TX séparé (RS-232), mais le lecteur et le protocole sont conçus pour être compatibles avec un bus RS-485.

2.2. PROTOCOLE SIMPLIFIÉ POINT A POINT

2.2.1. Principes

Ce protocole est destiné à la mise au point ou au prototypage. L'absence de contrôle de validité et les *timings* « lâches » ne le destinent pas à une utilisation industrielle.

Les trames sont échangées en ASCII (1 octet est représenté par sa transcription hexadécimale en ASCII : `hA2` devient « A2 »). Ceci permet une saisie manuelle des commandes (au prix d'une multiplication par 2 de la longueur des trames).

2.2.2. Format de trame serveur → lecteur

- L'en-tête de trame est le caractère « \$ »,
- La **commande** est exprimée sur 2 caractères (0→9, A→F),
- La **longueur des données** (L) est exprimée sur 2 caractères (0→9, A→F),
- Les **données** (si L>0) sont exprimées sur 2xL caractères (0→9, A→F),
- La trame est terminée par CR (LF ignoré si présent).

2.2.3. Format de trame lecteur → serveur

- L'en-tête de trame est le caractère « + »,
- Le **résultat** (acquiescement ou code d'erreur) est exprimé sur 2 caractères (0→9, A→F),
- La **longueur des données** (L) est exprimée sur deux 2 caractères (0→9, A→F),
- Les **données** (si L>0) sont exprimées sur 2xL caractères (0→9, A→F),
- La trame est terminée par CR et LF.

¹ Le débit peut être modifié par configuration, cf. § 5.5.1 .

2.3. PROTOCOLE MULTIPOINT

2.3.1. Principes

Les trames sont échangées « brutes » (1 octet = 1 octet). L'en-tête contient un octet d'adressage et un octet de numéro de séquence pour permettre la cohabitation de plusieurs lecteurs sur un même bus.

Un LRC permet de détecter les erreurs de communication.

2.3.2. Format de trame serveur → lecteur

- La trame commence par le caractère STX ($_{h}02$),
- **Adresses** sur 1 octet,
- **Séquence** sur 1 octet,
- **Commande** sur 1 octet,
- **Longueur des données** (L) sur 1 octet,
- **Données** (si $L > 0$) sur L octets,
- **LRC** sur un 1 octet (= **XOR** de tous les octets de la trame, sauf STX, ETX, et le LRC lui-même),
- La trame se termine par le caractère ETX ($_{h}03$).

2.3.3. Format de trame lecteur → serveur

- La trame commence par le caractère STX ($_{h}02$),
- **Adresses** sur 1 octet,
- **Séquence** sur 1 octet,
- **Résultat** sur 1 octet,
- **Longueur des données** (L) sur 1 octet,
- **Données** (si $L > 0$) sur L octets,
- **LRC** sur un 1 octet (= **XOR** de tous les octets de la trame, sauf STX, ETX, et le LRC lui-même),
- La trame se termine par le caractère ETX ($_{h}03$).

2.3.4. Règles pour le champ Adresses

- Le quartet de poids fort est l'adresse du serveur. Le serveur positionne la valeur qu'il souhaite (sauf $_{h}F$, valeur interdite),
- Le quartet de poids faible est l'adresse du lecteur. Le serveur positionne indique le numéro du lecteur avec lequel il souhaite communiquer. La valeur $_{h}F$ correspond à l'adresse de *broadcast*.

a. Comportement en mode unicast

Si l'adresse de lecteur indiquée est différente de $_hF$, le message est dit « adressé » (*unicast*).

Si l'adresse de lecteur indiquée est différente de l'adresse courante du lecteur (registre de configuration $_h68$, § 5.5.2), le lecteur ignore la trame.

Si l'adresse de lecteur indiquée est égale à l'adresse courante du lecteur, le lecteur accepte la trame (et y répondra obligatoirement).

Dans sa réponse, le lecteur recopie la valeur du champ *Adresses* indiquée par le serveur :

- Le quartet de poids fort est l'adresse du serveur,
- Le quartet de poids faible est l'adresse du lecteur.

b. Comportement en mode broadcast

Si l'adresse de lecteur indiquée est égale à $_hF$, le message est dit « non adressé » (*broadcast*).

Selon l'adresse courante du lecteur (registre de configuration $_h68$, § 5.5.2) et selon la commande, le lecteur va accepter ou ignorer la trame.

Le lecteur ne répond JAMAIS aux commandes reçues sur l'adresse de *broadcast*, SAUF à la commande **Query Version Info** (§ 3.1.4)².

Dans ce cas, le lecteur recopie la valeur du champ *Adresses* indiquée par le serveur :

- Le quartet de poids fort est l'adresse du serveur,
- Le quartet de poids faible est l'adresse de *broadcast* ($_hF$).

2.3.5. Règles pour le champ Séquence

Le serveur impose à chaque commande le numéro de séquence qu'il souhaite. Le lecteur envoie systématiquement sa réponse avec le même numéro de séquence.

Si le numéro de séquence reçu du serveur est le même que celui de la dernière réponse envoyée, le lecteur répète la réponse sans re-exécuter la commande.

Dans tous les autres cas, il exécute la commande puis envoie la réponse.

Ceci permet au serveur de demander au lecteur de répéter sa réponse en cas d'erreur de réception.

2.3.6. Timings

A compléter

² Et encore, seulement lorsque l'adresse du lecteur n'a pas encore été configurée.

3. JEU DE COMMANDES



Toutes les commandes doivent être passées dans le protocole point à point ou dans le protocole multipoint unicast.

Le protocole multipoint broadcast est limité à un sous-ensemble du jeu de commandes.

Code	Commande	Unic.	Broadc.	§
Commandes d'état				
_h 80	Get Version Info	✓	-	3.1.1
_h 81	Get Status	✓	-	3.1.2
_h 8C	Read Config	✓	(a)	3.1.3
_h 8F	Query Version Info	-	(a)	3.1.4
Commandes de paramétrage				
_h 90	Set Date and Time	✓	✓	3.2.1
_h 9A	Apply Config	✓	(a)	3.2.3
_h 9C	Write Config	✓	(a)	3.2.2
_h 9E	Reset	✓	✓	3.2.4
Commandes de lecture				
_h A0	Stop polling	✓	✓	3.3.2
_h A1	Start polling	✓	✓	3.3.1
_h AC	Get Card Status	✓	-	3.3.3

(a) *Broadcast* accepté seulement si l'adresse du lecteur n'a pas encore été configurée.

3.1. COMMANDES D'ETAT

3.1.1. Get Version Info

La commande **Get Version Info** permet d'obtenir les informations sur le firmware (type, version), et le hardware du lecteur, ainsi que son numéro de série.

Le lecteur n'accepte cette commande que dans le protocole point à point ou dans le protocole multipoint *unicast*.

a. Commande

Octet	Valeur	Description	Valeurs autorisées
0	_h 80	Commande Get Version Info	
1	_h 00	Longueur à suivre	

b. Réponse

Octet	Valeur	Description	Valeurs autorisées
0	h00	Réponse OK	
1	h10	Longueur des données	16
2		Type hardware	<u>h31</u>
3 à 6		Code hardware	« CW31 »
7 à 10		Code firmware	« VOJJ »
11		Version majeure <u>en BCD</u>	<u>h00 à h99</u>
12		Version mineure <u>en BCD</u>	<u>h00 à h99</u>
13		Release	<u>h00 à hFF</u>
14 à 17		Numéro de série du lecteur	<u>h00000000 à hFFFFFFF</u>

3.1.2. Get Status

La commande **Get Status** permet d'obtenir l'état courant du lecteur, ainsi que sa date et son heure.

Le lecteur n'accepte cette commande que dans le protocole point à point ou dans le protocole multipoint *unicast*.

a. Commande

Octet	Valeur	Description	Valeurs autorisées
0	h81	Commande Get Status	
1	h00	Longueur à suivre	

b. Réponse

Octet	Valeur	Description	Valeurs autorisées
0	h00	Réponse OK	
1	h08	Longueur des données	
2		Etat du lecteur	voir § 0 ci-après
3		Etat des SAMs	voir § d ci-après
4		L'année <u>en BCD</u>	De 0 à 100, 0 → 2000
5		Le mois <u>en BCD</u>	De 1 à 12
6		Le jour dans le mois <u>en BCD</u>	De 1 à 31
7		L'heure <u>en BCD</u>	De 0 à 23
8		La minute <u>en BCD</u>	De 0 à 59
9		La seconde <u>en BCD</u>	De 0 à 59

c. Valeurs pour l'octet 2

L'octet 2 de la réponse à la commande **Get Status** est un champ de bits qui contient l'état courant du lecteur.

