Bull CP8

GUIDE UTILISATEUR

DE LA CARTE CP8 MASQUE 4

Réf. BULL CP8 : TU.0047.F.01
octobre 1986

SOMMAIRE

FIGURES

TABLEAUX

AVANT - PROPOS

Ce document est destiné aux concepteurs et aux réalisateurs d'applications mettant en oeuvre la carte à Micro-Circuit CP8 MASQUE 4.
Elle est un des éléments de l'offre BULL CP8, comprenant:

a) Des produits pouvant être intégrés physiquement à l'intérieur de systèmes existant:

   - connecteur mécanique.
   - coupleur assurant la gestion de l'interface électronique entre un connecteur et le système hote.

b) Des lecteurs encodeurs connectables à des PC ou compatibles.

c) Des outils de personnalisation aux capacités de traitement diverses:

   - La MPM, Machine de Personnalisation Manuelle pour les petites quantités de carte.
   - L'ALEC, Automate de Lecture Ecriture, pour les grandes quantités.

d) Le PSA, Processeur de Sécurité Associé, qui, connecté à un serveur permet de sécuriser l'accès à une base de données.

e) Le Certificateur.

f) Des outils logiciel de développement d'application carte à mémoire pour PC ou compatibles.

Ce document est conçu de la manière suivante:

Le chapitre 1 est une présentation générale de la carte CP8.
Les chapitres 2, 3 et 4 présentent de manière détaillée l'organisation de la mémoire et la mise en oeuvre des ordres élémentaires. Leur lecture est nécessaire pour développer une application carte à mémoire.
Enfin, le dernier chapitre est un aperçu du processus de personnalisation d'une carte.

1 PRESENTATION GENERALE

1.1 Aspects physiques externes et spécifications techniques

La carte CP8 se présente extérieurement comme une carte de crédit plastique à la norme ISO 2896.

Sur la face recto de la carte, est inséré dans le coin supérieur gauche du support plastique le composant CP8, recouvert par un circuit imprimé réalisant l'interface physique entre le composant et le monde extérieur.

Cette face peut également supporter optionnellement un graphisme (logo), et des caractères embossés dans la zone d'estampage réservée à cet effet.

Enfin, sur le verso peuvent être implantées des pistes magnétiques telles que ISO1, ISO2, ISO3, T2, T3.

