IBSI TBS

LECAM

SPECIFICATIONS TECHNIQUES

D'UTILISATION

25 août 1987

SIEGE SOCIAL : 3, CHEMIN DU TOREY - BP 58 - 69340 FRANCHEVILLE - TEL. 78 34 80 40
SARL AU CAPITAL DE [illegible] - RCS LYON B 325942829 - TELEX 305 540

INTRODUCTION

PARTIE 1 - GENERALITES

PARTIE 2
SPECIFICATIONS D'INTERFACE DU LECAM

CHAPITRE 8 - Le module Application Carte 88

PARTIE 3
LES INSTRUCTIONS DE L'INTERPRETEUR LECAM

INTRODUCTION

PRESENTATION

Le LECAM est un LEcteur de CArtes à Mémoire connectable au Minitel. Utilisé à travers le réseau d'accès Télétel, il permet de mettre en œuvre de multiples fonctions selon la carte utilisée :

. connexion automatique à un service Télétel,
. contrôle de l'accès à un service par authentification de la carte présentée et éventuellement, vérification du code confidentiel du porteur par la carte,
. calcul de signature électronique des messages émis permettant au serveur de s'assurer de l'intégrité des messages reçus,
. mémorisation certifiée de transactions dans la carte et lecture certifiée d'informations contenues dans la carte,
. confidentialité des échanges par chiffrement et déchiffrement des données transmises sur le réseau.

...

Ce lecteur a pour caractéristique essentielle son **universalité** car il accepte les cartes respectant le projet de norme DIS 7816 de l'ISO. Son usage sera donc multiple et évolutif.

Cette documentation est relative aux LECAM 100 et 101. Des compléments seront édités pour les versions futures.

Qu'est-ce qu'une carte à mémoire ?

La carte à mémoire est le résultat de l'insertion, ou encartage d'un micro-circuit électronique, appelé parfois "puce", dans un support en plastique au format d'une carte de paiement. Depuis le dépôt des premiers brevets en 1974, divers produits, différents sous des apparences identiques, sont apparus sur le marché. Tous ces produits ont en commun la fonction de mémorisation, d'où l'appellation générique "carte à mémoire". Les cartes de haut de gamme contiennent un micro-circuit constitué d'un microprocesseur doté de sa mémoire de programme ROM et de sa mémoire de travail RAM et d'une mémoire de stockage des données, aujourd'hui, en technologie EPROM (une seule écriture), demain, en technologie EEPROM (réécriture possible). **Leur atout majeur est la sécurité** : le micro-circuit est conçu de telle façon que le comportement de la carte se trouve entièrement contrôlé de l'intérieur par le microprocesseur, élément de passage obligé entre la mémoire de données et l'extérieur.

Le microprocesseur réagit en fonction du programme, souvent appelé masque, car inséré dans la ROM lors de la fabrication du circuit par opération de masquage, qu'il exécute et dont les fonctions essentielles sont :

. la gestion des échanges avec le lecteur,
. le contrôle d'accès à la mémoire de données,
. la mise en œuvre d'un algorithme de sécurité à des fins d'authentification, de signature et de gestion des clés.

La mémoire de données contient trois types d'informations :

. **des informations libres**, accessibles de l'extérieur sans formalité particulière ; ce sont, par exemple, l'identité du porteur, le numéro de carte, le numéro de série du micro-circuit,

. **des informations confidentielles**, lisibles seulement après présentation du code confidentiel du porteur ou d'un code de l'émetteur de la carte,

. **des informations secrètes**, accessibles uniquement au microprocesseur qui interdit leur communication vers l'extérieur ; ce sont les clés secrètes, le code confidentiel du porteur, les codes de l'émetteur.

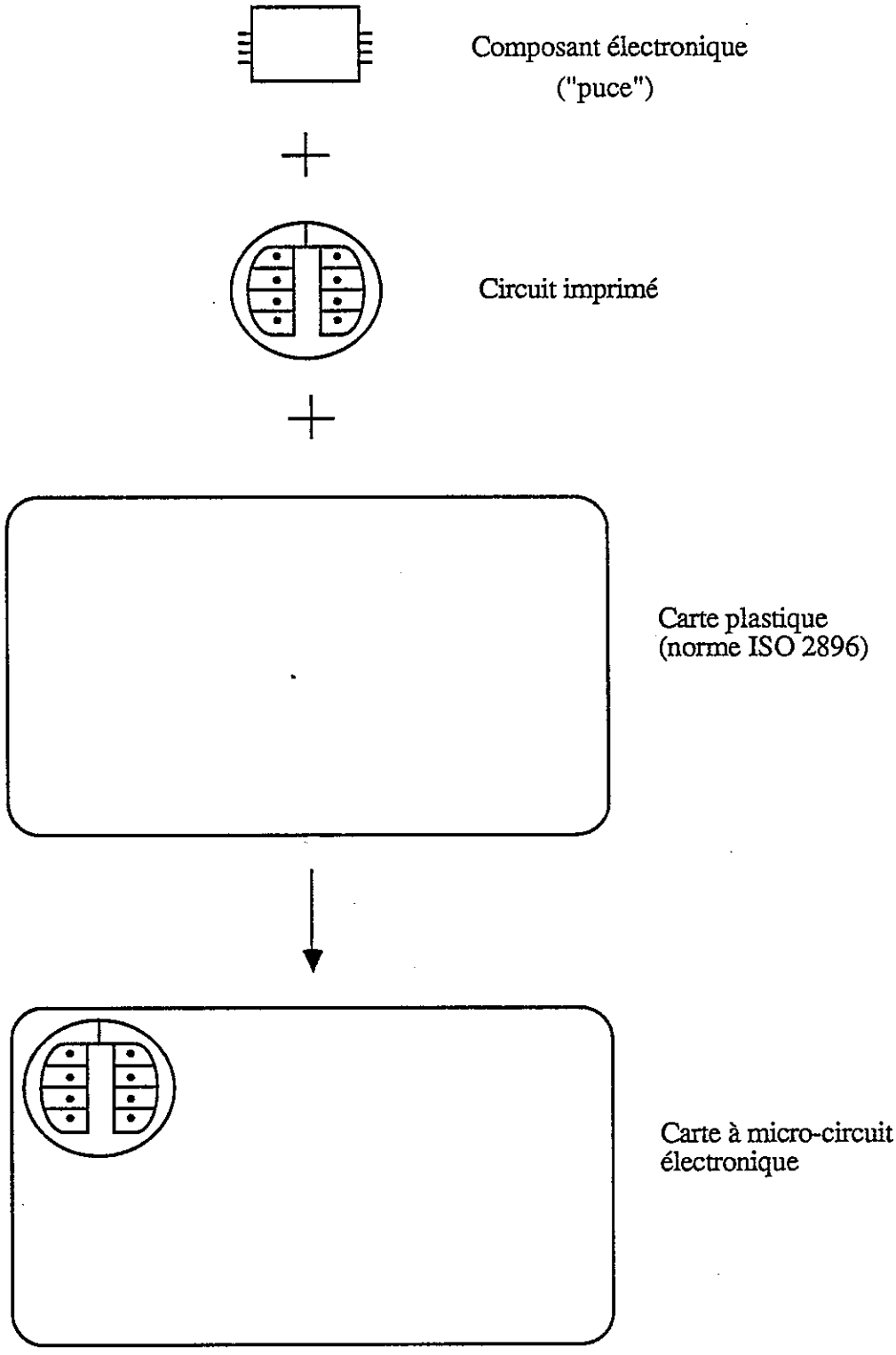
L'organisation de la mémoire de la carte, les conditions d'accès aux informations, les instructions exécutées par la carte sont inhérentes au programme du microprocesseur et sont donc susceptibles de variation, lors du développement de nouveaux programmes ou masques.

La gestion de la mémoire de données

Dès sa fabrication, le micro-circuit contient le programme ; le code de fabrication est inscrit dans sa mémoire secrète,

Après l'encartage de la puce dans le support de plastique, la personnalisation consiste à configurer la mémoire de données, à préciser les règles d'écriture et de lecture de la zone des transactions et à inscrire les données nécessaires à l'utilisation ultérieure de la carte : en zone libre, le numéro de la carte défini par l'émetteur, la période de validité et le nom du porteur ; en zone secrète, les codes confidentiels de l'émetteur, le code confidentiel du porteur et la clé secrète.

FABRICATION D'UNE CARTE A MEMOIRE



PARTIE 1

GENERALITES

CHAPITRE 1 - PRESENTATION GENERALE

1 . CARACTERISTIQUES GENERALES

Le LECAM se présente comme un périphérique du Minitel à alimentation autonome.

1. 1 - Les voyants de contrôle

L'emploi du LECAM est facilité par la présence en face avant de trois voyants :

. le voyant rouge (1) "M-A" allumé, signale la mise sous tension du lecteur,

. le voyant jaune (2) "CARTE" s'éclaire durant chaque dialogue entre la carte et le lecteur ; il est maintenu éclairé tant que la carte est alimentée,

. le voyant vert (3) "SECRET" s'éclaire de façon fixe :

- à la mise sous tension du LECAM pendant les tests de bon fonctionnement ; il s'éteint si le résultat est correct et si le réseau Minitel est libre,
- pour indiquer que la saisie de caractères sur le clavier du Minitel est sous le contrôle absolu du LECAM (cas de la saisie du code confidentiel, par exemple),

. le voyant vert (3) "SECRET" clignote pendant la transmission de données chiffrées sur le réseau, quel que soit le sens du transfert.

1. 2 - La connectique

En face avant, le LECAM présente une fente pour l'introduction de la carte dans le connecteur. L'interface électrique, le protocole d'échanges et la structure des commandes sont conformes au projet de norme DIS 7816/3 de l'ISO.

En face arrière, le LECAM est muni de deux prises péri-informatiques DIN, banalisées, pour le branchement au terminal Minitel d'une part, et à un autre périphérique d'autre part. Le LECAM envoie des commandes au Protocole du Minitel tel qu'il est défini dans le document "Minitel 1B", "Spécifications Techniques d'Utilisation" (STUM 1B) ; il assure ainsi la gestion des aiguillages entre les modules du Minitel (prise, modem, clavier, écran) et les affichages sur l'écran.

Le LECAM est également compatible avec le Système d'Echanges assurant la gestion des échanges entre les divers périphériques raccordés au Minitel et les serveurs accessibles à travers le réseau Télétel. Cette communication est construite pour une connexion en chaîne de périphériques selon le protocole décrit dans le document "Spécifications Techniques d'Utilisation du Réseau Minitel" (STURM).

2 . ENVIRONNEMENT MINITEL

Le LECAM est conçu pour fonctionner avec tous les Minitel en mode Vidéotex diffusés par la DGT.

Toutefois, pour une question de performances, il sera préférable d'utiliser un Minitel dont le modem est du type "retournable". Cette information est repérée sur la plaque d'identification du Minitel par un "R" à la suite du Numéro de série.

L'usage d'un Minitel 10, pour l'utilisation de la fonction de "connexion automatique" offerte par le LECAM, améliore sensiblement l'ergonomie de la mise en relation usager-serveur, car il offre en plus la possibilité de composition automatique du numéro téléphonique.

3. RACCORDEMENT AU RESEAU ELECTRIQUE, ENVIRONNEMENT ET SECURITE D'UTILISATION

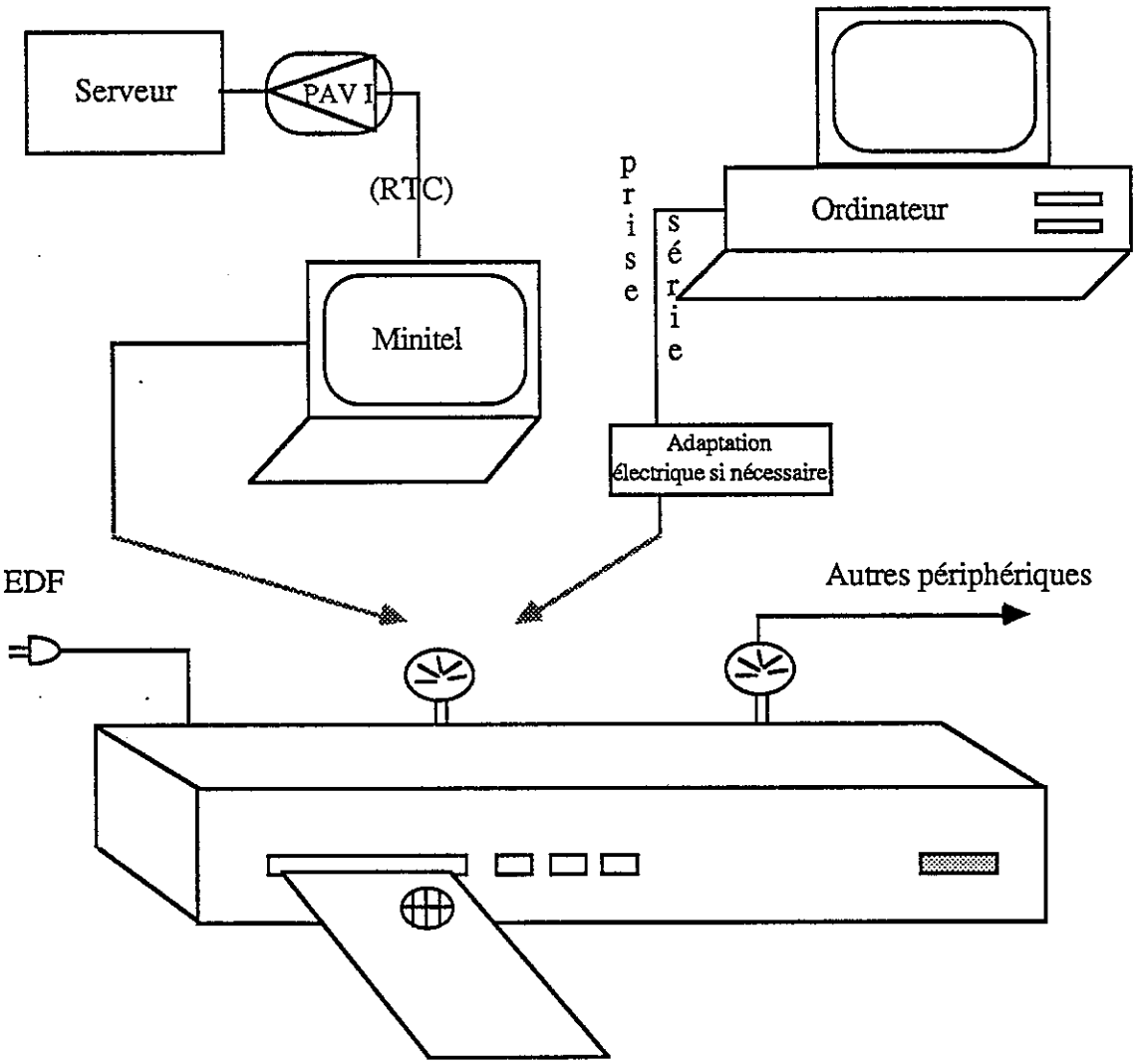
Ces spécifications, définies dans le document "Minitel 1Bistandard, "Spécifications Techniques d'Utilisation" (STUM 1B) s'appliquent au lecteur de cartes à microprocesseur LECAM.

4. AUTRES CAS D'UTILISATION

Le LECAM peut également être utilisé connecté à un ordinateur local, via une interface d'adaptation physique, électrique, et des signaux, si nécessaire.

Les références des constructeurs proposant de telles interfaces peuvent être consultées dans le "Répertoire des périphériques pour le Minitel" édité par la DGT et remis à jour de façon périodique.

ENVIRONNEMENT LECAM



CHAPITRE 2 - DOMAINES D'APPLICATION DU LECAM

Une application LECAM est la mise en relation d'une carte à microprocesseur et d'un centre serveur à fin d'échanger des informations confidentielles et permettant d'offrir des solutions adaptées aux besoins des entreprises : applications de paiement, de sécurité d'accès logique et physique, de dossiers portables,...

La mise en relation d'un usager et d'un serveur peut s'effectuer grâce à la possibilité de connexion automatique, mise en œuvre en local par le LECAM : cette fonctionnalité originale permet de réaliser la numérotation (automatique dans le cas de l'utilisation d'un LECAM avec un Minitel 10) puis la connexion à un serveur (envoi du numéro Transpac, mot de passe,...).

Outre la protection que l'usager est en droit d'attendre quant aux tentatives d'utilisation frauduleuse de sa carte, en cas de perte ou de vol par exemple, celui-ci doit également être assuré de l'intégrité des transactions effectuées au travers d'un réseau télématique.

Pour assurer cette sécurité, quatre fonctions essentielles sont mises en œuvre :

. **l'authentification**
le serveur vérifie la validité de la carte utilisée

. **la certification**
permet de donner la preuve à un serveur de la présence d'une information dans la carte

. **le chiffrement**
pour se prémunir contre la malveillance d'un tiers qui voudrait se mettre à l'écoute d'un message émis d'un usager A vers un usager B, seul habilité à le recevoir, les messages transitent chiffrés sur le réseau : cette fonctionnalité permet d'assurer la **confidentialité** d'un message.

. **la signature**
pour se prémunir contre la malveillance d'un tiers qui voudrait modifier le contenu d'un message émis d'un usager A vers un usager B, les textes envoyés par A sont accompagnés d'une signature électronique, garantissant à B l'**intégrité** du message reçu.

1 . IDENTIFICATION DU PORTEUR

a - Phase d'identification en local

A la demande du serveur, le LECAM demande au porteur son code confidentiel qui est présenté pour contrôle à la carte : trois erreurs successives entraînent le blocage de la carte qui ne peut être débloquée que par la mise en œuvre simultanée du code du porteur et d'un code de l'émetteur (la carte garde l'historique des présentations des codes dans la zone de contrôle), cette opération ne peut donc se faire qu'en liaison avec le centre émetteur.

Le voyant vert "SECRET" est allumé de façon fixe pendant la durée de la saisie du code confidentiel, garantissant ainsi à l'usager que les caractères saisis ne sont pas émis sur la ligne.

La saisie du code porteur reste valide tant que la carte est sous tension, et donc que le voyant jaune "CARTE" est allumé.

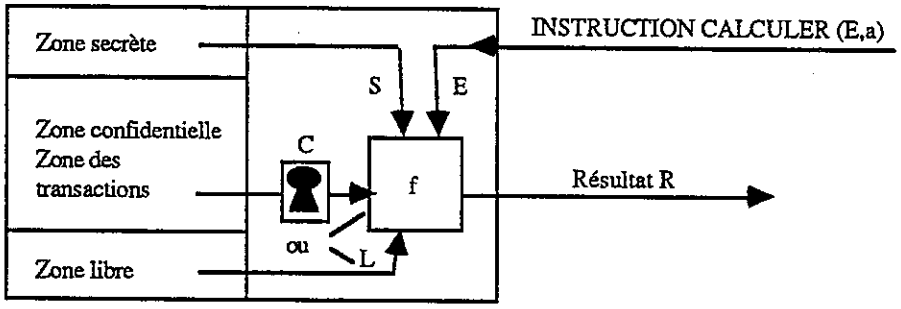
b - Identification par le serveur

Le serveur est averti de façon sûre et inimitable du résultat correct de la saisie du code confidentiel par certification de la réponse de la carte.

2 . L'EXECUTION PAR LA CARTE DE L'ALGORITHME DE SECURITE

Le microprocesseur de la carte exécute un algorithme de sécurité fournissant un résultat à partir d'un message reçu (en général, un nombre aléatoire), de la clé secrète de la carte et d'un mot désigné de la mémoire. Cet algorithme est utilisé à des fins d'authentification, d'identification, de signature et de gestion des clés.

Principe d'exécution de l'algorithme de sécurité



soit R = f (E//a, S, C)
si code porteur présenté correctement, sinon pas de résultat.

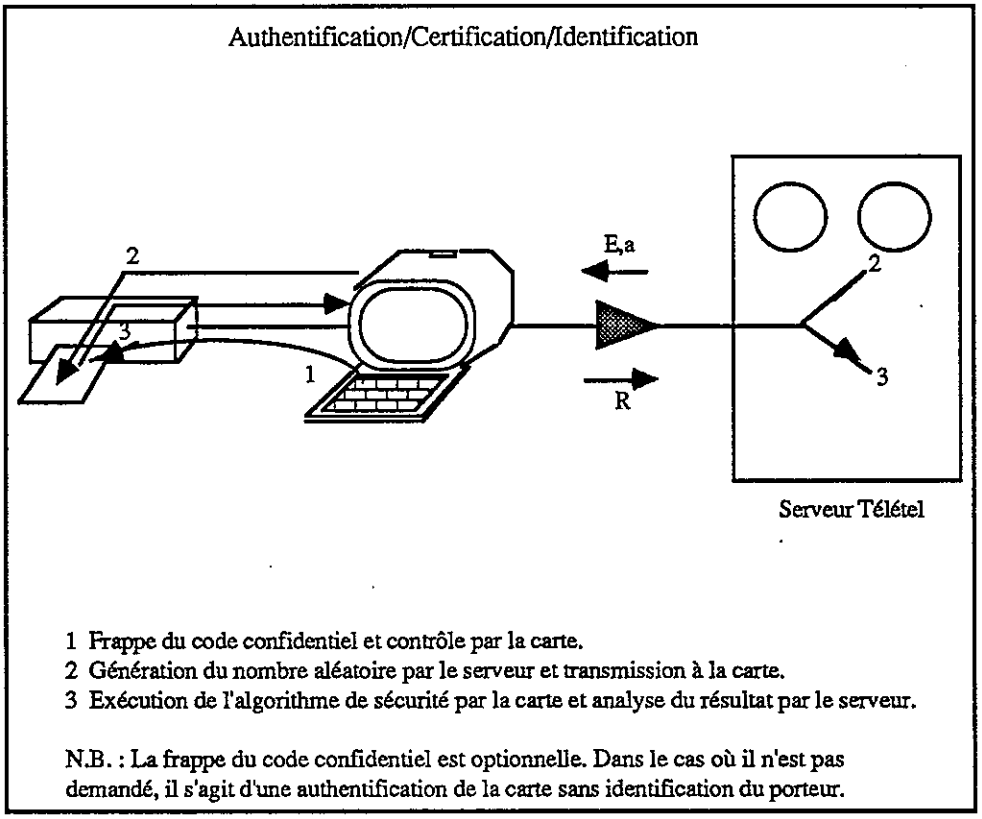
soit R = f (E//a, S, L)
sans obligation de présentation du code porteur.

E = donnée externe (en général nombre aléatoire)
a = adresse du mot à certifier
// = opération de concaténation
C = mot d'adresse a de la zone confidentielle ou de la zone des transactions
L = mot d'adresse a de la zone de lecture libre
S = clé secrète

3 . AUTHENTIFICATION DE LA CARTE-CERTIFICATION

Le serveur s'assure qu'il dialogue avec une carte émise par lui-même ou par un émetteur autorisé. Pour cela, il lit un paramètre spécifique de l'application inscrit dans la carte (n° série, n° iso,...) et demande le résultat de l'exécution de l'algorithme de sécurité sur ce numéro.

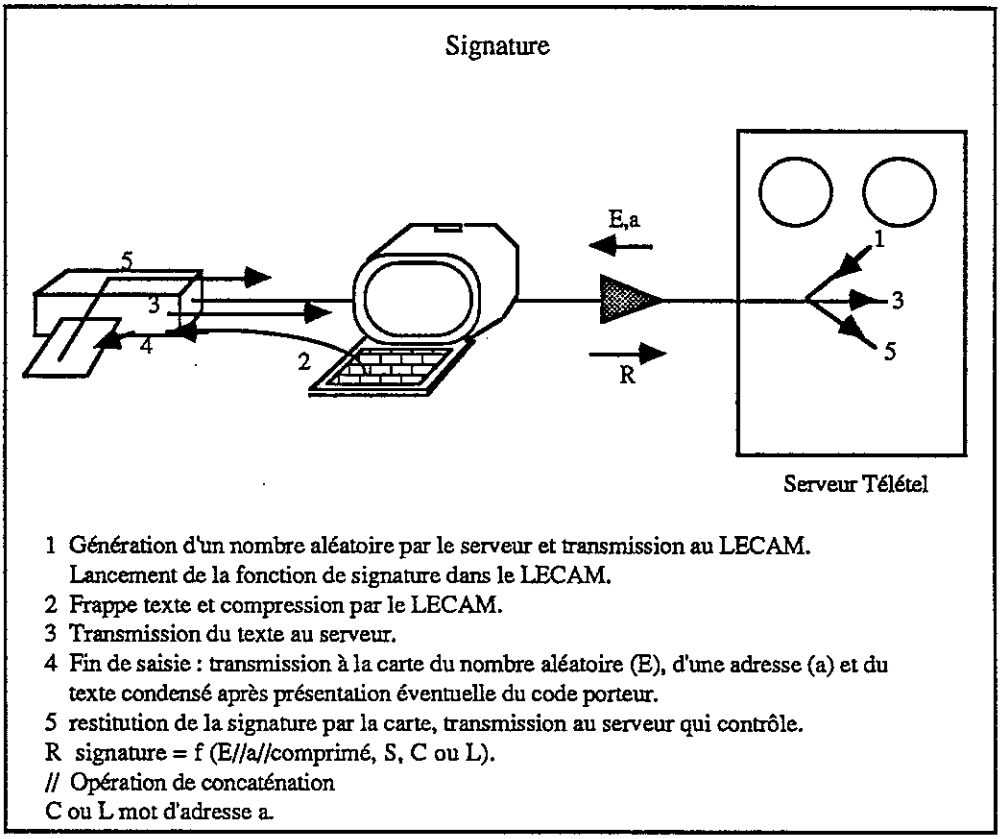
Cette dernière opération est également appelée certification lorsqu'elle est appliquée à d'autres données inscrites dans la carte.



Ces fonctionalités sont notamment utilisées pour des transactions de paiement électronique, pour lesquelles il faut s'assurer que la carte a bien été émise par l'autorité bancaire.

4 . SIGNATURE ELECTRONIQUE

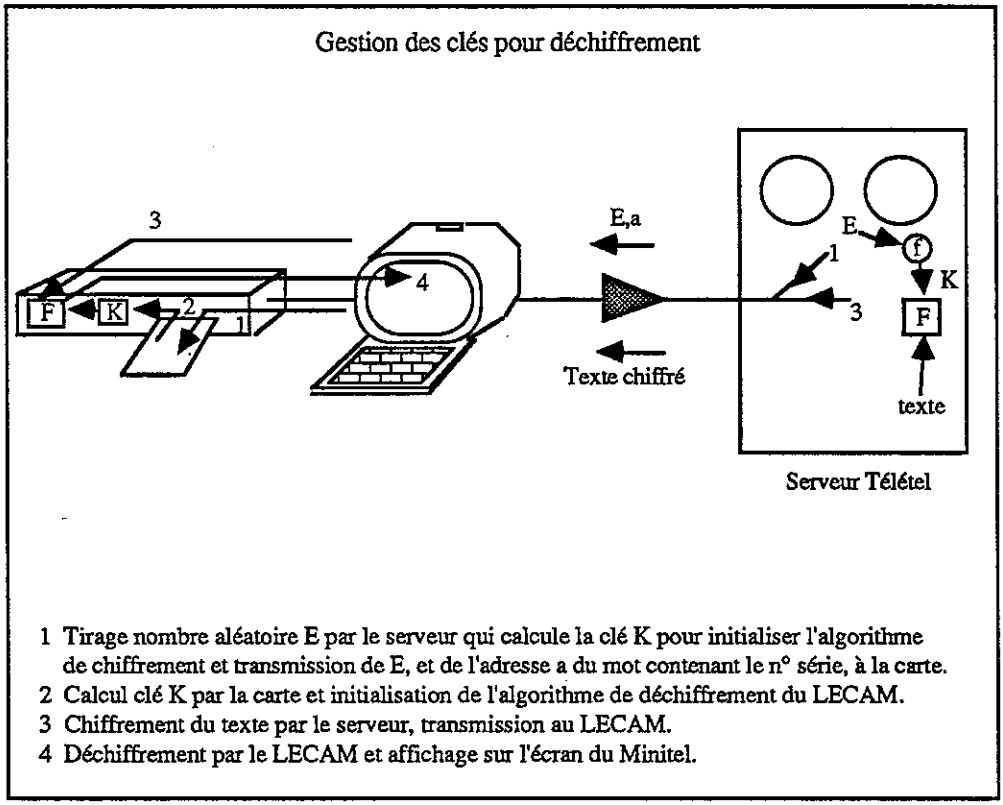
Un texte frappé sur le clavier du Minitel, est comprimé par le LECAM ; la certification, par la carte, du résultat de cette opération sert de signature au texte transmis au serveur.



1 Génération d'un nombre aléatoire par le serveur et transmission au LECAM.
Lancement de la fonction de signature dans le LECAM.
2 Frappe texte et compression par le LECAM.
3 Transmission du texte au serveur.
4 Fin de saisie : transmission à la carte du nombre aléatoire (E), d'une adresse (a) et du texte condensé après présentation éventuelle du code porteur.
5 restitution de la signature par la carte, transmission au serveur qui contrôle.
R signature = f (E//a//comprimé, S, C ou L).
// Opération de concaténation
C ou L mot d'adresse a.

5 . CHIFFREMENT, DECHIFFREMENT

Par le même algorithme de sécurité, la carte à mémoire calcule la clé qui initialise l'algorithme de chiffrement / déchiffrement résident dans le lecteur de cartes.



1 Tirage nombre aléatoire E par le serveur qui calcule la clé K pour initialiser l'algorithme de chiffrement et transmission de E, et de l'adresse a du mot contenant le n° série, à la carte.
2 Calcul clé K par la carte et initialisation de l'algorithme de déchiffrement du LECAM.
3 Chiffrement du texte par le serveur, transmission au LECAM.
4 Déchiffrement par le LECAM et affichage sur l'écran du Minitel.

CHAPITRE 3 - MISE EN ŒUVRE DU LECAM

1 . MISE SOUS TENSION

La mise sous tension du LECAM s'effectue en enfonçant le bouton Marche / Arrêt situé sur la face avant du lecteur. Le voyant rouge s'allume. Le voyant vert s'éclaire quelques secondes (tests de bon fonctionnement) puis s'éteint.

2 . ETAT LOCAL (possibilité de connexion automatique)

Dès l'introduction d'une carte et si le Minitel n'est pas connecté, le LECAM recherche dans la carte s'il existe des données de connexion à un serveur. Ces données sont contenues dans une partie de mémoire de la carte, repérée par un en-tête particulier.

Si un bloc de connexion est trouvé et en fonction des données enregistrées dans la carte, le LECAM procède à l'établissement de la communication téléphonique avec le réseau Télétel (cas du Minitel 10) puis à la connexion avec le serveur et avec le service requis. Si le Minitel est du type Minitel 1, le LECAM demande à l'utilisateur d'établir la communication téléphonique puis il gère la connexion au service.

3 . ETAT CONNECTE (fonctionnement sous contrôle d'un serveur)

Une fois la connexion établie, le LECAM agit en fonction des instructions téléchargées par le serveur précisant l'enchaînement des ordres à destination de la carte, les traitements locaux (saisie d'information au clavier, opérations arithmétiques et logiques, conversions, branchements en fonction de la réponse de la carte...) et la destination des données manipulées (carte, écran, serveur). Le LECAM met ainsi en œuvre les fonctions de la carte pour y rechercher une information particulière, demander l'exécution de l'algorithme de sécurité, inscrire une transaction au premier emplacement libre... sans que le serveur ait la visibilité des traitements élémentaires, ce qui a pour effet de minimiser les échanges sur le réseau.

Le serveur a la possibilité de demander l'exécution du programme résident de saisie du code confidentiel et d'utiliser les programmes de traitement local des anomalies.

Le serveur peut également demander au LECAM de chiffrer les données frappées au clavier ou lues dans la carte et de déchiffrer les données reçues pour affichage sur l'écran ou chargement dans la carte ou transfert vers un périphérique.

Enfin, le serveur peut placer le LECAM en mode "saisie signée", opération qui consiste à comprimer le texte frappé par l'utilisateur. Le texte est saisi par champs de 40 caractères avec la possibilité de correction lors de la frappe. En fin de saisie du champ, le texte est alors transmis au serveur et à l'algorithme de compression du LECAM. En fin de saisie d'un texte constitué d'un ou plusieurs champs, l'utilisateur donne son accord en actionnant la touche ENVOI. Le condensé peut alors être soumis à la carte pour calcul de la signature que le LECAM transmet au serveur en fin de texte.

Les échanges entre le serveur et le LECAM sont régis par un protocole assurant la transparence du réseau aux données et la protection contre les erreurs en ligne.

4 . ARRET

L'usager appuie sur le bouton Marche / Arrêt du lecteur. Le voyant rouge s'éteint.

CHAPITRE 4 - FONCTIONNEMENT DU LECAM

1 . LA CONNEXION AUTOMATIQUE (principe de fonctionnement)

A l'introduction de la carte et si le Minitel est sous tension et n'est pas connecté, le LECAM recherche les informations correspondant à une connexion automatique à un serveur.
Si ces informations sont protégées, il demande à l'usager de saisir son code confidentiel. Pour faciliter cette saisie, le lecteur dispose d'un éditeur de texte qui permet la correction des erreurs de frappe et analyse la réponse de la carte afin de demander au besoin un nouvel essai.
Seules les cartes dont le jeu d'instructions est équivalent à l'un des suivants : M4, B1, PC1, M6 peuvent contenir les informations permettant la connexion automatique.
Ces informations ont la même structure quel que soit le type du Minitel utilisé, et décrivent les données nécessaires à la connexion à un serveur (numéro téléphonique du point d'accès, code du service ou numéro Transpac) et à la sélection d'un service interne ainsi que toutes les actions répétitives conduisant à l'information requise (log on).

La partie connexion automatique est détaillée dans le chapitre 6.

2 . LES PHASES DU FONCTIONNEMENT SERVEUR - LECAM

2. 1 - Connexion du Minitel sur un serveur

La mise en œuvre d'une application LECAM nécessite l'établissement de la connexion, à travers le réseau téléphonique commuté ou le réseau Télétel, du Minitel sur un serveur. On pourra par exemple utiliser la possibilité de connexion automatique évoquée plus haut. Cette phase de connexion est inutile dans le cas d'un fonctionnement avec un serveur local.

2. 2 - Etablissement de la session avec le LECAM

L'établissement de la session avec le LECAM ne peut se faire que si le réseau Minitel est disponible, c'est -à-dire que le serveur est déjà maître ou que le fil PT est inactif. Si tel n'est pas le cas, le serveur doit utiliser le protocole "Système d'Echanges" décrit dans les STURM afin de libérer le réseau. Lorsque le réseau Minitel est libre, le serveur adresse au LECAM une demande d'ouverture de session, appelée aussi demande de connexion logique. Le serveur attend alors l'acquittement à sa demande de connexion logique pour débuter le dialogue avec le lecteur.

Ce dialogue s'effectue à l'aide de consignes : ce sont des commandes envoyées par le serveur qui sont par exemple destinées à initialiser le mode de fonctionnement du LECAM, à charger des programmes, ou à exécuter des fonctions internes (saisie, chiffrement,...).

La première commande transmise au lecteur par le serveur est une consigne de mise en mode. Cette consigne, encadrée par des commandes de transparence Minitel ou de modification des aiguillages du Minitel pour que les caractères reçus ne soient pas affichés sur l'écran, indique au LECAM quel va être son mode de fonctionnement.

Dès lors, les demandes de retournement du modem du Minitel sont gérées par le LECAM, ceci afin d'optimiser le délai d'acheminement de chaque réponse du lecteur, émise alors à 1200 bauds.

La réponse à la consigne de mise en mode est constituée d'informations décrivant l'état du lecteur, et éventuellement de la carte si celle-ci est présente dans le lecteur. Le serveur pourra alors vérifier la validité de la carte puis, si l'application nécessite l'utilisation d'un module de sécurité, elle devra établir la liaison logique avec ce dernier.
La phase applicative pourra alors commencer.

2. 3 - Téléchargement de programmes

La réalisation de l'application carte à microprocesseur s'effectue par téléchargements successifs de programmes ou de données dans la mémoire du LECAM.
Chaque programme peut réaliser une fonction plus ou moins complexe avec la carte de l'utilisateur et peut utiliser le Minitel pour dialoguer avec l'usager.

2. 4 - Exécution des programmes téléchargés

L'exécution par le LECAM du programme téléchargé est initialisée par le serveur à l'aide de consignes spécifiques. Le lecteur renvoie éventuellement le résultat de l'exécution ainsi qu'un certain nombre d'informations (mot d'état) renseignant le serveur sur le déroulement du programme en cours et lui permettant d'analyser la réponse.

Si l'application nécessite la réalisation d'autres fonctions, les opérations de téléchargement et d'exécution des programmes LECAM sont renouvelées autant de fois que nécessaire, sinon le serveur envoie au lecteur une demande de fin de session à l'aide d'une séquence de contrôle.

2. 5 - Fermeture de la session

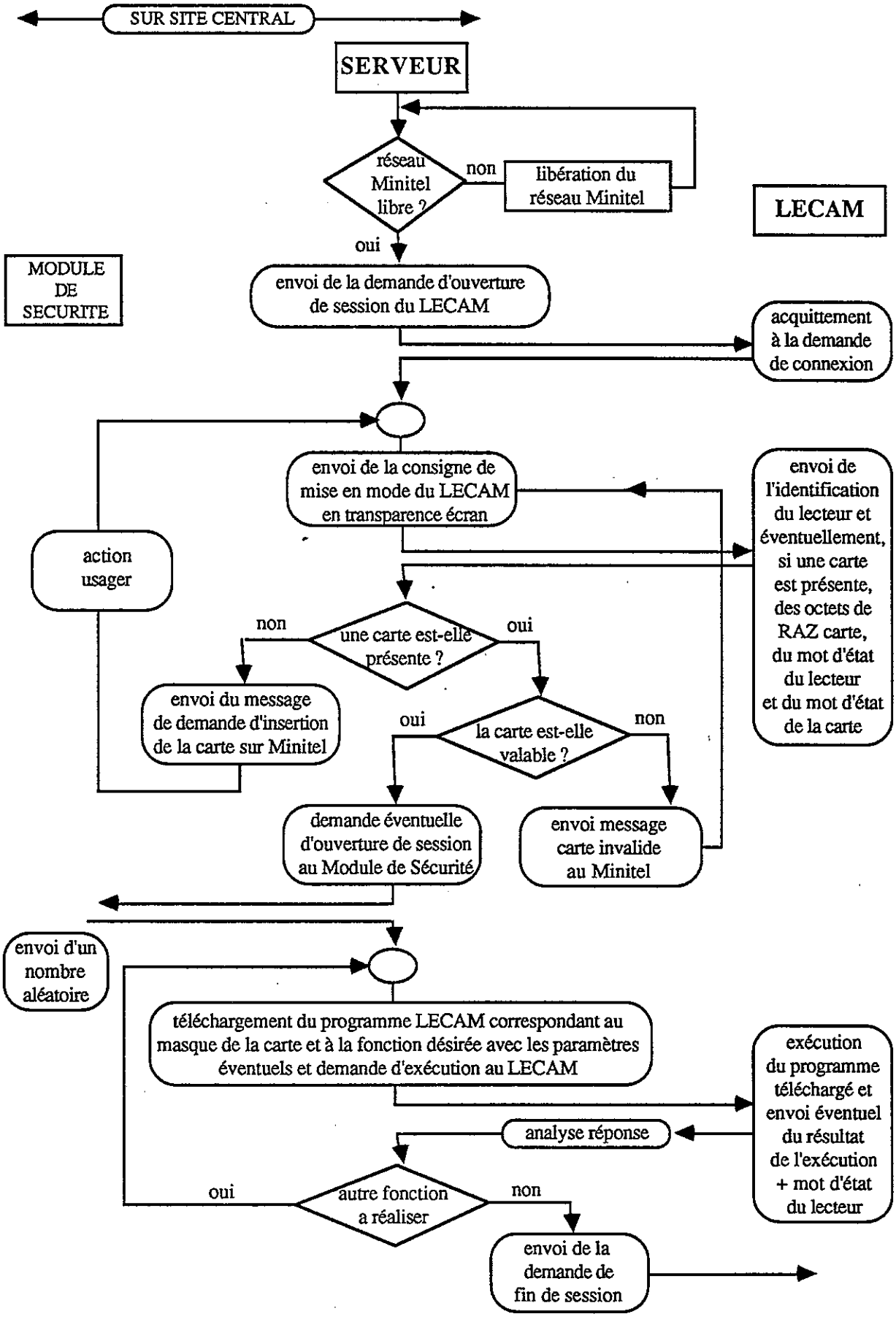
La fin de session est provoquée :

- par le lecteur, après échec du dialogue avec le serveur,
- par le serveur, après échec du dialogue avec le lecteur,
- par une fin normale décidée par le serveur, qui envoie une commande de déconnexion,
- par une déconnexion du Minitel,
- par un autre périphérique ou le point d'accès qui envoie une demande de déconnexion,
- par la modification abusive des aiguillages du Minitel, de la part du serveur, en cours de saisie chiffrée ou d'affichage chiffré, et lors d'une saisie en zone locale (par exemple,saisie de code confidentiel).