Bit	Nom	Si = 0	Si = 1
msb 7	Erreur hardware	Pas d'erreur	Le lecteur n'est pas opérationnel
6	RFU		
5	RFU		
4	RFU		
3	RFU		
2	RFU		
1	RFU		
lsb 0	Erreur date/heure	Pas d'erreur	Utiliser la commande <i>Set Date & Time</i> (§ 3.2.1) pour mettre le lecteur à l'heure.

d. Valeurs pour l'octet 3

L'octet 3 de la réponse à la commande **Get Status** est un champ de bits qui contient l'état courant des SAMs du lecteur.

Bit	Nom	Si = 0	Si = 1
msb 7	RFU		
6	RFU		
5	RFU		
4	RFU		
3	Erreur SAM B	Pas d'erreur	Le SAM n'est plus actif
2	Absence SAM B	SAM présent	SAM absent
1	Erreur SAM A	Pas d'erreur	Le SAM n'est plus actif
lsb 0	Absence SAM A	SAM présent	SAM absent



Si le lecteur n'est pas configuré pour utiliser un SAM, la présence du SAM n'est pas testée. Le bit « présence » est maintenu à 0 quel que soit le statut « physique » du slot.

3.1.3. Read Config

Le lecteur dispose de registres de configuration non-volatiles pour stocker son paramétrage (voir chapitre 5).

La commande **Read Config** permet de consulter la valeur d'un de ces registres.



Si le registre n'est pas programmé, une valeur par défaut est utilisée par le lecteur. La commande *Read Config* ne permet pas de consulter la valeur par défaut.

Le lecteur accepte cette commande dans tous les protocoles, y compris en multipoint *broadcast* tant que son adresse n'est pas configurée. Dès que son adresse est configurée, le lecteur n'accepte plus cette commande que dans le protocole point à point ou dans le protocole multipoint *unicast*.

a. Commande

Octet	Valeur	Description	Valeurs autorisées
0	h8C	Commande Read Config	
1	h01	Longueur à suivre	
2		Le numéro du registre à consulter	De h01 à hFE

b. Réponse

Octet	Valeur	Description	Valeurs autorisées
0	h00	Réponse OK	
1		Longueur des données	0 à 32
2 à 2+L		Les données actuelles du registre	Dépend du registre, se reporter au chapitre 5

Si le registre n'est pas programmé, la trame est renvoyée sans donnée (longueur 0).

3.1.4. Query Version Info

La commande **Query Version Info** permet d'obtenir les informations sur le firmware (type, version), et le hardware d'un lecteur AVANT de lui affecter une adresse.



Le serveur peut utiliser cette commande pour identifier un nouveau lecteur connecté à son bus.

Il doit ensuite lui affecter une adresse en modifiant le registre $_h68$ (§ 5.5.2).

Le lecteur n'accepte cette commande que dans le protocole multipoint *broadcast*, et seulement si son adresse n'est pas configurée. Dès que son adresse est configurée, le lecteur ignore cette commande quel que soit le protocole.

a. Commande

Octet	Valeur	Description	Valeurs autorisées
0	$_h8F$	Commande Query Version Info	
1	$_h00$	Longueur à suivre	

b. Réponse

Idem réponse à **Get Version Info** (cf. § 0)

3.2. COMMANDES DE PARAMETRAGE

3.2.1. Set Date & Time

La commande **Set Date & Time** permet de transmettre au lecteur la date et l'heure courantes. Ces éléments sont indispensables pour pouvoir vérifier la validité des titres de transport.



Le lecteur ne dispose pas d'une véritable horloge interne. La dérive peut atteindre quelques minutes par heure.

Il est recommandé d'émettre la commande **Set Date & Time** à intervalle régulier, typiquement toutes les 10 minutes.

Le lecteur accepte cette commande dans tous les protocoles. Ceci permet d'envoyer la date et l'heure en *broadcast* à tous les lecteurs.

a. Commande

Octet	Valeur	Description	Valeurs autorisées
0	h90	Commande Set Date & Time	
1	h06	Longueur à suivre	
2		L'année <u>en BCD</u>	De 0 à 100, 0 → 2000
3		Le mois <u>en BCD</u>	De 1 à 12
4		Le jour dans le mois <u>en BCD</u>	De 1 à 31
5		L'heure <u>en BCD</u>	De 0 à 23
6		La minute <u>en BCD</u>	De 0 à 59
7		La seconde <u>en BCD</u>	De 0 à 59

b. Réponse

Acquittement ou message d'erreur, voir paragraphe 3.4.

3.2.2. Write Config

Le lecteur dispose de registres de configuration non-volatiles pour stocker son paramétrage (voir chapitre 5).

La commande **Write Config** permet de modifier la valeur d'un de ces registres, ou de la supprimer (le logiciel utilise alors la valeur par défaut).



Les modifications apportées aux registres de configuration sont écrites immédiatement dans la mémoire non-volatile, mais ne sont prises en compte qu'au démarrage suivant.

Utiliser la commande **Apply Config** (§ 3.2.3) pour forcer la prise en compte sans redémarrage.



L'endurance de la mémoire non-volatile est limitée à 1000 cycles d'écriture ou d'effacement. Ne pas utiliser abusivement la commande **Write Config**.

Le lecteur accepte cette commande dans tous les protocoles, y compris en multipoint *broadcast* tant que son adresse n'est pas configurée. Dès que son adresse est configurée, le lecteur n'accepte plus cette commande que dans le protocole point à point ou dans le protocole multipoint *unicast*.

a. Commande

Octet	Valeur	Description	Valeurs autorisées
0	h9C	Commande Write Config	
1		Longueur à suivre	1 pour effacement 1 + longueur des données pour écriture
2		Le numéro du registre à modifier	De h01 à hFE
3 à 3+L		Les données à écrire dans le registre	Dépend du registre, se reporter au chapitre 5

b. Réponse

Acquittement ou message d'erreur, voir paragraphe 3.4.

3.2.3. Apply Config

Le lecteur dispose de registres de configuration non-volatiles pour stocker son paramétrage (voir chapitre 5).

La commande **Apply Config** permet de provoquer la relecture de ces registres, et la prise en compte des valeurs pour le fonctionnement du logiciel.

Le lecteur accepte cette commande dans tous les protocoles, y compris en multipoint *broadcast* tant que son adresse n'est pas configurée. Dès que son adresse est configurée, le lecteur n'accepte plus cette commande que dans le protocole point à point ou dans le protocole multipoint *unicast*.

a. Commande

Octet	Valeur	Description	Valeurs autorisées
0	h9A	Commande Apply Config	
1	h00	Longueur à suivre	

b. Réponse

Acquittement ou message d'erreur, voir paragraphe 3.4.



La nouvelle configuration est prise en compte après l'envoi de l'acquittement. Attendre 250ms avant d'envoyer la commande suivante pour que le lecteur ait terminé son initialisation.

3.2.4. Reset

La commande **Reset** permet de redémarrer le lecteur.



L'effet de la commande **Reset** est analogue à celui de la commande **Apply Config** (§ 3.2.3), sauf qu'en plus

- Le lecteur « perd » la date et l'heure courante (qu'il faut lui redonner par la commande Set Date & Time, § 3.2.1),
- Le lecteur passe en mode inactif (il faut le réactiver par la commande Start Polling, § 3.3.1),
- Le lecteur réinitialise les SAMs.

Le lecteur accepte cette commande dans tous les protocoles.

a. Commande

Octet	Valeur	Description	Valeurs autorisées
0	h9E	Commande Reset	
1	h02	Longueur à suivre	
2	hDE	Constante	
3	hAD	Constante	

b. Réponse

Aucune. Le lecteur redémarre sans envoyer d'acquiescement.

Attendre 500ms avant d'utiliser la commande **Get Version Info** (§ 3.1.1) pour re-tester la présence du lecteur.

3.3. COMMANDES DE LECTURE

3.3.1. Start Polling

La commande **Start Polling** demande au lecteur de se mettre en recherche de cartes sans contact.

La commande **Get Card Status** (§ 3.3.3) doit être envoyée périodiquement pour savoir si une carte a été lue.