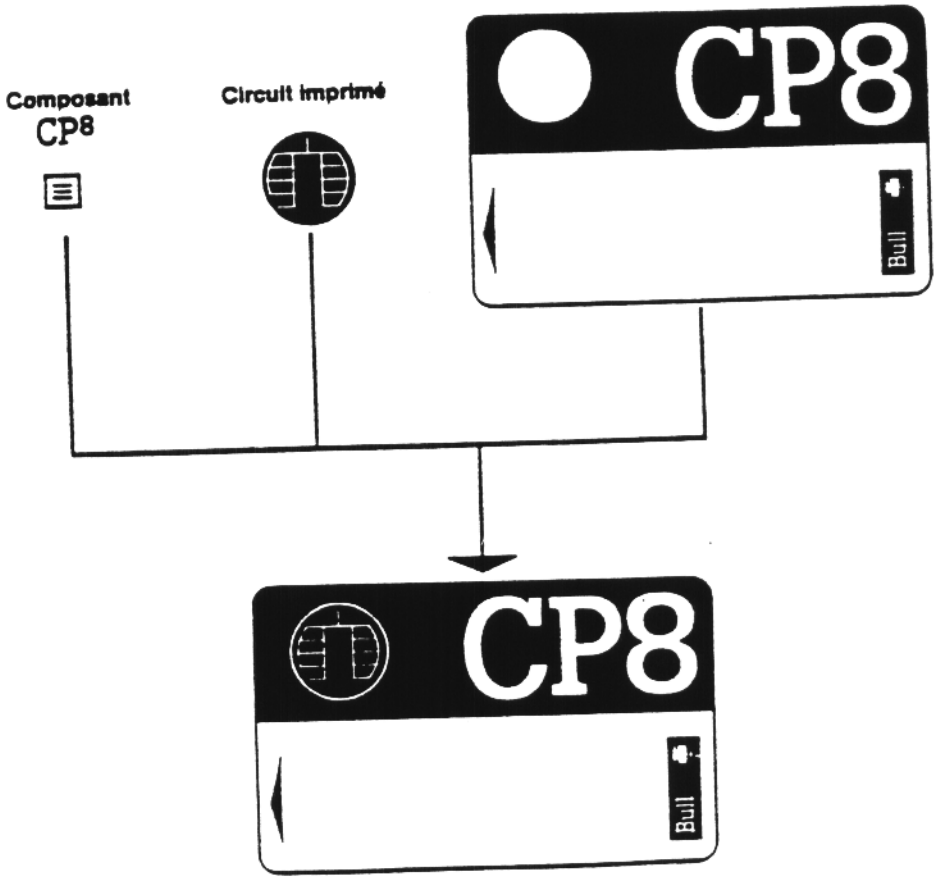

Figure 1.1 : Aspects physiques externes

Les spécification techniques

Carte à micro-circuit	normes ISO
Epaisseur de la carte	compatible norme ISO (0,76 mm)
Hauteur	54 mm
Largeur	85 mm
Pistes magnétiques	ISO et/ou TRANSAC (option)
LOGO	Spécifique client (option)

Durées de mise sous tention à une température ambiante de 0°C à 50°C :

La phase d'écriture (sous Vpp) = 5 secondes

La phase de lecture (sous Vcc) = 30 secondes

1.2 Le composant CP8

1.2.1 Architecture interne :

Le composant CP8 est un mono-chip, intégrant:

- Un micro-processeur
- Un initialisateur
- Un séquenceur
- Un buffer d'entrée/sortie
- Des mémoires PROM, ROM, RAM