Remarque
Le changement d'état du Minitel provoqué par l'usager (inhibition de la prise péri-informatique d'un Minitel 1B, changement de la vitesse de transmission de la prise péri-informatique), perturbe le réseau Minitel et provoque un arrêt de la session à plus ou moins brève échéance.

2. 6 - Synoptique récapitulatif

SYNOPTIQUE DIALOGUE ENTRE CENTRE SERVEUR ET LECAM



CHAPITRE 5 - CARACTERISTIQUES DU LECAM

1 . CARACTERISTIQUES GENERALES

Le LECAM est un outil dédié qui, raccordé au terminal Minitel, assure la gestion de cartes à mémoire.

Disposant d'un système d'exploitation, dont les commandes sont appelées **consignes**, d'un langage de programmation appelé macrolangage, et d'un interpréteur chargé d'analyser les programmes écrits en macrolangage, il est comparable à un micro ordinateur, capable de s'adapter de façon totalement transparente aux applications ou aux cartes à mémoire existantes ou à venir, pourvu que les cartes utilisées soient compatibles avec le projet de norme ISO référencé DIS 7816/3.

Ce micro ordinateur a ceci de particulier qu'il ne peut fonctionner de façon autonome : c'est un périphérique "intelligent" dont la vocation est de recevoir et d'exécuter des programmes téléchargés par un centre serveur afin d'établir un dialogue sécurisé entre un usager, par l'intermédiaire de sa carte à microcircuit, et une application déterminée.

Le LECAM est donc doté de deux modules logiciels distincts, communiquant entre eux :

- un module "Application Carte" chargé d'analyser les consignes et d'exécuter les programmes reçus de l'application distante, puis de renvoyer un compte rendu,

- un module "Télécommunications" chargé de gérer l'interface du LECAM avec le monde extérieur.

2 . ARCHITECTURE LOGIQUE

2. 1 - Le module Télécommunications

Pour dialoguer avec les différents éléments avec lesquels le LECAM peut être mis en relation, et gérer au mieux les échanges nécessaires à une application donnée, le LECAM est doté d'un module logiciel chargé de gérer le Système d'Echanges du réseau Minitel, le Protocole du Minitel, et le protocole d'échanges avec le serveur.

2. 1. 1 - Le Système d'Echanges du réseau Minitel

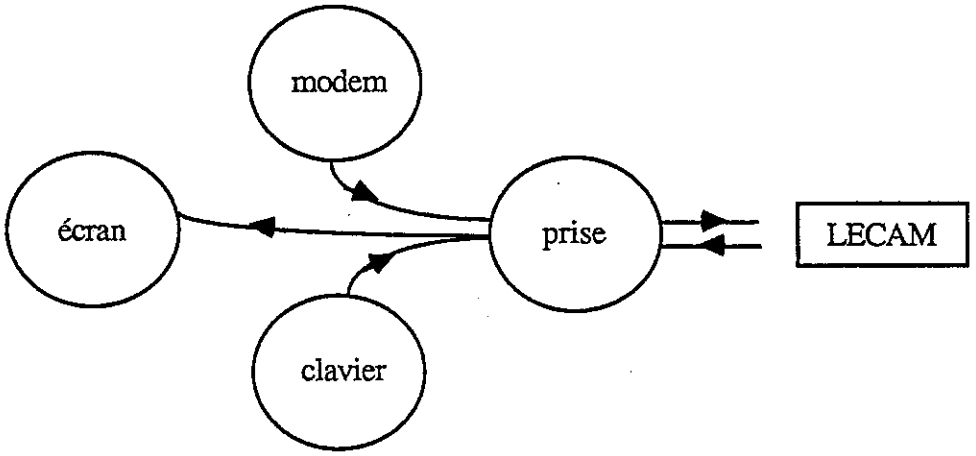
Le **Système d'Echanges** est le protocole de dialogue de tout périphérique connecté au réseau Minitel. Ce protocole assure la mise en relation, par un système d'adressage, d'au moins deux périphériques, la gestion des conflits et la prise de parole. Le serveur distant est assimilé à un périphérique.

Le Système d'Echanges est décrit dans le document "Spécifications Techniques d'Utilisation du Réseau Minitel" (STURM).

2. 1. 2 - Le Protocole du Minitel

Le **Protocole du Minitel** permet l'aiguillage des flots de données entre les différents modules du Minitel, à savoir l'écran, le clavier, le modem et la prise. Selon les fonctions à réaliser, le LECAM peut commander les aiguillages du Minitel pour établir, ou interdire, la relation entre tel ou tel autre module.

Par exemple, lorsque le LECAM demande à l'usager de saisir son code confidentiel, les caractères frappés sur le clavier du Minitel sont envoyés au lecteur qui renvoie sur l'écran du Minitel un caractère "*" chaque fois qu'une touche, autre qu'une touche de fonction, est frappée par l'usager. Les aiguillages réalisés sont donc les suivants :

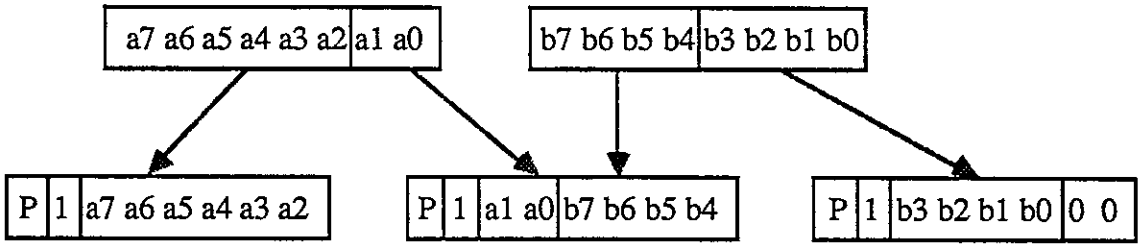


Si l'environnement le permet, le LECAM gère automatiquement le retournement du modem du Minitel : le serveur envoie ses messages à 1200 bauds ; le LECAM, après retournement du modem du Minitel, émet sa réponse également à 1200 bauds, ce qui a pour effet de réduire sensiblement le délai d'acheminement des messages entre le LECAM et l'application distante.

2. 1. 3 - Le protocole d'échanges avec le serveur

Le **protocole d'échanges avec le serveur** assure la transparence des données échangées sur le réseau Télétel entre le LECAM et le serveur. Cette transparence est réalisée par la transformation en code appelé P/1/6 de chaque octet transmis et par l'encadrement des données échangées, qui sont rassemblées à l'intérieur de "drapeaux" indiquant au LECAM que les données ainsi transmises constituent un bloc d'informations qui lui est destiné.

Le codage en P/1/6 assure une conversion sur 7 bits de caractères codés sur 8 bits utiles et permet d'interdire aux caractères, jugés indésirables à certains moments de la transmission, de circuler sur la ligne. Ce codage supprime les combinaisons de positions binaires correspondant aux valeurs hexadécimales 0/0 à 1/F, et est réalisé de la manière suivante :

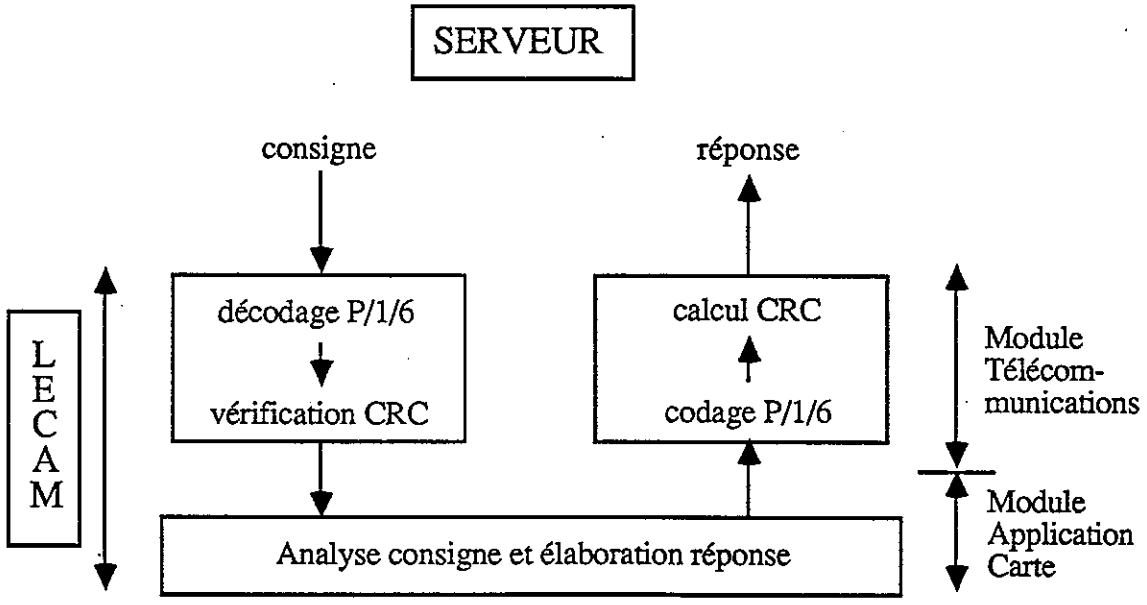


Les messages sont constitués de blocs d'informations. Chacun de ces blocs est encadré par un drapeau de début et un drapeau de fin de bloc. Le rôle des drapeaux est d'indiquer quelle est la nature des informations transmises. En effet, ces informations peuvent être des données Vidéotex à afficher sur l'écran du Minitel ou des commandes que le LECAM doit intercepter pour les traiter. Dans ce dernier cas, les blocs sont constitués d'un nombre variable de structures au format TLV. Ce format est utilisé par le serveur pour décrire une consigne et par le LECAM pour définir la nature de sa réponse.

L'abréviation TLV signifie :

Type	de consigne ou de réponse
Longueur	en octets, du champ V
Valeur	des données transmises

Le protocole d'échanges avec le serveur gère également la protection contre les erreurs de transmission. Cette protection est triple : le LECAM contrôle la parité de chaque caractère, la cohérence du codage en P/1/6 ainsi que le CRC des blocs reçus, si cette protection est mise en œuvre. Dans le cas où une erreur est détectée, le LECAM interrompt la réception en cours et demande au serveur de réémettre le bloc erroné.



2. 2 - Le module Application Carte

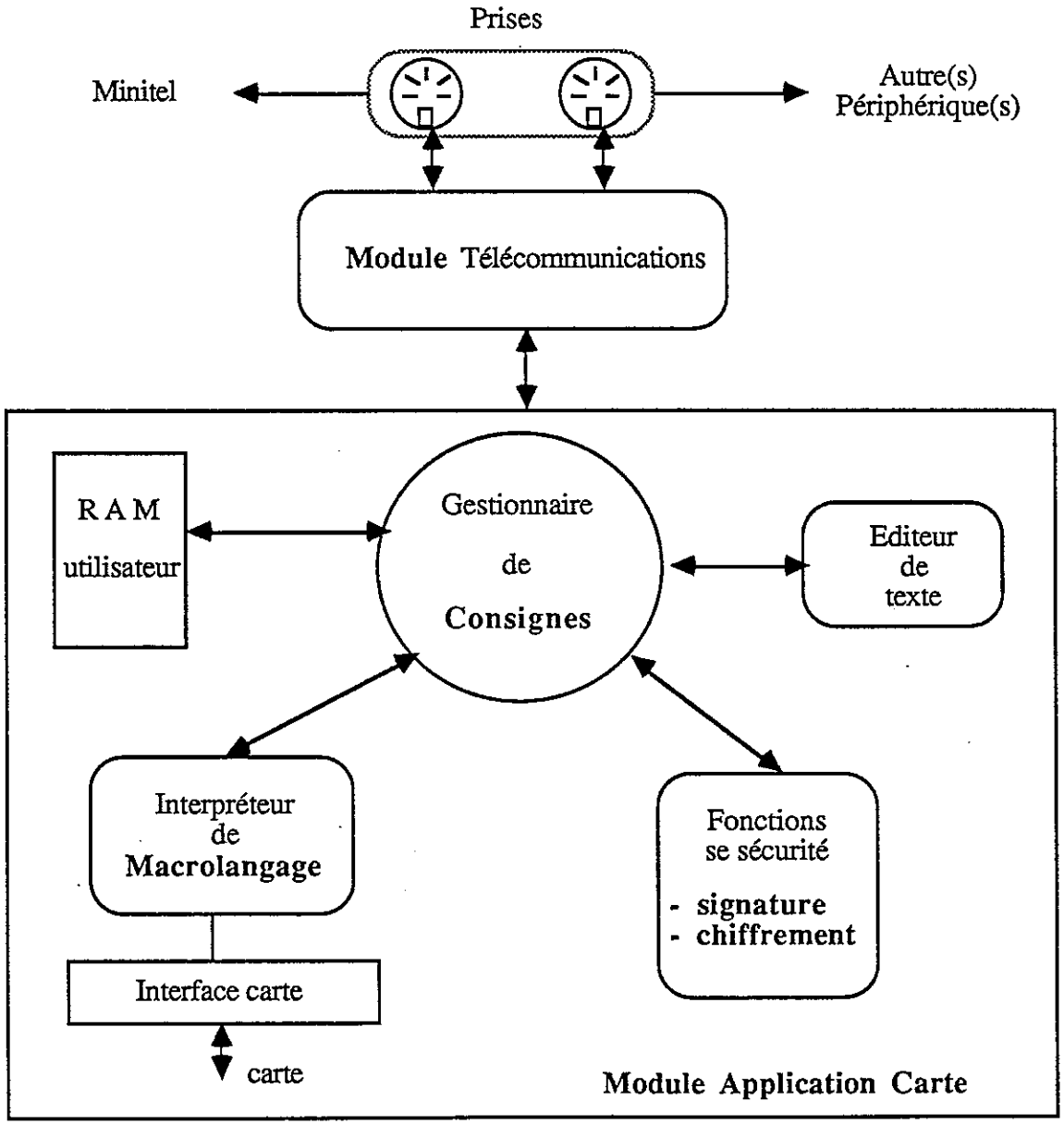
Les outils dont dispose le LECAM pour la mise en œuvre d'une application carte à mémoire sont réunis dans un module logiciel qui comporte les éléments suivants :

- la gestion de la mémoire utilisateur,
- l'éditeur de texte,
- le gestionnaire de consignes,
- l'interpréteur de programmes,
- l'interface carte,
- les fonctions de sécurité.

L'interconnexion de ces différents éléments constitue le module Application Carte. Ce module est en relation permanente avec le module Télécommunications.

Le schéma suivant présente l'architecture logique du LECAM.

Architecture logique du LECAM

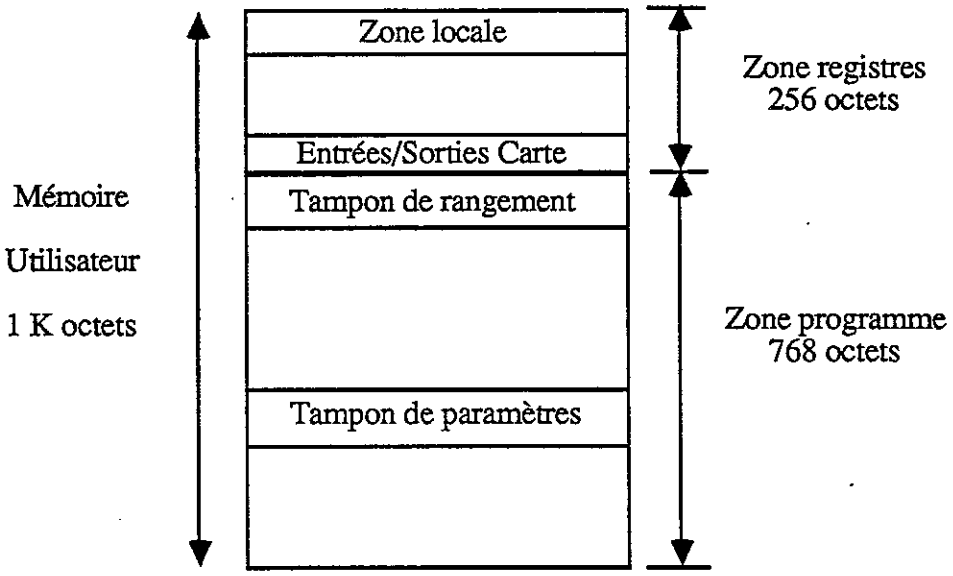


2. 2. 1 - Gestion de la mémoire utilisateur

Le LECAM dispose d'une mémoire vive (RAM) d'une capacité de 1 K octets. Cette mémoire est découpée en deux zones distinctes :

768 octets constituent la zone programme qui inclut, en plus des programmes téléchargés par l'application distante, un tampon de paramètres et un tampon de rangement qui est destiné à recevoir les données à émettre vers le serveur.

les 256 octets restants forment la zone registres qui inclut les données manipulables par l'interpréteur de macrolangage, et notamment le tampon d'entrées/sorties carte et la zone locale.



La zone locale est formée de 32 octets qui ont un statut particulier : ils sont inscriptibles ou modifiables de l'extérieur, mais ne peuvent être ni relus, ni testés par l'extérieur ; leur seule destination possible est une utilisation dans le cadre d'un ordre entrant vers la carte. Cette zone sert par exemple à stocker le code secret de l'usager avant d'être présenté à la carte pour contrôle.

Les programmes téléchargés dans le LECAM sont conservés en mémoire jusqu'à la mise hors tension de l'appareil. Par exemple, et à condition de respecter certaines précautions (se référer au Chapitre 8, paragraphe 7. 2. 4 -), il est donc possible d'utiliser un programme téléchargé le matin pendant le restant de la journée.

2. 2. 2 - Le gestionnaire de consignes

Le LECAM est pourvu d'un système d'exploitation dont les commandes, appelées consignes, sont adaptées aux spécificités du lecteur.

L'initiative du dialogue avec le LECAM revient au serveur : chaque consigne émise par le serveur est une "question" adressée au lecteur. A chaque question correspond une réponse du lecteur.

La consigne d'initialisation du fonctionnement du LECAM définit les modalités du dialogue à venir : mode de fonctionnement du lecteur (gestion ou non du Minitel), gestion des erreurs de transmission, envoi de compte rendu d'exécution lors d'échanges avec la carte ou avec le serveur.
Cette commande n'est généralement utilisée qu'une seule fois en cours de session, et c'est obligatoirement la première consigne envoyée au LECAM par le serveur.

Le LECAM connaissant désormais l'environnement dans lequel il travaille, est prêt à recevoir d'autres consignes, et notamment celles de chargement et d'exécution des programmes.

Le dialogue avec l'utilisateur est rendu possible grâce à l'éditeur de texte. Cet éditeur est paramétrable par l'intermédiaire d'un certain nombre de consignes qui permettent de définir des variables telles que temps intercaractères maximum en saisie, nature des caractères saisis (numérique, alphabétique,...), caractère d'écho,...

La mise en œuvre des fonctions de sécurisation internes au lecteur telles que chiffrement et signature électronique sont l'objet de consignes permettant d'initialiser la fonction de chiffrement, la fonction de signature ou de signaler la fin d'un message ou d'une saisie signés.

2. 2. 3 - L'interpréteur de programmes

Le programmeur d'applications LECAM dispose d'un langage de programmation évolué appelé macrolangage qui est proche, dans sa conception et sa mise en œuvre, d'un langage assembleur. Il comporte, en plus des instructions utilisées par tout micro-ordinateur (chargement de zone mémoire, fonctions arithmétiques et logiques, fonctions de test, fonctions de saut, utilitaires de conversion,...), les outils spécifiques nécessaires à la mise en œuvre des fonctionnalités du lecteur :

le dialogue usager est assuré par la présence d'instructions gérant :

- l'affichage sur l'écran,
- la saisie clavier, libre ou contrôlée,
- la combinaison d'affichage et de saisie clavier ;

le dialogue serveur est géré par les instructions d'envoi en clair ou en chiffré de données vers le serveur depuis diverses zones mémoire du LECAM ;

les opérations avec la carte sont réalisées par :

- ordres entrant et sortant de la carte,
- combinaison d'ordres entrant et sortant,
- recherche d'un mot dans la carte à l'aide d'un profil donné,
- lecture ou écriture dans la carte avec incrémentation ou décrémentation automatique de l'adresse carte.

2. 2. 4 - L'interface carte

Les échanges avec la carte sont réalisés conformément au projet de norme ISO référencé DIS 7816/3.

40 octets de la zone registres de la mémoire utilisateur sont réservés à ces échanges :

- 5 octets représentent l'ordre envoyé à la carte,
- les 3 octets suivants contiennent les comptes-rendus d'exécution de chaque ordre carte,
- les 32 octets restants sont les données échangées entre la carte et le LECAM.

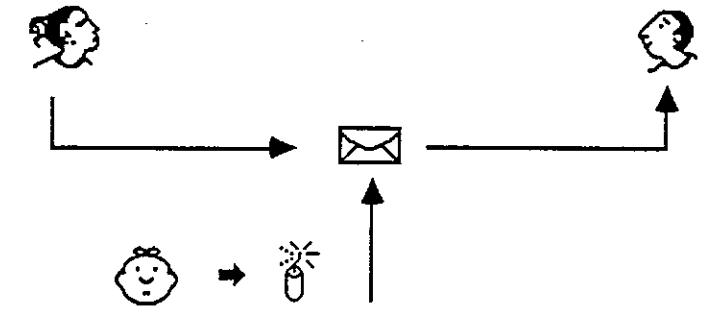
2. 2. 5 - Fonctions de sécurité

Le LECAM possède, en interne, un certain nombre de fonctions de sécurité (ceci en plus de la sécurité apportée par la carte à mémoire). Ces fonctions sont le chiffrement et la signature des messages circulant entre le LECAM et le serveur. Ces fonctions peuvent être contrôlées par des blocs de sécurité inscrits dans la carte de l'usager.

a - Signature
La signature est le moyen de se prémunir contre la malveillance active d'un tiers qui voudrait modifier le contenu d'un message émis d'un usager A vers un usager B de façon à modifier la signification du message ; il s'agit dans cette opération d'assurer l'**intégrité** du message émis de A vers B ou si les données sont falsifiées entre A et B de prouver, par la signature, que le texte reçu par B ne peut avoir A pour origine.

Un schéma type de la malveillance vis-à-vis de l'intégrité d'un message est le suivant :

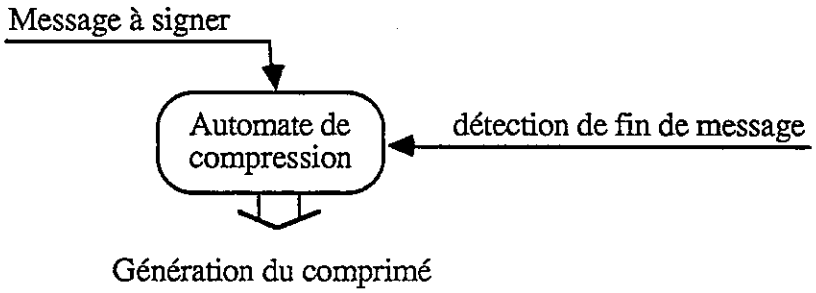
Schéma d'atteinte à l'intégrité des données



Ecoute active et malveillante

Cette fonctionnalité, incluse dans le LECAM, permet de signer un message de longueur variable par initialisation de l'automate de compression, le comprimé du message sur 4 octets étant engendré sur détection de fin de message à signer. Le comprimé est mémorisé dans la zone interne du LECAM et peut, par la suite être utilisé dans un calcul à l'aide de l'algorithme de sécurité de la carte pour signer le texte. La signature ainsi obtenue est bien représentative du texte signé (c'est lui qui initialise l'automate de compression et est à l'origine du comprimé) et de l'auteur du texte (puisque le calcul de la carte met en œuvre le comprimé bien sûr, mais aussi une clé secrète de la carte personnalisée pour chaque usager). Ce mécanisme de signature est aussi utilisé lorsque cette opération vise à faire signer par l'utilisateur son accord pour une transaction monétaire (ce certificat peut être inscrit dans la carte de l'usager) ; c'est ce certificat qui, présenté à une tierce personne, permet de prouver la bonne foi de l'une ou l'autre des parties en cas de contentieux.

Le principe de fonctionnement de la signature dans le LECAM est le suivant :



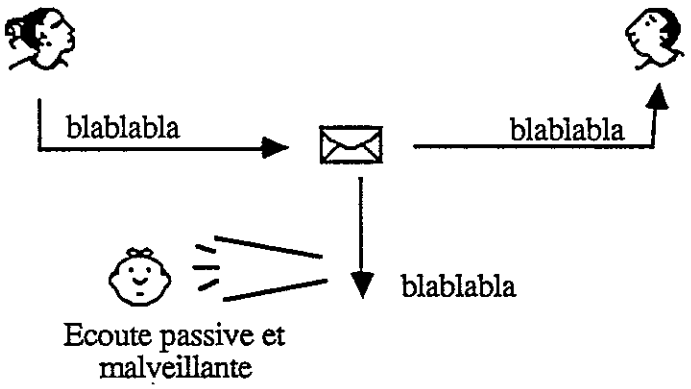
Grâce à cette fonctionnalité, le LECAM est à même d'assurer les fonctions de sécurisation pour lesquelles l'intégrité des données est un point important.

b - Chiffrement

Le chiffrement permet de se prémunir contre la malveillance d'un tiers qui voudrait se mettre à l'écoute (passive et non plus active) d'un message émis d'un usager A vers un usager B, alors que ce message ne doit être connu que de l'usager B ; le chiffrement, opération qui tend à rendre illisible un texte, sauf à posséder le moyen de le déchiffrer assure la **confidentialité** d'un message.

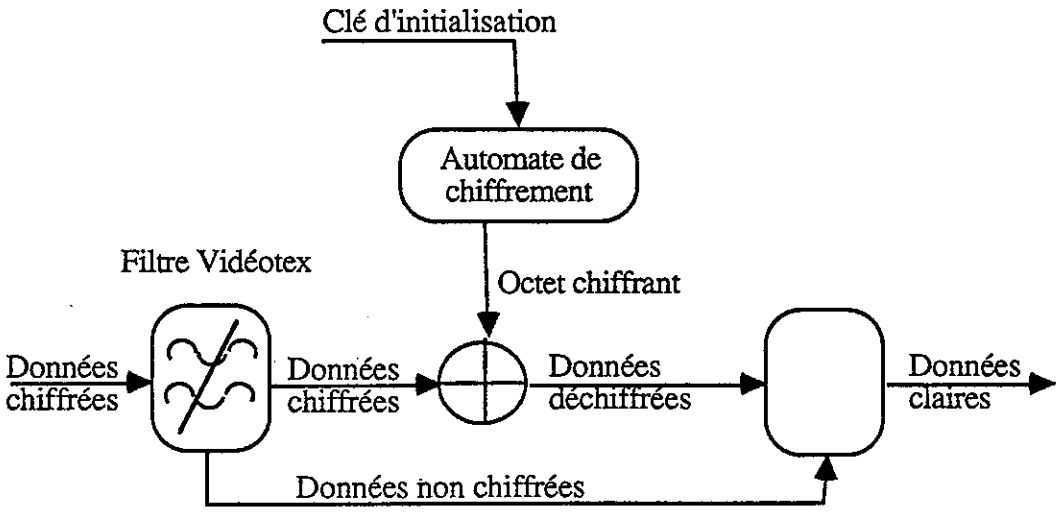
Un schéma type de la malveillance contre la confidentialité dont on se prémunit en mettant en œuvre une fonction de chiffrement est le suivant :

Schéma d'atteinte à la confidentialité des données

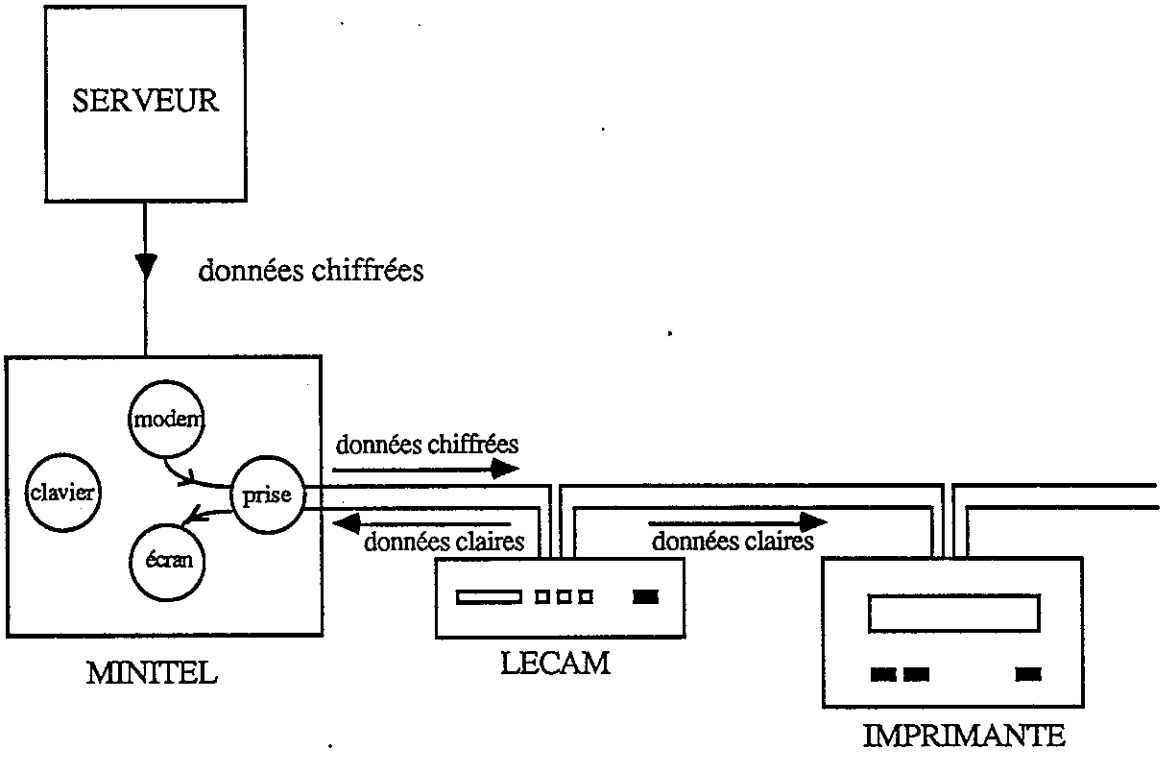


Cette fonctionnalité, incluse dans le LECAM, permet donc de chiffrer des saisies-clavier réalisées par l'usager avant d'être émises vers le serveur ou de déchiffrer des messages Vidéotex émis par le serveur. L'opération de chiffrement/déchiffrement prend en considération le niveau de présentation Vidéotex et Télétel de façon à éviter le chiffrement de certaines séquences qui pourraient engendrer la création de séquences perturbatrices (protocole Minitel, Système d'Echanges, codes des colonnes 0 et 1...). Le chiffrement est obtenu à partir d'un automate de chiffrement ; serveur et LECAM possèdent le même automate et le déchiffrement n'est possible que si les deux extrémités possèdent la même clé d'initialisation pour leur automate.

Le principe de fonctionnement du chiffrement est le suivant :



Exemple d'application du chiffrement
Un serveur peut envoyer des données chiffrées à destination d'une imprimante connectée au réseau Minitel. Pour réaliser la fonction de déchiffrement, le LECAM doit être situé entre le Minitel et l'imprimante. Le serveur, ayant pris soin de communiquer les informations permettant au LECAM de calculer la clé de déchiffrement, envoie les données chiffrées au lecteur. Ce dernier, après les avoir déchiffrées, les renvoie simultanément sur ses deux prises, et donc vers l'écran du Minitel et vers l'imprimante, si celle-ci a été adressée lors de l'ouverture de session.



Remarque :
Le LECAM est capable de réaliser du déchiffrement pour n'importe quel type de périphérique, qu'il soit "bout de chaîne" ou compatible avec le Système d'Echanges.

c - Blocs de sécurité
La prise en compte d'un comprimé dans une opération de signature et la prise en compte d'un mot d'initialisation pour l'automate de chiffrement qui sont deux fonctions de sécurité internes au LECAM, peuvent être complètement contrôlées par la carte à mémoire si elle comporte un bloc de sécurité. Présents dans les masques bancaires B1 ou porte-clés PC1, ils permettent à l'émetteur de la carte de préciser les conditions uniques de mise en œuvre des fonctions de sécurité incluses dans le LECAM et donc de contrôler l'usage de ces fonctions sensibles pour le couple carte-LECAM considéré. Pour les cartes M4, B0 ou M6, le bloc de sécurité est implicite dans le LECAM et n'est donc pas à inscrire dans la carte. Donc, au préalable de l'activation d'une quelconque des fonctions de sécurité, le LECAM vérifie la concordance entre l'ordre émis par le serveur et le bloc de sécurité de la carte (le bloc de sécurité d'une carte est lu à chaque initialisation du lecteur, les données lues étant remises à 0 sur fin de session du lecteur ou sur arrachement carte) ; s'il n'y a pas concordance entre l'ordre émis et le bloc de sécurité, le LECAM refuse d'activer la fonction de sécurité concernée.

Remarque :
Il n'est pas possible de réaliser de signature en l'absence de bloc de sécurité dans la carte.

d - Générateur d'octets chiffrants (GOC)
L'automate de chiffrement et l'automate de compression fonctionnent par l'intermédiaire d'un générateur d'octets chiffrants, dont les spécifications sont en diffusion contrôlée par le CCETT (Centre Commun d'Etudes de Télédiffusion et Télécommunications - Département ASP - rue du Clos Courtel - BP 59 - 35512 CESSON SEVIGNE CEDEX).

PARTIE 2

SPECIFICATIONS D'INTERFACE DU LECAM

CHAPITRE 6 - LA CONNEXION AUTOMATIQUE

1 . DESCRIPTION GENERALE

La fonction "Connexion automatique" du LECAM permet de réaliser automatiquement l'appel à un service, c'est à dire la composition du numéro téléphonique du serveur, ainsi que le dialogue aboutissant à l'établissement de la connexion. Les données nécessaires (numéro de téléphone, message(s) à transmettre) sont inscrites dans un bloc (au profil particulier) de la carte de l'usager.

Le lecteur LECAM offre cette possibilité pour les cartes M4, B0, M6, B1 et PC1 ainsi que pour toutes les cartes simulant un de ces masques.

La connexion automatique est initialisée par l'introduction d'une carte dans le LECAM, à condition toutefois que le Minitel soit sous tension et ne soit pas déjà connecté. Dans le cas où le LECAM n'est pas connecté à un Minitel, il n'y a pas de phase de connexion automatique (cas d'un LECAM connecté à un micro-ordinateur par exemple).

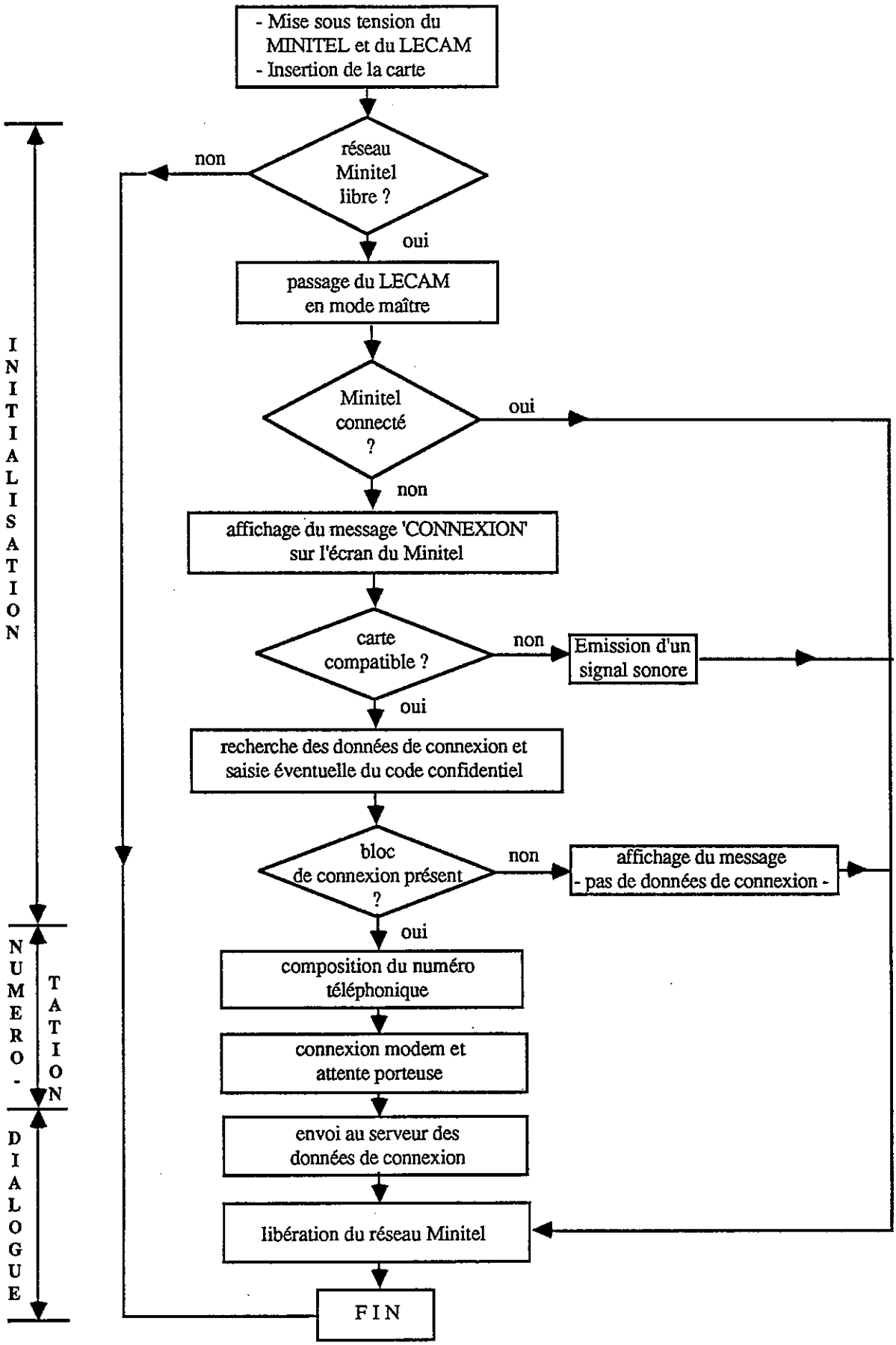
L'utilisation d'un Minitel 10 permet en outre la composition automatique du numéro par le module téléphonique, ce qui réduit d'autant les manipulations par l'usager, dont la seule tâche reste donc l'insertion de sa carte dans le lecteur, après l'appui sur les boutons de mise en service du Minitel et du LECAM.