Le lecteur accepte cette commande dans tous les protocoles. Ceci permet par *broadcast* d'activer tous les lecteurs.

a. Commande courte

Octet	Valeur	Description	Valeurs autorisées
0	hA1	Commande Start Polling	
1	h00	Longueur à suivre	

Lorsque la commande courte est utilisée, le lecteur se met en recherche de cartes sans contact et s'arrête dès qu'une carte a été lue (mode *autostop*).

b. Commande longue

Octet	Valeur	Description	Valeurs autorisées
0	hA1	Commande Start Polling	
1	h01	Longueur à suivre	
2		Paramètre	Voir ci-dessous

Valeurs pour l'octet paramètre :

- **h00** : Mode *autostop* (idem commande courte),
- **h01** à **hFF** (1 à 255) : Recherche permanente (le lecteur ne s'arrête pas après la lecture d'une carte). Lorsque qu'une carte a été lue, le lecteur marque une pause de 0,1 à 25,5 secondes (la valeur indiquée est la durée de la pause exprimée en dixièmes de secondes).

c. Réponse

Acquittement ou message d'erreur, voir paragraphe 3.4.

Dès qu'une carte est découverte, le lecteur arrête sa recherche. Il attend ensuite une commande **Get Card Status** (§ 3.3.3) pour en renvoyer les données.

3.3.2. Stop Polling

La commande **Stop Polling** interrompt la recherche de cartes sans contact.

Le lecteur accepte cette commande dans tous les protocoles. Ceci permet par *broadcast* de désactiver tous les lecteurs.

a. Commande

Octet	Valeur	Description	Valeurs autorisées
0	hA0	Commande Stop Polling	
1	h00	Longueur à suivre	

b. Réponse

Acquittement ou message d'erreur, voir paragraphe 3.4.

3.3.3. Get Card Status

La commande **Get Card Status** permet d'interroger le lecteur pour savoir s'il a lu une carte, et dans ce cas en obtenir les données.

Le lecteur n'accepte cette commande que dans le protocole point à point ou dans le protocole multipoint *unicast*.

a. Commande

Octet	Valeur	Description	Valeurs autorisées
0	hAC	Commande Get Card Status	
1	h00	Longueur à suivre	

b. Réponse en présence d'une carte

Octet	Valeur	Description	Valeurs autorisées
0	h00	Réponse OK	
1	5+l ₁ +l ₂	Longueur totale des données	62 au maximum
2		Type de carte	Se reporter au chapitre 4
3	l ₁	Longueur du numéro de série	
4 à 3+l ₁		Numéro de série de la carte	
4+l ₁ à 5+l ₁		Résultat du traitement (2o, <u>MSB first</u>)	
6+l ₁	l ₂	Longueur des informations	
7+l ₁ à 6+l ₁ +l ₂		Informations complémentaires	

c. Réponse si le lecteur est inactif

Si le lecteur n'est pas actif (**Get Card Status** non précédé de **Start Polling**) :

Octet	Valeur	Description	Valeurs autorisées
0	h0A	Réponse Reader not active	
1	h00	Longueur à suivre	

d. Réponse en l'absence de carte :

Octet	Valeur	Description	Valeurs autorisées
0	h0C	Réponse Card absent	
1	h00	Longueur à suivre	

e. En présence d'une carte en erreur fatale de lecture

Octet	Valeur	Description	Valeurs autorisées
0	h0E	Réponse Card error	
1	h00	Longueur à suivre	



Lorsqu'une erreur de lecture non fatale survient, le lecteur renvoie **h00 (OK)**, et indique dans le champ *résultat du traitement* l'erreur survenue. Se reporter au chapitre 4.

3.4. ACQUITTEMENT ET MESSAGES D'ERREURS

3.4.1. Comportement en mode multipoint *broadcast*

Le lecteur ne répond JAMAIS (ni acquittement, ni erreur) à une trame envoyée en *broadcast*, SAUF à la commande **Query Version Info** (§ 3.1.4).

3.4.2. Acquittement

Lorsqu'une commande est correctement reçue et correctement exécutée par le lecteur, la réponse est :

Octet	Valeur	Description
0	h00	Réponse OK
1	h00	Longueur à suivre

3.4.3. Erreurs liées au protocole ou au jeu de commandes

a. Commande reçue en erreur (CRC)

Octet	Valeur	Description
0	h1E	Réponse CRC error
1	h00	Longueur à suivre

b. Le code de la commande est inconnu du lecteur

Octet	Valeur	Description
0	h1C	Réponse Unknown code
1	h00	Longueur à suivre

c. La longueur des données n'est pas acceptable pour cette commande

Octet	Valeur	Description
0	h10	Réponse Wrong length
1	h00	Longueur à suivre

d. La valeur des données n'est pas acceptable pour cette commande

Octet	Valeur	Description
0	h1D	Réponse Wrong data
1	h00	Longueur à suivre

3.4.4. Erreurs du lecteur

a. Erreur d'écriture dans la mémoire non-volatile

Octet	Valeur	Description
0	h2E	Réponse E2PROM error
1	h00	Longueur à suivre

4. DONNEES DES CARTES

4.1. PRINCIPES

Dès qu'une carte a été reconnue, le lecteur effectue le traitement défini dans son paramétrage.

Quel que soit le résultat du traitement, la commande *Get Card Status* renverra le code $_{h}00$ (**OK**), suivi du type et du numéro de série de la carte, et du résultat du traitement ($_{h}0000$ = traitement nominal ; valeur non nulle = erreur ou avertissement).

Si le traitement permet d'extraire d'autres informations de la carte (ex : lecture d'un bloc fatale ou récupération d'un champ dans un fichier Calypso), ces éléments sont ajoutés à la suite de la réponse dans le champ *informations complémentaires*.

Voici le format de la trame de données (cf. § 3.3.3.b) :

Octet	Valeur	Description
0	$_{h}00$	Réponse OK
1	$5+l_1+l_2$	Longueur totale des données
2		Type de carte
3	l_1	Longueur du numéro de série (4 à 16)
4 à $3+l_1$		Numéro de série de la carte
$4+l_1$ à $5+l_1$		Résultat du traitement (2o, MSB first)
$6+l_1$	l_2	Longueur des informations (0 à 32)
$7+l_1$ à $6+l_1+l_2$		Informations complémentaires

4.2. TYPE DE CARTE

Le champ **type de carte** (1 octet) prend l'une des valeurs suivantes, selon le type de carte qui a été lue :

Valeur	Type de carte
$_{h}01$	ISO 14443-A (<i>hors carte portant l'application Calypso</i>)
$_{h}02$	ISO 14443-B (<i>hors carte portant l'application Calypso</i>)
$_{h}04$	ISO 15693
$_{h}08$	NXP ICODE1
$_{h}10$	Inside Contactless PicoPass (ou HID iClass)
$_{h}20$	ST MicroElectronics SRxxx
$_{h}40$	ASK CTS256B ou CTS512B
$_{h}80$	Innovatron
$_{h}81$	Carte ISO 14443-A portant l'application Calypso ³
$_{h}82$	Carte ISO 14443-B portant l'application Calypso ⁴

Les autres valeurs sont *RFU*.

³ Cette valeur peut être forcée à $_{h}80$, cf. § 5.3.5.

⁴ Cette valeur peut être forcée à $_{h}80$, cf. § 5.3.5.

4.3. NUMERO DE SERIE

Le champ **numéro de série** est préfixé par l'octet I_1 qui en précise la longueur.

Dans le cas général, la longueur du numéro de série dépend à la fois du type de carte et de la configuration du lecteur (cf. § 5.2.5).

L'utilisation typique est de forcer la longueur du numéro de série à 8 octets.



Le lecteur transmet les numéros de série « bruts ». Si une conversion décimale (BCD) est nécessaire avant traitement, elle doit être effectuée par le logiciel côté serveur.

4.4. RESULTAT DU TRAITEMENT

Le champ **résultat du traitement** contient un code d'erreur ou d'avertissement lié à la lecture et à l'authentification de la carte.

4.4.1. Pour les cartes hors Calypso

Le champ **résultat du traitement** vaut $_h0000$.

4.4.2. Pour les cartes Calypso

Voir sur les pages suivantes la liste des valeurs possibles pour les cartes Calypso.