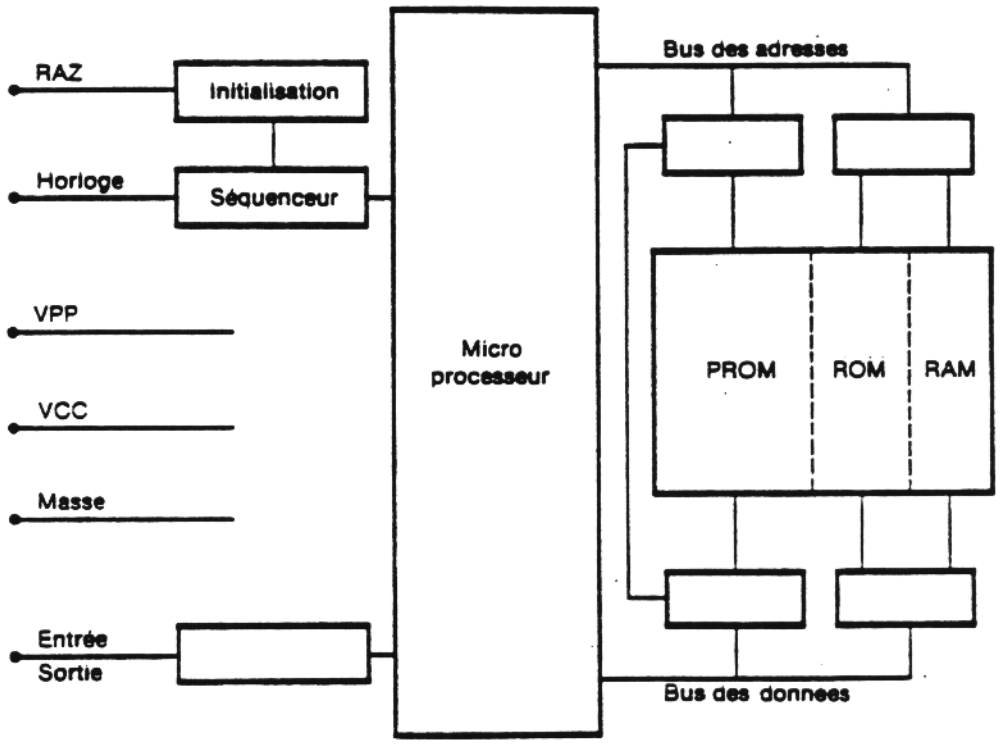

Figure 1.2 : Schéma fonctionnel du composant CP8 Masque 4

Le MICROPROCESSEUR :

C'est un microprocesseur 8 bits, type MOTOROLA 6805 ou EUROTECHNIQUE 8048.

Il s'interpose entre les mémoires et le monde extérieur et exécute un programme inscrit dans la mémoire ROM.

La Mémoire ROM : (Read Only Memory)

Elle contient le programme inscrit par masque lors de la fabrication du composant, d'où la dénomination "MASQUE 4", le chiffre 4 définissant un ensemble de fonctionnalités propres à ce programme.

Par procédé de fabrication, le programme est inaccessible et ainsi non altérable et non duplicable.

Le "binôme" microprocesseur-programme assure le fonctionnement général du composant. En particulier, il gère les transferts d'informations entre le monde extérieur et la mémoire PROM.

La Mémoire PROM : (Programmable Memory)

(En toute rigueur, on devrait l'appeler O.T.PROM,
c'est à dire One Time Programmable Memory.)

Sa taille est de 8 K8its, soit 256 mots de 32 bits chacun.
A la fabrication, l'ensemble des bits de la mémoire est positionné au niveau logique 1, l'écriture consistant à faire positionner par le microprocesseur les bits que l'on désire au niveau logique 0 . Tout bit positionné à 0 ne peut plus revenir à l'état 1.

Le contenu de cette mémoire évoluera tout au long de la vie de la carte, car y seront mémorisées (entre autres), les informations propres à l'application (transactions, unités, paramètres de log in etc...).

La mémoire RAM : (Random Access Memory)

Totalement inaccessible de l'extérieur, elle est utilisée comme mémoire de travail temporaire interne.

Le composant CP8 : un M.A.M.

En résumé le composant CP8 est un MICRO-CALCULATEUR AUTOPROGRAMMABLE MONOLITHIQUE, ou M.A.M.;

MICRO-CALCULATEUR, parce qu'il contient un microprocesseur pouvant exécuter un programme et donc des fonctions arithmétiques, logiques etc...

AUTO PROGRAMMABLE, parce que, contrairement aux architectures à base de microprocesseurs classiques, il réalise lui-même la programmation de la mémoire, sans aucune implication fonctionnelle externe.

Enfin MONOLITHIQUE, l'ensemble microprocesseur-mémoires - bus..., étant intégré dans un seul et même composant.

Microcalculateurs Autoprogrammables		MAM 01	MAM 02
Type de l'unité centrale		6805	8048
Taille des mémoires (en octets)	RAM (travail)	36	44
	ROM (programme)	1600	2048
	PROM (transaction)	1024	1024
Fabricant du circuit		MOTOROLA	EUROTECHNIQUE

Tableau 1.1 : Différents types de M.A.M

1.2.2 Interface physique

Le composant CP8 est relié au monde extérieur par 6 contacts. Leurs positions respectives et leurs spécifications sont définies par la norme ISO.