Le déroulement général d'une connexion automatique est résumé par le diagramme suivant, qui laisse apparaître trois phases :

- initialisation
- numérotation
- dialogue

Pendant la phase d'initialisation, le LECAM vérifie en particulier que les données contenues dans le bloc de connexion automatique sont accessibles librement. Si ce n'est pas le cas, le lecteur fait saisir son code porteur à l'usager, à l'aide des programmes résidents (voir ce paragraphe dans le chapitre 8) dont il dispose, avant de procéder à la suite.

DESCRIPTION GENERALE D'UNE CONNEXION AUTOMATIQUE



2 . EXECUTION D'UNE CONNEXION AUTOMATIQUE

2. 1 - Phase d'initialisation

Lorsqu'une carte est introduite dans le LECAM, celui-ci vérifie que le réseau Minitel est libre, caractérisé par l'état inactif du fil PT et que le Minitel n'est pas connecté avant de débuter la phase de connexion :

- l'écran du Minitel est effacé,
- le texte "CONNEXION" est affiché en double hauteur,
- si la carte n'est pas reconnue par le lecteur, il y a émission d'un signal sonore et la procédure de connexion est abandonnée,
- le lecteur recherche les données de connexion selon le processus décrit dans le paragraphe "Description des blocs de connexion".

Si le bloc de connexion est protégé par un code confidentiel, le LECAM invite l'usager à saisir ce code par le message :

"Tapez votre code : "

qui apparaît sur la ligne 12 de l'écran. L'usager doit alors frapper son code et le valider par l'appui sur la touche <ENVOI>.

L'usager dispose de trois essais. S'il échoue au bout du troisième essai, la connexion automatique est abandonnée et la carte est bloquée.

Le voyant "SECRET" est allumé de façon fixe pendant la saisie du code confidentiel. Le LECAM vérifie en permanence que les données frappées par l'usager ne sont pas émises vers le serveur, et range ces données dans la zone locale de la mémoire.

Les caractères frappés par l'usager pendant cette saisie ne sont pas affichés sur l'écran : l'écho du code confidentiel est visualisé par des "*".
Si la carte est arrachée pendant la saisie, le LECAM passe en mode repos et le Minitel envoie la séquence SEP, 5/4 indiquant que le réseau Minitel est libéré.

Si le lecteur ne trouve pas de données de connexion, le message :

--- Pas de données de connexion ---

est affiché sur l'écran du Minitel et le réseau Minitel est libéré au bout d'environ 160 ms.

Si des données de connexion sont trouvées, le lecteur passe à la phase suivante.

2. 2 - Phase de numérotation

Le bloc de connexion automatique peut ne pas comporter de numéro d'appel à un serveur. Dans ce cas, le lecteur affiche :

"Composez le numéro"

pour inviter l'usager à composer le numéro de téléphone permettant la mise en relation du terminal avec le point d'accès ou le serveur.

Si un numéro de téléphone est inscrit dans la carte, le lecteur réagit selon le type de Minitel :

Minitel M1 :
Le lecteur affiche sur l'écran :

... COMPOSEZ LE NUMERO XX XX ...

pour inviter l'usager à composer lui-même le numéro.
Puis, s'il n'y a pas de données de connexion à un serveur, le LECAM libère le réseau Minitel. Sinon, il attend que le Minitel lui signale la réception d'une porteuse pour passer à la phase suivante.

Minitel M10 :
Le lecteur affiche sur l'écran :

... NUMEROTATION AUTOMATIQUE ...

puis charge le numéro de téléphone dans la mémoire écran numéro 9 et demande l'appel par le module téléphonique du Minitel. L'usager voit donc apparaître sur la rangée 0 de l'écran les deux caractères "> 9" suivis du numéro composé par le Minitel.

Au préalable, le Minitel aura été initialisé correctement (préfixe d'accès au réseau public, indicatif interurbain...).

Le LECAM attend que le Minitel lui signale la réception d'une porteuse ; puis, si la carte ne comporte pas de bloc de connexion automatique, le lecteur libère le réseau Minitel en desactivant le fil PT, sinon il passe à la phase dialogue.

Remarques :

1 - Si la carte est arrachée pendant cette phase, l'écran du Minitel est effacé et un signal sonore est émis. Le réseau Minitel est libéré.

2 - Le Minitel 10 dispose d'une fonction MEM (mémorisation d'un agenda pouvant comporter jusqu'à vingt numéros de téléphone).
Si cette fonction est active au moment de l'introduction de la carte, la connexion automatique ne peut avoir lieu. Il faut donc sortir de cette fonction (appui sur la touche <RETOUR>), ce qui a pour effet de poursuivre la procédure de connexion automatique.

3 - Si le combiné est décroché ou que la prise de ligne est détectée, le LECAM libère le réseau Minitel et la connexion automatique est arrêtée.

2. 3 - Phase de dialogue

Le bloc de connexion automatique contenu dans la carte de l'usager peut contenir la description du dialogue à effectuer avec le serveur.

Deux modes de fonctionnement sont possibles : un mode implicite où le texte à transmettre par le lecteur est simplement indiqué, séparé en plusieurs messages par le codage des touches de fonction du Minitel (SEP, x/y), ou un mode explicite permettant de décrire plus précisément comment sont réalisés les échanges avec le serveur.

Mode implicite
Dans ce mode, le lecteur attend d'abord la réception de la page d'accueil provenant du point d'accès (connexion via le réseau Télétel) ou la réception de la page d'accueil du serveur (connexion par le réseau téléphonique commuté).

Une fois cette page reçue, le texte contenu dans le bloc de connexion est émis, cadencé en pseudo 75 bauds (émission à 1200 bauds vers le Minitel cadencée pour tenir compte de la vitesse de réémission).

Chaque touche de fonction rencontrée dans le texte à émettre (SEP, x/y) provoque l'attente par le lecteur d'une réponse du point d'accès ou du serveur.

La réception de la réponse est terminée lorsqu'un délai maximal s'est ecoulé après le dernier caractère reçu par le LECAM. Cette fin provoque la reprise de l'émission par le lecteur.

Mode explicite
Ce mode permet de décrire plus précisément le comportement que doit avoir le lecteur de façon à pouvoir s'adapter à tout cas particulier.

Dans ce mode, les informations décrivant le texte à émettre sont de deux natures :

- le texte proprement dit, toujours émis en pseudo 75 bauds,
- des séparateurs indiquant à partir de quand le lecteur doit se placer en attente d'une réponse de la part du serveur (ou du point d'accès). Ces séparateurs indiquent combien de caractères peuvent être éventuellement reçus en écho du dernier caractère émis, afin de ne pas confondre ces échos avec la réponse du serveur.

Le texte débute toujours par un séparateur indiquant si le texte doit être émis dès la réception de la porteuse, ou après réception d'une page d'accueil.

Remarques :

1 - Dans tous les cas, un délai maximum de surveillance est contrôlé lorsque le lecteur se place en attente de réception du premier caractère de la réponse provenant de la ligne. Ce délai écoulé, la phase de connexion automatique est abandonnée.

2 - Une fois la connexion automatique terminée, le lecteur passe en mode repos. Le réseau Minitel est libéré et le Minitel transmet donc le code SEP, 5/4. Les serveurs doivent prendre toutes les précautions nécessaires pour ne pas être perturbés par cette séquence.

3 - Il est important de noter que le lecteur ne contrôle pas le texte reçu du serveur. Il n'est donc pas conseillé de prévoir des connexions automatiques comportant un trop grand nombre d'échanges, le lecteur ne pouvant s'adapter à des variations éventuelles du dialogue, ou à des demandes de répétition du serveur.

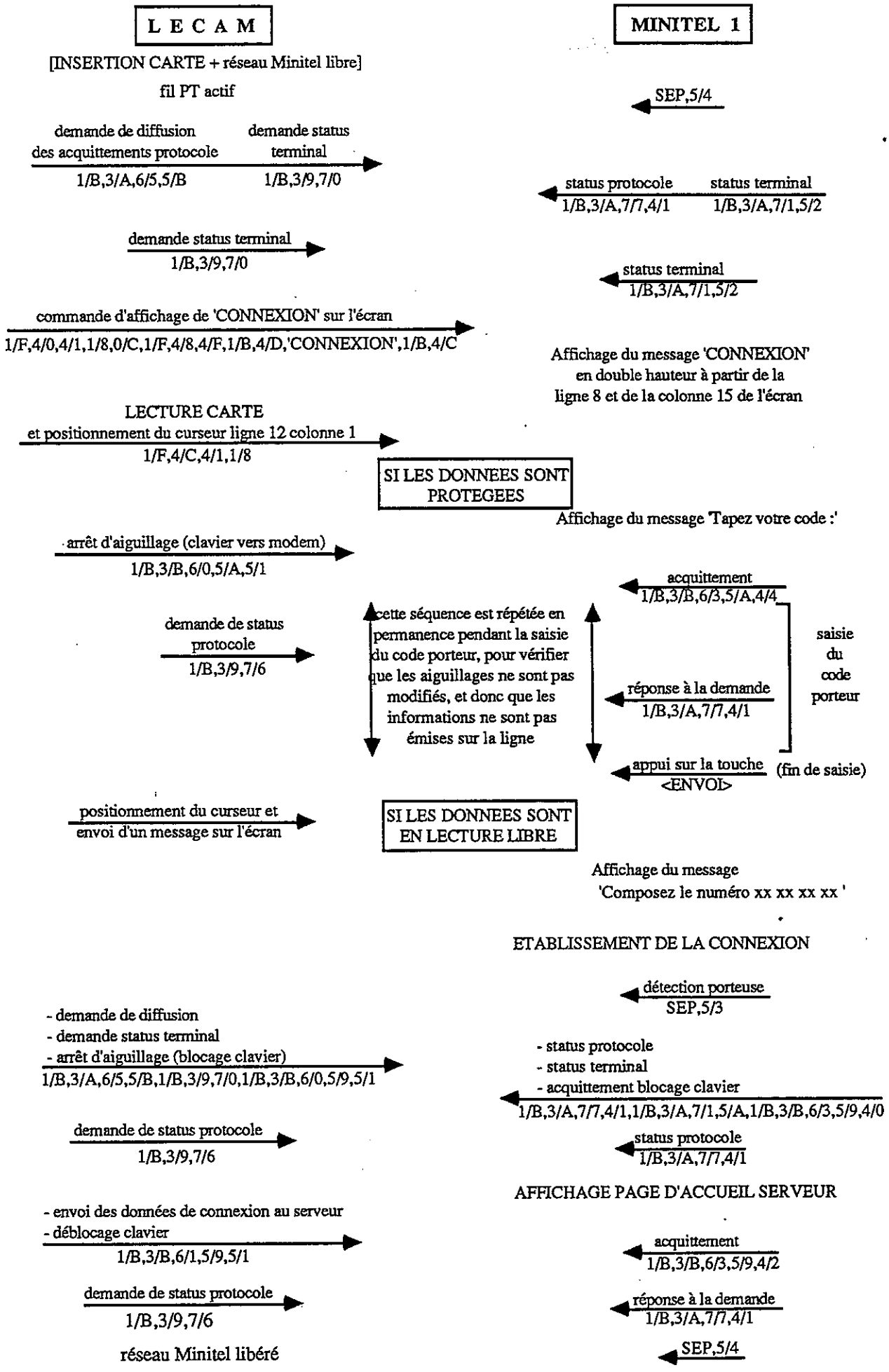
2. 4 - Diagrammes récapitulatifs des échanges réalisés entre un LECAM et un Minitel

Les deux diagrammes suivants présentent les échanges effectivement réalisés entre un LECAM et un Minitel 1 d'une part, et entre un LECAM et un Minitel 10 d'autre part.

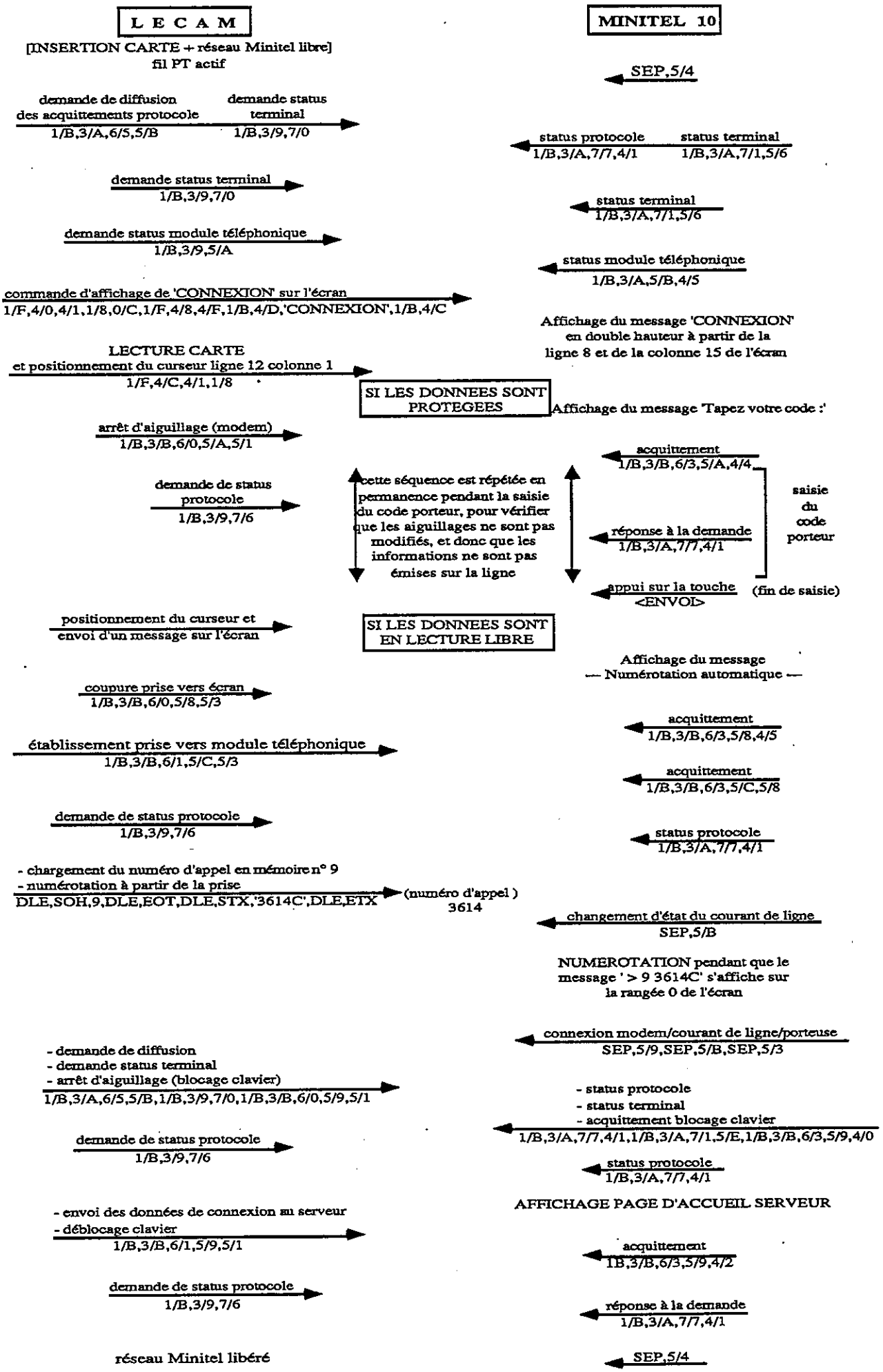
Les cartes utilisées pour la réalisation de ces diagrammes contiennent un bloc de connexion automatique comportant un numéro téléphonique et des données de connexion à un serveur.

Les séquences de contrôle correspondant aux différents messages du protocole sont notées en hexadécimal.

CONNEXION AUTOMATIQUE AVEC UN MINITEL 1



CONNEXION AUTOMATIQUE AVEC UN MINITEL 10



3 . DESCRIPTION DES BLOCS DE CONNEXION AUTOMATIQUE

3. 1 - En-tête du bloc

Le bloc de connexion automatique est caractérisé par un en-tête au profil particulier qui varie selon le type de carte utilisé.Sa longueur totale est limitée à 255 octets.
Pour les cartes de type M4, M6, B0 ou B1, l'en-tête correspond à un en-tête de bloc prestataire écrit sous clé émetteur ou sous clé d'ouverture.

Le numéro de prestataire utilisé est le numéro 35 (23 en notation hexadécimale).

Par analogie, les cartes de type PC1 ont un en-tête dont la valeur est (en notation hexadécimale) :

40 23 00 00

a - Cas des cartes M4, M6 et B0

Le bloc de connexion automatique peut être inscrit soit en zone de lecture libre, soit en zone de transaction. Si cette dernière est en lecture protégée (choix effectué lors de la personnalisation de la carte), le LECAM fait saisir le code porteur de l'usager avant de poursuivre la procédure de connexion.

L'en-tête du bloc de connexion automatique est recherché de la manière suivante :

- lecture dans la carte du mot d'adresse 09C8, qui contient les adresses de début de la zone de lecture libre et de la zone de transaction (ADL, ADT),

- lecture de la zone de lecture libre, pour rechercher l'en-tête caractéristique dont les quatre premiers quartets sont de la forme :

00x0	xxxx	0010	0011	(notation binaire)
		2	3	(notation hexadécimale)

l'ordre utilisé pour la lecture est donc :

(M4/B0) BC
(M6) CC
B0 A_1 A_2 04 | 4 octets recherchés | (notation hexadécimale)

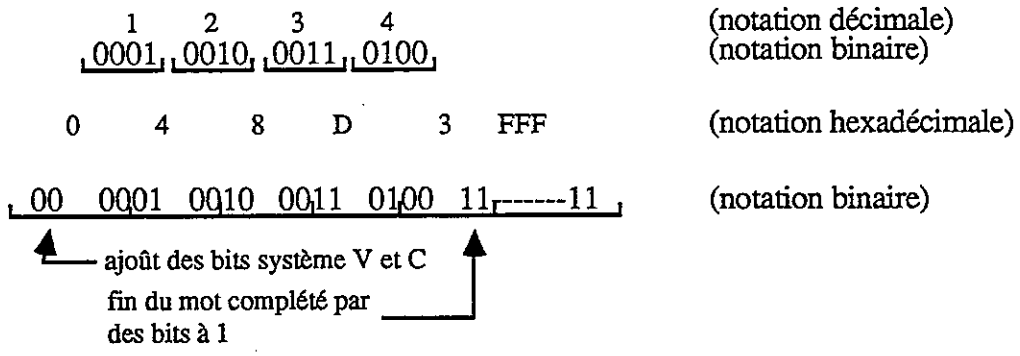
Si cet en-tête est trouvé, le premier quartet des mots constituant le contenu du bloc de connexion automatique est de la forme :

0xx1	(notation binaire)

Le contenu du bloc de connexion automatique est intégralement lu, jusqu'à ce que le lecteur rencontre un mot dont le premier quartet est différent de celui cité précédemment ou jusqu'à rencontrer la fin du bloc.

La recherche du bloc en zone de lecture libre se fait de l'adresse ADL jusqu'à la fin de la zone.

Si l'en-tête n'est pas trouvé en zone de lecture libre, le lecteur relit le mot de RAZ (octets envoyés au lecteur par la carte à l'introduction de celle-ci). Si le verrou LP (protection lecture) est positionné, le LECAM fait procéder à la saisie du code porteur. Le code saisi est transformé en binaire au format interne de la carte pour permettre la comparaison avec le code inscrit dans la zone secrète de la carte. Par exemple, si le code saisi est "1234", le LECAM le transforme de la façon suivante :



ce qui donne donc le code : 04 8D 3F FF et lui permet donc d'enchaîner l'ordre de présentation de clé de la forme :

(M4/B0) BC
M6 CC] 20 00 00 04 04 8D 3F FF (notation hexadécimale)

le lecteur enchaîne l'ordre de validation de lecture de la forme :

(M4/B0) BC
(M6) CC] 40 00 00 00 (notation hexadécimale)

La carte renvoie alors les mots d'état ME1 et ME2 qui permettent au LECAM de savoir si la clé présentée est valide ou non.

Le résultat obtenu conditionne donc la suite des opérations nécessaires à la fonction de connexion automatique.

Si le code présenté est correct le lecteur recherche alors l'en-tête et le contenu du bloc de connexion automatique par lecture de la zone de transaction. La lecture commence à l'adresse la plus basse (ADT) et se termine à l'adresse la plus haute (ADL). Les quatre premiers quartets de l'en-tête recherché sont de la forme :

01x0 xxxx 0010 0011 (notation binaire)
2 3 (notation hexadécimale)

l'ordre utilisé pour la lecture est donc :

(M4/B0)
(M6)] B0 A_1 A_2 04 4 octets recherchés (notation hexadécimale)

Si la zone de transaction n'est pas protégée en lecture, l'en-tête recherché est le même que celui décrit précédemment.

Que la zone de transaction soit ou non en lecture protégée, le premier quartet des mots constituant le contenu du bloc de connexion automatique est de la forme :

0xx1 (notation binaire)

Exemple d'en-tête au format M4/M6/B0

		2.3			
0yx0	xxxx	0010 0011	LONG	111	CCR

x quelconque

y = 0 données en zone de lecture libre

y = 1 données en zone de transaction

L'ensemble de ces informations est décrit dans le guide d'utilisation des cartes masque 4, édité par BULL CP8 et dans le "Recueil des Normes et Spécifications de la Carte à Mémoire Bancaire" édité par le GIE Cartes Bancaires pour les cartes B0.

Ces brochures peuvent être commandées aux adresses suivantes :

- Guide d'Utilisation de la Carte CP8 Masque 4 :

  BULL CP8
  Service de Documentation
  rue Eugène Hénaff
  78190 - TRAPPES

  Tél. : (16 - 1) 30 69 50 50

- La Carte à Mémoire Bancaire :

  GIE Cartes Bancaires
  62 avenue d'Iéna
  75116 - PARIS

  Tél. : (16 - 1) 47 23 78 18

b - Cas des cartes B1

Les données du bloc de connexion automatique peuvent être protégées ou non par le code porteur selon le choix effectué lors de l'écriture de ce bloc.

Quatre recherches sur argument sont nécessaires pour trouver l'en-tête du bloc prestataire. Les deux premiers octets de l'en-tête peuvent en effet prendre les valeurs hexadécimales suivantes :

25 23	[lecture protégée	mot validé par clé d'ouverture
26 23	[par code porteur]	mot validé par clé banque

2D 23	[lecture libre]	mot validé par clé d'ouverture
2E 23	[	mot validé par clé banque

Ces quatre recherches s'effectuent systématiquement : le bloc pris en compte est celui dont l'adresse est la plus basse.

L'ordre de recherche sur argument donné à la carte par le LECAM est donc de la forme :

CB A0 00 00 02 2x 23 (notation hexadécimale)

(x prend successivement les valeurs 5, 6, D et E)

Cet ordre est suivi par l'ordre de demande de résultat :

CB C0 00 00 08 (notation hexadécimale)

Si la recherche aboutit, et que le premier bit du quartet "type" est égal à zéro (valeurs 25 et 26), le LECAM fait saisir le code porteur à l'usager.
Le résultat de la saisie est comparé aux données inscrites dans la zone secrète de la carte à l'aide de l'ordre :

CB 20 00 00 08 message d'entrée (notation hexadécimale)

Le message d'entrée est le code client présenté par le porteur (CCP) combiné par "OU exclusif" avec le message code client complémentaire (MCCC) pour que le calcul exécuté par la carte donne un résultat cohérent.

Si le code porteur présenté est correct, la lecture du bloc de connexion automatique est exécutée mot par mot par l'ordre de lecture :

CB B0 A1 A2 04 (notation hexadécimale)

Le bloc est considéré comme terminé lors de la rencontre d'un mot dont le premier quartet est différent de "0xx1".

Se référer au "Recueil des Normes et Spécifications de la Carte à Mémoire Bancaire" édité par le GIE Cartes Bancaires et datant de juin 1986 pour plus de détails (et en particulier pour les valeurs de MCCC).

Exemple d'en-tête au format B1

Type 2 . 3

VMSB	C	NP	LONG	IND	CCR
0010	Clxx	00100011		111	

xx = 10 clé banque
= 01 clé d'ouverture

C = 0 données protégées

c - Cas des cartes PC1

Les données de connexion sont toujours en lecture libre, la saisie du code porteur n'est donc jamais activée pour la fonction connexion automatique avec ce type de carte.

L'ordre exécuté par le LECAM pour rechercher un bloc de connexion automatique dans ce type de carte est un ordre de recherche sur argument :

AC A0 00 00 04 40 23 00 00 (notation hexadécimale)

suivi par un ordre de demande de résultat :

AC 20 00 00 08 (notation hexadécimale)

Si la recherche sur argument aboutit, la lecture du bloc de connexion automatique est exécutée mot par mot par l'ordre de lecture :

AC B0 A_1 A_2 04 (notation hexadécimale)

jusqu'à rencontrer la fin du bloc par détection d'un mot de profil différent de "0x1x" dans le premier quartet.

Exemple d'en-tête au format PC1

4	0	2	3	0	0	0	0	(codage hexadécimal)
VSB								
010	0 0000	0010	0011	0000	0000	0000	0000	(codage binaire)

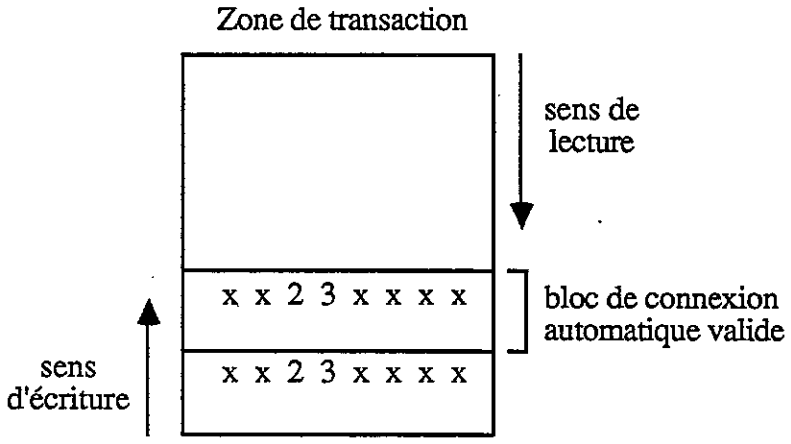
Se référer au guide d'utilisation des cartes PC1 pour plus de détails.

Remarques concernant les trois types de cartes :

1 - Le LECAM lit deux fois le mot correspondant à l'en-tête du bloc de connexion automatique.

2 - Plusieurs blocs de connexion automatique peuvent être inscrits dans les cartes : l'écriture se faisant dans l'ordre décroissant des adresses et la lecture dans le sens contraire, l'information valide est donc celle qui se trouve à l'adresse la plus basse de la mémoire de la carte.

Cette remarque est sans valeur dans le cas où le bloc de connexion automatique est rangé en zone de lecture libre (cartes M4/B0, M6) la recherche dans cette zone étant prioritaire.



3. 2 - Contenu du bloc prestataire

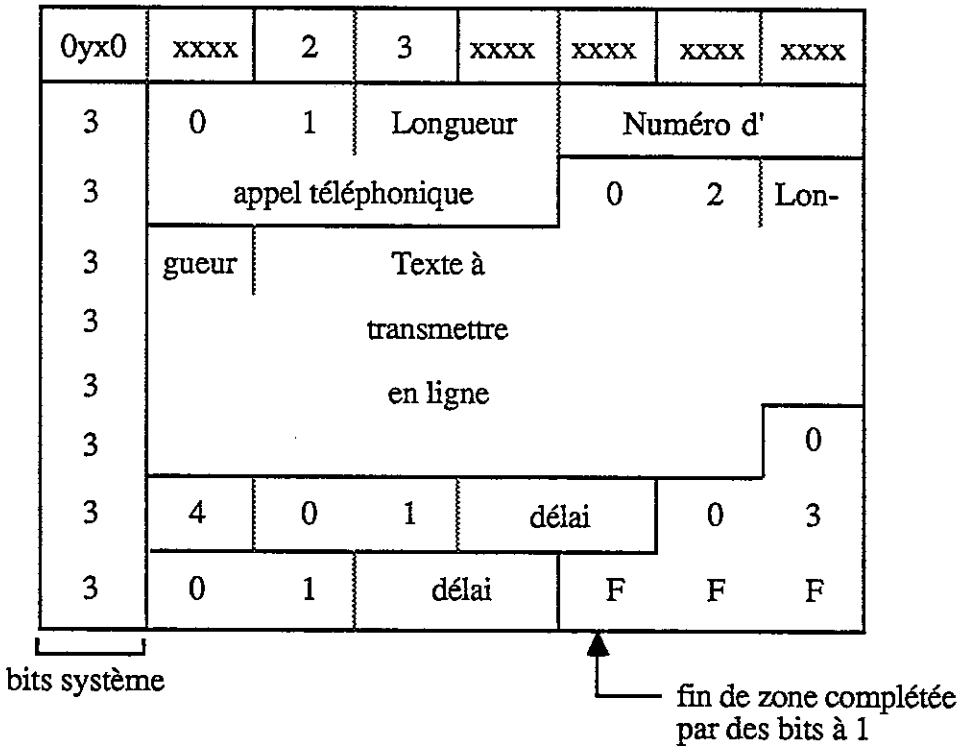
Les informations suivantes peuvent être codées à l'intérieur du bloc de connexion automatique :

- le numéro d'appel téléphonique,
- le texte à transmettre vers le point d'accès ou le serveur,
- le délai de détection de fin de message,
- le délai d'abandon de la phase de connexion.

Ces informations sont codées sur une suite d'octets structurée selon un modèle TLV. Les octets sont rangés à raison de trois octets et demi par mot de 32 bits, chaque mot est complété par un premier quartet correspondant aux bits "système". La longueur L du format TLV indique le nombre d'octets utiles, le premier quartet de chaque mot étant ignoré.

L'ordre des blocs TLV est indifférent. Les TLV sont indépendants et optionnels.

Structure du bloc (exemple avec en-tête M4/B0/M6)



Les valeurs attribuées aux différents types de données sont les suivantes :

NA	(= 01)	numéro d'appel
TX	(= 02)	texte à transmettre
DF	(= 03)	délai de détection de fin de message
DS	(= 04)	délai de suspension

3. 3 - Numéro d'appel

La zone numéro d'appel téléphonique est introduite par le type NA. Les données sont rangées à raison de un caractère du numéro d'appel par quartet, le dernier octet étant éventuellement complété par des bits à 1.

Le numéro d'appel peut contenir les chiffres 0 à 9 et les caractères de contrôle du Minitel 10. Le codage est le suivant :

CARACTERE		VALEUR HEXA	
Chiffres	0 à 9	0 à 9	(DCB)
Parenthèse	(	A	
Parenthèse	)	B	
Lettre	C	C	Connexion automatique du Minitel
	+	D	Numéro international
	-	E	Numéro à utiliser sans préfixe si en début de numéro, ou temporisation sinon

3. 4 - Textes à transmettre

Les textes à transmettre vers le serveur sont contenus dans un seul sous-ensemble TLV introduit par le type TX.

Les textes sont rangés à raison de un caractère ASCII par octet, le bit de parité étant à zéro.

Mode implicite

Les textes peuvent contenir les séquences de deux caractères permettant de simuler les touches ENVOI, SUITE... (codes SEP,4/x).

Ce sont ces séquences qui permettent de séparer les textes à transmettre en plusieurs échanges avec le serveur. La première émission ne débute qu'après réception d'une page d'accueil.

Mode explicite

Le texte à transmettre contient des séparateurs explicites indiquant comment transmettre le texte qui suit. Ces séparateurs sont signalés par leur bit de poids fort positionné à 1 : ils sont de la forme hexadécimale "80" "C0", ou "8x".

Le texte débute obligatoirement par l'un des séparateurs "80" ou C0" indiquant que le lecteur fonctionne en mode explicite (la rencontre éventuelle de séquences SEP,4/x ne placera pas, dans ce mode, le lecteur en attente de réception du serveur).

"80" précise qu'une page d'accueil doit être reçue avant l'émission du texte par le lecteur.

"C0" indique que le lecteur doit débuter l'émission dès la réception de la porteuse.

Un séparateur "8x" doit se trouver dans le texte chaque fois que le lecteur doit attendre une réponse du serveur. La valeur du champ x indique au lecteur combien de caractères il doit ignorer après l'émission du dernier caractère qu'il a transmis (afin de ne pas confondre l'écho de ce caractère avec la réponse du serveur).

Exemple

La séquence implicite suivante :

A, B, C, SEP,4/1, D, E, F, SEP,4/3.

est similaire à la séquence explicite :

"80", A, B, C, SEP,4/1, "80", D, E, F, SEP,4/3.

Le premier séparateur "80" indique qu'une page d'accueil doit être attendue.

Le second indique que le lecteur doit attendre une réponse du serveur. Le paramètre x est à zéro car il ne peut y avoir confusion entre le message du serveur et l'écho des caractères émis, SEP,4/1 n'étant pas échoplexés par le point d'accès.

3. 5 - Délai de détection de fin de message

Ce délai, introduit par le type DF, est codé sur un octet selon le format binaire :

00yy xxxx

les deux bits yy indiquent l'unité de temps de définition du délai,

yy =	00	100 ms
	01	1 s
	10	10 s
	11	100 s

les quatre bits de poids faibles xxxx indiquent la valeur du délai dans l'unité choisie.

Par défaut le délai est de 2 secondes.

Lorsque le lecteur reçoit un message du serveur, une absence de réception de caractères pendant cette durée est interprétée comme une fin de message.

3. 6 - Délai de suspension

Ce délai est introduit par le type DS. Il est codé sur un octet selon le même format que le délai DF.

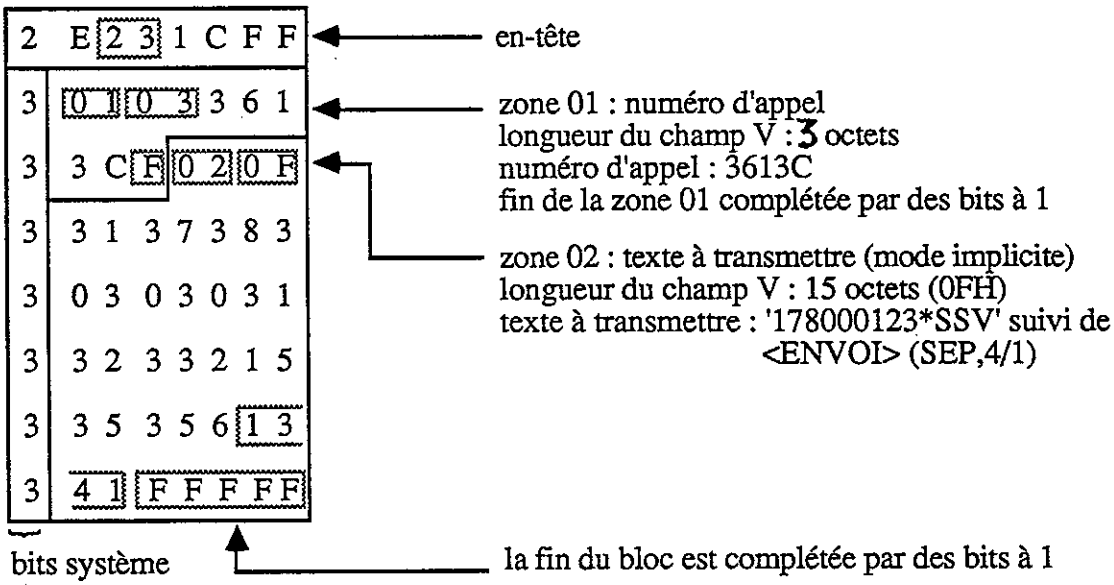
Il permet de mettre fin à la phase de connexion automatique en cas de non-réception du premier caractère d'un message attendu du serveur ou du point d'accès.

La valeur par défaut est de 60 secondes.

3. 7 - Exemples de blocs de connexion automatique

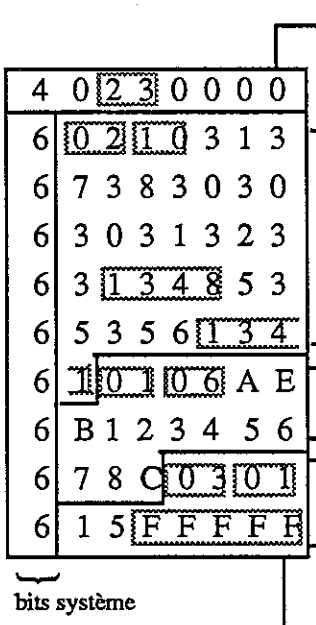
La représentation des données contenues dans la carte pour les trois exemples suivants est en notation hexadécimale.

Carte B1



Le délai de détection de fin de message et le délai de suspension ne sont pas renseignés dans ce bloc. Le LECAM prend donc les valeurs par défaut, qui sont respectivement de 2 et de 60 secondes.

Carte PC1



en-tête

zone 02 : texte à transmettre (mode implicite)
longueur du champ V : 16 octets (10 H)
texte à transmettre : '178000123' suivi de <SUITE> (SEP,4/8)
qui provoque une temporisation de
5 secondes après lesquelles 'SSV' suivi de
<ENVOI> (SEP,4/1) sont transmis au
serveur.

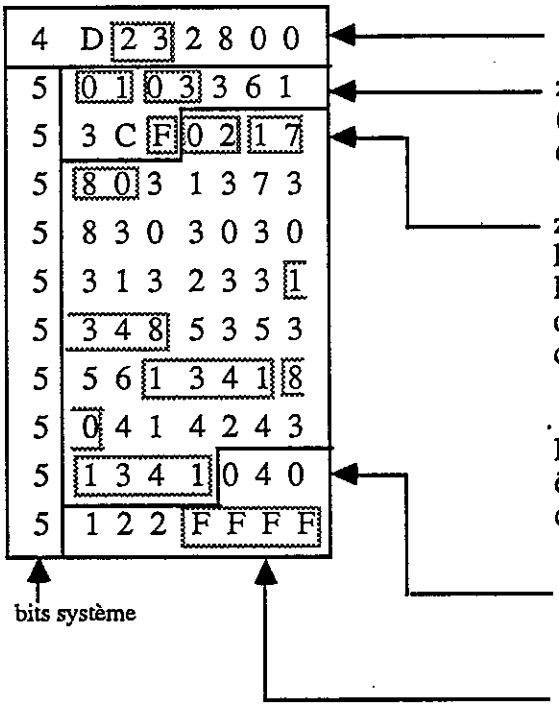
zone 01 : numéro d'appel
longueur du champ V : 6 octets
numéro d'appel : (-) 12 34 56 78C

zone 03 : délai de détection de fin de message
longueur du champ V : 1 octet
délai de détection de fin de message :
. unité de temps : 1 seconde
. délai dans l'unité choisie : 5 secondes
le délai de détection de fin de message est donc de 5 secondes

la fin du bloc est complétée par des bits à 1

Le délai de suspension n'apparaît pas dans ce bloc : c'est donc la valeur par défaut, c'est-à-dire 60 secondes, qui est retenue par le LECAM.