Succès :

Code	Explication	Message utilisateur	Action serveur recommandée
h0000	OK	PASSEZ	Accepter la carte

Avertissements :

Code	Explication	Message utilisateur	Action serveur recommandée
h1002	Le lecteur n'a pas été en mesure de vérifier la zone (<i>ContractValidityZone</i>)		Accepter la carte Configurer le registre h33 (§ 5.4.4)
h1004	Le lecteur n'a pas été en mesure de vérifier les dates (<i>EnvApplicationEndDate</i> , <i>ContractValidityStartDate</i> , <i>ContractValidityEndDate</i>)		Accepter la carte Mettre le lecteur à l'heure (§ 3.2.1)
h1010	L'authentification par le SAM n'a pas été effectuée : le lecteur ne sait pas quelles clés d'authentification utiliser		Accepter la carte Désactiver le SAM (registre h2F, § 5.3.6) ou paramétrer les clés (registre h3A, § 5.4.7)
h2020	L'authentification par le SAM n'a pas été effectuée : le SAM est absent, muet, ou trop d'erreurs de communication ont été détectées		Accepter la carte Désactiver le SAM (registre h2F, § 5.3.6) ou insérer un SAM fonctionnel
h2040	L'authentification par le SAM n'a pas été effectuée : la communication avec le SAM a échoué pendant la transaction		Réactiver le lecteur (si <i>autostop</i>), répéter <i>Get Card Status</i>
h2080	L'authentification par le SAM n'a pas été effectuée : le SAM est bloqué		Accepter la carte Désactiver le SAM (registre h2F, § 5.3.6) ou remplacer le SAM



Les codes d'avertissements sont des valeurs combinables par la fonction OU logique.

Par ex. le code h3083 signale que le SAM bloqué, que le lecteur ne connaît pas la date et l'heure, et que les zones à accepter ne sont pas configurées.

Erreurs de communication :

Code	Explication	Message utilisateur	Action serveur recommandée
h8000	Echec d'activation (carte détectée, mais erreur sur ATTRIB ou ATS)	ERREUR LECTURE, REESSAYEZ	Retenter
h8001	Transaction interrompue (carte retirée ou en limite de portée)	ERREUR LECTURE, REESSAYEZ	Retenter
h8002	Plusieurs cartes dans le champ (anticollision)	UNE CARTE A LA FOIS SVP	Retenter
h8010	Erreur de communication persistante (niveau physique)	ERREUR LECTURE, REESSAYEZ	Retenter
h8011	Erreur de communication persistante (niveau protocole)	ERREUR LECTURE, REESSAYEZ	Retenter
h8020	Erreur carte fatale (carte non conforme aux spécifications)	CARTE ILLISIBLE	Refuser la carte

Retenter = réactiver le lecteur par *Start Polling* (si *autostop* actif) puis répéter *Get Card Status*.

Erreurs liées au protocole Innovatron :

Code	Explication	Message utilisateur	Action serveur recommandée
h8100	REPGEN incorrect	CARTE ILLISIBLE	Refuser la carte
h8101	ATR incorrect	CARTE ILLISIBLE	Refuser la carte
h8102	Carte en erreur physique (E2PROM H.S.)	CARTE ILLISIBLE	Refuser la carte
h8103	Carte invalidée	CARTE ILLISIBLE	Refuser la carte

Erreurs liées à l'application Calypso de la carte :

Code	Explication	Message utilisateur	Action serveur recommandée
h4100	Répertoire Calypso manquant sur la carte	PASSE INVALIDE	Refuser la carte
h4101	Répertoire Calypso bloqué	PASSE EN OPPOSITION	Refuser la carte
h4102	Un des fichiers Calypso à traiter est manquant	PASSE INVALIDE	Refuser la carte
h4103	Un des fichiers Calypso à traiter est bloqué	PASSE EN OPPOSITION	Refuser la carte
h4104	Un des enregistrements Calypso est manquant	PASSE INVALIDE	Refuser la carte
h4105	Un des enregistrements Calypso est corrompu (mal formaté)	PASSE INVALIDE	Refuser la carte

Causes de refus d'une carte :

Code	Explication	Message utilisateur	Action serveur recommandée
h4200	La carte n'est pas autorisée sur ce réseau (<i>EnvNetworkId</i> refusé)	NON VALABLE ICI	Refuser la carte
h4201	La carte est périmée (<i>EnvApplicationEndDate</i> dépassée)	PASSE PERIMÉ	Refuser / accepter avec avertissement
h4202	Le sceau du fichier « environnement » est incorrect (<i>EnvAuthenticator</i>)	PASSE EN OPPOSITION	Refuser la carte
h4203	Tous les enregistrements du fichier « contrat » sont vides	PASSE INVALIDE	Refuser la carte
h4204	Pas de contrat valide ici (<i>ContractValidityZone</i>)	NON VALABLE ICI	Refuser / accepter avec avertissement
h4205	Trop tôt pour le contrat (<i>ContractValidityStartDate</i>)	NON ENCORE VALABLE TC	Refuser / accepter avec avertissement
h4206	Trop tard pour le contrat (<i>ContractValidityEndDate</i>)	TITRE TC PERIME	Refuser / accepter avec avertissement
h4207	Le contrat est invalidé (<i>ContractStatus</i>)	PASSE EN OPPOSITION	Refuser la carte
h4208	Le sceau du contrat est incorrect (<i>ContractAuthenticator</i>)	PASSE EN OPPOSITION	Refuser la carte

Echecs d'authentification (SAM) :

Code	Explication	Message utilisateur	Action serveur recommandée
h4300	Le SAM a refusé la signature de la carte	PASSE INVALIDE	Refuser la carte
h4301	La carte a refusé la signature du SAM	PASSE INVALIDE	Refuser la carte
h4302	Le SAM ne connaît pas la version de clé demandée par la carte	PASSE INVALIDE	Refuser la carte

NB : ces trois cas d'erreurs ne doivent pas se produire... S'ils surviennent néanmoins, il serait judicieux de confisquer la carte pour analyse...

Erreurs spécifiques RCTIF :

Code	Explication	Message utilisateur	Action serveur recommandée
h4400	L'ATR de la carte n'est pas supporté	PASSE INVALIDE	Refuser la carte
h4401	La version des données est incorrecte (<i>EnvVersionNumber</i>)	PASSE INVALIDE	Refuser la carte
h4402	L'émetteur de la carte est inconnu (<i>EnvApplicationIssuerId</i>)	PASSE INVALIDE	Refuser la carte
h4403	Le vendeur du contrat est inconnu (<i>ContractProvider</i>)	PASSE INVALIDE	Refuser la carte
h4404	Le code-tarif contrat n'est pas accepté (<i>ContractTariff</i>)	PASSE INVALIDE	Refuser la carte

4.5. INFORMATIONS COMPLÉMENTAIRES

Le champ **informations complémentaires** est préfixé par l'octet I_2 qui en précise la longueur.

Le contenu et la longueur du champ **informations complémentaires** dépend à la fois du type de carte et de la configuration du lecteur.

4.5.1. Pour les cartes hors Calypso

Le champ **informations complémentaires** est absent (longueur = 0).

4.5.2. Pour les cartes Calypso

Selon la configuration (cf. § 5.3.5), le champ **informations complémentaires** est :

- Absent (longueur = 0),
- Présent, de longueur 2 octets, et égal au champ *EnvAuthenticator* lu dans le fichier environnement de la carte.

5. REGISTRES DE CONFIGURATION

Le lecteur est largement configurable grâce à ses **registres de configuration**. Les registres de configuration sont stockés dans une mémoire non-volatile (E²PROM).

5.1. LISTE DES REGISTRES DE CONFIGURATION

Registre	Description	Taille	§
Fonctionnement du lecteur			
h10	Liste des protocoles à rechercher	2	5.2.1
h11	Liste des protocoles à afficher	2	5.2.2
h12	Options de recherche	1	5.2.3
h13	Options diverses	2	5.2.4
h14	Format de sortie des numéros de série	1	5.2.5
Protocole Calypso			
h20	Protocoles supportant Calypso	1	5.3.1
h21	Identifiant de l'application télé-billetique	Var.	5.3.2
h22	Options ISO 14443-4 (T=CL) pour Calypso	1	5.3.3
h23	Options Innovatron pour Calypso	1	5.3.4
h24	Format de sortie Calypso	1	5.3.5
h2F	Options du SAM Calypso	1	5.3.6
Lecture et authentification Calypso			
h30	Tests Calypso à effectuer	1	5.4.1
h31	Réseaux Calypso autorisés	3 x N	5.4.2
h32	Emetteurs Calypso autorisés	1 x N	5.4.3
h33	Zones Calypso autorisées	1	5.4.4
h34	Emetteurs de contrats Calypso autorisés	1 x N	5.4.5
h35	Tarifs de contrats Calypso autorisés	2 x N	5.4.6
h3A	Paramètres d'authentification Calypso	2	5.4.7
Paramètres de communication			
h67	Débit et mode	1	5.5.1
h68	Adressage	1	5.5.2

NB : pour chaque registre, nous indiquons deux valeurs :

- la *valeur par défaut* est la valeur utilisée par le firmware lorsque le registre n'a pas été configuré,
- la *valeur usine* est la valeur configurée avant livraison.