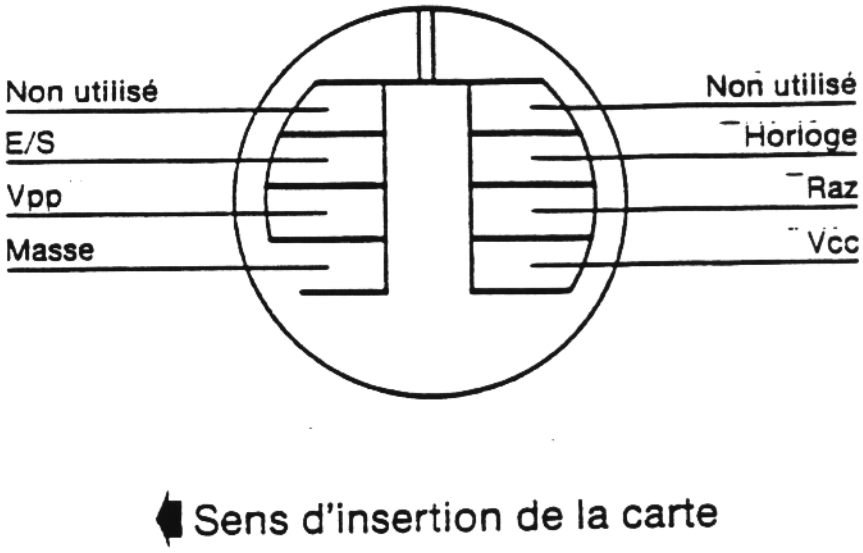

Figure 1.3 : Position des contacts sur le circuit imprimé

RAZ :

Une tension appliquée sur ce contact déclenche l'initialisation physique et logique du composant. A l'issue de cette phase, la carte envoie un ensemble d'informations définissant ses caractéristiques techniques et "historiques".

Horloge :

Une base de temps (F=3,6 MHz) doit être fournie au microprocesseur sur le contact Horloge.

Vcc :

Sur ce contact est appliquée la tension d'alimentation du composant, suffisante pour les opérations de lecture.

Vpp :

Sur ce contact, est appliquée, à la demande de la carte, la tension nécessaire à la programmation de la PROM.

Zéro :

Contact de masse.

E/S :

Par ce contact, transitent les données échangées entre la carte et le monde extérieur. Les données sont échangées à l'alternat, en mode asynchrone, à la vitesse de 9600 bauds, sous forme de caractères.

Un caractère est constitué comme suit :

1 bit START, 8 bits de DONNEES, 1 bit de PARITE PAIRE.

1.2.3 Fonctionnalités du programme MASQUE 4

1.2.3.1 Gestion des échanges Carte-Monde extérieur.

Le programme MASQUE 4 assure la gestion physique et logique des échanges d'informations entre la carte et le monde extérieur.

1.2.3.2 Gestion de la mémoire PROM

Les 8 Kbits ou 256 mots de la mémoire PROM sont logiquement divisés en 7 zones distinctes.

Ce partitionnement est défini par un ensemble de pointeurs, mémorisés dans la ZONE DE FABRICATION localisée dans les adresses hautes de la mémoire.

Ces pointeurs sont écrits pendant la phase précédant la mise en service de la carte, phase dite de PERSONNALISATION.

1.2.3.3 Gestion de l'accès aux différentes zones

Le monde extérieur ne peut accéder à n'importe quelle zone, n'importe comment. Telle zone est totalement inaccessible, telle autre l'est seulement en "lecture".

Le programme se charge de faire respecter les règles d'accès. Dans le cas où une règle ne serait pas respectée, le composant devient muet, dans le sens propre du terme. Seul une "RAZ", c'est à dire l'application d'une tension sur le contact RAZ peut réinstaurer le dialogue.

1.2.3.4 La fonction TELEPASS

Sur demande, le programme MASQUE 4 peut exécuter une fonction logico-mathématique appelée fonction TELEPASS.

1.2.3.5 Notion de CLASSE D'INSTRUCTION

Certaines de ces fonctionnalités peuvent être activées directement de l'extérieur grâce à un jeu d'ordres élémentaires (lecture, écriture, présentation de clé, ordre de calcul, etc..).