Carte M4 / B0 /M6



en-tête

zone 01 : numéro d'appel
(le contenu de cette zone est identique à celui décrit dans l'exemple utilisé pour une carte B1).

zone 02 : texte à transmettre (mode explicite)
longueur du champ V : 23 octets (17 H)
l'octet '80' définit le mode explicite en indiquant qu'une page d'accueil doit être reçue avant d'émettre le texte :
'178000123' suivi de <SUITE> (SEP,4/8)
puis de 'SSV' et de <ENVOI> (SEP,4/1)
l'octet suivant (80) indique qu'une réponse doit être attendue avant d'envoyer le reste du texte, c'est-à-dire 'ABC' suivi de <ENVOI> (SEP,4/1).

zone 04 : délai de suspension
ce délai est de 20 secondes (10s x 2).

fin de bloc complétée par des bits à 1

Le délai de détection de fin de message n'apparaît pas dans ce bloc : c'est donc la valeur par défaut, c'est-à-dire 2 secondes, qui est retenue par le LECAM.

CHAPITRE 7 - LE MODULE TELECOMMUNICATIONS

1 . GESTION DES PRISES PERI-INFORMATIQUES

1. 1 - Généralités

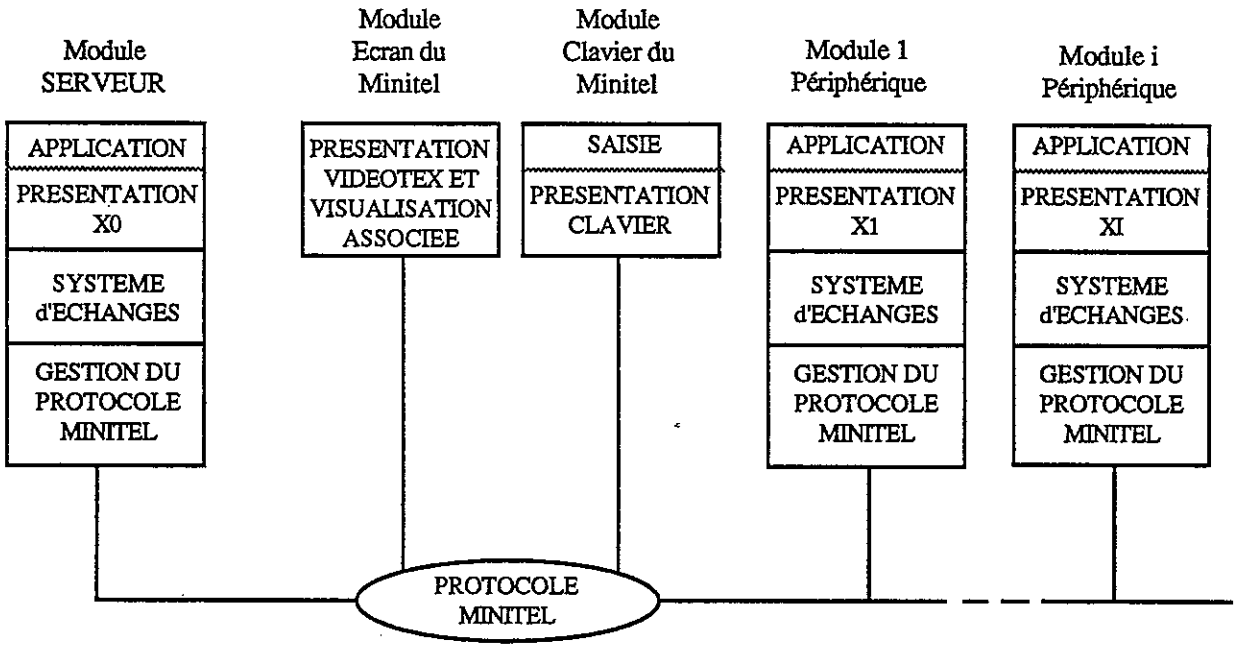
Le serveur, le Minitel et le LECAM sont des éléments hétérogènes qu'il faut relier entre eux pour réaliser une application destinée à effectuer des opérations sur la carte à mémoire d'un usager.

Le Minitel est connecté au serveur par son modem, et au LECAM par sa prise. Le protocole du Minitel, tel qu'il est défini dans le document "Minitel 1 : Spécifications Techniques d'Utilisation" assure essentiellement les aiguillages entre la prise et les autres modules du Minitel (modem, clavier, écran).

Une gestion plus globale incluant les divers périphériques, dont fait partie le LECAM, doit donc s'effectuer à l'extérieur du terminal Minitel : le "Système d'Echanges", décrit dans le document "Spécifications Techniques d'Utilisation du Réseau Minitel" (STURM), permet la mise en relation de ces différents modules dans le cadre d'une même application.

Pour pouvoir gérer correctement les échanges, chaque module doit posséder un niveau de gestion du Protocole Minitel ainsi qu'un niveau de gestion du Système d'Echanges, selon le modèle suivant :

Architecture générale du réseau MINITEL



1. 2 - Fonctionnement sous Système d'Echanges

1. 2. 1 - Ouverture de session

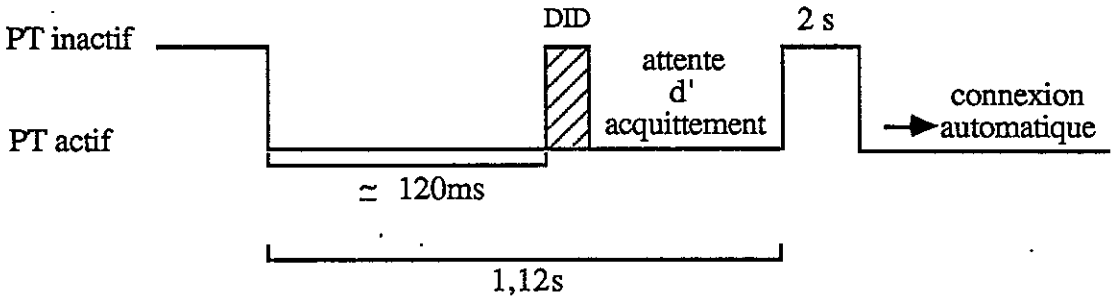
Lors de la mise sous tension du lecteur, dès que le réseau Minitel est libre, le LECAM effectue une demande d'identification (DID).

1. 2. 1. 1 - Demande d'identification

A la mise sous tension le LECAM scrute l'état du fil PT. Si PT est actif (état logique 0), il attend que le canal de transmission se libère (PT inactif, état logique 1) et laisse le relais permettant d'établir la continuité électrique entre les prises péri-informatiques gauche et droite du LECAM en position repos, afin de ne pas perturber la ligne.

Le voyant vert "SECRET" reste allumé pendant les tests de vérification des composants internes du lecteur, mais aussi tant que le relais n'est pas en position travail : le lecteur n'est donc pas forcément en panne si ce voyant reste allumé pendant un délai assez long, car cela peut signifier une activité sur le réseau Minitel.

Si le signal PT est inactif, le LECAM envoie une demande d'identification (DID) sur ses deux prises :



Le fil PT passe à l'état actif pendant environ 1,12s, la DID étant émise au bout d'environ 120ms. Le lecteur attend alors un acquittement. Si, au bout d'une seconde, le lecteur n'a reçu aucun acquittement sur l'une ou l'autre des prises, il passe en état "bout de chaîne" sur la ou l les prises muettes.

Si la présence d'un autre LECAM est détectée, le LECAM émetteur de la DID libère le réseau Minitel. En effet, deux LECAM ne peuvent pas être branchés simultanément sur le même réseau Minitel. Le voyant vert reste allumé pour signaler que le lecteur ne peut fonctionner dans cet environnement.

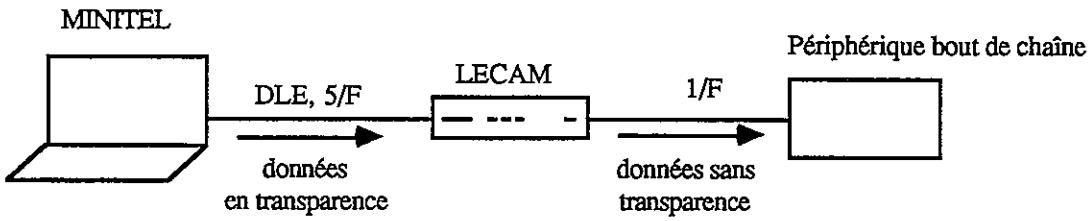
Si la séquence SEP,5/4 est reçue sur l'une des prises, cela signifie qu'un Minitel est présent. Si, en plus, une carte est présente dans le LECAM, celui-ci enchaîne la procédure de connexion automatique. La séquence SEP,5/4 est envoyée par le protocole du Minitel à la fois sur le modem et sur la prise si le Minitel est connecté : le serveur doit donc prendre les précautions nécessaires pour que cette séquence ne le perturbe pas.

A la fin de cette période d'initialisation ou de la phase de connexion automatique si elle a lieu, le fil PT est desactivé par le LECAM qui passe alors en mode repos.

Le LECAM et le bout de chaîne

Un LECAM initialisé avec une prise en état "bout de chaîne" prend à sa charge la gestion du Système d'Echanges pour la prise correspondante.
Il doit donc gérer les commandes Demande de Connexion (DC) et Indication de Libération de Connexion (ILC) pour l'adresse 2/D ainsi que les changements d'état du fil PT.

Dans le cas où la transparence Système d'Echanges est activée, le LECAM ne transmet au périphérique bout de chaîne que les données sans transparence. Par exemple, si le LECAM reçoit la séquence DLE, 5/F il retransmet le caractère 1/F au bout de chaîne :



Le LECAM filtre les données entre <d> et <f> quand il gère un bout de chaîne.

Pour casser un état bout de chaîne, il suffit d'envoyer depuis la ou les prises initialisées dans ce mode, une commande du Système d'Echanges.

1. 2. 1. 2 - Disponibilité du réseau Minitel

Un périphérique ou un serveur désirant utiliser le LECAM et qui n'est pas déjà maître au sens Système d'Echanges doit auparavant s'assurer de la disponibilité du réseau Minitel.

Celui-ci est dit disponible ou libre si le fil PT est à l'état inactif. Si tel n'est pas le cas, le périphérique ou le serveur doit envoyer une demande de libération de connexion (DLC) et attendre la libération du réseau, détectable par le passage du fil PT à l'état inactif associé à la réception de la séquence SEP,5/4 provenant du Minitel.

Cette libération doit intervenir dans un délai maximal de 2 s après l'envoi de la DLC.

Si tel n'est pas le cas, une commande de déconnexion générale (CDG) pourra être envoyée pour essayer à nouveau de libérer le réseau ; si cette libération n'intervient pas dans un nouveau délai de 2 s, il y a incident réseau et l'ouverture de session avec le LECAM est impossible.

1. 2. 1. 3 - Demande de connexion (DC)

L'ouverture de session entre une application et le lecteur est toujours initialisée par l'application. Elle ne peut se faire que si le réseau Minitel est disponible. Elle débute par l'envoi d'une demande de connexion logique (DC) de syntaxe :

ESC, P, 3/8 où P est une liste d'octets de la forme 2/x, représentant la liste des modules à connecter, et comportant donc l'adresse lecteur, soit 2/3.

Si P contient plusieurs fois la valeur 2/3, le lecteur considère l'ordre valide mais ne renvoie qu'un seul acquittement.

Le LECAM ne gère pas le sous-adressage. Ceci implique que deux LECAM ne peuvent pas être branchés sur le même réseau Minitel (le second LECAM allumé refusant de se connecter lorsqu'il réalise sa DID, sur détection de l'acquittement du premier LECAM). Le voyant vert du second LECAM reste donc allumé pour signaler une impossibilité logique de fonctionnement.

Sur réception d'une demande de connexion avec 2/3 dans le champ adresse, le LECAM vérifie que l'aiguillage prise vers modem est actif après avoir activé le fil PT.

L'acquittement à la demande de connexion est de la forme :

ESC, 2/3, 3/9, CR

Dès lors, la session est établie. Après la première demande de connexion suivant la mise sous tension du LECAM, la première commande à adresser au lecteur doit obligatoirement être une consigne de mise en mode, dont le rôle est d'indiquer au LECAM son mode de fonctionnement.

Remarque :
La séquence Demande de Connexion peut être transmise par un serveur distant ou par un module de la chaîne péri-informatique, sans que le lecteur puisse en déceler l'origine.
Le premier acquittement suivant la mise sous tension est donc transmis sur le réseau Minitel sans modification des aiguillages du Minitel. Un serveur désirant recevoir un acquittement doit donc s'assurer, au préalable, de la position des aiguillages du Minitel.

Pour les DC suivantes, il y a activation systématique par le LECAM de l'aiguillage prise vers modem si la consigne de mise en mode a demandé la gestion du Minitel (paramètre 'd' égal à 1 dans cette consigne).

1. 2. 2 - LECAM esclave inactif

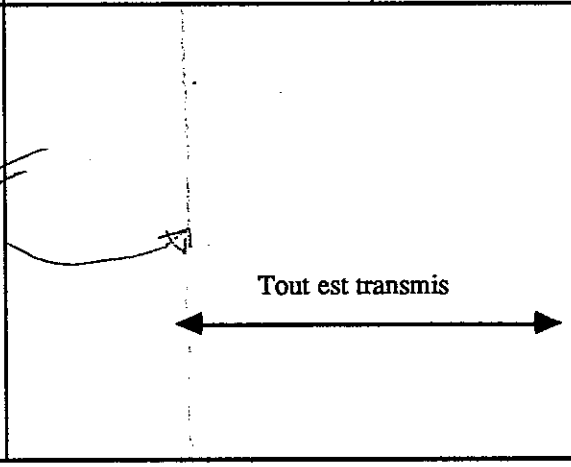
Le LECAM passe à l'état esclave inactif s'il reçoit une demande de connexion ne le concernant pas alors qu'il a reçu une demande de connexion préalable l'ayant fait passer en mode esclave actif.

Lors du passage du mode esclave actif vers le mode esclave inactif, le LECAM repositionne les aiguillages du Minitel en mode standard et réinitialise son état applicatif.

Il garde cependant en mémoire l'information "gestionnaire de Minitel" qui est décrite dans la consigne de mise en mode (bit 'd' de CM ; se référer au chapitre 8. 1. 2. 1).

1. 2. 3 - Transfert de données assuré par le LECAM

Les informations transmises vers la deuxième prise péri-informatique sont données par le tableau suivant :

<table>
<tr><td>Demande de connexion</td><td>ESC,2/3,xx,2/D,3/8</td><td>ESC,2/3,xx,3/8</td><td>ESC,xx,3/8</td><td>ESC,xx,2/D,3/8</td></tr>
<tr><td>Mode du lecteur</td><td colspan="2">Esclave actif</td><td colspan="2">Esclave inactif</td></tr>
<tr><td>Mot du bout de chaîne</td><td>Actif</td><td colspan="2">Inactif</td><td>Actif</td></tr>
<tr><td>Le lecteur est situé en bout de chaîne</td><td>Le lecteur filtre :
- <dc><fc><r>
- <d>...<f> CR
- les séquences protocole et les séquences S.E., ainsi que l'écho des données émises par le lecteur.
Le lecteur transmet tout le reste, les informations entre <dc> et <fc> étant déchiffrées si une carte est présente.</td><td colspan="2">Rien n'est transmis</td><td>Le lecteur filtre les séquences S.E., le reste est transmis sans changement.</td></tr>
<tr><td>Le lecteur n'est pas situé en bout de chaîne.</td><td>Le lecteur filtre seulement <dc>, <fc> et l'écho de <r>.
Le reste est transmis (y compris les séquences protocole et S.E. et les messages <d>...<f>CR), les informations entre <dc> et <fc> sont déchiffrées si une carte est présente.</td><td colspan="3">  </td></tr>
</table>

S. E. = Système d'Echanges
xx = liste d'adresses, éventuellement vide, autres que 2/3 ou 2/D

<d> <f> <dc> <fc> <r> : se reporter au paragraphe 3. 3. 2 et suivants.

1. 2. 4 - Fin de session

Les commandes du Système d'Echanges provoquant une fin de session sont :

pour un esclave :
- . ILC : Indication de Libération de Connexion
- . CDG : Commande de Déconnexion Générale

pour un maître :
- . DLC : Demande de Libération de Connexion
- . CDG : Commande de Déconnexion Générale

1. 2. 2. 1 - Indication de Libération de Connexion (ILC)

Sur réception d'une indication de libération de connexion avec le code adresse 2/3, le LECAM libère le réseau Minitel après avoir replacé les aiguillages du Minitel et le retournement du modem du Minitel en mode standard.

1. 2. 2. 2 - Commande de Déconnexion Générale (CDG)

Lorsque le LECAM reçoit cette commande, il libère le réseau Minitel après avoir replacé les aiguillages et le retournement du Minitel en mode standard.

Le LECAM est capable de générer cette commande si les événements suivants se produisent :

- . trois demandes de reprise infructueuses en cas d'erreur de transmission ,
- . modification depuis l'extérieur du contexte d'aiguillages pendant une saisie ou un affichage chiffré ou pendant une saisie en zone locale,
- . réception d'une DID ou d'une DC alors que le LECAM est en phase d'initialisation décrite au paragraphe 1. 2. 1. 1. ou en phase de connexion automatique.

Dans ce cas, il place la valeur 2/F dans le champ adresse pour signaler une erreur à l'application.

L'appui sur <TS> (touche spéciale) et <CONNEXION/FIN> de façon simultanée génère la séquence SEP,4/9 et est émise sur la prise péri-informatique. Cette séquence est interprétée comme une Commande de Déconnexion Générale et provoque donc la fin de session. La spécification Système d'Echanges voudrait que l'on appuie deux fois consécutives sur les touches mentionnées précédemment : il s'avère qu'un seul appui sur ces deux touches est interprété par le LECAM comme une Commande de Déconnexion Générale.

Si le LECAM reçoit la séquence SEP,5/3 alors qu'il est en session, cette séquence est équivalente à une Commande de Déconnexion Générale.

1. 2. 5 - Réactions du lecteur aux services complémentaires du Système d'Echanges

1. 2. 3. 1 - Demande de Modification des Caractéristiques de Transmission (DMCT)

Le LECAM libère le réseau Minitel et place le relais assurant la continuité électrique entre ses prises gauche et droite au repos après un délai de 50 ms, sur réception d'une DMCT.

Il attend que le signal PT soit dans l'état inactif pour remettre ce relais en activité.

1. 2. 3. 2 - Commandes de début et de fin de transparence

Tous les caractères transmis après une commande de début de transparence sont susceptibles d'être transcodés.

Les caractères des colonnes 0 et 1 des spécifications Vidéotex sont transcodés de la façon suivante : le bit 7 du caractère à émettre est forcé à 1 binaire ; un caractère DLE est placé devant le caractère ainsi modifié. Par exemple, si l'on veut transmettre le caractère US (1/F), il est transformé en : DLE, 5/F avant transmission.

Les caractères des colonnes 2 à 7 sont transmis sans modification.

Un LECAM n'est jamais initiateur d'une demande de transparence, par contre il est capable de la traiter.

1. 2. 3. 3 - Jeton

Le LECAM ignore la commande d'envoi de jeton qui lui serait destinée et n'est jamais initiateur d'une demande de jeton.

1. 2. 3. 4 - Demande de Libération de Connexion (DLC)

Le LECAM ignore toute demande de libération de connexion.

1. 2. 6 - Les états Système d'Echanges du LECAM

Lorsqu'il réalise une connexion automatique, le LECAM est maître, au sens Système d'Echanges. Le lecteur passe à l'état repos s'il reçoit une commande Système d'Echanges au cours de l'exécution d'une connexion automatique.

Pendant une session avec un serveur, le LECAM est toujours en mode esclave.

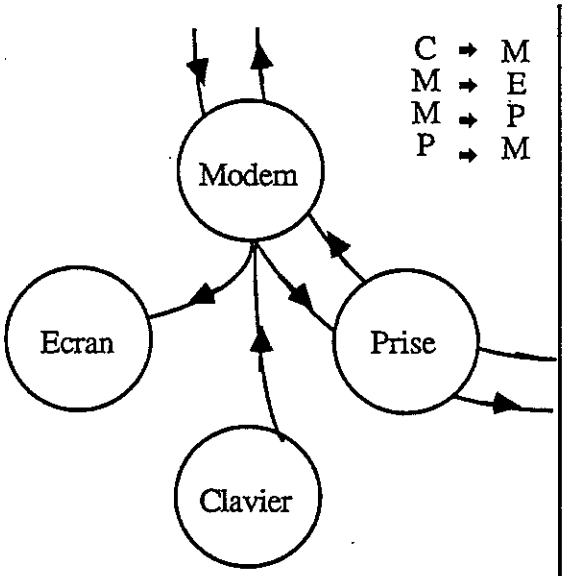
2 . GESTION DU MINITEL ET DE SES AIGUILLAGES

Le déroulement d'une application LECAM est constitué de différentes phases de dialogues faisant intervenir un serveur, un Minitel, un LECAM et bien entendu un usager.

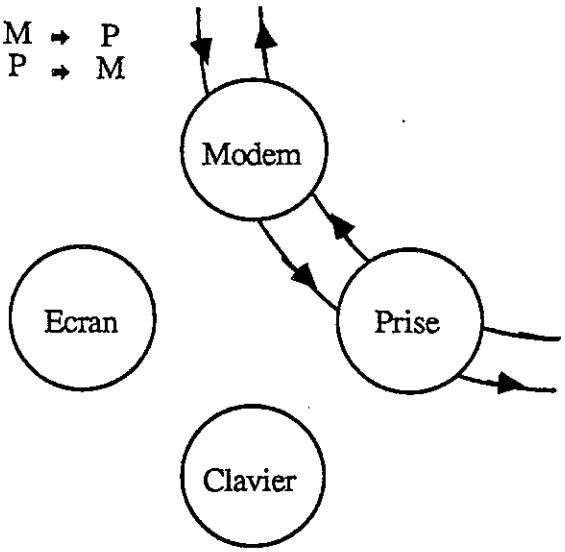
La mise en relation de ces quatre éléments est rarement à réaliser simultanément : certaines fonctions de l'application nécessitent en effet un dialogue local entre l'usager et le LECAM au travers d'un Minitel, d'autres nécessitent un dialogue entre le serveur et le LECAM sans faire intervenir l'usager, d'autres enfin nécessitent un dialogue entre le serveur et l'usager sans intervention "active" de la part du LECAM.

Le Minitel dispose d'aiguillages inter-modules qui permettent, selon les choix effectués, de ne faire intervenir que les "interlocuteurs" nécessaires à la réalisation d'une fonction commandée par l'application à un instant donné.

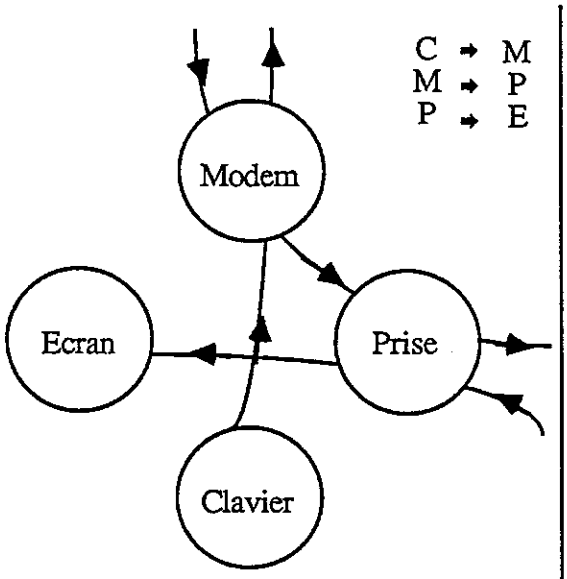
Les aiguillages réalisés sont les suivants :



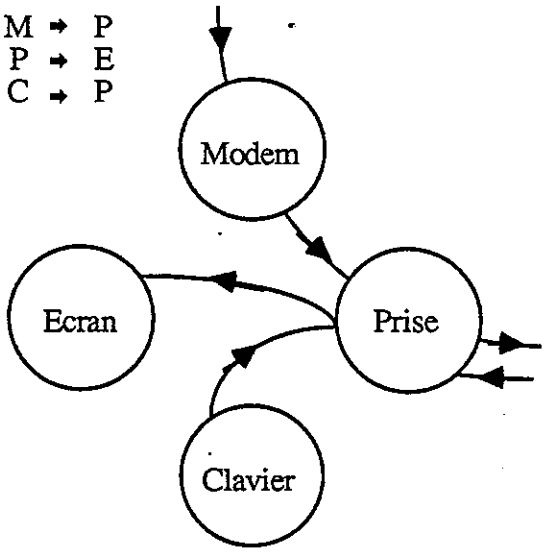
Mode standard Minitel connecté
(Dialogue standard Serveur/Minitel)



Mode lecteur dialogue distant
(Dialogue Serveur/LECAM)

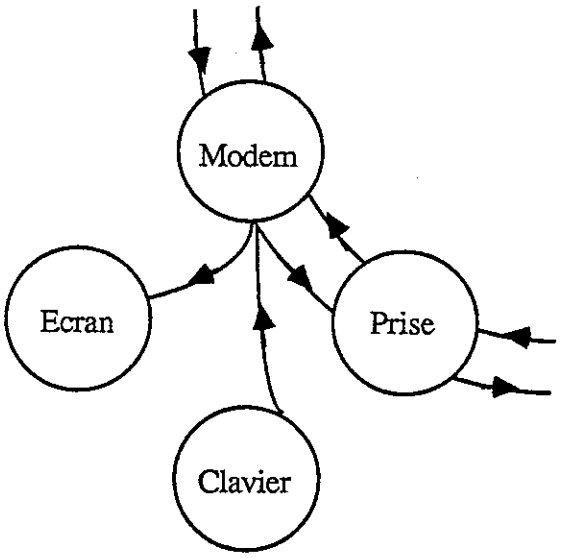


Mode lecteur transparent
(Dialogue Serveur/Minitel en session)



Mode lecteur dialogue local
(Dialogue LECAM/usager)

2. 1 - Aiguillages pour le mode standard, Minitel connecté



Un Minitel connecté à un serveur réalise en standard les aiguillages suivants :

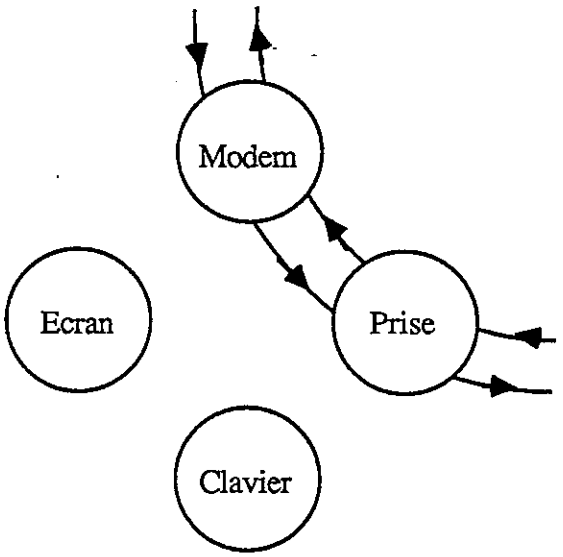
- Clavier vers Modem
- Modem vers Ecran
- Modem vers Prise
- Prise vers Modem

Les données Vidéotex reçues par le modem sont transmises simultanément à l'écran et à la prise péri-informatique.

Le lecteur repositionne les aiguillages du Minitel dans ce mode sur fin de session.
Cette opération nécessitant un certain temps (jusqu'à 500 ms),il est déconseillé à un serveur de tenter l'ouverture d'une session avec un périphérique pendant ce délai.

Le LECAM ne vérifie pas l'état du retournement du modem du Minitel sur fin de session.

2. 2 - Aiguillages pour le mode lecteur en dialogue distant

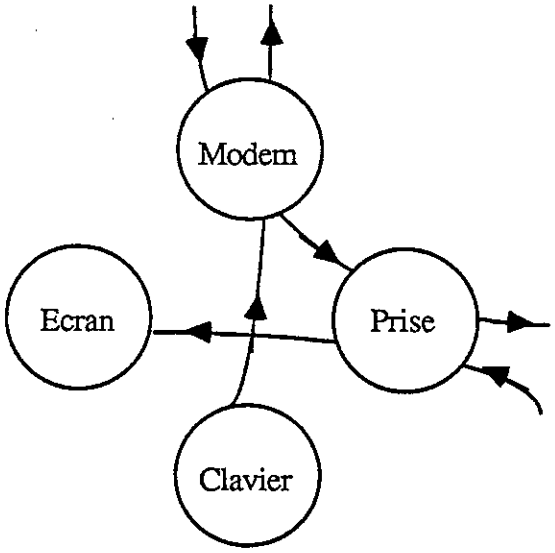


Dans ce mode, seuls les modules modem et prise sont actifs : le dialogue est établi entre le serveur et le LECAM sous le contrôle permanent du Système d'Echanges.

Le LECAM positionne les aiguillages de cette façon chaque fois qu'il dialogue directement avec le serveur, c'est-à-dire lorsqu'il doit émettre un compte-rendu d'exécution ou une demande de répétition <r> d'un message mal reçu.

Les modules clavier et écran sont inhibés, respectivement pour éviter que le serveur soit perturbé par le multiplexage de données provenant à la fois du LECAM et du clavier et pour éviter que l'usager soit perturbé par des caractères abscons s'affichant sur l'écran.

2. 3 - Aiguillages pour le mode lecteur transparent



Les aiguillages du Minitel sont ainsi positionnés à la suite d'une consigne de mise en mode (avec d = 1) entre une application et un LECAM : les données Vidéotex reçues par le modem sont envoyées vers le LECAM au travers de la prise et retransmises sans altération par le lecteur à destination du module écran.

Le lecteur surveille les caractères échangés sur la ligne afin de reconnaître une commande éventuelle pouvant lui être destinée.

Les consignes de mise en mode doivent être protégées par le serveur car le LECAM n'est pas encore gestionnaire du Minitel. Il est conseillé d'utiliser la séquence de transparence écran Vidéotex 1/B,2/5,3/F et la séquence de fin de transparence 1/B,2/F,3/F pour encadrer la consigne de mise en mode.

Fonctionnement en mode transparent

Après avoir envoyé la réponse à la première commande reçue, le lecteur se place en mode "lecteur transparent".

A partir de cet instant, les aiguillages du Minitel sont gérés par le LECAM et le serveur peut dialoguer avec l'usager du Minitel de façon totalement transparente : le format des messages envoyés par le serveur à destination du module écran du Minitel est le même, quels que soient les aiguillages réalisés (mode standard Minitel connecté ou mode transparent).

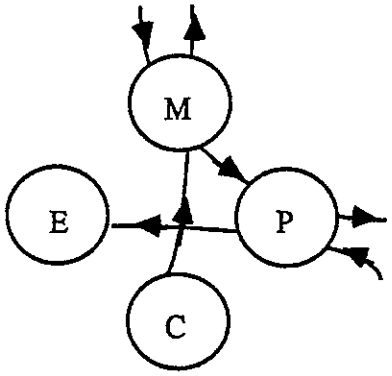
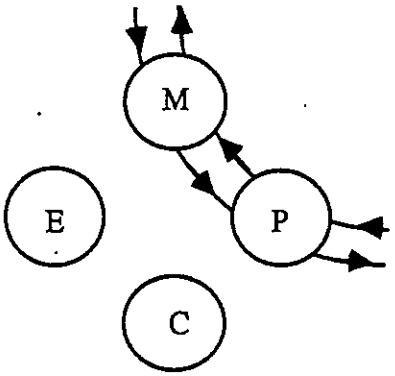
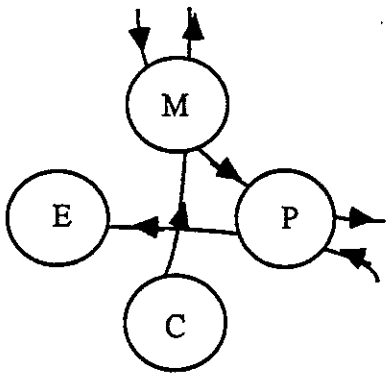
Les caractères frappés sur le clavier sont directement transmis vers le modem ; les caractères reçus par le modem sont acheminés, via la prise péri-informatique, vers le LECAM qui les renvoie sans modification sur l'écran.

Ces caractères sont filtrés par le LECAM s'il s'agit de demandes qui lui sont destinées et auxquelles il doit répondre : lorsque le serveur désire effectuer une transaction avec le lecteur, il place sa commande entre des drapeaux de début <d> et de fin <f> de message ; le LECAM peut donc intercepter la commande et la traiter.

Lorsque la réponse est prête, le lecteur place les aiguillages du Minitel en mode distant, émet la réponse, et repositionne les aiguillages en mode lecteur transparent.

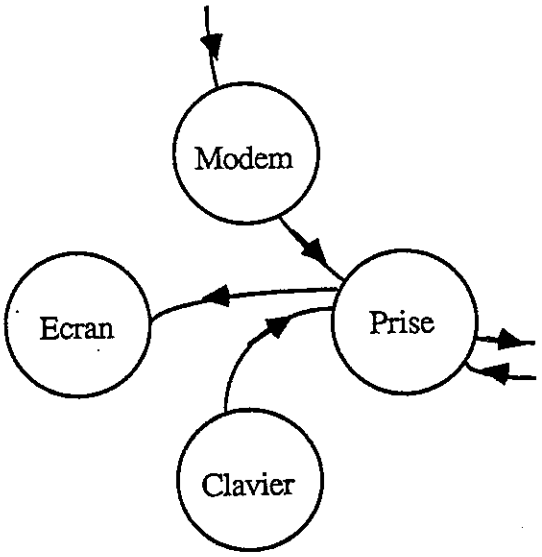
La forme générale d'une transaction serveur/LECAM est résumée par le schéma suivant :

DEROULEMENT GENERAL D'UNE TRANSACTION SERVEUR/LECAM

SERVEUR	LECAM	Aiguillages du MINITEL
envoi d'une transaction <d> commandes <f> CR →		 Mode lecteur transparent
	exécution des commandes, avec demande de modification éventuelle des aiguillages du Minitel	dépendent des fonctions réalisées par l'application
	envoi de la réponse, après demande de modification des aiguillages ← <d> réponse <f> CR	 Mode distant
	demande de modification des aiguillages du Minitel	 Mode lecteur transparent

Toutes les transactions entre le serveur et le lecteur se font sous la forme de question(s)/réponse(s), la question étant toujours à l'initiative du serveur.

2. 4 - Aiguillages pour le mode lecteur en dialogue local



Dans ce mode, les liaisons vers le modem sont supprimées : les caractères frappés au clavier sont dirigés vers la prise ; les informations destinées à être affichées transitent directement de la prise vers l'écran.

Les aiguillages du Minitel sont positionnés de la sorte à chaque fois que l'usager doit saisir des données sur le clavier. En particulier, lors de saisie de données confidentielles, le LECAM vérifie que les caractères frappés ne sont jamais émis vers le réseau de transmission.

L'affichage des messages destinés à guider l'usager peuvent se faire sur la rangée de l'écran réservée à cet effet et préalablement définie par la consigne de mise en mode (voir le rôle de cette consigne au chapitre 8).

Les caractères saisis au clavier sont rangés dans la mémoire du lecteur et sont exploités selon le programme téléchargé par l'application distante.

Si ces données sont destinées à être uniquement présentées à la carte (code confidentiel par exemple), elles sont rangées dans la zone locale de la mémoire du lecteur, et sont inaccessibles de l'extérieur. Le voyant "SECRET" reste alors allumé pendant toute la saisie, garantissant à l'usager que les caractères frappés ne sont jamais transmis en ligne.

Ce même voyant clignote lorsque les informations saisies sont destinées à être chiffrées avant d'être transmises vers le serveur.

2. 5 - Interactions avec les points d'accès et les serveurs

Les points d'accès peuvent transmettre des données destinées à la rangée 0 du Minitel. Ces données peuvent intervenir pendant n'importe quelle phase du fonctionnement du lecteur.

Ces données sont considérées comme des parenthèses par le lecteur. Elles doivent débuter par la séquence : US, 4/0,x/x , et être terminées par LF.

Selon le mode de fonctionnement du lecteur, et donc des aiguillages du Minitel, ces données sont traitées de la façon suivante :

Mode standard, Minitel connecté :

. le message rangée 0 est filtré par le lecteur ; il est affiché normalement à l'écran.

Lecteur en mode transparent :

. réception de données Vidéotex : le message rangée 0 est transmis à l'écran, même s'il apparaît au milieu de données chiffrées (le chiffrement n'est pas altéré),

. réception de données "application lecteur" : le message rangée 0 peut apparaître n'importe quand ; il est alors retransmis vers l'écran, sans perturber les contrôles de la réception des messages "application",

Lecteur en mode local ou distant :

. le message rangée 0 est filtré par le lecteur ; il n'est pas affiché à l'écran.

Remarque :
Il est recommandé de ne pas laisser le curseur du Minitel en rangée 0 avant la connexion du LECAM.

3 . PROTOCOLE D'ECHANGES AVEC LE SERVEUR

3. 1 - Généralités

3. 1. 1 - Types de messages échangés par une application serveur/LECAM

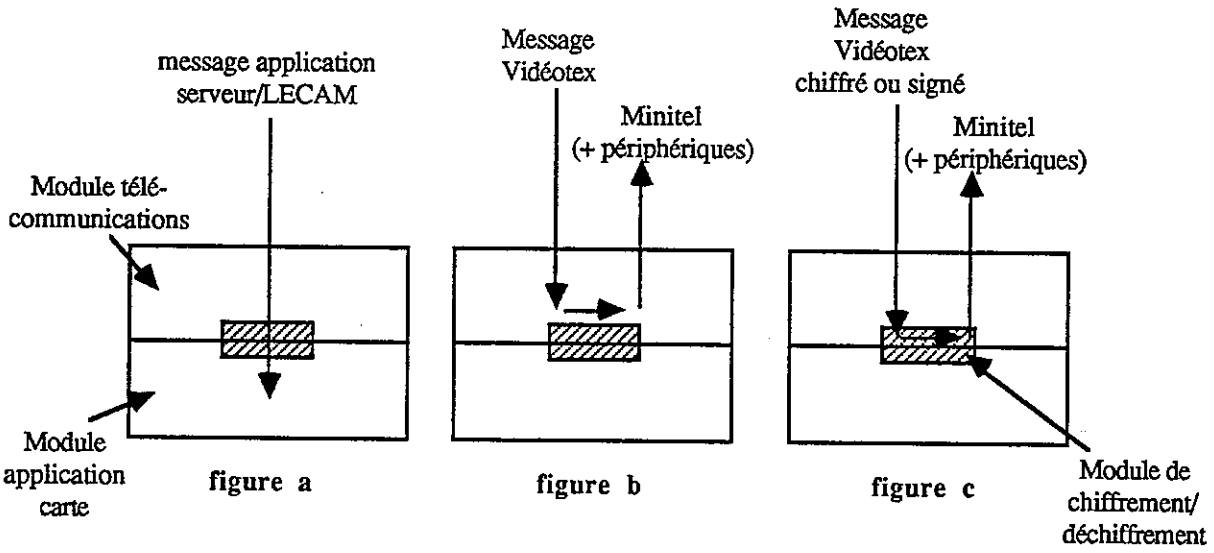
Les messages échangés entre un serveur et un LECAM sont de trois types :

- les messages application serveur/LECAM (figure a),
- les messages Vidéotex (figure b),
- les messages Vidéotex chiffrés ou signés (figure c).

Dans le sens serveur vers LECAM, les trois types de messages peuvent être émis ; le LECAM quant à lui n'émet que des messages applicatifs ~~ou des messages Vidéotex n'étant pas destinés à être chiffrés ou signés~~.