5.2. REGISTRES GENERAUX

5.2.1. Liste des protocoles à rechercher

Le registre $_h10$ indique la liste des protocoles que le lecteur doit utiliser pour rechercher des cartes sans contact.

Sur deux octets (poids fort en tête) :

	Bit	Protocole activé si 1	Note
<i>msb</i>	15	RFU	
	14	RFU	
	13	RFU	
	12	RFU	
	11	NXP ICODE1 (fast)	
	10	ISO 15693 (fast)	
	9	RFU	
	8	RFU	
	7	Innovatron	obligatoire pour les cartes Calypso ne supportant pas encore ISO 14443-B
	6	ASK CTS256B et CTS512B	
	5	ST MicroElectronics SRxxx	
	4	Inside Contactless PicoPass	y compris HID iClass
	3	NXP ICODE1 (std.)	
	2	ISO 15693 (std.)	
	1	ISO 14443-B	Obligatoire pour les cartes Calypso ne supportant plus le protocole Innovatron
<i>lsb</i>	0	ISO 14443-A	y compris Mifare

Valeur par défaut : $_hFFFF$ (tous les protocoles actifs).

Valeur usine : $_h0083$ (ISO 14443-A, ISO 14443-B, Innovatron).

5.2.2. Liste des protocoles à afficher

Le registre $_h11$ indique la liste des protocoles que le lecteur peut afficher⁵, sur deux octets (poids fort en tête) interprétés comme un champ de bits. Les bits disponibles sont les mêmes que ci-dessus.

Valeur par défaut (et valeur usine) : copie de la valeur du registre $_h10$.

⁵ Rechercher $_h0083$ et n'afficher que $_h0080$ permet par exemple d'afficher toutes les cartes Calypso, y compris au-dessus des protocoles ISO 14443, mais de masquer les cartes ISO 14443 qui ne contiennent pas l'application Calypso.

5.2.3. Options de recherche

Registre $_{h12}$, sur un octet :

Bit	Valeur	Comportement
<i>msb</i> 7	1	Séquence de recherche conforme RCTIF (alternance REQB/APGEN pendant plus de 100ms)
	0	Séquence de recherche simplifiée (plus rapide)
6 - 5	$_{b11}$	Lecteur actif à la mise sous tension, recherche permanente
	$_{b10}$	Lecteur actif à la mise sous tension, en mode « Autostop »
	$_{b01}$	<i>RFU, ne pas utiliser</i>
	$_{b00}$	Lecteur inactif à la mise sous tension (attente d'une commande d'activation pour commencer la recherche de carte)
4		<i>RFU, mettre à 0</i>
3		<i>RFU, mettre à 0</i>
2		<i>RFU, mettre à 0</i>
1		<i>RFU, mettre à 0</i>
<i>lsb</i> 0		<i>RFU, mettre à 0</i>

Valeur par défaut (et valeur usine) : $_{hE0}$ (conforme RCTIF, recherche permanente dès la mise sous tension).

5.2.4. Options diverses

Registre $_{h13}$, sur deux octets.

To be written

Valeur par défaut : $_{h03}$.

Valeur usine : $_{h00}$.

5.2.5. Format de sortie des numéros de série

Registre $_{h14}$, sur un octet :

Bit	Valeur	Comportement
<i>msb</i> 7 - 6	11	ISO 14443-A : intervertir tous les numéros de série
	10	ISO 14443-A : intervertir les numéros courts (4 octets) ⁶
	01	<i>RFU, ne pas utiliser</i>
	00	ISO 14443-A : ne pas intervertir les numéros de série
6		<i>RFU, mettre à 0</i>
5		<i>RFU, mettre à 0</i>
4	1	ISO 14443-B : transmettre l'ATQB complet (11 octets)
	0	ISO 14443-B : transmettre seulement le PUPI (4 octets)
3		<i>RFU, mettre à 0</i>
4		<i>RFU, mettre à 0</i>
<i>lsb</i> 1 - 0	$_{b11}$	Les numéros de série sont transmis sur 16 octets
	$_{b10}$	Les numéros de série sont transmis sur 8 octets
	$_{b01}$	Les numéros de série sont transmis sur 4 octets
	$_{b00}$	Les numéros de série sont transmis sur 4 à 16 octets selon ce qui est physiquement disponible ⁷

Valeur par défaut (et valeur usine) : $_{h82}$ (sortie sur 8 octets, interversion des numéros ISO 14443-A courts).



Ce registre de configuration concerne toutes les cartes, hors Calypso.
 Pour les cartes Calypso, c'est la configuration décrite au § 5.3.5 qui s'applique.

⁶ C'est le format usuel pour les applications basées sur les documentations Mifare

⁷ 4, 7 ou 12 pour ISO 14443-A, 4 pour ISO 14443-B, 8 pour ISO 15693, etc...

5.3. REGISTRES POUR LE PROTOCOLE CALYPSO

5.3.1. Protocoles supportant Calypso

Le registre $_h20$ donne la liste des protocoles au-dessus desquels le lecteur va tenter d'effectuer le traitement Calypso.

Sur deux octets (poids fort en tête) :

	Bit	Protocole activé si 1	Note
<i>msb</i>	15	RFU	
	14	RFU	
	13	RFU	
	12	RFU	
	11	RFU	
	10	RFU	
	9	RFU	
	8	RFU	
	7	Calypso sur Innovatron	
	6	RFU	
	5	RFU	
	4	RFU	
	3	RFU	
	2	RFU	
	1	Calypso sur ISO 14443-B	
<i>lsb</i>	0	Calypso sur ISO 14443-A	

Valeur par défaut : $_h0083$ (ISO 14443 A et B, Innovatron).

Valeur usine : $_h0082$ (ISO 14443-B, Innovatron).

5.3.2. Identifiant de l'application télé-billetique

Le registre $_h21$ définit l'identifiant qui sera utilisé pour le SELECT APPLICATION en début du traitement CALYPSO.

La longueur de l'identifiant est libre entre 0 et 32 octets.

Valeur par défaut (et valeur usine) : $_h315449432E494341$ (« 1TIC.ICA »).

5.3.3. Options ISO 14443 (T=CL) pour Calypso

Le registre $_h22$ définit les options du protocole ISO 14443-4 pendant le traitement Calypso.

Sur un octet :

	Bit	Valeur	Comportement
<i>msb</i>	7		RFU, mettre à 0
	6		RFU, mettre à 0
	5		RFU, mettre à 0
	4	1	Inclure $L_E=_h00$ dans tous les APDU
		0	Ne pas inclure L_E dans les APDU
<i>lsb</i>	3 - 0	$_hF$	Ne pas utiliser de CID
		$_h1$ à $_hE$	Utiliser la valeur de CID spécifiée (1 à 14)
		$_h0$	RFU, ne pas utiliser

Valeur par défaut et valeur usine : $_h1F$ (inclure $L_E=00$, pas de CID).

5.3.4. Options Innovatron pour Calypso

Le registre $_h23$ définit les options du protocole Innovatron.

Sur un octet :

	Bit	Valeur	Comportement
<i>msb</i>	7	1	Communication Innovatron conforme RCTIF (coupure du champ sur certaines erreurs cartes)
		0	Ne pas couper le champ pendant la communication Innovatron
	6		<i>RFU, mettre à 0</i>
	5	1	SELECT APPLICATION en échec est fatal
		0	Traitement possible même si SELECT APPLICATION a échoué
	4	1	REPGEN invalide est fatal
		0	Traitement possible même si REPGEN est invalide
	3		<i>RFU, mettre à 0</i>
	2		<i>RFU, mettre à 0</i>
	1		<i>RFU, mettre à 0</i>
<i>lsb</i>	0		<i>RFU, mettre à 0</i>

Valeur par défaut (et valeur usine) : $_h90$ (conforme RCTIF, valider REPGEN, ignorer les échecs de SELECT APPLICATION).

5.3.5. Format de sortie Calypso

Le registre $_h24$ définit les options de présentation des données des cartes Calypso.