Ce jeu d'ordres définit une CLASSE D'INSTRUCTION donnée, à laquelle est attribué un code hexadécimal, mémorisé dans le coeur même du composant.

Le code de la Classe d'Instruction du composant MASQUE 4 est BC (hexadécimal).

1.3 Les Zones

Qu'est-ce qu'une zone ? Nous avons vu que la mémoire PROM avait une taille de 8 Kbits. Ces 8 Kbits sont répartis en 256 mots de 32 bits chacun, ou 8 quartets, un quartet valant 4 bits. Ces 256 mots sont regroupés en 7 ZONES, de tailles, de contenu et d'accessibilité différents.

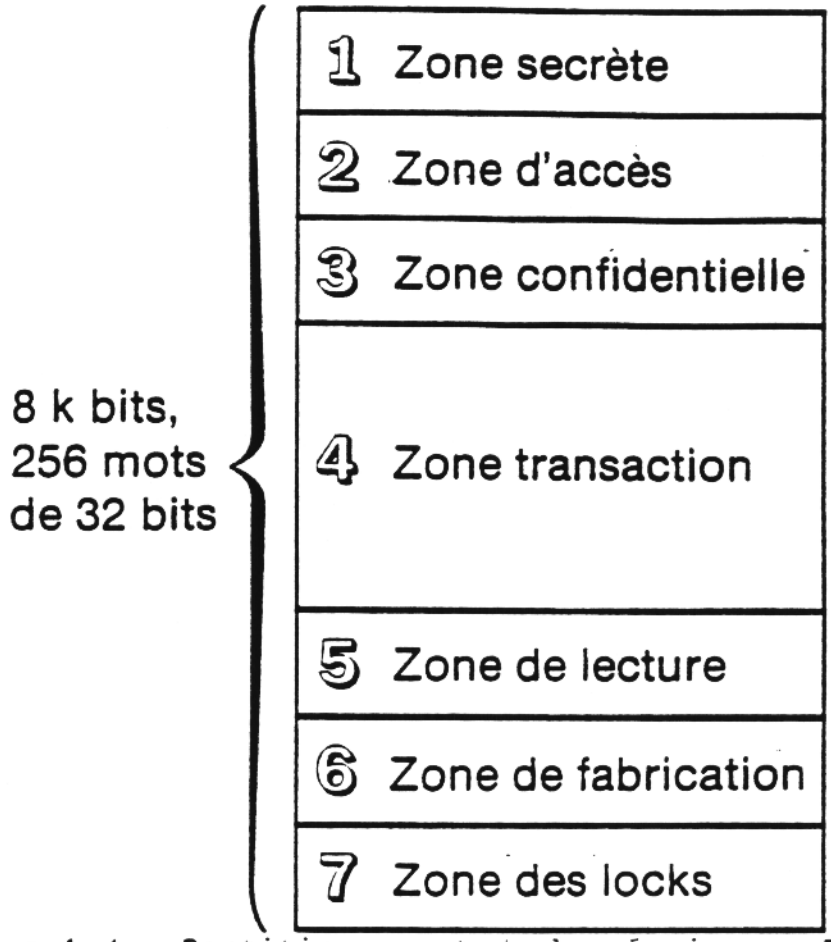

Figure 1.4 : Partitionnement de la mémoire en 7 zones

Ces zones peuvent être regroupées en 4 grands types:

- Les Zones Sécuritaires, dont les informations sont utilisées par le micro-calculateur pour autoriser ou refuser l'accès aux zones de données. Ce sont la ZONE SECRETE et LA ZONE D'ACCES.

- Les Zones de Données, où sont mémorisées les informations propres à l'application. Ce sont la ZONE CONFIDENTIELLE, la ZONE TRANSACTION et la ZONE DE LECTURE.

- La Zone de FABRICATION contenant les pointeurs des zones précédemment citées.

- La Zone des LOCKS, où sont signées les grandes phases de la vie de la carte.