Les messages Vidéotex (chiffrés ou non) ne sont pas analysés par le niveau applicatif du LECAM ; ils sont en fait retransmis vers l'écran du Minitel ou vers les périphériques après un éventuel déchiffrement.

Il ne doit pas y avoir de multiplexage entre les messages Vidéotex (chiffrés ou non) et les messages applicatifs.



Pour la connaissance du sens de transfert des informations, se reporter au paragraphe 1. 2. 3.

3. 1. 2 - Protocole de transport des messages applicatifs

Les blocs d'informations échangés entre l'application distante et le LECAM sont encadrés par des drapeaux de début et de fin de bloc, notés respectivement <d> et <f>.

Selon les choix faits par l'application distante, ces données peuvent être structurées sous une forme particulière appelée TLV et comporter ou non un CRC dont le rôle est de détecter les erreurs de transmission.

Il faut adapter le format des échanges serveur/LECAM au format Télétel. Pour cela il faut d'abord faire la conversion des données codées sur 8 bits utiles en 7 bits plus un bit de parité paire. De plus, il faut éviter que les données transmises soient considérées comme des séquences de contrôle destinées au protocole du Minitel ou au point d'accès : elles sont donc acheminées à l'intérieur d'octets dont le codage particulier, appelé P/1/6 permet d'éliminer les caractères 0/0 à 1/F (notation hexadécimale).

Ce sont les drapeaux de début de bloc qui permettent d'indiquer la nature et la forme des informations transmises.

3. 2 - Structure des messages applicatifs

Un message échangé entre le LECAM et le serveur a la structure suivante :

<d> données 1 <f><d> données 2 <f><d>...<f> CR

Un message peut donc être constitué de plusieurs blocs d'informations. La fin du message est signalée par le caractère 'CR' (0D en hexadécimal).

3. 2. 1 - Messages au format TLV

Les données comprises entre les drapeaux de début et de fin de bloc peuvent être soit des données purement Vidéotex, auquel cas elles sont transmises telles quelles, soit un dialogue sous forme de questions/réponses entre le serveur et le LECAM.

Dans ce dernier cas, chaque bloc de données contient un nombre entier d'éléments de forme TLV, c'est-à-dire codés de la façon suivante :

T :	1 octet	représente le type des informations
L :	1 octet	longueur en octets du champ V
V :	L octets	informations proprement dites le champ V peut être absent, dans ce cas L = 0.

Chaque élément TLV reçu par le lecteur est appelé "consigne". Il est appelé "réponse" lorsqu'il est reçu par l'application distante. Les consignes émises et les réponses correspondantes sont décrites dans le chapitre suivant.

3. 2. 2 - CRC

La protection contre les erreurs de transmission est assurée par une procédure de détection d'erreur implantée dans l'application distante et dans le lecteur de carte. Cette procédure permet un contrôle de bout en bout des informations échangées, et cela dans les deux sens de transmission. Cette procédure de contrôle est réalisée grâce à un code à redondance cyclique (CRC).

Le CRC est calculé sur 16 bits à partir du polynôme générateur :

$$X^{16} + X^{12} + X^5 + 1$$

le registre à décalage étant initialisé à zéro.

Le CRC est calculé sur l'ensemble des données constituant le bloc avant codage en P/1/6, et est placé immédiatement avant le drapeau de fin de bloc.

Le choix d'utiliser ou non le contrôle par CRC est commandé par le serveur. La procédure peut être mise en œuvre indépendamment dans un sens de transmission ou dans l'autre.

Les blocs échangés sont donc de la forme suivante :

<d> TLV , TLV, ..., TLV, CRC <f>

Exemple :

Calcul de CRC sur consigne de mise en mode
TLV = 41 02 81 18
CRC = CD D8

Note :
De plus amples informations concernant les codes correcteur d'erreurs pourront être trouvées dans le manuel suivant :

Error-Correcting Code
Second Edition
WESLEY PETERSON & E.J. WELDON Jr.
MIT PRESS
CAMBRIDGE - Massachussets 02142 - (USA)

3. 3 - Transparence des données (messages applicatifs et messages Vidéotex chiffrés)

3. 3. 1 - Codage des données au format P/1/6

Pour assurer une transmission sur 7 bits utiles et pour éviter que les caractères transmis ne représentent accidentellement des caractères de contrôle (colonnes 0 et 1 des spécifications Vidéotex), les données sont acheminées à l'intérieur d'octets au format P/1/6.

Un octet au format P/1/6 a la structure suivante :

b8 b7 b6 b1

b8 : bit de parité
b7 : 1
b1 à b6 : 6 bits utiles

Le bit 7 d'un octet P/1/6 étant "forcé" à 1, les octets contenus entre les drapeaux de début et de fin de bloc ne peuvent donc prendre que les valeurs comprises entre 4/0 et 7/F, ces deux valeurs incluses.

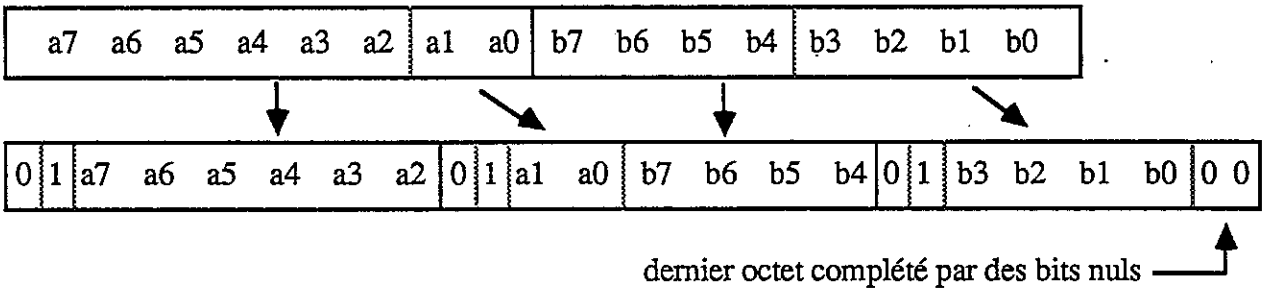
Le principe de la transformation est le suivant :

- les n caractères à transformer représentent n x 8 = m bits,
- les m bits sont découpés en "tranches" de 6 bits soit m = 6 p + x (x représente le reste de la division et est donc inférieur ou égal à 5),
- chaque tranche ainsi obtenue sert à former un octet dont les deux bits de poids fort auront été préalablement initialisés à 01.

On obtient donc p + 1 octets qui représentent le message logique à transmettre.
Le dernier octet (si x est différent de 0) est complété par des zéros : si x = 4, l'octet obtenu est donc 01xxxx00.

Exemple :

On veut transmettre 2 octets :



Lors de la réception du message, celui-ci doit être converti pour retrouver le même nombre d'octets :

soit n le nombre d'octets P/1/6 reçus, le nombre d'octets que l'on doit retrouver est la partie entière du résultat de la division : $q = (n \times 6) / 8$ le reste correspond au nombre de bits ayant servi à compléter le dernier octet du message.

Dans l'exemple précédent $n = 3$

$$q = (n \times 6) / 8 = 2 \quad \text{reste : } 2$$

Dans le cas particulier d'une saisie signée ou chiffrée, les informations frappées au clavier sont transmises par le lecteur sous la forme de données Vidéotex et ne sont donc pas codées en P/1/6.
Si le CRC doit être calculé sur ces informations, il doit alors être transcodé sous forme de quatre caractères alpha-numériques, ceci pour éviter de transmettre des données purement binaires à l'intérieur des blocs de données : les seize bits composant le CRC sont alors éclatés en quatre quartets x, y, z, t et transmis en quatre octets 3/x, 3/y, 3/z, 3/t à la suite du texte saisi (x représente le quartet de poids fort du CRC).

Remarques :
Le bit de parité de l'octet P/1/6 étant géré par les coupleurs de télécommunication émetteur et récepteur, les applications (serveur et LECAM) peuvent considérer que ce bit est toujours à zéro.

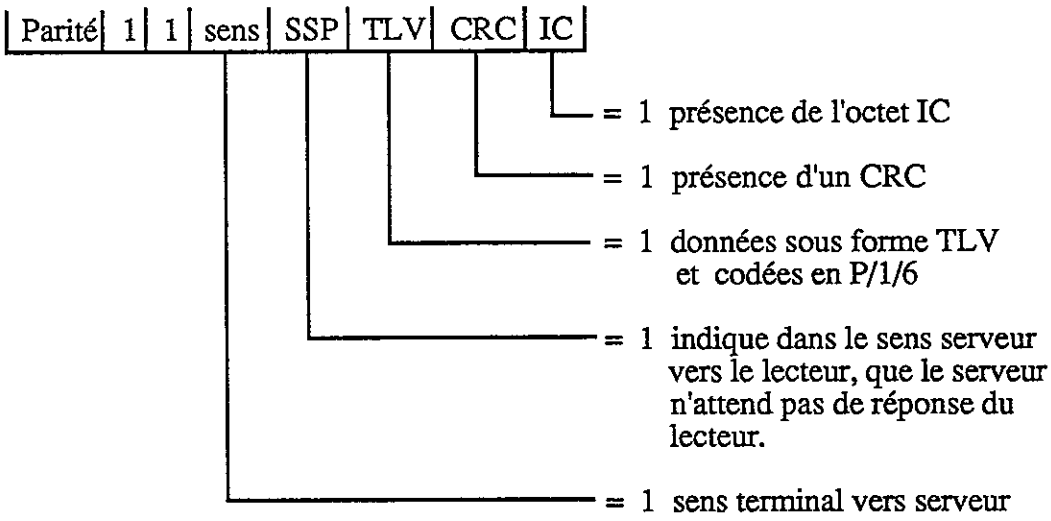
Si les données sont au format TLV, elles sont obligatoirement codées en P/1/6.

3. 3. 2 - Codage des drapeaux de début

Le drapeau <d> a la forme suivante :

<d> : US, 3/C, IT [,IC]

IT : indicateur de transmission (1 octet) indique



IC : indicateur de continuité (1 octet)

La présence de IC est conditionnée par la valeur du bit de poids faible de IT. Si IC est présent, il est de la forme

nnnn : 4 bits de bloc du message de 0 à 14 (ré-initialisé à 0 à chaque message),
rép : 1 bit indicateur de répétition

= 0 lorsque les blocs sont émis la première fois
= 1 lorsque les blocs sont émis suite à une demande de répétition.

Remarque
IC est facultatif dans le sens serveur vers lecteur et est toujours présent dans les blocs émis par le lecteur si la procédure de détection d'erreur a été activée lors de la consigne de mise en mode (voir chapitre suivant).

3. 3. 3 - Codage des drapeaux de fin

Le drapeau <f> a la forme suivante :

<f> : US, 3/C, 2/8 dans le sens serveur vers terminal
US, 3/C, 3/8 dans le sens terminal vers serveur.

3. 3. 4 - Drapeaux de début et de fin de chiffrement

Ces drapeaux ne sont utilisés que dans le sens serveur vers lecteur pour émettre des messages Vidéotex.
Ils indiquent que les données émises sont :

- soit du texte chiffré destiné à être affiché sur l'écran du Minitel après déchiffrement par le LECAM,
- soit du texte clair destiné à être affiché sur l'écran du Minitel.

Par ailleurs, et ceci est vrai pour les deux cas cités, ce texte peut être également destiné à être signé par le LECAM (la signature portant soit sur le texte clair, soit sur le texte chiffré).

Le codage de ces drapeaux est le suivant :

<dc> : US, 3/C, 2/B
<fc> : US, 3/C, 2/E

3. 3. 5 - Drapeau de demande de répétition

Le rôle de ce drapeau est décrit au paragraphe 4 concernant la méthode de récupération des erreurs transmission.

Le format de ce drapeau est le suivant :

<r> : US, 3/C, 2/A, IC dans le sens serveur vers terminal
US, 3/C, 3/A, IC dans le sens terminal vers serveur

IC peut prendre les valeurs hexadécimales comprises entre 6/0 et 6/E et entre 7/0 et 7/E s'il s'agit d'un message qui est répété.

3. 4 - Déroulement général des échanges

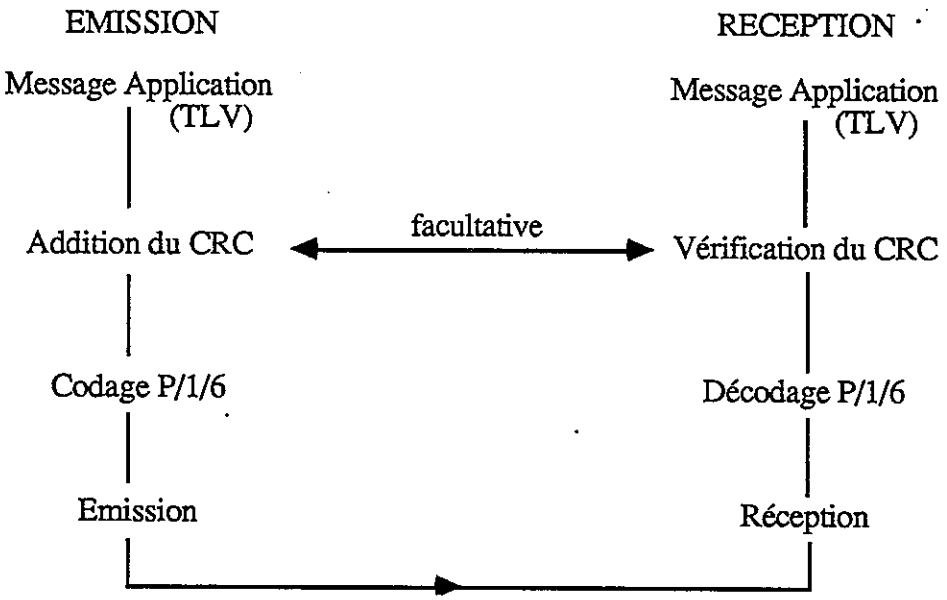
Les données échangées par les applications du serveur et du LECAM (programmes à télécharger, compte-rendus d'exécution) correspondent à un jeu de questions (consignes)/réponses, et sont normalement échangées avec les attributs :

TLV = 1 CRC = 1 ou 0

Les informations saisies au clavier par l'usager lors d'une saisie chiffrée ou signée correspondent à des données Vidéotex du jeu G0 (codes 2/0 à 7/F) et n'ont pas à être codées en P/1/6. En effet, un octet chiffré est le résultat d'un OU exclusif entre un octet de données et les 5 bits de poids faible d'un octet chiffrant, et donc la valeur binaire d'un octet chiffré n'appartient jamais aux colonnes 0 et 1 des spécifications Vidéotex. Ces informations sont donc échangées avec les attributs :

TLV = 0 CRC = 1 ou 0

La constitution des messages échangés se fait selon la séquence suivante :



La longueur maximale d'un bloc émis par le lecteur est de 96 octets, avant mise en forme pour l'émission (hors CRC). La longueur transmise est donnée par le tableau ci-dessous :

LECAM VERS SERVEUR	TAILLE INITIALE	NOMBRE D'OCTETS ENTRE <d> et <f>
sans P/1/6 sans CRC	96 (*)	96
sans P/1/6 avec CRC	96 (*)	100
avec P/1/6 sans CRC	96	128
avec P/1/6 avec CRC	96	131

(*) en fait limité à 40 (messages faisant suite à des saisies chiffrées ou signées)

En réception le lecteur peut recevoir des blocs de 96 octets utiles maximum :

SERVEUR VERS LECAM	LONGUEUR RECUE ENTRE <d> et <f>	LONGUEUR UTILE
avec P/1/6 sans CRC	128	96
avec P/1/6 avec CRC	131	96

4 - RECUPERATION DES ERREURS DE TRANSMISSION

Le LECAM reçoit des messages constitués de blocs suivis d'un caractère CR.

Ces blocs sont numérotés de façon explicite ou implicite, selon la présence de l'octet IC dans le drapeau de début de bloc. Si cette indication est présente, le lecteur contrôle la succession des numéros ; si cette indication est absente, le LECAM numérote implicitement les blocs à partir du numéro 6/0.

Les caractères et le CRC de chaque bloc reçu sont contrôlés par le lecteur. Dès qu'une erreur est détectée (parité caractère ou CRC faux, codage en P/1/6 erroné, ou délai inter-blocs supérieur à 900 ms), il positionne les aiguillages du Minitel pour se placer en mode distant, puis envoie une séquence <r> de demande de répétition suivie du caractère CR.

La séquence <r> transmise par le lecteur a la forme suivante :

<US, 3/C, 3/A, IC> CR

L'octet IC permet d'indiquer à l'application distante quel est le bloc qu'elle doit ré-émettre.

IC prend les valeurs hexadécimales comprises entre 6/0 et 6/E lorsqu'il est transmis dans un drapeau de demande de répétition, et entre 7/0 et 7/E lorsqu'il se trouve dans le drapeau de début d'un bloc répété.

IC est ré-initialisé à 6/0 à chaque nouveau message. Le premier bloc est donc compté 6/0, le deuxième 6/1, ...

Par exemple, si le bloc erroné est le septième, l'octet IC compris dans le drapeau <r> vaut donc 6/6.

Lorsqu'il a émis la séquence <r>, le lecteur ignore tous les caractères reçus jusqu'à réception d'un drapeau <d> comportant explicitement l'indicateur de continuité IC attendu avec le bit indiquant la répétition de bloc positionné à 1. (L'octet IC attendu correspondant à l'exemple précédent est donc 7/6). Même si le serveur ne paramètre pas l'envoi de ses blocs de données par l'octet IC, le bloc ayant fait l'objet d'une demande de répétition doit obligatoirement comporter l'octet IC avec le bit 'rép' positionné ; pour les blocs suivants, IC est facultatif.

L'attente de cette séquence est limitée par un délai de 10 secondes. La séquence <r> est ré-émise à l'expiration du délai. Après trois émissions infructueuses de <r>, le lecteur génère une Commande de Déconnexion et met fin à la session Système d'Echanges.

Dans le cas où la transmission est perturbée après la réception du dernier bloc constituant le message et que seul le caractère CR n'est pas reçu, le lecteur demande la répétition d'un bloc supplémentaire. Le serveur doit alors répondre en envoyant le bloc de numéro demandé. Ce bloc contient uniquement les drapeaux, soit :

<d> <f> CR

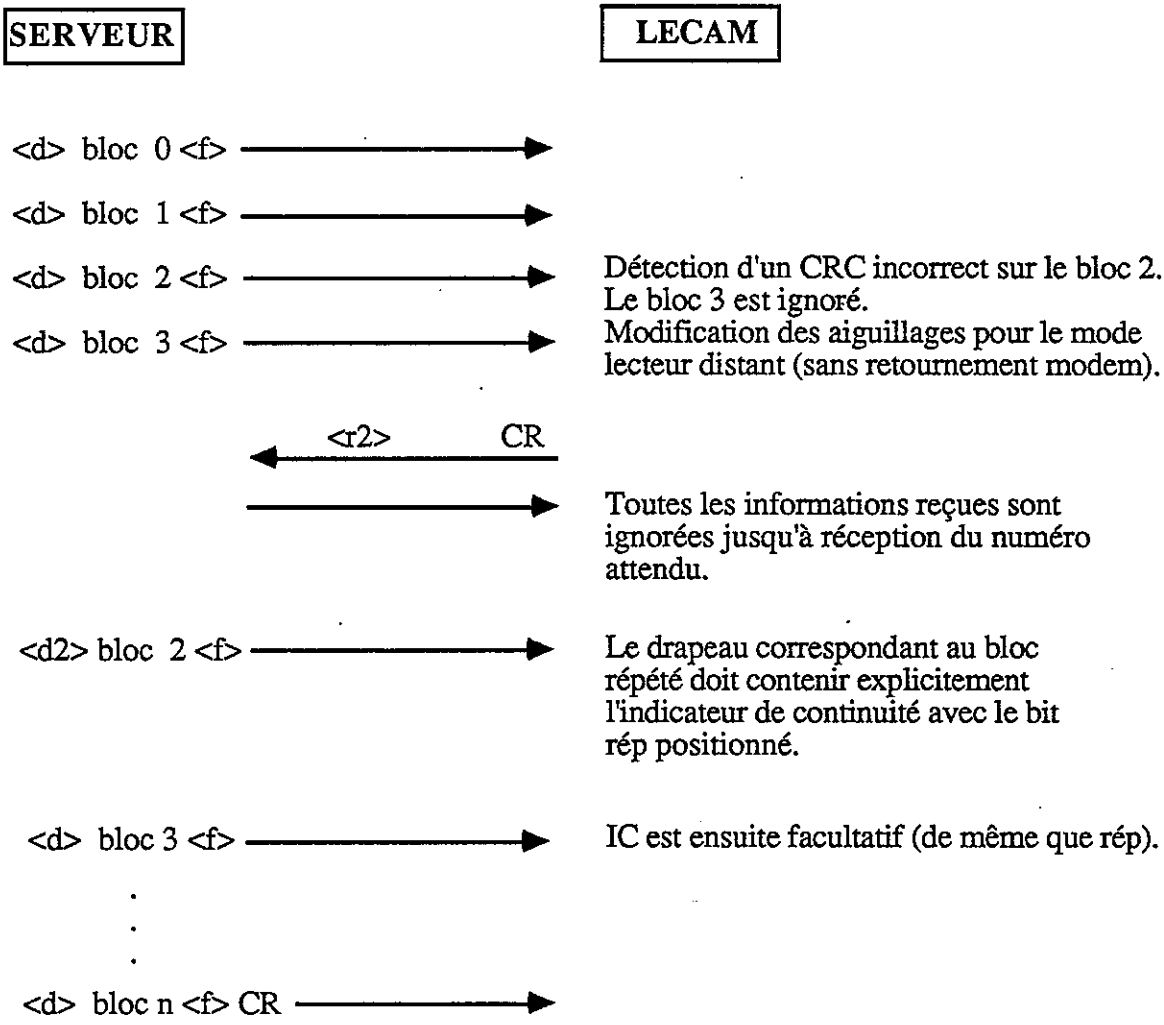
La procédure de détection d'erreur mise en œuvre par l'application distante est analogue. Le drapeau de demande de répétition a dans ce cas la forme suivante :

<US, 3/C, 2/A, IC>

Si un serveur émet une demande de répétition < r >, le LECAM ré-émet les blocs à partir du rang demandé et jusqu'à la fin du message.Les blocs ré-émis par le LECAM comportent l'octet IC avec le bit 'rép' positionné, et ceci quelle que soit la valeur du paramètre 'e' de la consigne de mise en mode.

Remarque
La séquence <r>, dans le sens terminal vers serveur, est toujours émise sans retournement du modem du Minitel, donc à 75 bauds.

Diagramme des échanges après réception d'un bloc incorrect



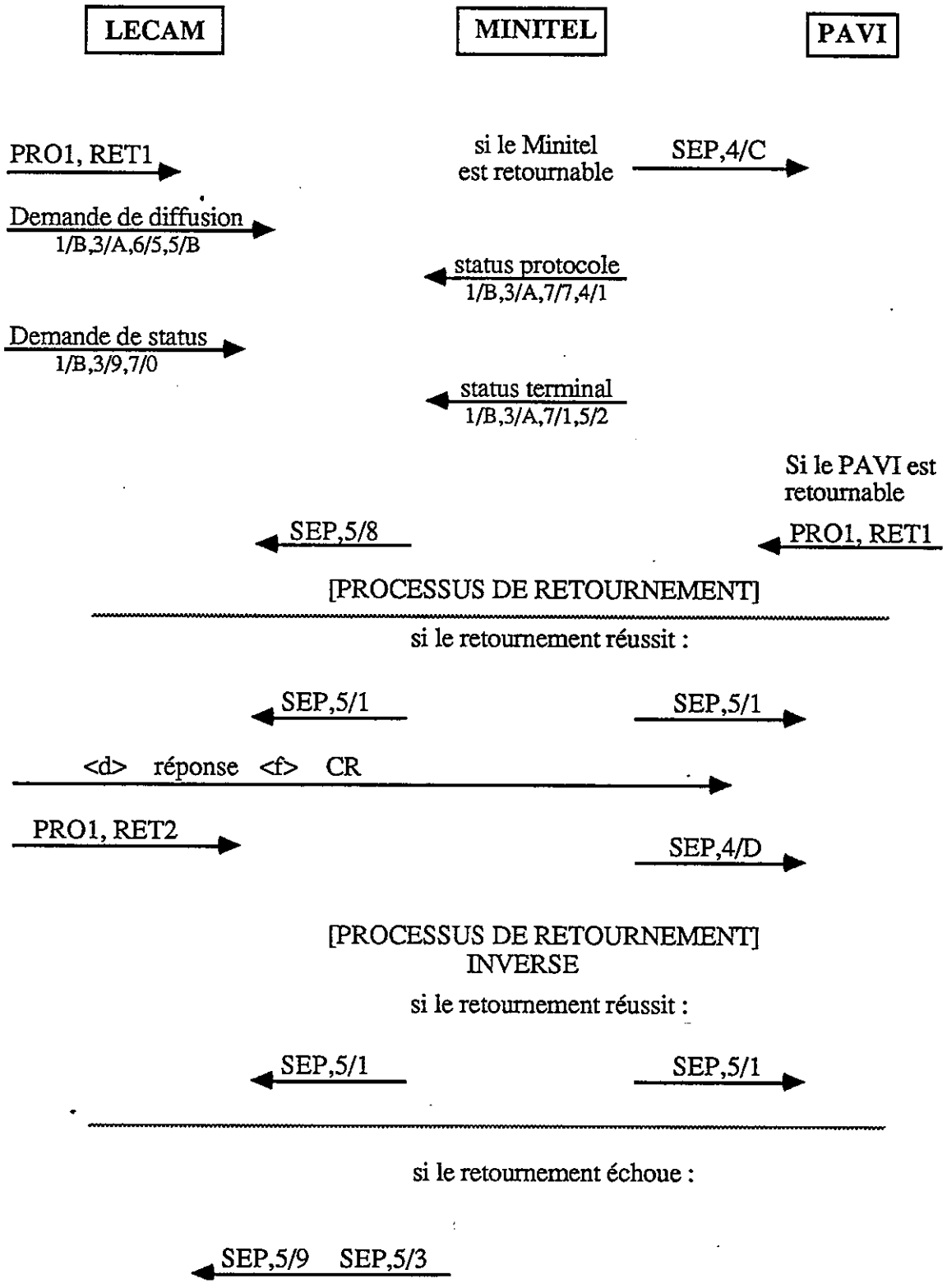
5 - GESTION DU RETOURNEMENT DU MODEM

Pour réduire le temps de la transmission des données entre un LECAM et un serveur, le lecteur gère le retournement du modem du Minitel, à condition que celui-ci soit du type "retournable". Les données émises par le lecteur sont donc transmises à 1200 bauds vers le réseau Vidéotex et à 75 bauds dans l'autre sens.

La première tentative de retournement du modem suit immédiatement la réponse à la consigne de mise en mode. Si le retournement réussit, toutes les réponses du LECAM sont transmises avec retournement, à l'exception des demandes de répétition, lorsque la procédure de détection d'erreurs est active. Dès que le LECAM a terminé d'émettre sa réponse, il opère le retournement inverse pour permettre au serveur d'émettre à nouveau à 1200 bauds. Si le retournement échoue, le LECAM ne fait plus aucune tentative de retournement du modem du Minitel. Le LECAM émet alors sa réponse à 1200 bauds, mais cadencée à 75 bauds, de façon à ne pas engorger la liaison modem du Minitel.

La mise en œuvre du retournement du modem est expliquée dans le manuel des "Spécifications Techniques d'Utilisation du Minitel 1B".

Le dialogue échangé à la première demande de retournement du modem du Minitel par le LECAM est le suivant :



Le LECAM initialise la demande de retournement par la séquence Protocole PRO1, RET1 qui est analysée par le Minitel et transmise au point d'accès Vidéotex (PAVI) sous la forme SEP,4/C. Le lecteur continue à dialoguer avec le Minitel pendant l'attente de la réponse du PAVI (demandes de diffusion vers la prise et de status terminal). Le PAVI indique qu'il accepte le retournement par l'envoi de la commande PRO1, RET1 qui est acquittée par le Minitel et renvoyée au LECAM sous la forme SEP,5/8.Le Minitel rend compte de la réussite du retournement de son modem par la séquence SEP,5/1, envoyée à la fois au LECAM et au PAVI. Si le retournement échoue, la séquence SEP,5/9, SEP,5/3 est émise vers le LECAM.

La reprise du dialogue entre l'application LECAM et l'application distante est donc conditionnée par la réception, de part et d'autre, d'une séquence SEP,5/1 indiquant la fin du processus de retournement.

Les retournements suivants sont initialisés par le Protocole du Minitel pendant le reste de la session, par le changement immédiat de la vitesse du modem à chaque demande du LECAM.

Lorsque le LECAM a terminé d'émettre sa réponse, il émet la commande PRO1, RET2 qui est transformée en SEP,4/D à destination du PAVI pour initialiser le retournement inverse.

Remarques

- Les points d'accès peuvent transmettre des données destinées à la rangée 0 du Minitel.
  Si le message rangée 0 apparaît immédiatement après le message émis par le serveur et destiné à l'application lecteur, il peut être perturbé par le retournement du modem du Minitel. En effet, dès que le lecteur reçoit un message qui lui est destiné et demandant une réponse (bit SSP de l'octet IC égal à 0), il initialise une demande de retournement du modem afin que le retournement soit effectif lorsque la réponse du LECAM est prête à être transmise.

- Si, lors d'un premier retournement du modem le LECAM trouve le Minitel dans l'état opposé (par PRO1, OPPO) ou retourné (par un autre périphérique par exemple) il en tiendra compte pour rétablir un contexte correct : si le Minitel est à l'état opposé, il envoie sa réponse à 1200 bauds puis émet PRO2, OPPORE suivi de PRO1, RET1 pour se retrouver à l'état normal ; si le Minitel est déjà retourné, le lecteur n'envoie pas le premier PRO1, RET1 et émet directement sa réponse à 1200 bauds.

CHAPITRE 8 - LE MODULE APPLICATION CARTE

1 . LE GESTIONNAIRE DE CONSIGNES

1. 1 - Généralités

Les messages reçus par le LECAM sont interprétés par le protocole Application Carte comme une succession de consignes. Celles-ci se rattachent à six familles distinctes, à savoir :

- consigne de mise en mode,
- consignes d'initialisation et de chargement de programmes et de paramètres,
- consigne d'exécution de l'interpréteur,
- consignes d'initialisation de l'éditeur de texte,
- consignes d'initialisation des fonctions de sécurité,
- consignes de confidentialité et de saisie chiffrée ou signée.

La consigne de mise en mode est obligatoire et doit être la première à être reçue par le lecteur. Pour être valable, la consigne de demande d'exécution de l'interpréteur doit être précédée par au moins une consigne de chargement de programme.

En règle générale, toute consigne demandant une réponse du lecteur (consignes d'exécution de l'interpréteur, de fin de signature, de saisie,...) doit être la dernière d'un groupe de consignes envoyé au LECAM.

Les consignes sont constituées par des groupes d'octets au format TLV. Le champ "T" correspond au type de la consigne, auquel est associé un mnémonique ; le champ "L", noté "Lg" dans la suite du chapitre, indique le nombre d'octets constituant le champ "V" qui contient les paramètres de la consigne.

1. 2 - Les consignes

1. 2. 1 - Consigne de mise en mode

Le LECAM est connecté (au sens "Système d'Echanges") mais ne sait pas encore comment travailler : il rejette tous les messages reçus jusqu'à réception de la consigne de mise en mode. Le rôle de cette consigne est donc d'initialiser le dialogue et notamment de définir si le lecteur est en liaison avec un Minitel, ou s'il est en relation avec un élément local, comme par exemple un micro ordinateur.

La consigne de mise en mode provoque aussi la recherche d'un bloc de sécurité dans la carte si celle-ci n'est pas de type M4, B0 ou M6.

CM, Lg, mode, rg

CM = 41 (hexa)
Lg = 02
mode = d... .tce

'd' conditionne le mode de gestion du Minitel

d = 1 : Le LECAM gère les aiguillages, le retournement modem et le curseur du Minitel.

d = 0 : Le LECAM ne gère absolument pas le Minitel.

t = 1 : Les comptes-rendus de fonctionnement interne du LECAM sont transmis vers le serveur lors de chaque réponse du lecteur.

t = 0 : Les comptes-rendus de fonctionnement interne du LECAM ne sont transmis qu'en cas d'erreur. Seul l'état carte actuel est transmis.

c = 1 : Les trois octets mots d'état carte et mot d'état coupleur (ME1, ME2, MDC) sont transmis à l'application à chaque opération carte réalisée (ou tentée) lors de la prochaine réponse du lecteur.

c = 0 : Ces trois octets sont transmis au serveur avec la réponse du lecteur si une erreur carte a été détectée. La dernière erreur carte détectée par le coupleur carte est transmise même si l'état carte actuel est différent.

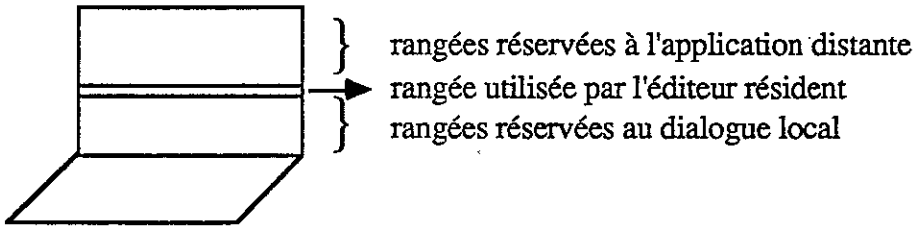
e = 1 : Mise en œuvre de la procédure de détection d'erreurs de transmission dans le sens lecteur vers serveur (dans le sens serveur vers lecteur la procédure est activée ou non par le contenu de l'octet 'IT' du drapeau de début - voir chapitre précédent-).

e = 0 : La réponse du lecteur ne comporte ni CRC ni octet 'IC'.

rg = Numéro de la rangée à utiliser par l'éditeur résident du LECAM (valeur comprise entre 0 et 24).

Cette rangée peut servir à partager l'écran entre les informations à afficher ou à saisir pour l'application distante et celles pour l'application locale.

Exemple :



Remarques concernant le mode de fonctionnement du LECAM

si d = 1, et que le LECAM a reçu la séquence de caractères SEP,5/4 émise par le Minitel, le LECAM initialise le mode de fonctionnement correspondant : il gère la demande de retournement du modem du Minitel et positionne ses aiguillages en fonction des opérations à réaliser. Il vérifie notamment que pendant les opérations de saisie locale et d'affichage chiffré, le modem du Minitel reste inhibé, c'est à dire que les données saisies ou affichées ne sont pas émises sur la ligne, donc vers le serveur. Par ailleurs, il vérifie la cohérence des aiguillages demandés.

si d = 0, tous les transferts se font vers le maître (au sens Système d'Echanges), qu'il y ait ou non un Minitel connecté sur le LECAM. Il n'y a aucune tentative de gestion des aiguillages ou du retournement du modem du Minitel.

1. 2. 2 - Consignes de chargement

C1, Lg, adr, données

Chargement de programmes ou de données dans la mémoire vive de l'interpréteur du LECAM.

C1	=	43 (hexa)
Lg (1 octet)	=	variable
adr (2 octets)	=	adresse de chargement du premier octet de "données" (dans le cas de registres, adr : 03xx, avec xx = numéro du premier registre)
données (Lg - 2 octets)	=	information à charger à partir de l'adresse "adr"

Remarque :
La valeur du paramètre 'Lg' ne peut être supérieure à 94.

CC, Lg, adr, données

Chargement chiffré de programme. Tous les octets d'adresse et de données sont chiffrés quelle que soit leur valeur.

CC	=	44 (hexa)
Lg (1 octet)	=	variable
adr (2 octets)	=	adresse de chargement du premier octet de "données" (dans le cas de registres, adr : 03xx, avec xx = numéro du premier registre). Les deux octets d'adresse sont chiffrés.
données (Lg - 2 octets)	=	information à charger à partir de l'adresse "adr". Tous les octets de "données" sont chiffrés.

Le chiffrement est réalisé à partir de l'état courant du Générateur d'Octets Chiffrants (GOC), initialisé notamment par les consignes CH et éventuellement PR (voir plus loin).

On utilise les quatre bits de poids faibles de deux octets chiffrants successifs pour chiffrer un octet de données : le premier octet chiffrant obtenu permet de chiffrer le quartet de poids fort de l'octet de données, le second permet le chiffrement du quartet restant.

Remarques :
Il faut activer le GOC avant l'émission d'une consigne CC ; sinon, la clé de base étant égale à zéro, les données sont transmises en clair au lieu d'être chiffrées.

La valeur du paramètre "Lg" ne peut être supérieure à 94.

C2, Lg, données

C 2	=	45 (hexa)
Lg (1 octet)	=	variable (même restriction que pour la consigne C1)
données (Lg octets)	=	suite des informations à charger à partir de l'adresse précédemment atteinte par une consigne C1 ou CC ou C2. Si la consigne C2 exprime la continuation d'une consigne CC, les données sont chiffrées.

C3, Lg, n

C3	=	46 (hexa)
Lg (1 octet)	=	01
n (1 octet)	=	numéro du programme résident à transférer depuis la zone mémoire morte du LECAM, dans la mémoire vive (zone programme et zone registres) de l'interpréteur, et ceci à des adresses fixes.

1. 2. 3 - Consigne d'exécution de l'interpréteur

LI, Lg, adr

LI	=	47 (hexa)
Lg (1 octet)	=	02
adr (2 octets)	=	adresse de début du programme à exécuter. L'adresse est comprise entre les valeurs hexadécimales 0 à 2FF.

L'interpréteur exécute le programme chargé à partir de l'adresse (adr) indiquée.Du fait de la possibilité de paramétrage de l'adresse de début d'exécution du programme, le serveur peut demander plusieurs fois l'exécution d'un même programme, en changeant éventuellement le point d'entrée de ce programme.

Cette consigne doit être la dernière d'un message destiné au lecteur.

Le LECAM rejette toutes les autres consignes qui pourraient lui être envoyées tant qu'il n'a pas répondu à la consigne LI.

1. 2. 4 - Consignes d'initialisation de l'éditeur

1. 2. 4. 1 - Fonctionnement de l'éditeur

Le LECAM peut être amené à faire intervenir l'utilisateur pour ses propres besoins ou ceux de l'application distante : il dispose pour cela d'un éditeur qui permet la saisie d'informations sur le clavier du Minitel et l'affichage de messages sur l'écran (applications de saisie du code porteur, de fonctionnement du lecteur en mode local, de saisie chiffrée ou signée par exemple).

Le paramètre "rg" de la consigne de mise en mode permet d'indiquer au lecteur quelle est la rangée de l'écran du Minitel qu'il peut utiliser pour les besoins purement locaux. La valeur de "rg" est comprise entre 0 et 24, bornes incluses.

Ce paramètre est utilisé par l'ordre DISP de l'interpréteur, qui dirige systématiquement les messages sur le Minitel si le mode de gestion du Minitel est actif (fonction du bit 'd' de la consigne CM).