Sur un octet :

	Bit	Valeur	Comportement
<i>msb</i>	7	1	Le champ <i>type de carte</i> dépend du protocole : - $_h80$ pour les cartes Calypso sur Innovatron - $_h81$ pour les cartes Calypso sur ISO 14443-A - $_h82$ pour les cartes Calypso sur ISO 14443-B
		0	Le champ <i>type de carte</i> est forcé à $_h80$ pour toutes les cartes Calypso
	6		<i>RFU, mettre à 0</i>
	5		<i>RFU, mettre à 0</i>
	4		<i>RFU, mettre à 0</i>
	3		<i>RFU, mettre à 0</i>
	2	1	Le champ <i>EnvAuthenticator</i> de la carte est transmis dans les données (2 octets)
		0	Le champ <i>EnvAuthenticator</i> de la carte n'est pas transmis
<i>lsb</i>	1 - 0	$_b11$	Le numéro de série Calypso est transmis sur 16 octets
		$_b10$	Le numéro de série Calypso est transmis sur 8 octets
		$_b01$	Le numéro de série Calypso est transmis sur 4 octets
		$_b00$	Le numéro de série Calypso est transmis sur 4 ou 8 octets selon ce qui est disponible ⁸

Valeur par défaut : $_h82$ (numéro de série sur 8 octets, ne pas transmettre *EnvAuthenticator*, utiliser *type de carte* pour indiquer le protocole).

Valeur usine : $_h06$ numéro de série sur 8 octets, transmettre *EnvAuthenticator*, ne pas indiquer le protocole dans *type de carte*).

⁸ 8 octets pour une carte qui répond correctement au SELECT APPLICATION, 4 octets si seules les informations protocolaires (REPGEN ou ATQB) sont disponibles.

5.3.6. Options du SAM Calypso

Le registre $_{h}2F$ définit les options du SAM utilisé pour l'authentification des cartes Calypso.

	Bit	Valeur	Comportement
<i>msb</i>	7		RFU, mettre à 1
	6		RFU, mettre à 0
	5		RFU, mettre à 0
	4		RFU, mettre à 0
	3		RFU, mettre à 0
	2		RFU, mettre à 0
<i>lsb</i>	1 - 0	$_{b}11$	RFU, ne pas utiliser
		$_{b}10$	Authentifier la carte en utilisant le SAM B
		$_{b}01$	Authentifier la carte en utilisant le SAM A
		$_{b}00$	Ne pas utiliser de SAM

Valeur par défaut (et valeur usine) : $_{h}80$ (pas de SAM).

5.4. REGISTRES POUR LE TRAITEMENT CALYPSO

5.4.1. Tests Calypso à effectuer

Le registre $_{h}30$ précise la liste des tests Calypso à effectuer.

Sur un octet :

	Bit	Valeur	Comportement
<i>msb</i>	7	1	Vérifier le sceau du contrat (re-calcul et comparaison du champ <i>ContractAuthenticator</i>)
		0	Ne pas vérifier le sceau du contrat
	6		RFU, mettre à 0
	5	1	Vérifier le statut du contrat (le champ <i>ContractStatus</i> doit valoir $_{h}01$)
		0	Ne pas vérifier le statut du contrat
	4	1	Vérifier que le contrat est en cours de validité (<i>ContractValidityStartDate</i> et <i>ContractValidityEndDate</i>)
		0	Ne pas vérifier les dates de validité du contrat
	3		RFU, mettre à 0
	2		RFU, mettre à 0
	1		RFU, mettre à 0
<i>lsb</i>	0	1	Vérifier que la carte n'est pas périmée (champ <i>EnvApplicationEndDate</i>)
		0	Ne pas vérifier la péremption de la carte

Valeur par défaut : $_{h}00$ (aucun test).

Valeur usine : $_{h}FF$ (tous les tests).

5.4.2. Réseaux Calypso autorisés

Le registre $_h31$ contient la liste des réseaux (*EnvNetworkId*) qui doivent être acceptés. Chaque réseau occupe 3 octets (poids fort en tête), et il est possible d'en définir 4 au maximum.

Si ce registre est vide, tous les réseaux sont acceptés.

Valeur par défaut : vide (réseau non testé).

Valeur usine : $_h250901$ (France / Ile-de-France).

5.4.3. Emetteurs Calypso autorisés

Le registre $_h32$ contient la liste des émetteurs de cartes (*EnvApplicationIssuerId*) qui doivent être acceptés. Chaque émetteur occupe 1 octet, et il est possible d'en définir 8 au maximum.

Si ce registre est vide, tous les émetteurs sont acceptés.

Valeur par défaut : vide (émetteur non testé).

Valeur usine : $_h00CA$ (ensemble des exploitants Navigo + exploitant P+R).

5.4.4. Zones Calypso autorisées

Le registre $_h33$ contient la liste des zones (*ContractValidityZones*) qui doivent être acceptées.

Sur un octet :

	Bit	Zone acceptée si 1	Note
<i>msb</i>	7	Zone 8	
	6	Zone 7	
	5	Zone 6	
	4	Zone 5	
	3	Zone 4	
	2	Zone 3	
	1	Zone 2	
<i>lsb</i>	0	Zone 1	

Valeur par défaut et valeur usine : $_hFF$ (toutes zones autorisées).

5.4.5. Emetteurs de contrats Calypso autorisés

Le registre $_h34$ contient la liste des émetteurs de contrats (*ContractProvider*) qui doivent être acceptés. Chaque émetteur occupe 1 octet, et il est possible d'en définir 8 au maximum.

Si ce registre est vide, tous les émetteurs sont acceptés.

Valeur par défaut : vide (émetteur non testé).

Valeur usine : $_h00$ (ensemble des exploitants Navigo).

5.4.6. Tarifs de contrats Calypso autorisés

Le registre $_h35$ contient la liste des tarifs de contrats (*ContractTariff*) qui doivent être acceptés. Chaque émetteur occupe 2 octets, et il est possible d'en définir 8 au maximum.

Si ce registre est vide, tous les tarifs sont acceptés.

Valeur par défaut (et valeur usine) : vide (tous les tarifs sont acceptés).

5.4.7. Clés d'authentification Calypso

Le registre $_h3A$ contient sur deux octets les numéros de clés à utiliser pour l'authentification Calypso :

- Premier octet : numéro de clé (KEY) côté carte,
- Second octet : identifiant de clé (KIF) côté SAM.

Si ce registre est vide, l'authentification Calypso n'est pas effectuée.

Valeur par défaut : vide (pas d'authentification).

Valeur usine : $_h0330$ (clé et KIF de débit).

5.5. PARAMETRES DE COMMUNICATION

5.5.1. Débit et mode

Registre $_{h}67$, sur un octet :

	Bit	Valeur	Comportement
<i>msb</i>	7	1	La liaison USB (port série virtuel) est désactivée
		0	La liaison USB (port série virtuel) est activée
	6	1	La liaison série (physique) est désactivée
		0	La liaison série (physique) est activée
	5	1	Le protocole simplifié point à point est désactivé
		0	Le protocole simplifié point à point est activé
	4	1	RX/TX communs (RS-485)
		0	RX/TX séparés (RS-232)
	3		<i>RFU, mettre à 0</i>
<i>lsb</i>	2 - 0	$_{b}111$	<i>RFU, ne pas utiliser</i>
		$_{b}110$	<i>RFU, ne pas utiliser</i>
		$_{b}101$	Débit = 38400bps
		$_{b}100$	Débit = 19200bps
		$_{b}011$	Débit = 9600bps
		$_{b}010$	<i>RFU, ne pas utiliser</i>
		$_{b}001$	<i>RFU, ne pas utiliser</i>
		$_{b}000$	<i>RFU, ne pas utiliser</i>

Valeur par défaut (et valeur usine) : $_{h}05$ (38400bps, RX/TX séparés, protocole simplifié activé, liaison série et USB activées).

5.5.2. Adressage

Registre $_{h}68$, sur un octet :

	Bit	Valeur	Comportement
<i>msb</i>	7 - 4	$_{h}F$	Accepter n'importe quelle adresse de serveur
		$_{h}0$ à $_{h}E$	<i>RFU, ne pas utiliser</i>
<i>lsb</i>	3 - 0	$_{h}F$	Le lecteur ne répond qu'aux messages <i>broadcast</i>
		$_{h}0$ à $_{h}E$	Adresse du lecteur, de 0 à 14

Valeur par défaut (et valeur usine) : $_{h}FF$ (accepter n'importe quelle adresse de serveur, le lecteur n'a pas d'adresse et ne répond qu'aux messages *broadcast*).

Pour définir l'adresse d'un lecteur :



- Le brancher seul sur le bus,
- Utiliser la commande **Query Version Info** en *broadcast* pour l'identifier,
- Utiliser la commande **Write Config** sur ce registre pour lui affecter une adresse,
- Utiliser la commande **Apply Config** pour que le lecteur prenne en compte son adresse.