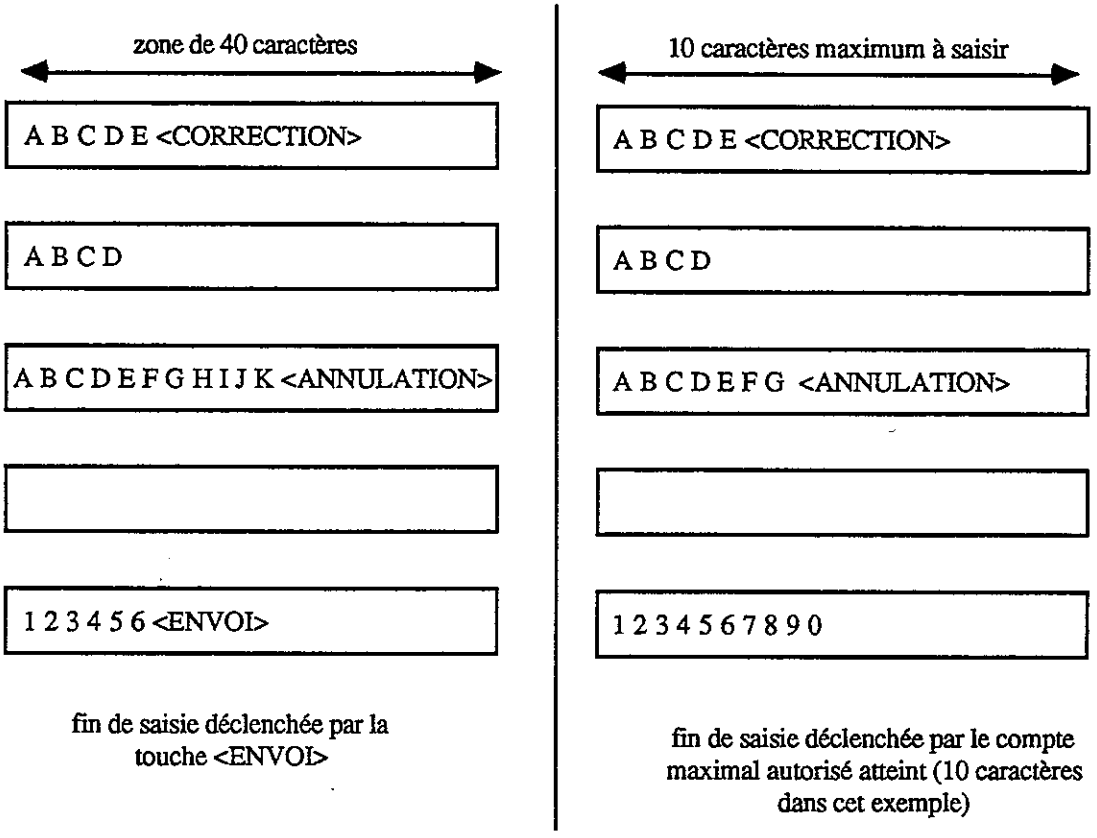
Lors de tout échange entre le serveur et le lecteur, le LECAM replace le curseur à sa position avant le début de l'échange, sauf dans le cas de saisie chiffrée ou signée, pendant lesquelles le curseur reste positionné derrière le dernier caractère frappé.

1. 2. 4. 2 - Saisies et affichages signés ou chiffrés

a - principe de fonctionnement

Le serveur peut être amené à donner le contrôle au LECAM pour la saisie d'une zone de 'n' caractères consécutifs, celle-ci ne pouvant excéder 40 caractères. La saisie de cette zone est faite de façon autonome par le lecteur, qui gère les touches <CORRECTION> et <ANNULATION> qui provoquent respectivement l'effacement du ou des caractères déjà saisis.
Les autres touches de fonction (ou l'utilisation des touches <CORRECTION> ou <ANNULATION> alors qu'aucun caractère n'a été saisi), provoque l'envoi au lecteur du tampon d'émission ainsi que des codes de la touche de fonction utilisée.

La fin d'une saisie peut être déclenchée soit par une touche de fonction, soit par un compte maximal de caractères à saisir, selon les exemples suivants :



Les consignes faisant intervenir l'éditeur du LECAM pour le compte du serveur peuvent être classées en trois catégories :

- les consignes permettant de garantir la confidentialité des informations saisies par l'usager,
- les consignes initialisant le mode de fonctionnement du lecteur,
- les consignes de saisie et d'affichage proprement dites.

b - Jeux de caractères

Le jeu de caractères utilisable pour la saisie chiffrée ou signée d'informations est le jeu G0 exclusivement. Les trois jeux (G0, G1, G2) peuvent être utilisés pour les fonctions d'affichage chiffré, les caractères des colonnes 0 et 1 (caractères 0/0 à 1/F) n'étant jamais chiffrés.
Seul le jeu G0 est utilisable pour initialiser une saisie chiffrée par un affichage chiffré, le résultat en cas d'utilisation des deux autres jeux n'étant pas prévisible.

Si la mise en œuvre de la fonction d'affichage chiffré n'est pas destinée à initialiser le tampon de saisie, le texte chiffré peut contenir des tabulations ou des attributs de visualisation, voire des séquences générées par le Minitel, qui ne sont jamais chiffrés.

Il en va de même pour les caractères du jeu G2, soit SS2 plus deux caractères pour la représentation des signes diacritiques (colonne 4 du jeu G2) et SS2 plus un caractère pour les autres.

Les séquences de caractères suivantes ne sont donc jamais chiffrées, et par conséquent ne "consomment" pas d'octets chiffrants :

0/x
1/x
ESC, 2/x, 2/x, ...{3/x à
{7/x
ESC, 3/9, x/x
ESC, 3/A, x/x, y/y
ESC, 3/B, x/x, y/y, z/z
ESC, 3/x à 7/x
SEP, x/x
SS2, y/x (y différent de 4)
SS2, 4/x, x/x
US , x/x, x/x
US , 4/0, ..., 0/A

Se reporter aux Spécifications Techniques d'Utilisation du Minitel 1B (STUM 1B) qui décrivent ces jeux de caractères.

1. 2. 4. 3 - Consignes de l'éditeur

Ces consignes servent à modifier le fonctionnement par défaut retenu par l'éditeur.

a - Modification du caractère d'appel

CA, Lg, texte

CA = 4D (hexa)
Lg (1 octet) = variable (ne peut excéder 12)
texte (Lg octets) = texte à transmettre vers l'écran en écho à une action sur la touche <CORRECTION>. La séquence utilisée par défaut est : BS, " ", BS.

b - Graphisme d'écho

CE, Lg, texte

CE = 4 F (hexa)
Lg (1 octet) = variable (ne peut excéder 12)
texte (Lg octets) = texte à renvoyer vers l'écran en écho à la frappe d'une touche dans le cas d'un écho brouillé. La séquence utilisée par défaut est "*".

Il est possible, pour ces deux consignes, de placer dans la zone "texte" des séquences de caractères permettant de modifier les attributs de visualisation, sous forme directement transmissible au module écran.

c - Contrôle des caractères saisis

CS, Lg, val

CS = 51 (hexa)
Lg (1 octet) = 01
val (1 octet) = type des caractères autorisés en saisie

"val" peut prendre les valeurs suivantes :

1 : seuls les caractères numériques sont autorisés
2 : seuls les caractères alphabétiques sont autorisés
3 : seuls les caractères alphanumériques sont autorisés
0 : tous les caractères sont autorisés (valeur par défaut).

En cas de saisie d'un caractère non autorisé, aucun écho n'est transmis. Le caractère saisi n'est pas pris en compte, et un signal sonore est émis pour en avertir l'usager.

d - Temporisation inter-caractères

TC, Lg, val

TC	= 53 (hexa)	
Lg (1 octet)	= 01	
val (1 octet)	= 1 à 127	valeur en secondes du délai maximum autorisé entre deux caractères saisis
	= 0	aucun délai n'est contrôlé

La valeur par défaut du paramètre "val" est 20.

e - Contrôle de fin de saisie

XS, Lg, val

XS	= 55 (hexa)	
Lg (1 octet)	= 01	
val (1 octet)	= 1	la fin de saisie est provoquée soit par la frappe d'une touche de fonction, soit automatiquement lorsque le dernier caractère prévu est introduit au clavier
	= 0	la fin de saisie est provoquée exclusivement par l'utilisation d'une touche de fonction (valeur par défaut). Si le nombre de caractères prévus est dépassé, il y a émission d'un signal sonore.

Remarque concernant les consignes de l'éditeur.
Ces consignes ne s'appliquent pas aux saisies réalisées à l'aide des instructions interpréteur ENTER, VALID et DIAL mais seulement aux consignes de saisie SC et SS, qui sont décrites dans la suite du chapitre. Les valeurs retenues pour les instructions interpréteur sont les valeurs par défaut.

1. 2. 5 - Consignes d'initialisation des fonctions de sécurité

a - Initialisation du chiffrement

Cette consigne a pour objet de récupérer la clé de base stockée en zone interne du LECAM, et de la manipuler éventuellement pour initialiser le Générateur d'Octets Chiffrants (GOC).

CH, Lg, type, synchro [, clé de déchiffrement]

CH = 57 (hexa)

Lg (1 octet) = - 02 si le paramètre "clé de déchiffrement" est absent
- 10 si le paramètre "clé de déchiffrement" est présent

type (1 octet) = cx.. ...e

c = 1 : en saisie signée, les caractères frappés sur le clavier du Minitel sont à chiffrer avant transmission ; en affichage, les caractères situés entre les drapeaux de début et de fin de chiffrement sont à déchiffrer.

c = 0 : en saisie signée, les caractères frappés sur le clavier du Minitel sont envoyés en clair ; en affichage, les caractères reçus entre <dc> et <fc> sont en clair.

x = 1 : la compression pour signature est calculée à partir des caractères chiffrés.

x = 0 : la compression pour signature est calculée à partir des caractères en clair.

e = 1 : la saisie doit avoir lieu avec écho local en clair.

e = 0 : la saisie doit avoir lieu avec écho local brouillé.

Les valeurs par défaut sont : c = 0 x = 0 e = 1 .

synchro (1 octet) = un octet quelconque qui est utilisé pour initialiser le GOC, grâce à l'application d'une fonction OU exclusif entre lui-même et chaque octet de la clé de base. La clé de base est rangée en zone interne de la mémoire du LECAM.

clé de déchiffrement (8 octets) = l'utilisation de ce paramètre est facultative. S'il est présent, le GOC est initialisé par l'application d'un OU exclusif entre cette clé et la clé obtenue selon la méthode décrite ci-dessus.

b - Positionnement du GOC pour obtenir l'octet chiffrant

PR, Lg, rang

PR = 58 (hexa)

Lg (1 octet) = 02

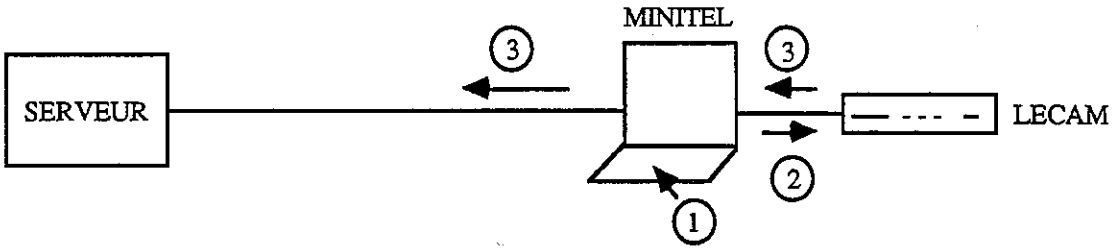
rang (2 octets) = permet de synchroniser le GOC pour fournir l'octet chiffrant correspondant au compteur d'octets "rang".

Cette consigne, facultative, permet la synchronisation des GOC serveur et LECAM en faisant tourner à vide le GOC du LECAM d'un nombre de tours égal à la variable 'rang'. Chaque tour de GOC génère un octet chiffrant.
La consigne PR permet de positionner le GOC à un rang donné, mais elle ne peut être utilisée qu'après une consigne CH dont l'octet de 'synchro' est égal à zéro et dont la 'clé de déchiffrement' est absente.

1. 2. 6 - Consignes de saisie et d'affichage chiffrés ou signés

Les fonctions réalisées à l'aide de ces consignes sont les suivantes :

Saisie chiffrée

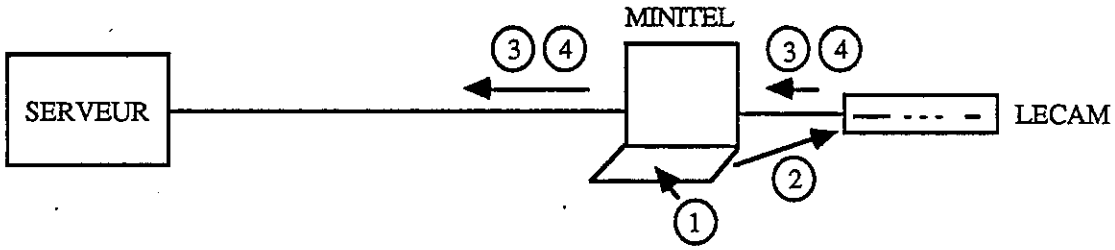


① frappe d'un texte sur le clavier du Minitel

② chiffrement par le LECAM

③ envoi du texte chiffré au serveur entre drapeaux

Saisie signée



① frappe du texte à envoyer avec une signature

② envoi du texte vers le LECAM pour calcul de la signature à partir de la compression du texte saisi

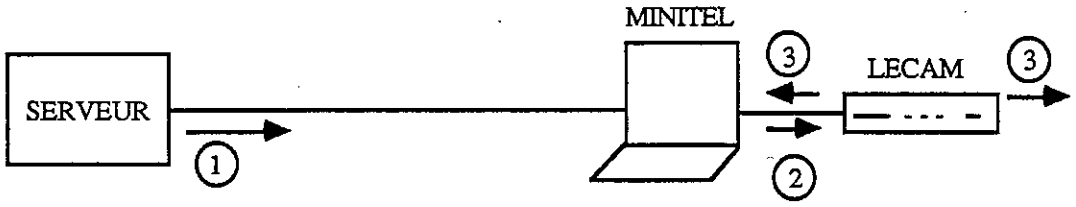
③ envoi du texte entre <d> et <f> par le LECAM vers le serveur sur consigne de fin de signature (FS)

④ envoi de la signature au serveur

Saisie chiffrée et signée

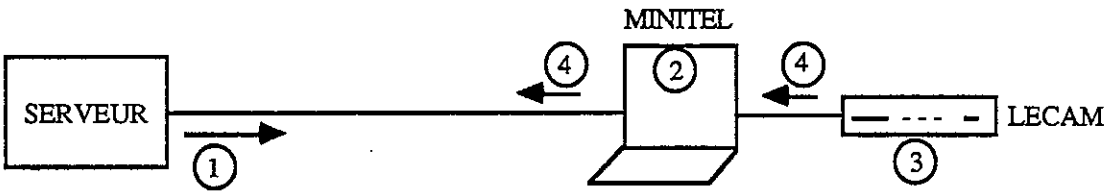
Combinaison de saisie chiffrée et de saisie signée : l'envoi de la signature succède à l'émission par le LECAM du message chiffré.

Affichage chiffré



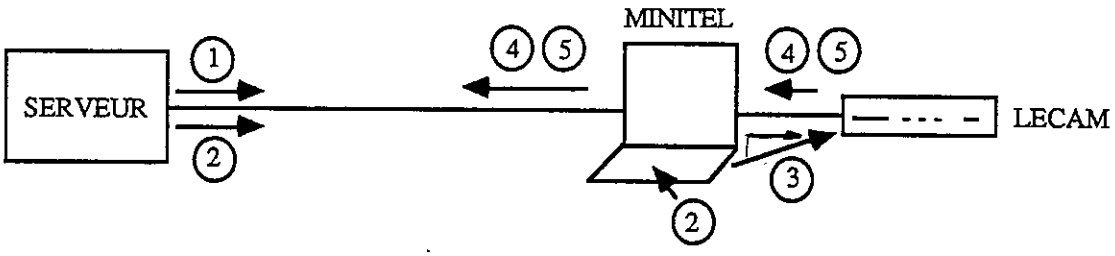
1. émission par le serveur d'un message chiffré
2. réception du message et déchiffrement par le LECAM
3. envoi du message déchiffré sur l'écran du Minitel et éventuellement sur les autres périphériques connectés sur le réseau Minitel

Affichage signé (et éventuellement chiffré)



1. émission par le serveur d'un message (en clair ou chiffré)
2. réception du message par le Minitel (après déchiffrement éventuel par le LECAM)
3. calcul d'une signature après compression par le LECAM du texte reçu (en clair ou chiffré)
4. la signature envoyée au serveur constitue un accusé de réception du message envoyé par lui-même

Affichage et saisie signés



① Initialisation de la signature : émission de la consigne AC (s = 1) ou de la première consigne SS.

② Emission par le serveur, entre <dc> et <fc>, du message à afficher et à signer et frappe du texte à envoyer avec une signature.

③ Envoi au LECAM du texte frappé au clavier du Minitel

④ Envoi au serveur, entre drapeaux <d> et <f>, du texte frappé, après passage dans l'algorithme de compression du LECAM.

⑤ Calcul et envoi de la signature au serveur sur réception de la consigne de fin de signature.

Affichage et saisie signés ou chiffrés en mode local

En mode local, tous les échanges se font avec le maître (c'est le cas, par exemple, de la connexion directe d'un LECAM avec un micro ordinateur). Ceci signifie que :

- le texte frappé au clavier (sur SS ou SC) est attendu du côté du maître,
- les messages affichés sur l'écran sont émis du côté maître (messages entre <dc> et <fc>,
- les messages à signer entre <dc> et <fc> doivent venir du côté du maître,
- la signature est émise du côté du maître.

Une description plus détaillée des mécanismes de signature et de chiffrement est donnée aux paragraphes 6. 1. 1 et 6. 1. 2.

1. 2. 6. 1 - Consignes de confidentialité

Pendant que le LECAM se prépare à faire exécuter une saisie chiffrée ou signée (initialisation du GOC, modification des aiguillages du Minitel), il faut éviter qu'il reçoive des caractères frappés au clavier qui pourraient alors transiter en clair sur la ligne, et qui n'entreraient pas dans le calcul de compression dans le cas d'une saisie signée. Le serveur peut contrôler la gestion de l'enchaînement correct des opérations d'initialisation et de début de saisie grâce aux consignes de début et de fin de confidentialité.
Il est **fortement recommandé** d'associer ces consignes aux consignes de saisie chiffrée ou signée.

a - Début de confidentialité

CD, Lg

CD = 49 (hexa)
Lg = 0

Le clavier est bloqué lors d'une émission vers le serveur (passage en mode distant).

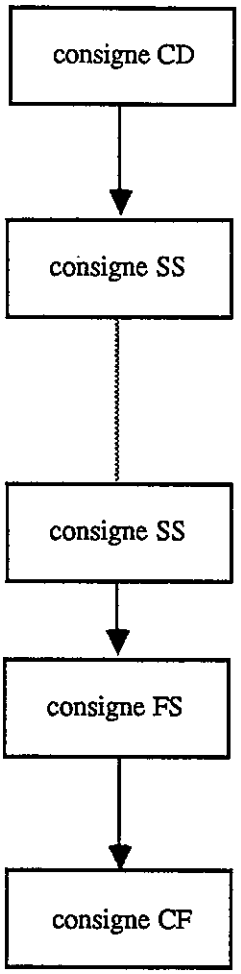
Cette consigne laisse le clavier du Minitel bloqué pour tous les passages en mode lecteur transparent qui vont suivre ; il est conseillé de faire précéder la première consigne de saisie chiffrée ou signée par cette consigne. Le clavier n'est débloqué par le lecteur que lorsque celui-ci est effectivement prêt à recevoir les caractères frappés par l'usager.

Cette consigne provoque, en plus des messages déjà affichés sur la rangée réservée du Minitel, l'apparition du message "Syst" pour signifier le mode "système", pendant lequel l'anticipation de lecture des touches frappées au clavier est interdite.

Le clavier est rebloqué automatiquement en fin de saisie.

Remarque :
Après réception de cette consigne par le LECAM, le dialogue usager n'est plus assuré en mode transparent entre le Minitel et le serveur.

Exemple :



- passage en mode distant pour acquitter CD
- retour au mode transparent avec le clavier du Minitel bloqué

- le LECAM débloque le clavier du Minitel pour autoriser la saisie
- aucune anticipation de frappe n'est possible

- fin de signature
- à l'issue de la réponse à FS, le clavier du Minitel est toujours bloqué

- déblocage clavier
- retour à une gestion normale du clavier

Note :
Toutes les consignes décrites ci-dessus font l'objet de messages applicatifs distincts (<d> une consigne <f> CR).

b - Fin de confidentialité

CF, Lg

CF = 4 B (hexa)
Lg = 0

Consigne inverse de la précédente, rétablissant l'aiguillage clavier vers modem, et effaçant le message "Syst".

1. 2. 6. 2 - Consignes de saisie

La gestion du curseur est à la charge du serveur pendant les consignes de saisie. La position du curseur n'étant pas restituée, le serveur doit donc repositionner le curseur sur le champ de saisie suivant après validation par l'usager de chaque champ saisi.

a - Saisie chiffrée

SC, Lg, ncs

SC = 59 (hexa)
Lg (1 octet) = 01
ncs (1 octet) = nombre de caractères à saisir, limité à 40.

Si la consigne CD a été activée, le clavier est débloqué lorsque le LECAM est prêt à faire effectuer la saisie. Le voyant "SECRET" clignote pendant tout le temps de la saisie. En fin de saisie, le lecteur bloque à nouveau le clavier et le message "Syst" réapparaît si la consigne CD est active.

b - Saisie signée

SS, Lg, ncs

SS = 5B (hexa)
Lg (1 octet) = 01
ncs (1 octet) = nombre de caractères à saisir, limité à 40.

Cette consigne provoque l'affichage du message "Sign" (signature) suivi de la lettre "D" (début) s'il s'agit de l'exécution de la première consigne de saisie signée.

Après validation de la saisie de chaque champ (par touche de fonction ou compte de caractères), le LECAM valide le tampon de saisie et fait entrer le message saisi dans le GOC de compression.

Si la consigne CD est active, le clavier est débloqué avant chaque saisie, et en fin de saisie, le lecteur bloque à nouveau le clavier et le message "Syst" réapparaît.

Lors d'une saisie signée ou chiffrée (les deux consignes pouvant se combiner), le lecteur s'assure que lors de la saisie, les données introduites au clavier ne sont jamais retransmises directement vers le modem, c'est-à-dire qu'il n'y a jamais modification des aiguillages du Minitel depuis la ligne de télécommunication.

c - Fin de signature

FS, Lg, adr

FS = 5 D (hexa)
Lg (1 octet) = 02
adr (2 octets) = adresse de lancement de l'interpréteur.

Cette fonction est activée pour comprimer un texte consécutivement à une saisie signée ou à un affichage signé.
Le comprimé du message est calculé puis rangé en zone interne de la mémoire du LECAM, non directement accessible par le serveur. L'interpréteur est activé à l'adresse "adr" pour calculer, par exemple, un certificat sur cette compression.
Le calcul de compression n'est effectué que si l'usager donne son accord : pour cela, le message "appuyer sur <ENVOI> pour signer le texte" est affiché sur la rangée de l'écran définie par la consigne de mise en mode. Si l'usager actionne une autre touche que la touche <ENVOI>, le résultat de la compression est annulé et un compte rendu d'erreur sur consigne est envoyé au serveur.
Le clavier n'est pas débloqué par cette consigne s'il y a eu une consigne CD émise par le serveur, d'autres saisies pouvant éventuellement suivre.

1. 2. 6. 3 - Consigne d'affichage chiffré ou signé

Cette consigne permet le déchiffrement par le LECAM de messages chiffrés envoyés par un serveur et destinés à être affichés sur l'écran du Minitel et éventuellement sur d'autres périphériques du réseau Minitel. De plus, la mise en œuvre de cette consigne permet d'envoyer une signature caractéristique du message reçu, et qui constitue donc un accusé de réception certifié.

AC, Lg, dest

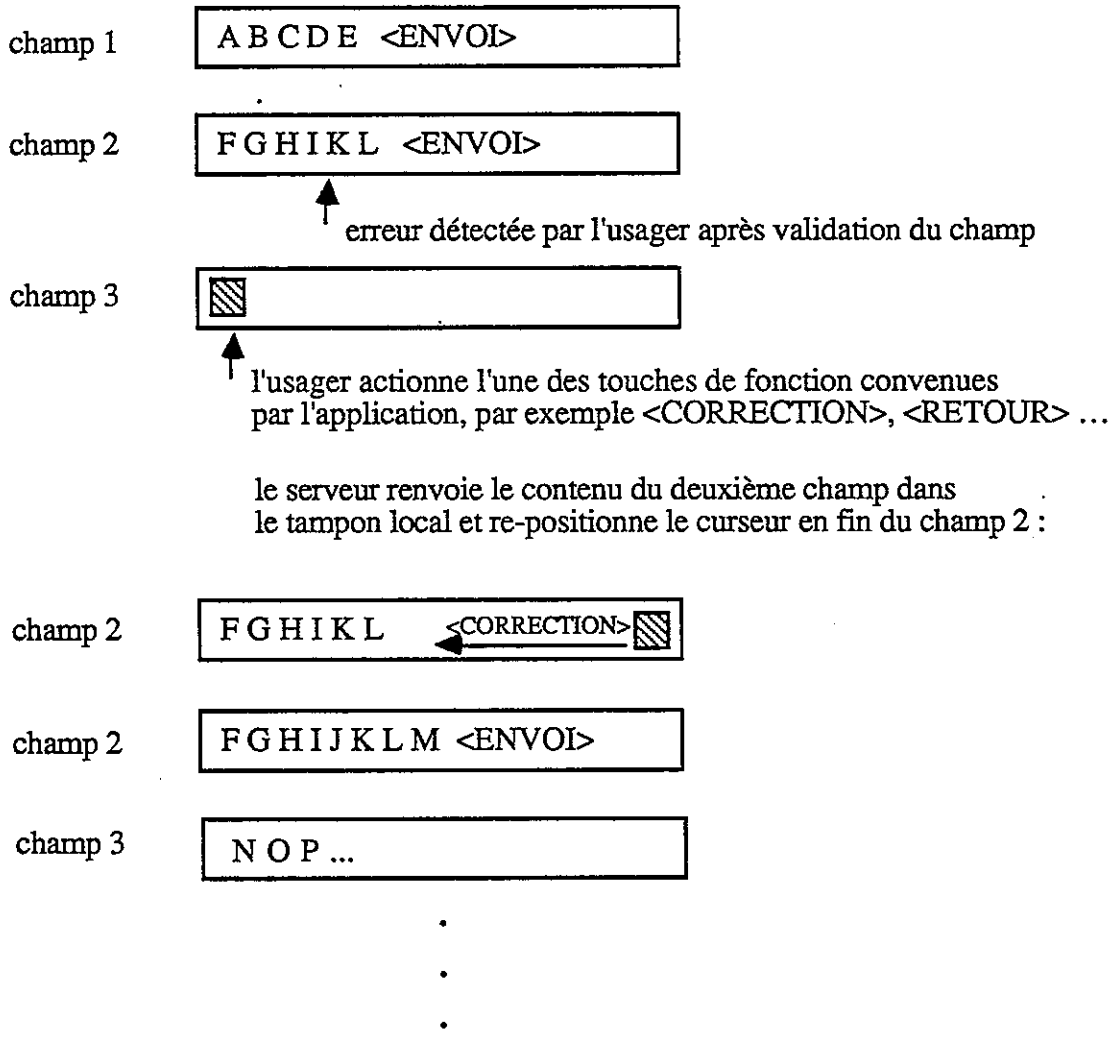
AC = 5F (hexa)
Lg (1 octet) = 01
dest (1 octet) = ... sab

- s = 1 les caractères entre les drapeaux de début et de fin de chiffrement interviennent dans un calcul de signature,
- s = 0 les caractères compris entre <dc> et<fc> n'interviennent pas dans un calcul de signature,
- a = 1 le texte chiffré reçu du module maître est renvoyé en écho sur l'écran du Minitel après déchiffrement. Il faut pour cela que la mise en mode ait été faite avec le bit 'd' égal à 1,
- a = 0 les données déchiffrées par le LECAM ne sont pas renvoyées vers l'écran du Minitel, quelle que soit la valeur du bit 'd' de la consigne de mise en mode,
- b = 1 le texte déchiffré par le LECAM doit servir à initialiser le tampon local de saisie du lecteur,
- b = 0 pas d'initialisation du tampon local de saisie.

Par défaut, les textes reçus chiffrés sont retransmis en clair, sans initialisation du tampon local de saisie : dest = 02.

Le texte déchiffré est aussi transmis vers les périphériques du réseau Minitel.

Remarque concernant le bit "b"
Le fait de positionner ce bit rend possible, en saisie chiffrée seulement, la correction d'un champ déjà validé par l'usager.
Par exemple, si l'usager a déjà saisi et validé deux champs, et qu'il se rend compte qu'il a fait une erreur dans la saisie du deuxième champ, il en informe le serveur en actionnant une touche de fonction autre que <ENVOI> au début du troisième champ à saisir. Le serveur peut alors renvoyer, dans le tampon local de saisie du LECAM, le contenu du deuxième champ, sans l'afficher à l'écran (celui-ci étant toujours visualisé sur le Minitel). Le curseur est impérativement positionné par le serveur en fin du deuxième champ de saisie, et l'usager peut donc corriger les données précédemment saisies avant de re-valider ce champ.



1. 2. 6. 4 - Contrôle par l'utilisateur

La rangée définie par la consigne de mise en mode (paramètre 'r') ainsi que le voyant vert "SECRET" sont utilisés par le LECAM pour indiquer son mode de fonctionnement :

le voyant "SECRET" clignote :
- pendant l'exécution de la consigne SC,
- pendant l'exécution de la consigne SS si elle est également chiffrée,
- pendant la phase de déchiffrement de données reçues entre <dc> et<fc>,

les consignes SS et AC provoquent l'apparition de "Sign" (signature), et éventuellement de "D" (début) s'il s'agit de l'exécution de la première consigne SS,

la consigne CD provoque l'apparition de "Syst" (mode système, anticipation de frappe clavier interdite).

Ces informations sont visualisées pendant toute la durée de la saisie (consignes SC et SS) ou jusqu'à l'appui sur <ENVOI> ou <ANNULATION> (consigne FS), ou pendant l'affichage du texte en clair. "Syst" est effacé par la consigne CF ou pendant la saisie de chaque champ se rapportant à une consigne SC ou SS.

Le voyant "SECRET" clignote, uniquement si les données sont chiffrées, pendant les saisies chiffrées ou signées ou en cours d'affichage chiffré.

Les textes sont affichés au début de la ligne réservée au lecteur, par exemple :

Syst

Syst Sign

Sign D

Sign

1. 2. 6. 5 - Tableau récapitulatif

Le tableau suivant présente les consignes à mettre en œuvre pour la réalisation des fonctions de sécurité, à savoir signature et chiffrement.

consigne mise en œuvre / fonctionnalités à réaliser	CH			CD	SC	SS	CF	AC			FS
	c	x	e					s	a	b	
Saisie chiffrée	oui			recommandé	n fois, selon le nombre de champs à saisir		recommandé				
	*	*	*								
Saisie signée	oui			recommandé		n fois, selon le nombre de champs à saisir	recommandé				oui
	0	*	*								
Saisie chiffrée et signée	oui			recommandé		n fois, selon le nombre de champs à saisir	recommandé				oui
	1	*	*								
Affichage chiffré	oui							facultative			
	1	*	*					0	*	*	
Affichage signé	oui							oui			oui
	0	*	*					1	*	*	
Affichage chiffré et signé	oui							oui			oui
	1	*	*					*	1	*	

chronologie d'envoi des consignes →

Si le bit 'a' de la consigne AC est égal à 1, il faut aussi que le bit 'd' de la consigne de mise en mode soit égal à 1.
Les bits désignés par '*' peuvent prendre les valeurs 0 ou 1.

Rappel :
La consigne CH est obligatoire pour faire du chiffrement, la consigne PR est facultative.

2 . LES REPONSES DU LECTEUR

2. 1 - Format des réponses

Le LECAM répond aux consignes qui lui sont destinées : à chaque consigne ou type de consignes envoyé par le serveur correspond une réponse émise par le lecteur. La forme générale de cette réponse est :

<d> données <f> <d> données <f> ..... <f> CR

<d> représente un drapeau "début"
<f> représente un drapeau "fin"
CR correspond au caractère de fin de message, codé 0D en hexadécimal.

On distingue trois types de réponses :

- la réponse à la mise en mode,
- la réponse à une demande de saisie signée ou chiffrée,
- la réponse à un fonctionnement normal du LECAM (consignes de chargement de programmes et de paramètres, d'exécution de l'interpréteur, d'initialisation de l'éditeur,...)

Les réponses correspondant à des demandes de saisie contiennent des données Vidéotex et sont donc transmises telles quelles, (elles ne sont pas sous la forme TLV), et comprises entre des drapeaux de début <d> et de fin <f>. Elles sont complétées par un deuxième bloc contenant des informations sur la façon dont la saisie s'est terminée.

Les autres réponses comportant des informations purement binaires (caractères non affichables par exemple) , sont transmises sous la forme de champs TLV et codées en P/1/6.

Le lecteur ne fournit une réponse que si le message transmis par le serveur l'a explicitement demandé.
Il faut pour cela que le bit SSP de l'octet IT contenu dans le dernier drapeau de début <d> émis par le serveur soit égal à zéro.
Dans le cas contraire, aucune réponse n'est envoyée au serveur par le LECAM, quelle que soit la consigne mise en œuvre et quel que soit l'état interne du LECAM après exécution de la consigne. Cependant, si le LECAM a détecté une erreur interpréteur, carte,... générant un mot d'état lecteur (MEL) ou un mot d'état carte (MEC) différent des valeurs par défaut, cette information est mémorisée dans le LECAM : elle est envoyée lors de la prochaine réponse du lecteur.

2. 2 - Codage des réponses sous forme TLV

2. 2. 1 - Identification lecteur

IL, Lg, TM, VM, TL, VL

IL = 70 (hexa)
Lg = 4
TM = 1 octet, type du matériel
VM = 1 octet, version du matériel
TL = 1 octet, type du logiciel
VL = 1 octet, version du logiciel

Ce bloc est transmis suite à une demande de mise en mode, quels que soient les paramètres utilisés dans la consigne CM.

Les lecteurs à connecteur simple "LECAM 100" (contacts en position haute) correspondent aux codes suivants :

TM : 01 VM : 00 TL : 01 VL : 02

Les lecteurs à connecteur double "LECAM 101" (contacts en position basse et haute) correspondent aux codes suivants :

TM : 01 VM : 01 TL : 01 VL : 03

2. 2. 2 - Mot d'état lecteur

EL, Lg, ME, [CC, TC] , [CI, adr] , [CT]

EL = 72 (hexa),
Lg = dépend du nombre de paramètres présents (les paramètres entre "[" et "]" sont facultatifs),
ME = un octet, toujours présent, indique l'état du lecteur.

ME = ... ET EI PC EC

Les bits de ME positionnés à 1 indiquent quelles sont les informations présentes dans le bloc :

ET = 1 une erreur de transmission a eu lieu, CT (1 octet) précise cette erreur,

PC = 1 carte présente (la carte n'a pas été arrachée depuis l'envoi du précédent mot d'état ou depuis la prise en compte de la consigne de mise en mode),

EC = 1 erreur consigne
CC : 1 octet indique le code erreur
TC : 1 octet indique le type de la consigne en erreur

EI = 1 erreur interpréteur
Deux cas sont à distinguer :
- erreur détectée par l'interpréteur (CI≥ 80 H)
  CI : 1 octet indique le code erreur
  adr : 2 octets indiquent l'adresse programme où l'erreur a été détectée

- erreur interpréteur générée par une instruction ABORT
  CI : 1 octet identique au code d'erreur application 'PAX' (CI < 80H)
  adr : si t = 0 (dans l'instruction ABORT),
  adr = R00,R01 (registres d'état application)
  si t = 1 (dans l'instruction ABORT),
  adr est égal à l'adresse de l'instruction de la dernière erreur traitée par ONERR.

Pour plus de détails se référer à l'instruction ABORT (partie III. chapitre 9.4).

Le mot d'état lecteur est transmis en fin de réponse du lecteur sauf pour les consignes de saisies chiffrées ou signées, si lors de la mise en mode on a demandé l'envoi systématique des compte-rendus de transmission (t = 1 dans la consigne CM).

Dans tous les cas, le mot d'état lecteur est fourni si une anomalie est rencontrée, par exemple si la carte a été arrachée (PC = 0). Si tel est le cas, cet état maintenu jusqu'à la prochaine consigne de mise en mode et la réponse EL avec le bit PC = 0 dans l'octet ME sera transmise systématiquement au maître.

La valeur par défaut (cas de bon fonctionnement) est :

ME = 02

Erreurs de transmission

L'octet CT peut être décomposé en deux quartets indépendants x et y :

CT = xE le modem n'est pas retournable

Les autres valeurs de y ne doivent normalement pas apparaître et correspondent à des anomalies dans les échanges : trafic anormal sur la liaison péri-informatique (provenant d'autres périphériques ou d'une mauvaise synchronisation entre les modules maître et esclave).

A titre indicatif les valeurs possibles exprimées en hexadécimal sont indiquées ci-dessous :

CT =	x1	PT inactif de façon anormale (défaut hardware)
	x2	pertes sur l'émission de données à gauche
	x3	pertes sur l'émission de données à droite
	x4	pertes sur l'émission d'éléments "Système d'Echanges" à gauche
	x5	pertes sur l'émission d'éléments "Système d'Echanges" à droite
	x6	pertes sur la réception d'éléments "Système d'Echanges" à gauche
	x7	pertes sur la réception d'éléments "Système d'Echanges" à droite
	x8	défaut sur la réception d'éléments "Système d'Echanges" à gauche
	x9	défaut sur la réception d'éléments "Système d'Echanges" à droite
	xA	pertes de données provenant du clavier
	xB	pertes de données P/1/6 (provoque l'envoi de la séquence <r>)

Le premier quartet peut prendre les valeurs suivantes :

CT =	8y	arrêt de réception de blocs P/1/6 (envoi de <r>)
	9y	envoi de 3 séquences <r> sans succès
	Ay	réception d'une séquence <r> incorrecte
	By	réception d'une séquence <r> pour un bloc inconnu
	Ey	interruption d'échanges à travers le LECAM supérieur à 10 s. Cette erreur n'est pas fatale et ne perturbe pas le fonctionnement du LECAM.

Erreurs interpréteur

L'octet CI peut prendre les valeurs suivantes :

CI =	80	instruction inexistante
	81	dépassement de capacité de la pile
	82	débordement de la zone programme
	83	instruction TRP avec pile pleine
	84	débordement de la zone registres
	85	instruction TPR avec pile vide
	88	violation de la zone locale
	90	erreur de syntaxe
	A0	opération impossible
	C0	délai d'acquisition clavier écoulé
	E0	erreur sur FS

Erreurs de consignes

Les erreurs sur les consignes sont codées sur huit bits décomposables en 2 quartets x et y.
Si y est différent de 0, le lecteur est occupé (par exemple, un programme interpréteur se déroule simultanément).Ce quartet n'a pas à être testé par l'application distante.

Le premier quartet peut avoir les valeurs suivantes :

CC =	1y	type de consigne inconnu
	2y	longueur incorrecte dans le TLV
	3y	paramètre incorrect
	4y	consigne refusée

2. 2. 3 - Mot d'état carte et mot d'état coupleur

EC, Lg, ME1, ME2, MDC

EC	=	74 (hexa)
Lg	=	3
ME1, ME2 (2 octets)	=	mot d'état carte. La signification de ces octets dépend du type de carte utilisée, et est donnée dans les différentes brochures d'utilisation des cartes
MDC (1 octet)	=	mot d'état coupleur carte.

La transmission du bloc EC est conditionnée par le bit 'c' de la consigne de mise en mode :

- si c = 0 : EC est envoyé en cas d'anomalie, avec les mots d'état représentant la dernière erreur rencontrée
- si c = 1 : EC est envoyé systématiquement avec la réponse du lecteur, mais les mots d'état reflètent l'état actuel de la carte après la dernière opération d'entrée/sortie carte, tentée ou réalisée.

La valeur par défaut du bloc EC est :

ME1 = 90 ME2 = 00 MDC = 00

Les valeurs de ME1 et ME2 ne sont exploitables que si MDC = 00.
Les valeurs que peut prendre MDC sont détaillées au paragraphe 5. 3.

2. 2. 4 - Octets de remise à zéro de la carte

RZ, Lg, données

RZ	=	76 (hexa)
Lg	=	nombre d'octets du champ "données" (variable)
données	=	octets transmis par la carte lors de la remise à zéro suivi du mot d'état carte (ME1, ME2) et du mot d'état coupleur carte (MDC).

Ces données sont transmises lors d'une mise en mode, à condition toutefois qu'une carte soit présente dans le LECAM à ce moment là.

Les données transmises représentent uniquement les données historiques décrites dans la documentation ISO référencée DIS 7816/3.

Le mot d'état coupleur (MDC) contenu dans la réponse RZ indique l'état actuel du coupleur carte.

2. 2. 5 - Données transmises par le LECAM

SE, Lg, données

SE	=	78 ou 79 (hexa) 78 : données transmises en clair 79 : données transmises chiffrées
Lg	=	nombre d'octets du champ "données" (variable)
données	=	octets transmis par le LECAM lors de l'exécution de l'instruction interpréteur SEND

Le LECAM transmet un ou plusieurs blocs d'informations à chaque fois qu'il rencontre une commande SEND dans le programme exécuté par l'interpréteur.

Ces blocs sont constitués d'ensembles au format TLV, dont les données sont automatiquement découpées de façon qu'un ensemble TLV ne soit jamais interrompu par les drapeaux de fin et de début de bloc : un champ TLV complet est donc rangé entre les drapeaux <d> et <f>.

Si l'octet type vaut 79, toutes les informations constituant la zone "V" du champ TLV sont chiffrées en fonction de la position courante du Générateur d'Octets Chiffrants, initialisé normalement par une consigne CH ou éventuellement PR (voir ces consignes).

On utilise les quatre bits de poids faibles de deux octets chiffrants successifs pour chiffrer un octet de données : le premier octet chiffrant obtenu permet de chiffrer le quartet de poids fort de l'octet de données, le second permet le chiffrement du quartet restant.

Le GOC n'est pas ré-initialisé implicitement entre deux ordres SEND.

2. 2. 6 - Indicateur de fin de saisie

IF, Lg, val

IF	=	7C (hexa)
Lg	=	1
val	=	1 octet 0 : fin de saisie sur compte de caractères maximum atteint 1 : fin de saisie sur délai inter caractères écoulé 2 : fin de saisie sur réception d'un message provenant du point d'accès (par exemple, réception, en cours de saisie, d'un message destiné à la rangée 0 du Minitel) autre valeur : "val" représente le code de la touche de fonction utilisée

Une touche de fonction est codée sous la forme SEP,X. "val" correspond à X.

Lors d'une saisie chiffrée ou signée (consignes SC et SS), un bloc sous forme TLV accompagne le texte Vidéotex saisi. Ce bloc renseigne le serveur sur la façon dont s'est terminée la saisie.

2. 3 - Réponse à une demande de mise en mode

La réponse à une demande de mise en mode est structurée en deux blocs.

<d> IL [RZ] <f> [<d> [EL] [EC] <f>] CR

Premier bloc
Réponse spécifique à la demande de mise en mode, c'est à dire :

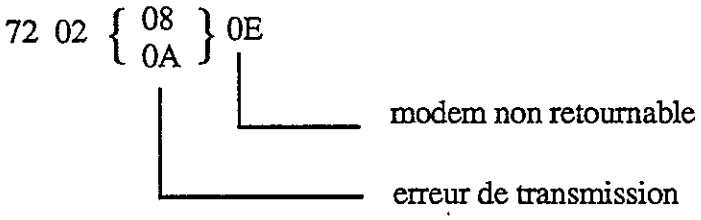
IL : identification lecteur ; cette information est toujours présente dans la réponse à une demande de mise en mode.

RZ : octets de RAZ de la carte, si une carte est présente.

Second bloc
Identique à une fin de réponse standard du lecteur, c'est à dire :

EL : état lecteur, si le bit 't' de la consigne de mise en mode est positionné, ou en cas d'anomalie.

Si la demande de mise en mode est la première après l'ouverture de session et si l'environnement modem utilisé n'est pas retournable, le LECAM envoie un mot d'état lecteur de la forme :



EC : état carte, état driver, si le bit 'c' de la demande de mise en mode est positionné, ou en cas d'anomalie.

Si le bloc est vide (EL et EC absents), les drapeaux <d> et<f> sont absents.

On a donc :

<d> IL [RZ] <f> CR

2. 4 - Réponse à une consigne de saisie ou d'affichage

a - Réponse à une consigne de saisie

La réponse est formée de deux blocs d'informations, chacun entre les drapeaux <d> et <f> :

<d> texte <f> <d> IF <f> CR

texte : il s'agit des informations Vidéotex (de 0 à 40 caractères) saisies au clavier, chiffrées ou signées, suivies éventuellement du CRC éclaté en 4 octets. Le CRC de 16 chiffres binaires s'écrivant en hexadécimal xyzt, est transmis sous forme de 4 octets : 3/x, 3/y, 3/z, 3/t.

IF: ce deuxième bloc, codé sous forme TLV-P/1/6 indique l'évènement fin de message.

b - Réponse à une consigne d'affichage

La réponse à la consigne d'affichage contient uniquement le mot d'état lecteur (EL) comme dans le cas d'une réponse standard du lecteur.

2. 5 - Autres réponses du lecteur

Si l'interpréteur a été lancé, la commande SEND provoque l'envoi d'un ou plusieurs blocs <d>...<f>, comportant chacun une seule unité TLV. Le découpage en plusieurs blocs est automatique si la longueur des informations transmises par l'ordre SEND contient plus de 96 octets utiles.

Les mots d'état lecteur ou carte, s'ils sont transmis, se trouvent dans un bloc séparé qui est le dernier bloc de la réponse.

La réponse standard du lecteur (hors mise en mode et saisie chiffrée/signée) est donc :

[<d> SE <f> ...] <d> [EL] [EC] <f> CR

Si EL et EC sont absents, les drapeaux <d> et <f> sont aussi absents.

La réponse à la plupart des consignes reçues par le LECAM est donc simplement : CR (consignes de chargement, d'initialisation de l'éditeur notamment).

3 . TABLEAU RECAPITULATIF : Réponses aux consignes reçues

Rappels

- Si le bit SSP du dernier drapeau de début de message <d> envoyé au LECAM est égal à 1, **aucune réponse** n'est faite par le lecteur.
- [<d> [EL] [EC] <f>] : l'envoi de ce bloc est conditionné par une anomalie devant être signalée (arrachage carte par exemple) ou par une demande de compte-rendu systématique faite lors de la mise en mode.
- [<d> SE <f>] : l'émission de ce bloc n'a lieu que si il y a exécution de l'ordre interpréteur SEND.
- [RZ] : n'est présent que si une carte se trouve dans le LECAM lors de la mise en mode.
- [EL] : est présent en cas d'anomalie ou si le bit 't' de la consigne de mise en mode est égal à 1.
- [EC] : est présent en cas d'anomalie ou si le bit 'c' de la consigne de mise en mode est égal à 1 et qu'une opération carte a été tentée suite à la dernière activation du lecteur.
- dans le cas où un bloc d'informations est vide, les drapeaux <d> et <f> sont absents.

Consigne reçue par le LECAM		REPONSE
Mise en mode	CM, Lg, mode, rg	<d>IL[RZ]<f>[<d>[EL][EC]<f>] CR
Chargement	C1, Lg, adr, données C2, Lg, données C3, Lg, n CC, Lg, adr, données	[<d>[EL]<f>] CR
Exécution	LI, Lg, adr FS, Lg, adr	[<d>SE<f>...][<d>[EL][EC]<f>] CR
Editeur	CA, Lg, texte CE, Lg, texte CS, Lg, val TC, Lg, val XS, Lg, val	[<d>[EL]<f>] CR
Sécurité	CH, Lg, type, synchro [,clé de déchiffrement] PR, Lg, rang	[<d>[EL]<f>] CR
Saisie et affichage	CD, Lg CF, Lg AC, Lg, dest	[<d>[EL]<f>] CR
	SC, Lg, ncs SS, Lg, ncs	<d>données Vidéotex saisies <f><d>IF<f> CR non codé en P/1/6 P/1/6

4 . L'INTERPRETEUR

4. 1 - Généralités

L'interpréteur est un sous-ensemble du module Application Carte. Il possède une mémoire de 1024 caractères dans laquelle sont chargés des programmes et des paramètres destinés à dialoguer avec la carte par le biais d'une application.

Il dispose pour cela d'instructions élémentaires de traitement des données, et d'instructions évoluées permettant la gestion de la mémoire, des échanges avec la carte, de l'interface avec le module Télécommunications, et du dialogue avec l'écran et le clavier du Minitel.

Certaines de ces instructions sont appelées **directives** parce qu'elles ne sont pas exécutées immédiatement, mais seulement après la rencontre d'une condition particulière.

Une instruction est l'opération la plus élémentaire de l'interpréteur, elle est intégralement exécutée avant passage à l'instruction suivante.
Les objets manipulés par les instructions de l'interpréteur sont des données situées à différents emplacements de la mémoire du lecteur :

- zone programme interpréteur,
- zone registres interpréteur,
- zone interne réservée à l'interpréteur,
- zone réservée aux entrées/sorties lecteur.

La zone programme est une zone de 768 octets contigus destinée à recevoir des données quelconques pouvant représenter une suite d'instructions interprétables, des tampons (de rangement ou de paramètres), éventuellement des textes,...

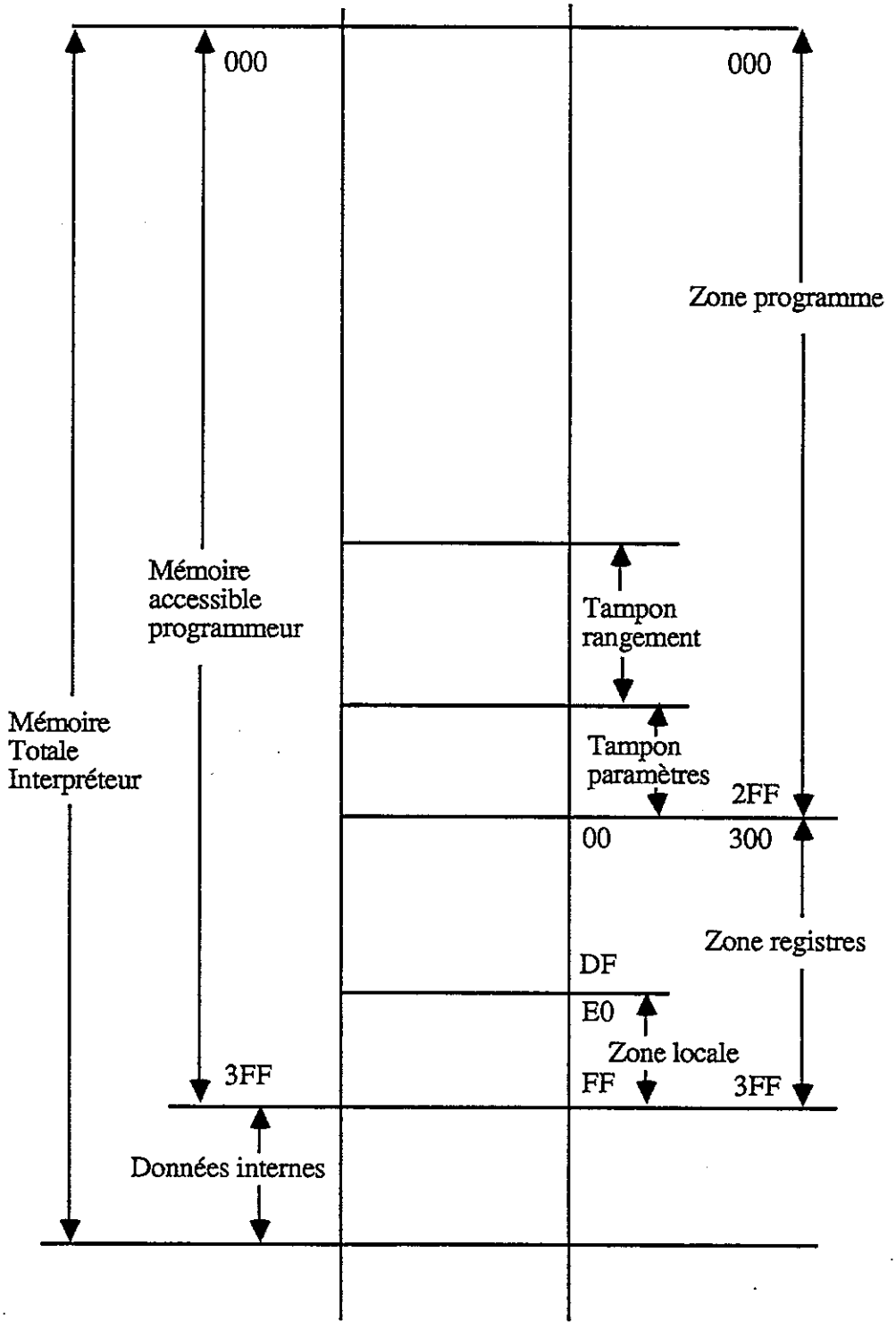
Cette zone, de l'adresse 0 à 2FF (hexadécimal) est accessible aux consignes de chargement et de lancement de l'interpréteur. Son organisation est soumise à l'initiative du programmeur.

La zone registres est une zone de 256 octets contigus constituant les données de l'interpréteur. Son adresse logique fait suite à la zone programme. Elle est accessible aux consignes de chargement, de l'adresse 300 à l'adresse 3FF (hexadécimal). Un registre est une donnée de un octet accessible par l'interpréteur par son numéro, qui est équivalent à son nom ou à son adresse. Le registre 0, noté R0, correspond à l'adresse mémoire 300.

Un bloc de registres est une collection de registres contigus qui est définie par sa longueur en nombre de registres et son adresse, qui est le numéro du premier registre de la collection (celui du numéro le plus faible).

Un tampon est une collection d'octets contigus définie par son adresse de base et sa longueur. L'adresse de base est définie dans les registres réservés et la longueur représente le nombre d'octets contenus dans le tampon. Elle est gérée par l'interpréteur et ne peut excéder 255 octets.

Illustration d'une partition mémoire de l'interpréteur



Remarque :
Pour le LECAM 100, le tampon de rangement est limité à 02FE (H) alors que pour le LECAM 101 il est limité à 02FF (H)

4. 2 - Fonctionnement

4. 2. 1 - Les instructions de l'interpréteur

Ce paragraphe a pour but de donner un aperçu des possibilités de l'interpréteur LECAM, la troisième partie de ce manuel décrira en détail les instructions de l'interpréteur.

a - Les directives
L'interpréteur dispose de deux directives : l'une (ONERR) sert à définir les conditions de débranchement en cas d'anomalie, l'autre (SWB) conditionne le prochain ordre entrant ou sortant.

b - Les instructions de chargement
Elles permettent d'initialiser ou de charger un bloc de registres de longueur prédéterminée.

c - Les instructions de transfert de données
Leur fonction est de permettre l'échange sélectif de données entre des éléments de la zone registres et tout autre élément de la mémoire interpréteur.

d - Les instructions arithmétiques et logiques
Ce sont les fonctions de calcul de l'interpréteur (addition et soustraction entre deux opérandes d'égales longueurs), les fonctions booléennes ("et logique", "ou logique", "ou exclusif"), les fonctions de complémentation à un et de complémentation à deux.

e - Les utilitaires binaires
Leur rôle est de faciliter la manipulation des données : décalage et rotation à gauche et à droite de positions binaires dans un registre ou un bloc de registres, conversion de données.

f - Les instructions de branchement
L'interpréteur du LECAM dispose d'instructions permettant d'évaluer la réalisation d'une condition logique ou arithmétique rendant possible le branchement conditionnel à une adresse définie du programme, et d'instructions de branchement inconditionnel ou d'appel à un sous-programme.

g - Les instructions d'entrées/sorties lecteur
Ces instructions ne sont pas "vues" de la même façon selon que le LECAM est gestionnaire du Minitel ou pas :

- dans le premier cas, ces instructions permettent de gérer l'affichage et la saisie d'informations sur le Minitel, et l'envoi de données au serveur (gestion de la rangée dédiée du Minitel, retournement du modem du Minitel, gestion des aiguillages du Minitel),

- dans le second cas, ces instructions permettent de gérer l'affichage et la saisie d'informations sur le maître, ainsi que l'envoi de données vers le maître (au sens Système d'Echanges du terme). Le maître peut être par exemple un micro ordinateur personnel.

h - Les instructions d'entrées/sorties carte
Le LECAM est doté d'instructions évoluées pour dialoguer avec la carte à micro-circuit. Ces instructions sont aussi appelées ordres entrants et ordres sortants : par exemple, une demande d'écriture dans la carte est un ordre entrant (les données "entrent" dans la carte), une demande de lecture dans la carte est un ordre sortant (les données "sortent" de la carte).

Le programmeur dispose de plusieurs instructions de lecture et d'écriture, d'instructions de recherche dichotomique ou séquentielle de données en fonction d'un profil déterminé, d'instructions permettant d'enchaîner automatiquement un ordre sortant après un ordre entrant (par exemple, demande de résultat d'un calcul) et d'ordres de mise sous-tension et hors-tension de la carte.

i - Les instructions d'arrêt de l'interpréteur

L'interpréteur dispose de deux instructions d'arrêt : l'une correspond à l'arrêt normal de l'interpréteur, l'autre à l'arrêt provoqué par la détection d'une anomalie.

Une erreur de programme rencontrée en cours d'exécution d'une instruction entraîne l'arrêt de l'interpréteur si l'instruction en question n'est pas précédée par une directive de débranchement en cas d'erreur (dans ce dernier cas le programme continue son déroulement à l'adresse indiquée par la directive de débranchement).

Les erreurs possibles sont :

- instruction inexistante
- débordement du programme
- débordement des registres
- violation de la zone locale
- erreur de syntaxe
- délai inter-caractères écoulé (en saisie)
- opération impossible (tentative d'utilisation de l'instruction RKEY avec une carte comportant un bloc de sécurité, par exemple)
- dépassement de la pile des adresses de retour programme
- débordement du tampon de rangement
- débordement du tampon de paramètres.
- erreur sur FS

5 . L'INTERFACE CARTE

5. 1 - Généralités

Les échanges avec la carte se font conformément au projet de norme DIS 7816/3 de l'ISO, et notamment :

- fréquence d'horloge : 3,579545 Mhz
- taux de modulation : 9600 bauds
- tension d'écriture dans la mémoire de la carte : 5 à 25 Volts par pas de 1V
- courant de programmation : 50 mA
- délai de détection carte muette : 1 seconde

Le nombre maximum d'octets échangés par un seul ordre carte est limité à 29 pour les ordres entrants et à 32 pour les ordres sortants.

L'universalité du LECAM fait qu'il peut recevoir, dans la fente d'introduction qu'il présente sur la face avant, tous les types de cartes répondant à cette norme.

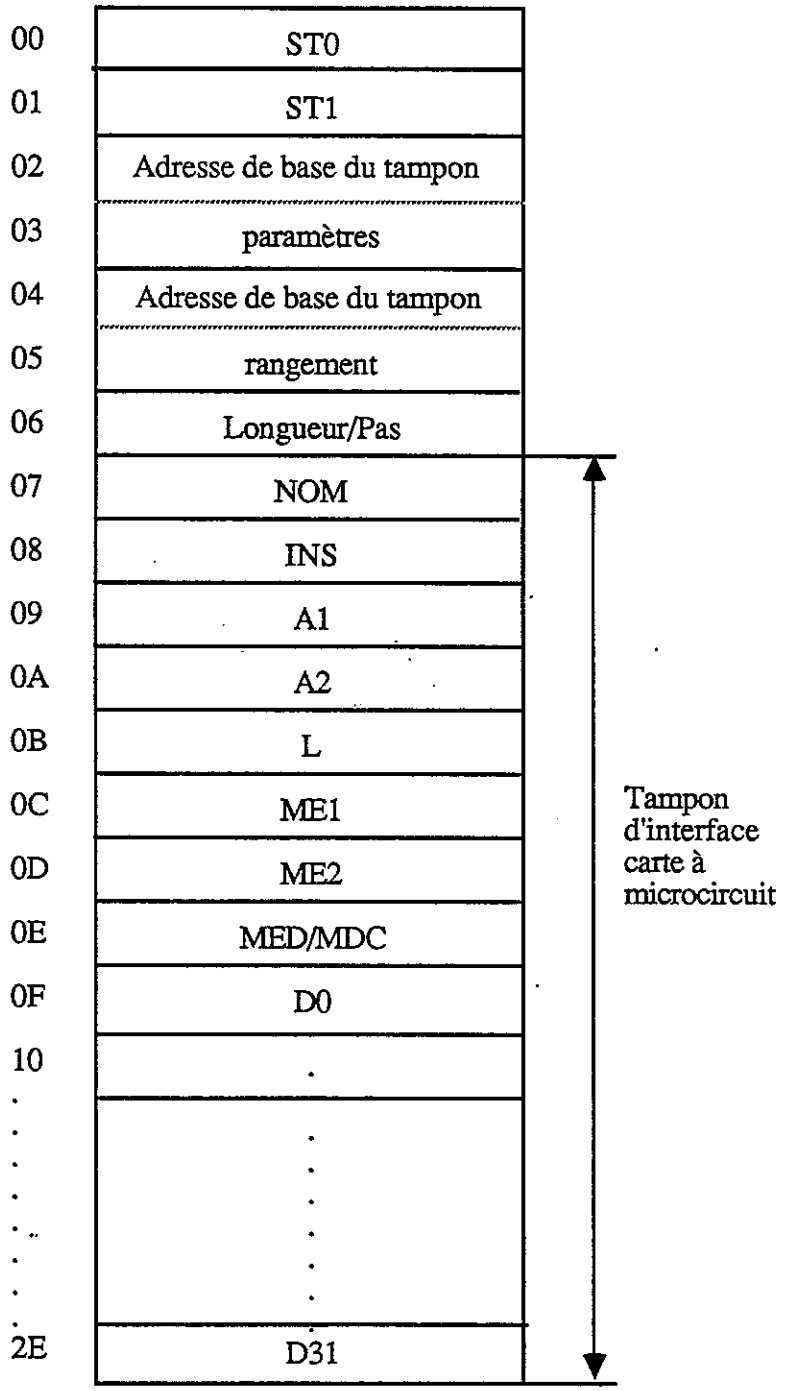
Le lecteur ne peut donc pas faire de contrôles spécifiques, et en particulier, les applications serveur doivent vérifier, si cela est nécessaire, que les durées de mise sous tension de la carte ne sont pas excessives.

En cas de déconnexion du Minitel ou du serveur, le lecteur met de toute façon la carte hors tension pour pallier l'absence de contrôle par le serveur.

5. 2 - Fonctionnement

L'interface carte constitue une passerelle entre l'interpréteur et la carte. Elle est capable de renseigner sur l'état de la carte et du coupleur ; c'est par elle que transitent les ordres entrants et sortants à destination de la carte, sauf ceux concernant les blocs de sécurité.

Les registres 07 à 2E (notation hexadécimale) de la mémoire RAM du LECAM constituent le tampon d'interface de la carte à micro-circuit.



Les registres réservés R00 à R06 sont décrits au chapitre 9. 1. 1.

Remarque :
Le tampon d'interface carte peut servir à stocker temporairement des données ne résultant pas d'une instruction d'entrée/sortie avec la carte.
Les registres d'adresses hexadécimales 0F à 2E correspondent en principe aux données lues ou à écrire dans la carte mais peuvent être utilisés par l'application si celle-ci n'a pas d'opération d'entrée/sortie à réaliser avec la carte.
Cette remarque s'applique également si les échanges avec la carte n'utilisent pas la totalité des registres disponibles pour ces opérations. Par exemple, si le nombre d'octets échangés par un ordre d'entrée/sortie avec la carte n'excède jamais 20, les 12 registres restants peuvent servir à stocker n'importe quel type de données.

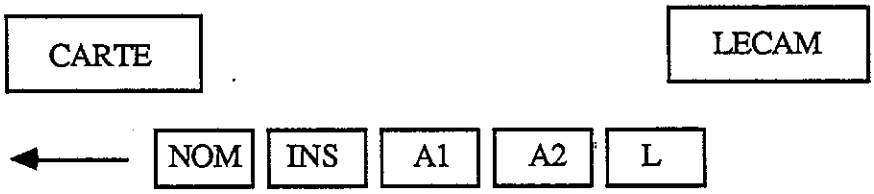
R07 : registre NOM d'application utilisé par toutes les instructions d'entrées/sorties carte par recopie de son contenu dans l'ordre AFNOR transmis à la carte. Par exemple, le NOM d'application pour les cartes M4 est "BC".

R08 : registre INStruction contenant l'ordre AFNOR transmis à la carte lors des opérations d'entrées/sorties carte. Un ordre de lecture sera par exemple codé "B0" pour les cartes M4.

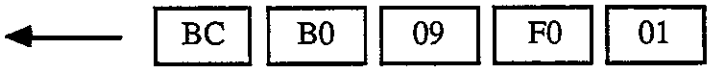
R09, R0A : bloc de registres "adresse carte" contenant les paramètres A1, A2 transmis à la carte lors des opérations d'entrées/sorties. A1 correspond à l'octet de poids fort de l'adresse, A2 à celui de poids faible.

R0B : ce registre contient la longueur en octets des données à transférer, dans un sens comme dans l'autre, entre la carte et le LECAM.Il est rappelé qu'on ne peut pas faire "entrer" dans la carte plus de 29 octets ou sortir de la carte plus de 32 octets à la fois. Ce registre est initialisé ou modifié par le registre R06 (pour les instructions de l'interpréteur utilisant ce registre de façon implicite telles que par exemple READ et WRITE) qui définit la longueur en octets d'un mot dans la carte et le pas d'adressage utilisé par les ordres entrants et sortants (le pas d'adressage correspondant à la différence d'adresse entre deux mots de la carte).

Le format général de l'en-tête des ordres entrants ou sortants à destination de la carte est donc de la forme :



Par exemple, l'ordre :



correspond, pour une carte M4, à une demande de lecture d'un octet à l'adresse 09F0.

R0C, R0D : registres "état carte" dans lesquels sont rangés les Mots d'Etat ME1 et ME2 à l'issue de chaque demande d'exécution d'un ordre entrant ou sortant dans la carte. Ces registres ne sont interprétables que si le contenu du registre R0E est égal à zéro.

R0E : registre "état coupleur carte à micro-circuit" contenant le Mot D'état Coupleur MDC à l'issue d'une opération d'entrées/sorties carte.

R0F à R2E : bloc de 32 registres de données contenant les données reçues de la carte à l'issue des opérations d'entrées/sorties carte comportant un ordre sortant. En particulier, les registres à partir de R0F contiennent, après exécution de l'ordre RAZ (qui n'est d'ailleurs pas un ordre au sens strict du terme, car il est activé par un signal électrique sur le contact RAZ de la carte à l'introduction de celle-ci dans le lecteur), les octets complémentaires consécutifs à l'ordre de RAZ de la carte qui permettent à l'application d'identifier la carte en présence et d'indiquer la phase de vie dans laquelle elle se trouve.

5. 3 - Les mots d'état carte et coupleur

A la fin de l'exécution de chaque ordre entrant ou sortant, la carte envoie deux octets ME1 et ME2 qui constituent le compte-rendu d'exécution de l'ordre, et qui sont appelés les mots d'état de la carte : ils sont stockés dans les registres R0C et R0D.

Un troisième mot d'état, noté MDC, rangé dans le registre R0E, constitue le mot d'état du coupleur du lecteur.

Ces trois mots d'état sont envoyés à l'application, selon que le bit "c" de l'octet "mode" de la consigne de mise en mode (CM) est positionné ou pas, ou systématiquement en cas d'erreur (mots d'états différents respectivement de 90, 00, 00).

Les valeurs que peuvent prendre ME1 et ME2 varient selon les cartes utilisées. Les valeurs (hexadécimales) prises par MDC varient selon les ordres exécutés ; elles sont les suivantes :

après un ordre de RAZ :

00	fonctionnement normal
04	ordre inconnu
05	erreur interne au coupleur
A0	carte non supportée
A2	carte muette
A3	erreur de parité
F0/F3	détection de court-circuit
F7	carte arrachée
FB	carte absente

après un ordre entrant :

00	fonctionnement normal
04	ordre inconnu
05	erreur interne au coupleur
E2	carte muette
E3	erreur de parité
E4	octet d'acquittement faux
E5	rupture de séquence à l'initiative de la carte
F7	carte arrachée

après un ordre sortant :

00	fonctionnement normal
04	ordre inconnu
05	erreur interne au coupleur
E2	carte muette
E4	octet d'acquittement faux
E5	rupture de séquence à l'initiative de la carte
F7	carte arrachée

6 . LE MODULE DE SECURITE DU LECTEUR

6. 1 - Généralités

Les fonctions d'identification, d'authentification et de certification sont des fonctions directement gérées par la carte à micro-circuit : le microprocesseur de la carte est donc totalement garant de la sécurité de ces opérations.

Les fonctions de chiffrement et de signature mettent en jeu la combinaison lecteur-carte : le lecteur doit donc dans ce cas garantir que les opérations effectuées avec la carte de l'usager servent uniquement à établir la clé du chiffrement, ou la signature du texte effectivement échangé.

Or la réalisation de ces calculs peut être extrêmement différente selon les types de cartes. L'universalité du lecteur nécessite donc, pour que ces fonctions soient réalisées en toute sécurité, que ce soit la carte elle-même qui indique au lecteur quelles sont les opérations réalisées pour calculer une clé de chiffrement ou établir une signature.

Le lecteur suppose seulement que l'obtention d'une clé de chiffrement corresponde au schéma suivant :

- exécution d'un ordre entrant permettant d'effectuer un calcul,
- exécution d'un ordre sortant fournissant la clé de chiffrement.

L'établissement d'une signature correspond à un schéma analogue :

- exécution d'un ordre entrant dont les données comportent le comprimé caractéristique du texte à signer, et permettant d'effectuer un calcul ,
- exécution d'un ordre sortant fournissant la signature (le LECAM accepte n'importe quel ordre sortant, il ne contrôle pas).

Dans les deux cas le LECAM doit donc surveiller tous les ordres entrant dans la carte, afin de vérifier s'ils correspondent à une demande de calcul ou de signature.

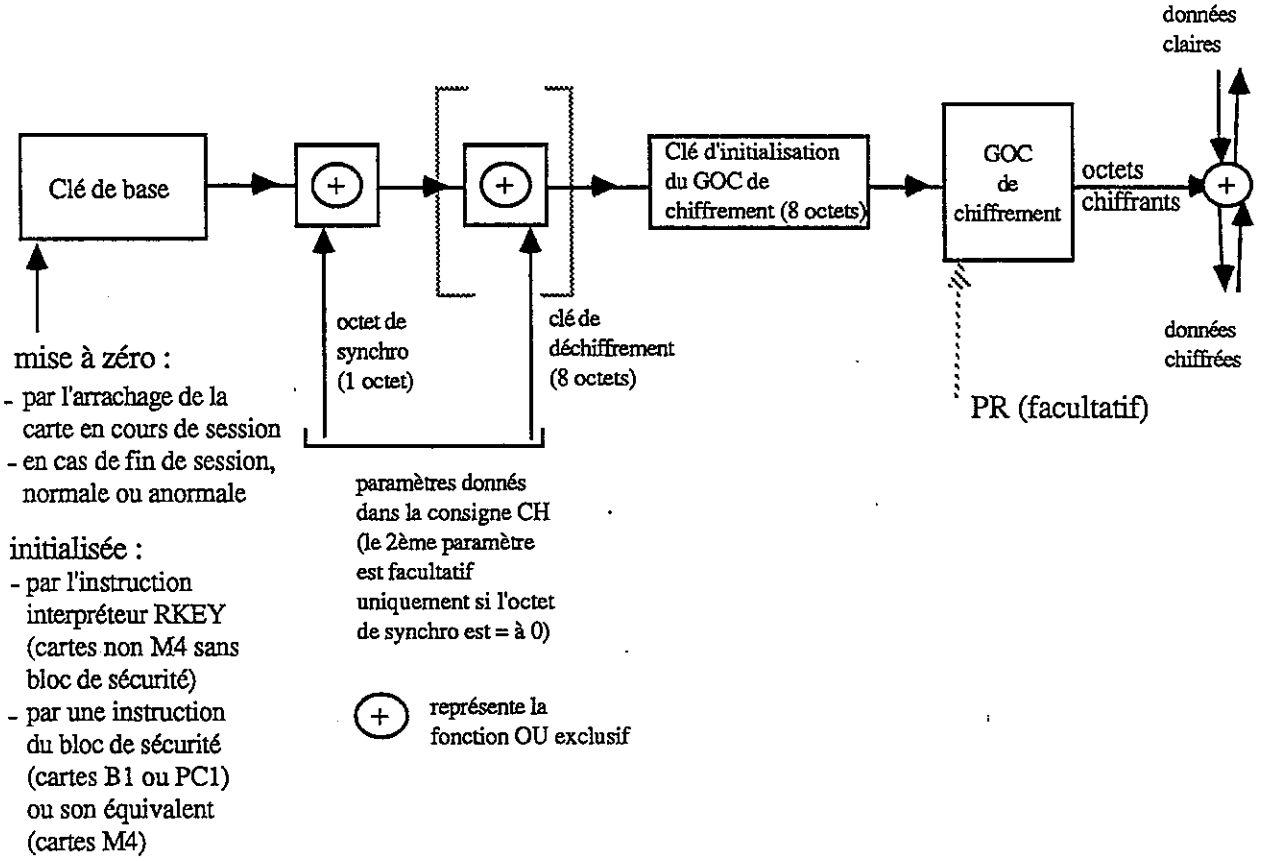
Si l'ordre entrant est une demande de calcul de clé de chiffrement, le lecteur provoque automatiquement l'ordre sortant de demande de résultat et initialise la clé de base, rangée en zone interne de la mémoire de l'interpréteur.

6. 1. 1 - Chiffrement

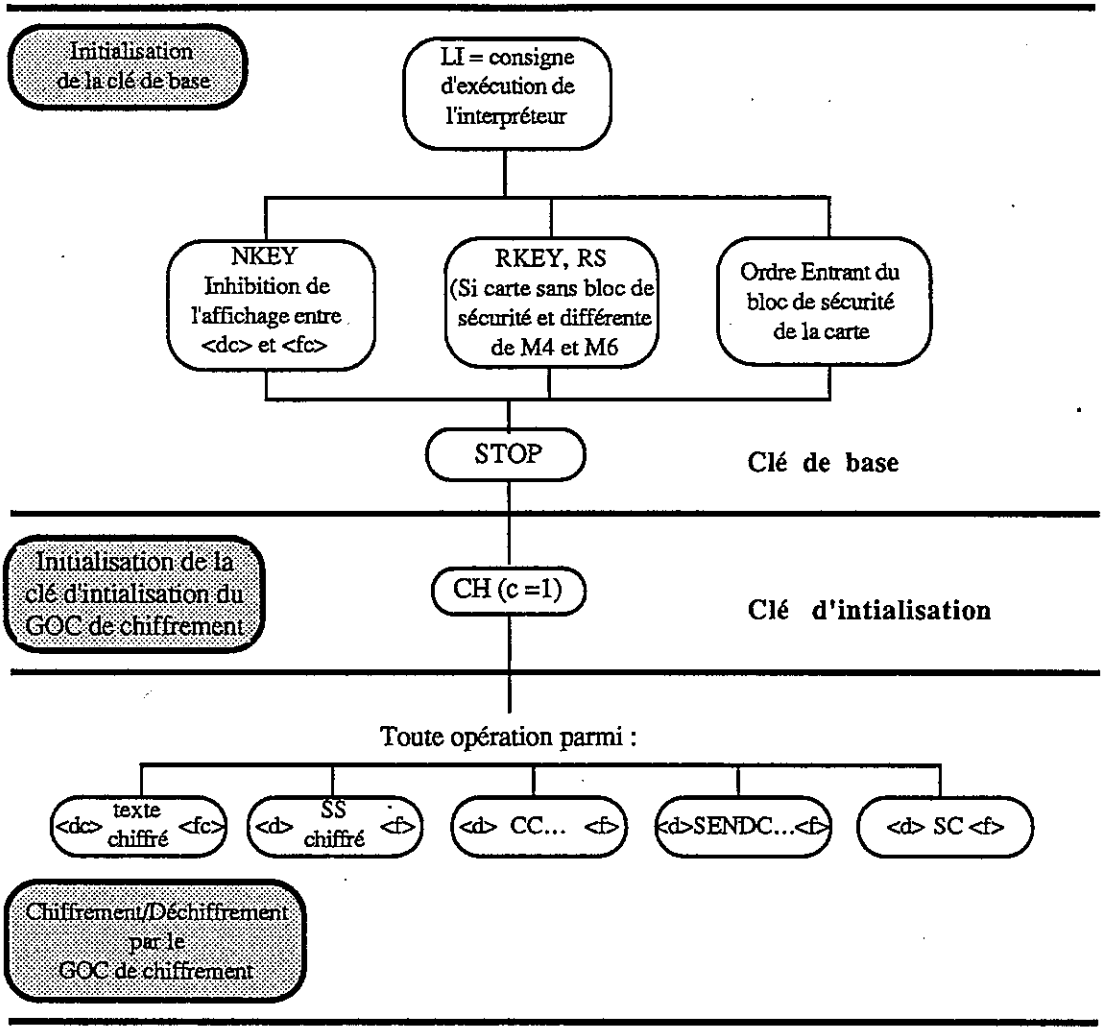
La clé de chiffrement est le résultat d'un calcul avec comme données entrantes une suite aléatoire. Lorsque le LECAM exécute l'ordre entrant de calcul , il enchaîne automatiquement l'ordre de demande de résultat correspondant et transfère le résultat obtenu dans une zone interne de la mémoire du lecteur .

Ce résultat est utilisé, conjointement avec une consigne CH, pour initialiser la clé du générateur d'octets chiffrants, selon le schéma suivant :

METHODE D'INITIALISATION DU GOC DE CHIFFREMENT



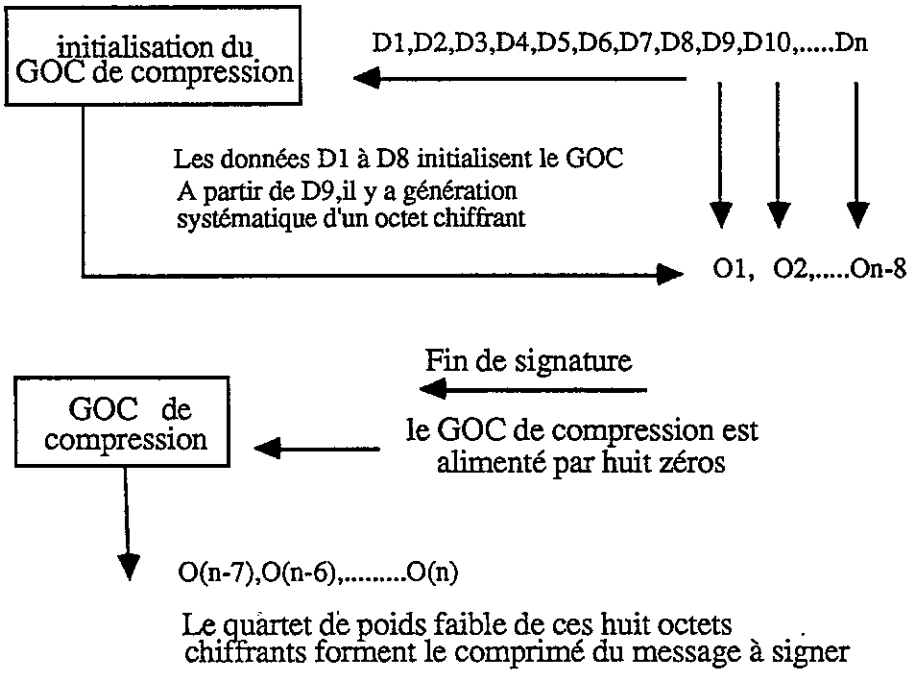
Mise en œuvre du chiffrement



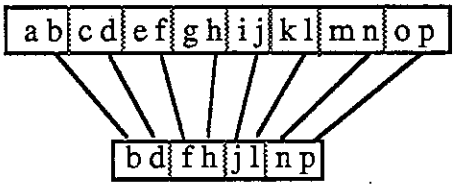
6. 1. 2 - Signature

Si l'ordre entrant est une demande de calcul pour signature, une partie des données entrant dans la carte est remplacée par le comprimé précédemment calculé : pour pouvoir établir une signature, le lecteur élabore une compression du texte échangé soit par l'instruction interpréteur DIAL, soit par les consignes de saisie ou d'affichage signé, suivies d'une fin de signature.