6. PROTOCOLE DE TEST RCTIF

Le lecteur contient une surcouche logicielle permettant de le tester dans le cadre du référentiel RCTIF.

A la date de conception du lecteur, le RCTIF est dans une phase de transition entre deux versions :

- La version 3.4 (sous-version B) est en fin de vie mais reste applicable,
- La version 4.0 est disponible en *draft* depuis plusieurs mois mais n'est toujours pas applicable.

Le lecteur a donc été conçu selon les recommandations de la version 4.0, mais ce chapitre présente également les tests de la version 3.4 .

6.1. ACCEDER AU MODE TEST

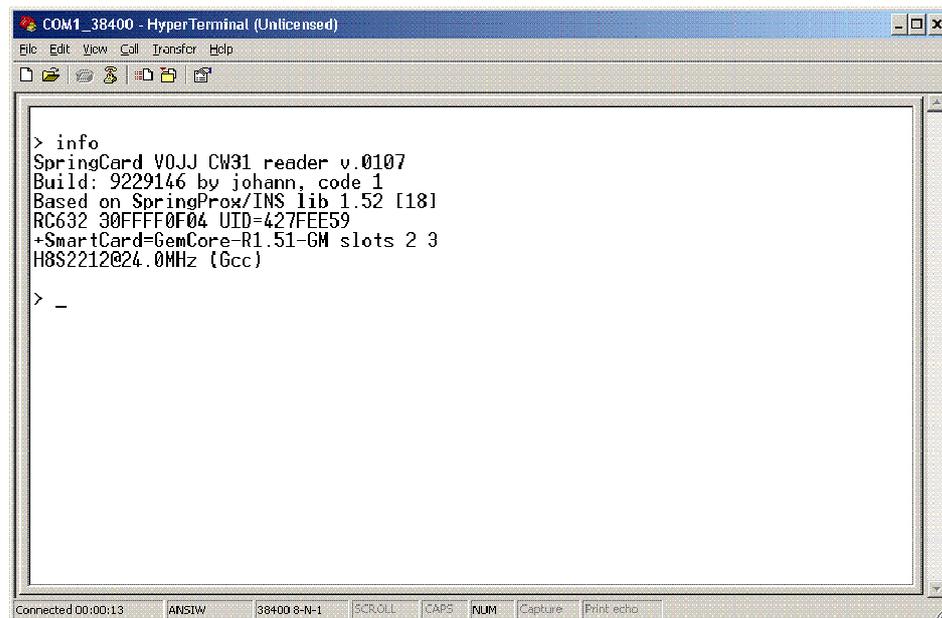
Utiliser un émulateur de terminal (comme HyperTerminal) pour accéder au lecteur via sa liaison série (port série physique, ou port série virtuel sur USB grâce au driver **SpringCard SDD470**).

Le lecteur communique à 38400bps⁹, 8 bits de données, 1 bit de stop, pas de parité, pas de contrôle de flux.

Appuyer sur la touche <Echap.> pour activer la console du lecteur.

Appuyer sur la touche <Entrée>. Le lecteur renvoie son *prompt*.

Saisir « info » puis <Entrée>. Le lecteur renvoie ses informations :



```
> info
SpringCard VOJJ CW31 reader v.0107
Build: 9229146 by johann, code 1
Based on SpringProw/INS lib 1.52 [18]
RC632 30FFF0F04 UID=427FEE59
+SmartCard=GenCore-R1.51-GM slots 2 3
H8S2212@24.0MHz (Gcc)
> _
```

⁹ Le débit peut être modifié par configuration, cf. § 5.5.1 . En accès USB, la valeur indiquée n'est pas significative.

6.2. JEU DE COMMANDES POUR LES TESTS

6.2.1. Passer en mode test

La commande « stop » permet d'interrompre le fonctionnement standard du lecteur, et de passer en mode test.

6.2.2. Retour au mode normal

La commande « exit » sort du mode test et restaure le fonctionnement standard du lecteur.

6.2.3. Commandes bas niveau

a. Activer le champ

La commande « rfon » active le champ (non modulé).

b. Couper le champ

La commande « rfoff » coupe le champ.

6.2.4. Commandes par protocole

a. Chasse ISO 14443-A

La commande « reqa » active la chasse ISO 14443-A (REQA uniquement). Dès qu'une carte conforme est détectée, le lecteur affiche le champ ATQA de la carte (pas d'anticollision, pas de sélection).

La touche <Échap.> permet de quitter ce mode.

b. Chasse, activation et échanges ISO 14443-A

La commande « reqa! » active la chasse ISO 14443-A.

Dès qu'une carte conforme est détectée, le lecteur effectue la boucle d'anticollision et de sélection de niveau 3 jusqu'à sélectionner la carte, et affiche les champs ATQA, UID et SAK de la carte sélectionnée.

Le lecteur effectue ensuite un GET ATS, puis effectue 10 échanges avec la carte. L'APDU envoyé est 00A40000023F00, la réponse n'est pas vérifiée. Après ces 10 échanges, le lecteur envoie un DESELECT puis repart en chasse ISO 14443-A.

La touche <Échap.> permet de quitter ce mode.

c. Chasse ISO 14443-B

La commande « reqb » active la chasse ISO 14443-B (REQB, champ AFI = 00).

Dès qu'une carte conforme est détectée, le lecteur affiche le champ ATQB de la carte (pas d'anticollision, pas d'ATTRIB).

La touche <Échap.> permet de quitter ce mode.

d. Chasse, activation et échanges ISO 14443-B

La commande « reqb! » active la chasse ISO 14443-B (REQB, champ AFI = 00).

Dès qu'une carte conforme est détectée, le lecteur affiche le champ ATQB de la carte (pas d'anticollision).

Le lecteur effectue ensuite un ATTRIB, puis effectue 10 échanges avec la carte. L'APDU envoyé est 00A4000023F00, la réponse n'est pas vérifiée. Après ces 10 échanges, le lecteur envoie un DESELECT puis repart en chasse ISO 14443-B.

La touche <Échap.> permet de quitter ce mode.

e. Chasse Innovatron

La commande « apgen » active la chasse Innovatron (Long REPGEN demandé).

Dès qu'une carte conforme est détectée, le lecteur affiche le champ REPGEN de la carte (pas d'anticollision, pas d'ATTRIB ni de COM_RA).

La touche <Échap.> permet de quitter ce mode.

f. Chasse, activation et échanges Innovatron

La commande « apgen! » active la chasse Innovatron (Long REPGEN demandé).

Dès qu'une carte conforme est détectée, le lecteur affiche le champ REPGEN de la carte (pas d'anticollision). Le lecteur effectue un premier échange COM_RA avec la carte, puis 9 échanges COM_R. L'APDU envoyé est 00A4000023F00, la réponse n'est pas vérifiée. Après ces 10 échanges, le lecteur envoie un DISC puis repart en chasse Innovatron.

La touche <Échap.> permet de quitter ce mode.

Remarque :

Cette séquence correspond à ce qui est demandé dans le plan de test du RCTIF. En utilisation « normale », le lecteur active la carte par un échange ATTRIB et non par COM_RA.

6.2.5. Fonctionnement « typique » du lecteur

a. Activer la chasse multi-protocoles

La commande « poll » active la chasse alternée ISO 14443-A, ISO 14443-B et Innovatron.

Selon le type de la carte détectée, le lecteur effectue la séquence décrite au paragraphe 6.2.4.a, 6.2.4.c ou 6.2.4.e.

La touche <Échap.> permet de quitter ce mode.

Remarque :

Cette séquence se limite aux modes prévus par le RCTIF. En utilisation « normale » et selon sa configuration, le lecteur peut utiliser d'autres modulations et d'autres protocoles, notamment :

- Modulation ISO 14443-B avec protocole ST (série SR176, SRiX, ...),
- Modulation ISO 14443-B avec protocole ASK (CTS256B et CTS512B),
- Modulation ISO 14443-B avec protocole Inside Contactless (PicoTag, HID iClass),
- Modulation ISO 15693, protocoles ISO 15693-3 ou NXP ICODE1.

6.2.6. Nouvelles commandes RCTIF 4

3 commandes permettent de dérouler le scénario de test prévu par le RCTIF 4.0. Se reporter au paragraphe 6.4.

6.2.7. Commandes diverses

a. Activer le mode trace

Utiliser la commande « tron ».

b. Désactiver le mode trace

Utiliser la commande « troff ».

6.3. SUITE DE TESTS DU RCTIF 3.4

Le tableau ci-dessous précise les commandes à utiliser pour chaque test prévu au RCTIF 3.4.