Méthode de formation du comprimé



Les huit premiers caractères du message à signer (D1 à D8) initialisent le GOC de compression.Tous les caractères suivants provoquent la génération d'un octet chiffrant (O1 à On-8), qui ne sert qu'à faire "tourner" le GOC de compression.Sur réception d'une fin de signature, le GOC de compression est alimenté par huit octets à zéro qui vont générer les huit derniers octets chiffrants; les quatre bits de poids faible de chacun de ces octets chiffrants servent à former le comprimé sur quatre octets selon le schéma suivant :



Le comprimé obtenu est parfaitement caractéristique du texte échangé, et est rangé dans une zone spécifique du lecteur. Cette zone ne peut être ni lue ni écrite directement par un programme téléchargé.

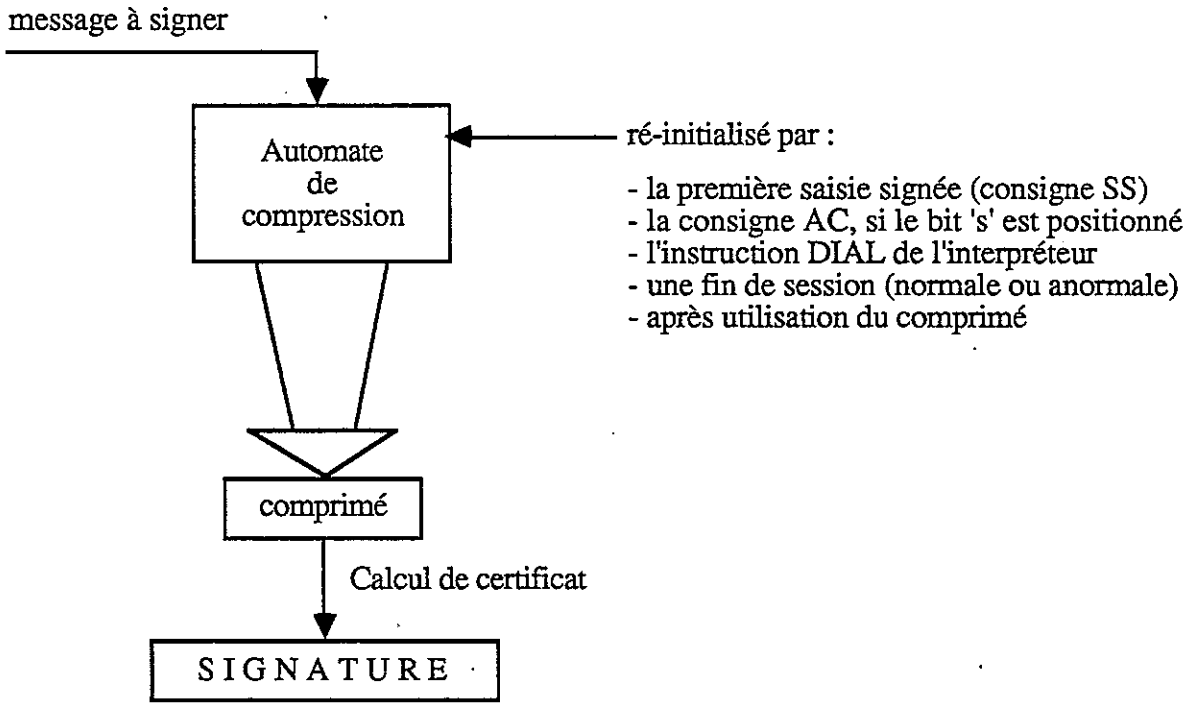
Lorsqu'un programme téléchargé exécute un ordre entrant correspondant à une demande de signature, le lecteur remplace alors automatiquement quatre octets des données entrantes par le comprimé précédemment obtenu :

données entrantes initiales : E1 E2 E3 E4 E5 E6 E7 E8
données effectivement entrantes : E1 E2 co-mp-ri-mé E7 E8

Le comprimé est remis à zéro après utilisation. Le programme téléchargé peut ensuite effectuer une demande de résultat : les données reçues de la carte forment la signature.

Rappel :
Le mécanisme de signature ne peut être activé s'il n'est pas décrit dans un bloc de sécurité.

Signature : principe de fonctionnement

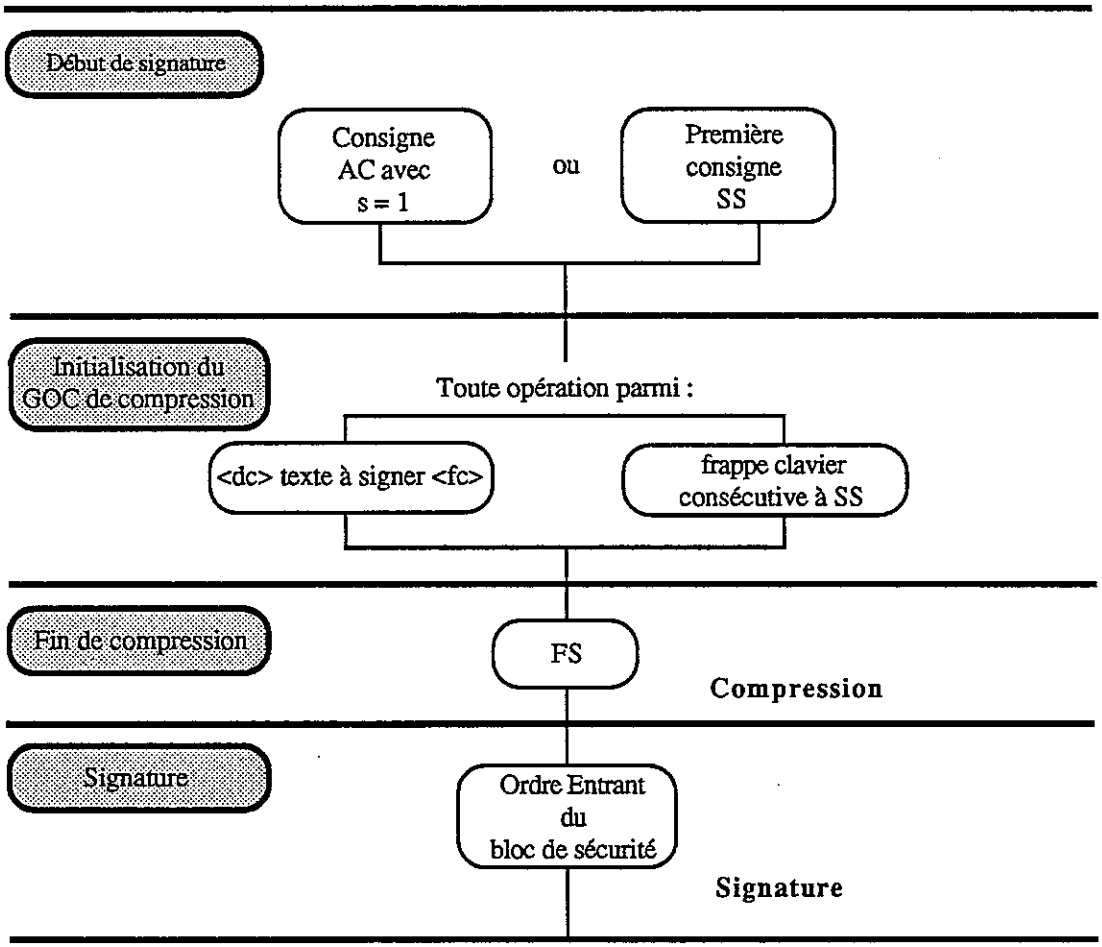


La description détaillée des ordres permettant la mise en œuvre du chiffrement et de la signature est contenue dans un bloc spécial de la carte de l'usager : c'est le bloc de sécurité.

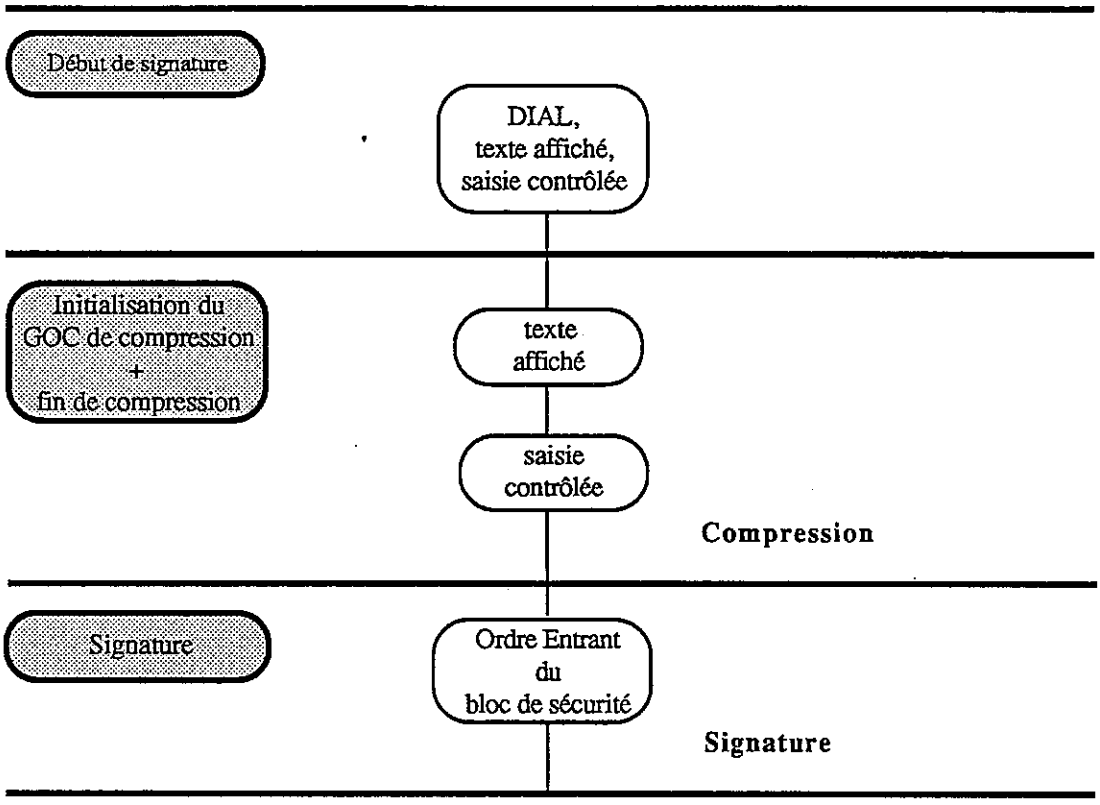
Les cartes de type M4 ou M6 ne contiennent pas de bloc de sécurité. Les informations nécessaires à l'obtention d'une clé de chiffrement ou à l'établissement d'une signature pour ces cartes sont implicites. Elles sont décrites à partir du paragraphe 6. 2. 3 -.

Mise en œuvre de la signature

Signature par consignes



Signature par DIAL



Conditions de RAZ du GOC de compression :

- arrachement carte,
- fin de session,
- FS,
- début d'exécution de DIAL,
- un caractère reçu hors <dc>.....<fc> alors qu'une compression est en cours (hors rangée 0 qui est filtrée).

Conditions de RAZ du comprimé sur fin de compression :

- arrachement carte,
- fin de session,
- utilisation de la compression pour signer (présentation de la compression dans le message d'entrée de l'ordre Entrant du bloc de sécurité).

6. 2 - Fonctionnement

6. 2. 1 - Blocs de sécurité

Le bloc de sécurité, pour les cartes dont le nom application est "BC" (cartes M4 et B0) ou "CC" (cartes M6), est stocké en permanence dans la mémoire du LECAM, et n'a donc pas à être enregistré dans la carte.

Pour toutes les autres cartes (B1 et PC1 notamment), ce bloc est recherché dans la carte elle-même lors de l'exécution de la consigne de mise en mode. Cela suppose que la carte est capable de comprendre l'un des ordres de recherche sur argument selon le protocole B1 ou PC1.

Le bloc de sécurité est formé d'un en-tête particulier permettant de l'identifier. Cet en-tête est constitué de deux octets pour les cartes B1 et d'un mot complet (quatre octets) pour les cartes de type PC1, dont les profils (en notation hexadécimale) sont les suivants :

B1 :	2E 24	(prestataire 36, ouvert sous clé émetteur)
PC1 :	40 24 00 00	(IAU = 24 00 00)

Ces informations sont en lecture libre, et donc accessibles sans condition.

Le contenu des blocs est constitué d'une suite d'octets, rangés à raison de 3,5 octets par mot (les quatre bits "système" sont ignorés). La fin de bloc est complétée par des bits à '1'.

La chaîne d'octets ainsi enregistrée est structurée sous forme TLV :

T	:	type	(un octet)	nature des informations qui suivent
L	:	longueur	(un octet)	longueur du champ suivant
V	:	données	(L octets)	

Les types d'informations sont les suivants (valeurs hexadécimales) :

T = 10 ordre entrant à surveiller pour les calculs de signature,
T = 11 position du champ où placer le comprimé dans les données entrantes,
T = 20 ordre entrant utilisé pour le calcul de la clé de chiffrement,
T = 21 ordre sortant à exécuter pour obtenir la clé de chiffrement,
T = 22 idem à 21, mais l'ordre sortant est suivi d'une mise hors tension.

Chaque information est facultative et un type inconnu ne perturbe pas le fonctionnement du lecteur. Les blocs de sécurité sont limités à 52 octets.

Exemples de blocs de sécurité

Carte B1

2	E 2 4 1 8 0 0
3	2 0 0 7 3 1 8
3	4 0 0 4 8 F F
3	F F F F 1 0 0
3	7 3 1 8 0 0 0
3	4 8 F F F F F
3	F F F F F F F

T = 20 ordre entrant pour l'établissement de la clé de chiffrement

T = 10 ordre entrant pour le calcul de signature

Carte PC1

4	0 2 4 0 0 0 0
6	2 0 0 A 1 1 1
6	0 F F 3 5 i i
6	a a u u F F F
6	F F F 2 1 0 5
6	A C 2 0 0 0 0
6	0 0 8 F F F F

T = 20 ordre entrant pour le calcul de clé de chiffrement

T = 21 ordre sortant délivrant cette clé

Pas de calcul de signature possible dans cet exemple

6. 2. 2 - Reconnaissance des ordres surveillés

6. 2. 2. 1 - Informations de type 10 et 20

Les ordres surveillés par le LECAM sont décrits dans la zone V (données) du TLV correspondant aux informations de type 10 et 20.
Il est possible de ne décrire que les champs dont le contrôle est nécessaire, ceci pour réduire le nombre d'octets à enregistrer dans la carte.

Chaque champ est défini par :

- son emplacement (un octet) : le premier quartet définit le nombre d'octets à tester, le second indique le déplacement par rapport au début de l'ordre,
- le profil binaire à rechercher,
- un masque définissant les caractères binaires à tester (en effet, toutes les informations sont décrites en octets et seules certaines positions binaires sont significatives).

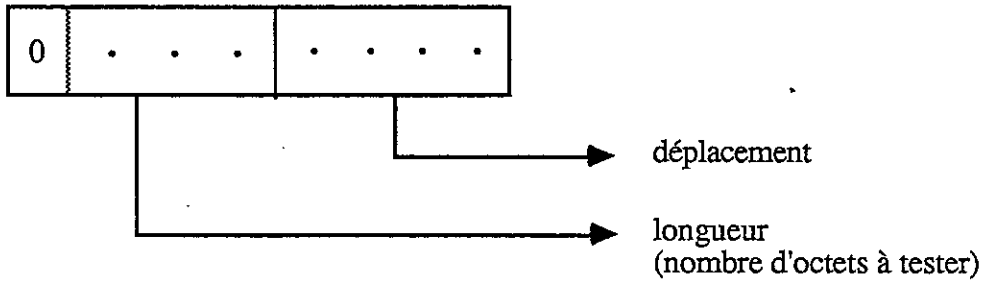
L'information de type 20 contenue dans l'exemple précédent de bloc de sécurité d'une carte B1 peut être décomposée comme suit :

T = 20
L = 07
V = 31 | 84 00 48 | FF FF FF

31	84 00 48	FF FF FF
emplacement du champ	profil binaire à rechercher	masque

a - emplacement du champ

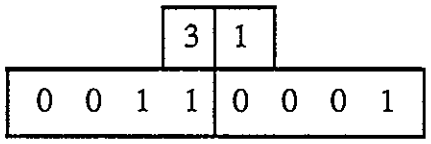
Le codage de l'emplacement est défini sur un octet :



Le déplacement indique l'octet de l'ordre entrant à partir duquel la recherche est effectuée :

déplacement	0	:	nom d'application
	1	:	code instruction (INS)
	2	:	adresse
	4	:	longueur
	5	:	premier octet de données de l'instruction
	6	:	2ème
	...		

La valeur du paramètre "emplacement", dans l'exemple précédent, est 31 (notation hexadécimale)



Cela signifie que le nombre d'octets à tester est de trois à partir du code instruction (INS) (déplacement 1).

Si la longueur est égale à zéro, le déplacement correspond à un repositionnement de l'origine des déplacements pour les champs suivants (nécessaire si le champ à tester correspond à un déplacement supérieur à 15).

Exemple :
Imaginons un ordre entrant pour l'établissement d'une clé de chiffrement de la forme :

nom : X
instruction : Y
adresse : $A_1\ A_2$
longueur : 16
données : $d_1\ d_2\ d_3\ d_4\ d_5\ d_6\ d_7\ d_8\ d_9\ d_{10}\ d_{11}\ d_{12}\ d_{13}\ d_{14}\ d_{15}\ d_{16}$

et que l'on veuille effectuer une recherche à partir de l'octet de données d_{13}. Cet octet correspond à un déplacement égal à 17. Le TLV nécessaire pour décrire l'information de type 20 est donc :

T	L	V					
20	06	0F	22	d_{13}	d_{14}	m_1	m_2

Cela signifie que le nombre d'octets à tester est de deux à partir de l'octet de données d_{13} qui correspond à un déplacement de 2 par rapport à la nouvelle origine (d_{10}).

b - Profil binaire recherché
Suite d'octets à rechercher par le lecteur.

L'exemple précédent donne 84 00 48 :

84 correspond au code de l'instruction
0048 est l'adresse du mot dans la carte

c - Masque
Le masque indiqué est appliqué, par une opération "ET logique", sur les ordres entrants effectués par le lecteur. Le résultat est comparé à la valeur recherchée. S'il y a égalité entre l'ordre recherché et le résultat du "ET logique", le LECAM enchaîne automatiquement l'ordre sortant correspondant.

En résumé, la clé de chiffrement (carte B1) est un certificat sur le mot d'adresse 0048 avec une clé prestataire.

L'ordre à surveiller est :

nom	xx
instruction	84
adresse	00 48
longueur	xx
données	xx xx xx xx xx xx xx xx

S'il est détecté, le LECAM enchaîne alors automatiquement l'ordre suivant :

nom	CB
instruction	C0
adresse	00 00
longueur	08

et initialise la clé de chiffrement.
Cet ordre sortant étant la valeur par défaut, il suffit, dans le bloc de sécurité, de décrire l'ordre entrant :

T = 20 L = 07 V = 31 84 00 48 FF FF FF

Remarques
Si le type 10 est absent du bloc de sécurité, la fonction de signature ne peut être mise en œuvre.

Si le type 20 est absent, la clé de chiffrement doit être initialisée par l'instruction interpréteur RKEY. Par contre, s'il est présent, l'emploi de cette instruction est interdit.

6. 2. 2. 2 - Informations de type 21 et 22

Cette zone contient l'ordre sortant ISO à exécuter pour initialiser la clé de chiffrement. Il est donc toujours formé des 5 octets de l'ordre sortant :

1 octet	:	nom d'application
1 octet	:	code de l'instruction
2 octets	:	adresse
1 octet	:	longueur

Si ces données sont introduites par le type 22 la carte sera mise hors tension après exécution de l'ordre sortant.

Par défaut (absence du type 21 ou 22 dans le bloc d'initialisation) le lecteur exécute l'ordre suivant pour obtenir la clé de chiffrement (uniquement pour les cartes B1) :

nom d'application	:	CB
ordre sortant	:	C0
adresse	:	00 00
longueur	:	08

et laisse la carte sous tension.

6. 2. 2. 3 - Information de type 11

Ce type d'information permet de définir où ranger le comprimé dans les données entrantes.
Le comprimé est formé de 4 octets qui seront rangés successivement à partir de la position indiquée.
La valeur par défaut (absence du type 11) correspond à un déplacement de 2 :

déplacement	:	0 1 2 3 4 5 6 7
rangement du comprimé	:	x x x x

Le TLV correspondant est donc :

T = 11 L = 01 V = 02

Le pouvoir d'imposer les données de comprimé à l'endroit le plus judicieux dans le message d'entrée de la clé est un des éléments significatifs de la transparence du LECAM vis à vis des cartes existantes ou à venir.

6. 2. 3 - Chiffrement avec les cartes M4, B0 et M6

La clé de chiffrement est obtenue comme résultat d'un calcul de certificat sur le numéro de série de la carte avec comme données entrantes une suite de 64 bits dont le premier quartet est égal à zéro et dont les deux derniers octets représentent l'adresse du numéro de série de la carte.

Lorsque le lecteur exécute l'ordre entrant suivant : (x représentant une valeur quelconque) :

nom d'application	:	xx
instruction	:	80
adresse	:	xx xx
longueur	:	xx
données entrantes	:	0x xx xx xx xx xx 09 F0

Il enchaîne automatiquement l'ordre de demande de résultat :

nom d'application	:	BC (M4/B0) CC (M6)
instruction	:	C0
adresse	:	00 00
longueur	:	08

et transfère le résultat obtenu dans une zone interne du lecteur puis met la carte hors tension. Ce résultat est utilisé, conjointement avec une consigne CH, pour initialiser la clé du générateur d'octets chiffrants, selon le schéma présenté au paragraphe 6. 1. 1 -.

Remarques

Si le code confidentiel a été saisi avant l'exécution d'un chiffrement, le résultat de la présentation du code à la carte n'est plus mémorisé dans le LECAM.

Si l'on voulait simuler la mise en oeuvre avec une carte quelconque du chiffrement tel que réalisé avec une carte de type M4, il faudrait inscrire dans cette carte un bloc de sécurité avec le TLV de type 20 suivant :

T = 20
L = 0B
V = 11 80 FF 15 00 F0 2B 09 F0 FF FF

La demande de résultat correspondante serait décrite par un TLV de type 22 et de longueur 5, tel que défini ci-dessus.

6. 2. 4 - Signature avec les cartes M4, B0 et M6

La signature avec les cartes M4, B0 et M6 est le résultat d'un calcul de certificat sur le mot des locks de la carte.
Lorsqu'un programme téléchargé exécute une demande de calcul sur le mot des locks (d'adresse 09F8), le lecteur remplace alors automatiquement quatre octets des données entrantes par le comprimé précédemment obtenu.

données entrantes initiales	:	E1 E2 E3 E4 E5 E6 09 F8
données effectivement entrantes	:	E1 E2 co-mp-ri-mé 09 F8

L'ordre de demande de calcul correspondant est donc modifié automatiquement par le LECAM pour que les données entrantes comprennent le comprimé caractéristique du texte à signer :

nom d'application	:	xx
instruction	:	80
adresse	:	xx xx
longueur	:	xx
données	:	xx xx co-mp-ri-mé 09 F8

Après utilisation, le comprimé est remis à zéro.

Les données reçues de la carte correspondant au résultat du calcul forment la signature.

Remarque

Si l'on voulait simuler la mise en oeuvre avec une carte quelconque de la signature telle que réalisée avec une carte de type M4, il faudrait inscrire dans cette carte un bloc de sécurité avec le TLV de type 10 suivant :

T = 10
L = 08
V = 11 80 FF 2B 09 F8 FF FF

7 . APPLICATIONS RESIDENTES

Pour faciliter la mise en œuvre du LECAM, et diminuer la part de programmes à télécharger, le lecteur met à la disposition du serveur un certain nombre de programmes résidents implantés pour les besoins du service "Connexion Automatique".

Ces programmes sont stockés dans la mémoire ROM du lecteur, et peuvent être "autochargés" dans la mémoire RAM utilisateur à l'initiative soit du LECAM (connexion automatique) soit du serveur. Le chargement de ces programmes résidents par le serveur se fait par la consigne C3. Cette consigne provoque le chargement de tables et de programmes, à des adresses pré-définies de la mémoire, qui peuvent être utilisés directement par le serveur. La modification par le serveur de ces programmes, une fois en RAM, ne peut être garantie.

La mise en œuvre de ces programmes est détaillée au paragraphe 7. 2. 3.

7. 1 - Programme de saisie du code porteur

Nous avons vu, dans le chapitre "Connexion Automatique", que si les données nécessaires à l'établissement de la connexion sont protégées en lecture par un code confidentiel, le LECAM demande à l'usager de saisir son code porteur.

Ceci est possible grâce au programme résident de saisie du code porteur, utilisable pour les cartes M4 (ou B0), M6 et B1.

Ce programme effectue le dialogue de présentation de code porteur avec l'usager ainsi que les vérifications nécessaires : en cas de code faux, le dialogue est poursuivi jusqu'à ce que le code soit correct ou jusqu'au blocage de la carte (après trois tentatives infructueuses).

Le LECAM contrôle les caractères saisis : seuls les caractères 0 à 9, A à F et les touches de fonction <CORRECTION>, <ANNULATION>, <ENVOI> sont autorisées pendant la frappe du code confidentiel.

Appel du programme	:	CALL 00, 09
Retour	:	- en séquence, carte sous tension, si le code présenté est correct - par un "ABORT", carte hors tension, sinon.

Les codes d'ABORT possibles sont les suivants :

ABORT, 1	:	défaut carte (carte bloquée ou retirée),
ABORT, 2	:	refus, par l'usager, de poursuivre le dialogue (appui sur une touche de fonction du Minitel autre que <ENVOI>, <CORRECTION> ou <ANNULATION>.

Le programme de saisie du code porteur comporte une directive ONERR qui permet, en cas d'erreur rencontrée dans le déroulement du programme (délai entre deux frappes clavier écoulé), d'interrompre l'exécution de celui-ci et de la reprendre à l'adresse indiquée par la directive ONERR.

Si le programme de saisie du code porteur est appelé par un programme téléchargé, il faut donc que ce dernier comporte une seconde directive ONERR dont le but est d'annuler l'effet de la première. Dans le cas contraire, la rencontre, en cours d'exécution du programme téléchargé, d'une erreur de type interpréteur, ré-initialiserait le programme de saisie du code porteur, ce qu'il faut éviter.

Remarque :
Le programme de saisie du code porteur est exécutable quel que soit le mode de fonctionnement du LECAM (qu'il soit connecté ou non à un Minitel).

- Le LECAM gère le Minitel pendant la phase de connexion automatique ou pendant le dialogue serveur-LECAM si ce dernier est connecté au Minitel.
- Si le LECAM n'est pas connecté à un Minitel (cas de la connexion à un micro-ordinateur par exemple), la saisie et l'affichage des données nécessaires au déroulement du programme résident de saisie du code porteur a lieu sur le maître (au sens Système d'Echanges).

7. 2 - Tables d'état

Les tables utilisées par les programmes résidents pour contrôler les échanges réalisés avec la carte peuvent aussi être "autochargés" par l'application distante.

L'une est la table de gestion générale (table ATG) qui permet de tester les mots d'état carte et coupleur, l'autre est la table de gestion du code porteur (table ATC), qui permet de vérifier l'état de la carte et la validité des codes saisis.

Le profil de ces tables est décrit ci-après.

7. 2. 1 - Tables de gestion générale (tables ATG)

Ces tables sont chargées à partir du registre R48. Ce sont des descripteurs d'état qui ont le contenu suivant :

Table pour M4,B0,M6 (module n°0)

C7	descripteur
90 F0 00 81 00 FF	mots d'état
00 00	adresse de branchement si erreur carte
00	fin de table

Table pour B1 (module n°1)

C7	descripteur 1
90 F0 00 81 00 FF	mots d'état
00 00	adresse de branchement si erreur carte
83	descripteur 2
90 FF 08 08	mots d'état
80 14	adresse de branchement si argument absent
00	fin de table

Table pour PC1 (module n° 4)

C7	descripteur 1
90 F0 00 81 00 FF	mots d'état
00 00	adresse de branchement si erreur carte
81	descripteur 2
91 F1	mots d'état
80 18	adresse de branchement si argument absent
00	fin de table

Le descripteur d'état est formé de :

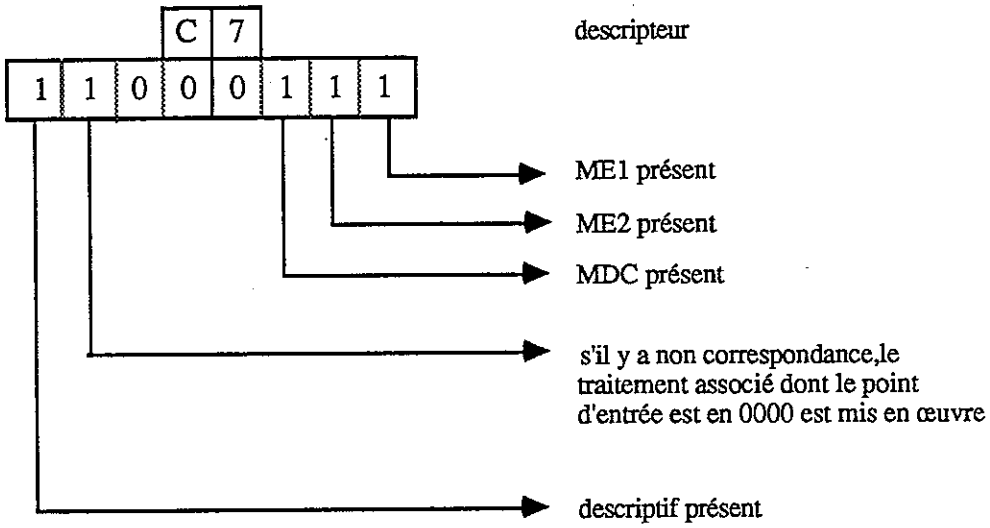
Descriptif 1	Identifiant descriptif	1 octet
	Valeur état 1 ME1	0 ou 2 octets
	Masque associé	
	Valeur état 1 ME2	0 ou 2 octets
	Masque associé	
	Valeur état 1 MDC	0 ou 2 octets
	Masque associé	
	Traitement 1 associé	2 octets
Descriptif n	Identifiant descriptif n	
	Traitement n associé	
Terminateur	Terminateur = 00	1 octet

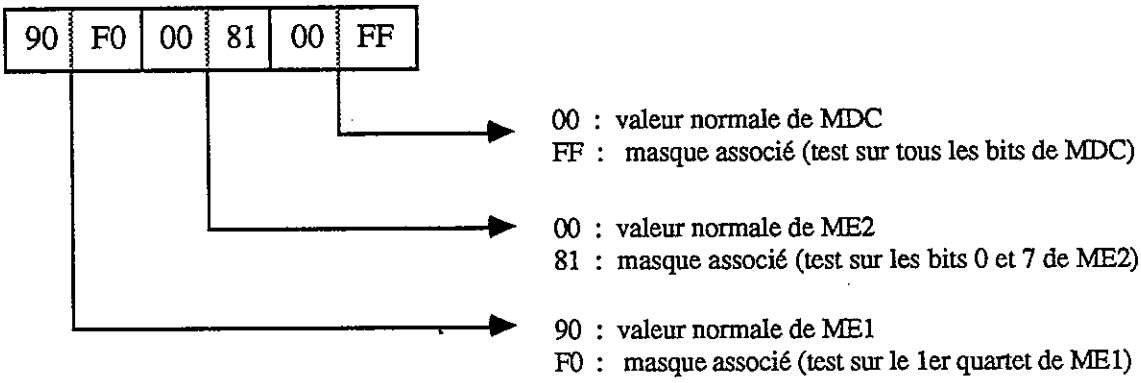
L'identifiant descriptif correspond à

	P	S	0	0	0	D	2	1	
Fin de table	0							0	ME 1 absent
Descriptif présent	1							1	ME 1 présent
Correspondance		0					0		ME 2 absent
Non correspondance		1					1		ME 2 présent
						0			MDC absent
						1			MDC présent

Le bit 'S' permet de tester la correspondance entre la valeur des mots d'état spécifiés et le résultat du masquage associé, ceci pour décider de la mise en oeuvre ou non du traitement associé à chaque descriptif.

Par exemple, la table correspondant aux cartes M4 a donc la signification suivante :





0 0	0 0

adresse de branchement si :

ME1 ≠ 90
ou ME2 ≠ 00
ou MDC ≠ 00

0 0

fin de table

7. 2. 2 - Table de gestion du code porteur (table ATC)

Cette table est chargée à partir du registre R2F.
Elle a le contenu suivant :

C7	descripteur 1
90 F0 00 81 00 FF	mots d'état
00 00	adresse de branchement si erreur carte
82	descripteur 2
10 F0	mots d'état
00 71	branchement si un code faux
82	descripteur 3
20 F0	mots d'état
00 7C	branchement si deux codes faux
82	descripteur 4
40 F0	mots d'état
00 87	branchement si la carte est bloquée
00	fin de table

(table pour cartes M4, M6, B0 et B1 uniquement).

7. 2. 3 - Mise en œuvre

Les programmes et les tables décrits ci-dessus sont chargés dans la mémoire vive du lecteur par les consignes C3 suivantes :

C3, 0	programme de saisie du code porteur M4, M6 et B0 tables ATG et ATC correspondantes,
C3, 1	programme de saisie du code porteur carte B1 tables ATG et ATC correspondantes,
C3, 4	table ATG pour la carte porte-clés PC1.

Après exécution de la consigne C3, le début de la mémoire contient les instructions suivantes :

adresse	instructions	
00 00	MHT	
	ABORT, 81	erreur carte
00 03	MHT	
	ABORT, 82	abandon du dialogue de la part de l'usager
00 09	instruction de relais vers le programme de saisie du code (cartes M4, B0, M6 et B1 uniquement).	

7. 2. 4 - Contraintes

Le tableau suivant résume les contraintes associées à chaque module, les informations de chaque colonne du tableau sont les suivantes :

C3	indique la valeur à utiliser derrière la consigne C3
cartes	indique le type de cartes concernées
mémoire chargée	indique la zone mémoire chargée par la consigne C3
mémoire disponible	indique la première adresse mémoire à partir de laquelle l'usager peut implanter des programmes s'il utilise le sous-programme de saisie du code porteur
registres chargés	indique les registres initialisés par la consigne C3
registres utilisés	indique les registres modifiés lors d'un appel du programme de saisie du code porteur.

C3	Cartes	Mémoires		Registres	
		chargées	disponibles	chargés	utilisés
C3, 0	M4 M6 B0	0000 à 00BD	00BE à 02FF	06 et 07 2F à 58	06 à 0E 2F à 51 6E et 6F 74 et 75 DF à EF
C3, 1	B1	0000 à 00E2	00CD à 02FF	06 et 07 2F à 58	06 à 0E 2F à 58 6E et 6F 74 et 75 DF à EF
C3, 4	Porte-clés PC1	0000 à 007D	0000 à 02FF	06 et 07 2F à 58	
Récapitulatif maximum		0000 à 00FF	0100 à 02FF	06 et 07 2F à 58	06 à 0E 2F à 58 6E et 6F 74 et 75 DF à EF

La dernière ligne du tableau indique des valeurs conseillées pour standardiser les programmes.

Remarques complémentaires

- La zone locale (registres E0H à FFH) est réinitialisée à chaque échange avec le serveur.

- La mémoire du lecteur est modifiée lors d'une opération de connexion automatique ou lors d'une mise en mode : en effet, dans ces deux cas, un programme est chargé automatiquement par le LECAM pour rechercher un bloc de connexion automatique ou un bloc de sécurité.Ce programme entraîne les modifications des zones mémoire suivantes :

  mémoire programme de 00H à 16FH,

  mémoire programme à partir de l'adresse 200H pour contenir le bloc de connexion automatique recherché dans la carte ou les données du bloc de sécurité implicite (cartes M4,B0,M6),

  registres 04H à 7FH.

7. 3 - Messages associés à la saisie du code porteur

Le message demandant à l'usager de saisir son code confidentiel est :

"Tapez votre code : "

Si le code est faux, le message :

"Tapez votre code - 2ème essai : "

est affiché. Si le code frappé au clavier n'est toujours pas correct, le message :

"Tapez votre code - 3ème essai ! : "

est affiché. Si le code est faux à nouveau, le message :

"CARTE BLOQUEE"

signale à l'usager que l'utilisation de sa carte n'est plus possible.

Remarques :
Le LECAM vérifie les caractères saisis. Seuls les caractères 0 à 9, A à F, et les touches de fonction <CORRECTION>, <ANNULATION> et <ENVOI> sont autorisées. Si le code saisi comporte un caractère interdit, le LECAM considère que l'usager a fait une faute de frappe : selon la phase de saisie du code confidentiel dans laquelle se trouve le LECAM (première, deuxième ou troisième tentative), il ré-affiche le message correspondant, sans incrémenter le nombre d'essais réalisés.

Si l'usager frappe un code confidentiel comportant plus de 7 caractères, le LECAM émet un signal sonore chaque fois qu'une touche, autre qu'une touche de fonction autorisée, est actionnée sur le clavier.

8 . CONDITIONS D'ARRET DU LECAM

Outre l'arrêt normal du LECAM en fin d'application, il peut exister des conditions provoquant l'arrêt immédiat des échanges. Ces conditions peuvent être dûes soit à l'usager, soit au serveur.

8. 1 - Actions provoquées par l'usager

- déconnexion du Minitel,
- mise hors tension du LECAM,
- action simultanée sur les touches <TS> (Touche Spéciale) et <CONNEXION/FIN> du Minitel, qui est équivalente à la commande CDG (Commande de Déconnexion Générale) du Système d'Echanges.

8. 2 - Conditions d'erreurs dûes au serveur

- le LECAM stoppe immédiatement le programme en cours d'exécution en cas de tentative abusive de modification des aiguillages du Minitel par le serveur pendant une saisie dont les données sont rangées en zone locale, ou lors de transfert de données chiffrées (saisie chiffrée ou affichage chiffré).

- il en va de même en cas de fermeture de session de la part du serveur ou en cas de perte de porteuse.