Pendant certains tests le lecteur doit signaler une erreur. Se reporter au tableau suivant pour la liste des codes d'erreur

a. Commandes à utiliser pour effectuer les tests RCTIF 3.4

Test	Commande	Remarque
IS2_CP_TN_0101 à IS2_CP_TN_0205	rfon	
IS2_CP_TN_0301	reqa <i>ou</i> reqb <i>ou</i> apgen	
IS2_CP_TN_0302 à IS2_CP_TN_0502	reqa! <i>puis</i> apgen!	
IS3_CP_TN_0101 à IS3_CP_TN_0103	poll	
IS2_CPA_TN_0101 à IS3_CPA_TN_0201	reqa	
IS2_CPB_TN_0101 et IS2_CPB_TN_0201	reqb	
IS2_CPB_TN_0202 et IS2_CPB_TN_0203	poll	
IS2_CPB_TN_0401 à IS2_CPB_TN_0601	reqb	
IS2_CPB_TN_0701 à IS3_CPB_TN_1001	apgen!	Pour certains tests l'utilisation de la commande apgen est suffisante.
VBT_CP_TN_0101 à VBT_CP_TN_3601	apgen!	
SES_CP_TN_0101 à SES_CP_TN_0404	apgen!	

b. Codes d'erreurs pouvant être signalés pendant les tests

Code	Signification	Interprétation
-1	Pas de réponse de la carte	Pas de carte, carte retirée ou délai dépassé dans l'attente de la réponse
-2	Erreur CRC	Erreur de transmission, collision entre deux cartes, carte non conforme
-5	Erreur de parité	Erreur de transmission, carte non conforme (ISO 14443-A seulement)
-6	Erreur d'en-tête	Un des champs constants dans la réponse de la carte n'est pas conforme aux spécifications (Innovatron : mauvaise valeur du champ CMD)
-8	Erreur de numéro de série ou d'ATR	La réponse initiale de la carte n'est pas conforme aux spécifications (Innovatron : REPGEN incorrect)
-11	Nombre de bits incorrect	Collision entre deux cartes, carte non conforme (ISO 14443-A seulement)
-12	Nombre d'octets incorrect	La longueur de la réponse de la carte n'est pas conforme aux spécifications
-21	Erreur d'alignement	L'assemblage des octets n'est pas conforme aux spécifications

Cette liste n'est pas exhaustive mais correspond aux erreurs typiques générées par les outils de test.

6.4. SUITE DE TESTS DU RCTIF 4.0

La liste des tests du RCTIF 4.0 est trop longue pour être reprise ici dans un tableau.

L'essentiel est la conformité du lecteur au « cahier des charges du logiciel de test RCTIF 4 », ce qui permet au laboratoire d'être autonome dans la réalisation des tests.

Dans la pratique, les fonctions demandées ne sont pas pilotées par un logiciel spécifique, mais directement activées en saisissant des commandes sous HyperTerminal.

a. Correspondance fonctions du logiciel / commandes

Fonction	Commande	Remarque
Carrier ON	rfon	
Carrier OFF	rfoff	
REQA	reqa	
REQB	reqb	
APGEN	apgen	
Nominal transaction type A	testa	Enchaîne REQA + anticollision + sélection + RATS, puis la transaction, puis DESELECT
Nominal transaction type B	testb	Enchaîne REQB + ATTRIB, puis la transaction, puis DESELECT
Nominal transaction type Innovatron	testi	Enchaîne APGEN + ATTRIB, puis la transaction, puis DISC

b. Ouverture / fermeture de session

La commande « testa » commence par ouvrir une session ISO 14443-A niveau 4 avec GET ATS. Les paramètres sont : pas de CID, pas de NAD. Il n'y a pas de PPS (106kbps dans chaque sens).

La commande « testb » commence par ouvrir une session ISO 14443-B niveau 4 avec ATTRIB. Les paramètres sont : pas de CID, pas de NAD, 106kbps dans chaque sens.

La commande « testi » commence par ouvrir une session ISO 7816 sur protocole Innovatron avec ATTRIB. Le lecteur n'utilise jamais COM_RA dans ce mode..

Les 2 commandes ISO se terminent par DESELECT, la commande Innovatron par DISC. Il n'y a pas de coupure du champ à la fin du test.

c. Transaction de référence ISO 14443-A et 14443-B

Le lecteur implémente la transaction de référence suivante :

- SELECT APPLICATION, AID=A0 00 00 04 04 01 25 09 01 01
- READ BINARY, Le=FE
- READ BINARY, Le=01
- READ BINARY, Le=FE,
- WRITE BINARY, Lc=FE
- WRITE BINARY, Lc=01
- WRITE BINARY, Lc=FE

Lorsque les commandes « testa » ou « testb » sont utilisées, les APDU sont passés dans un flux ISO 14443-4.

Lorsque la commande « testi » est utilisée, les APDU sont passés dans une suite de COM_R.

Remarque :

Les APDU READ BINARY et WRITE BINARY sont systématiquement passés avec CLA=94.

6.5. AUTRES COMMANDES POUVANT ETRE UTILISEES POUR LES TESTS

Les commandes de mise en service et de désactivation du lecteur peuvent être utilisées dans le cadre des tests :

- « ron » active le lecteur, avec désactivation implicite dès qu'une carte a été traitée (équivalent commande *Start Polling with autostop*),
- « ron! » active le lecteur sans désactivation implicite (équivalent commande *Start Polling*). La pause est de 1s.
- « roff » désactive le lecteur (équivalent commande *Stop Polling*).

Remarque :

Lorsque le lecteur est activé ainsi, selon sa configuration, il peut utiliser d'autres modulations et d'autres protocoles que ceux prévus par le RCTIF.

(End of document) ■

AVERTISSEMENT

Ce document est mis à votre disposition à titre d'information uniquement, et ne doit pas être considéré comme une offre commerciale, un contrat ou autre forme d'engagement entre PRO ACTIVE et vous. Aucune des informations fournies dans ce document ne peut remplacer l'obtention de données par vos propres moyens.

Les informations fournies dans ce document peuvent concerner ou faire référence à des produits et/ou des services qui ne sont pas disponibles dans votre pays.

Le présent document est fourni "tel quel" et ce sans aucune garantie, expresse ou implicite, dans les limites prévues par les lois applicables. Même si PRO ACTIVE fait son possible pour fournir des informations fiables, nous ne pouvons nullement garantir que ce document soit exempt d'inexactitudes, d'erreurs et/ou d'omissions, ni que son contenu soit pertinent pour votre besoin spécifique, ni qu'il soit à jour. PRO ACTIVE se réserve le droit de modifier les informations qu'il contient à tout moment et sans préavis.

PRO ACTIVE ne garantit aucunement les résultats obtenus par la mise en œuvre des produits décrits dans ce document. PRO ACTIVE ne peut être tenue pour responsable d'aucune conséquence ni d'aucun dommage direct ou indirect, d'aucune perte de profits, interruption de service, perte de données, défaut de fonctionnement, liés à l'utilisation ou à l'impossibilité d'utiliser les produits (matériel et/ou logiciel) décrits dans ce document.

Les produits décrits dans ce document ne sont pas conçus pour être utilisés avec ou dans des équipements médicaux, ni avec ou dans tout équipement où un dysfonctionnement peut provoquer des dommages corporels. Les clients de PRO ACTIVE qui choisissent d'utiliser ou de vendre les produits pour ce type d'applications le font à leurs seuls risques, et s'engagent à indemniser PRO ACTIVE de tout dommage résultant d'une mise en œuvre inappropriée des produits.

INFORMATION SUR LE COPYRIGHT

Les informations contenues dans ce document sont soit disponibles publiquement, soit constituent la propriété intellectuelle de PRO ACTIVE et/ou ses fournisseurs ou partenaires.

Vous pouvez télécharger, lire, copier et imprimer ce document en respectant les conditions suivantes : (1) ce document ne peut être utilisé qu'à des fins privées, éducatives, et non commerciales, et (2) ce document ne doit en aucun cas être modifié ou renommé. Vous ne pouvez pas utiliser, télécharger, copier, imprimer, exposer, reproduire, publier, certifier, poster, transmettre ou distribuer ce document, en entier ou en partie, sans la permission écrite préalable de PRO ACTIVE.

Copyright © PRO ACTIVE SAS 2009, tous droits réservés.

EDITEUR

PRO ACTIVE SAS au capital de 227 000 €
RCS EVRY B 429 665 482
Parc Gutenberg, 13 voie La Cardon
91120 Palaiseau – France