1.3.1 Les zones sécuritaires

1.3.1.1 La Zone Secrète

Un ensemble de cartes est émis par un prestataire de services : appelons-le EMETTEUR PRIMAIRE.
De plus, sous réserve d'accords préliminaires...., ces cartes peuvent également êtres utilisées pour des services fournis par un autre prestataire : appelons-le EMETTEUR SECONDAIRE.

Chacun de ces prestataires inscrira dans les cartes (en zone transaction) des informations propres à son service : plafonds financiers, droits d'accès, etc...

Ces informations sont sensibles et peuvent faire l'objet de fraude. Pour éviter cela, toute ECRITURE * sur carte aura été précédée par la PRESENTATION d'une clé. Comme il y a 2 prestataires potentiels, il y a deux clés émetteurs, appelées encore clés TYPE 1 :
- La CLE EMETTEUR PRIMAIRE
- La CLE EMETTEUR SECONDAIRE

On verra que grâce à la présence de BITS SYSTEMES, on saura, en lecture, sous la responsabilité de quel émetteur a été écrite telle ou telle information.

Cependant toutes les informations écrites en zone de transaction ne le sont pas nécessairement sous la responsabilité d'un émetteur.
Elles peuvent être écrites sous la responsabilité du PORTEUR, lors d'achat chez un commerçant par exemple.

Ainsi, la Zone Secrète contient une CLE PORTEUR, correspondant au code confidentiel classique des cartes de crédit.
Au moment de la PERSONNALISATION de la carte, une clé porteur est affectée par l'émetteur. Toutefois, le porteur a la possibilité de remplacer cette clé par une autre de son choix. La clé porteur est dite clé de TYPE 2.

Ces clés seront également utilisées pour lire dans les zones en LECTURE PROTEGEE. (zone confidentielle, zone d'accès ...)
Enfin, la zone secrète contient un JEU SECRET, valeur binaire entrant dans le calcul de la fonction TELEPASS

* ECRITURE est un abus de langage. On verra par la suite qu'il vaut mieux parler de VALIDATION EN ECRITURE.

1.3.1.2 La Zone D'Accès

Nous avons vu que l'écriture ou la lecture pouvaient nécessiter la présentation d'une des trois clés mémorisées dans la zone secrète

La Zone d'Accès est utilisée par le micro-calculateur pour mémoriser ces présentations de clé.
Les présentations de clés vraies et fausses sont mémorisées différemment.

1.3.2 Les zones de données

1.3.2.1 La Zone Confidentielle

Elle contient, comme son nom l'indique, des informations confidentielles propres à l'application. Ces informations sont non évolutives; elles ont été écrites en phase de personnalisation et sont figées jusqu'à la fin d'utilisation de la carte.

1.3.2.2 La Zone Transaction

Elle contient les informations propres à l'application inscrites dans la carte à partir de sa mise en service. C'est en principe la plus grande zone de la mémoire PROM.
Y sont inscrits les montants, plafonds, droit d'accès, ou plus généralement toutes informations évolutives concernant l'application.

1.3.2.3 La Zone de Lecture

Semblable à la zone confidentielle. Cependant les informations qui y sont stockées ne sont pas de nature confidentielle.

1.3.3 La Zone de Fabrication

Elle contient les pointeurs nécessaires au micro-calculateur pour savoir où sont implantées les différentes zones dans l'espace mémoire .

Elle contient également d'autres informations relatives à la carte, en particulier le NUMERO DE SERIE, et le type de PROTECTION D'ACCES de la Zone Transaction.

1.3.4 La Zone des Locks

Le contenu de la mémoire évolue, depuis la fabrication jusqu'à la mise en service de la carte, et finalement sa "mort".
Cette zone contient des bits, ou LOCKS, autant de "bougies d'anniversaire" qu'il y a passage d'un état à un autre de la mémoire .
La figure ci-après résume la présentation des zones et leur contenu respectif.

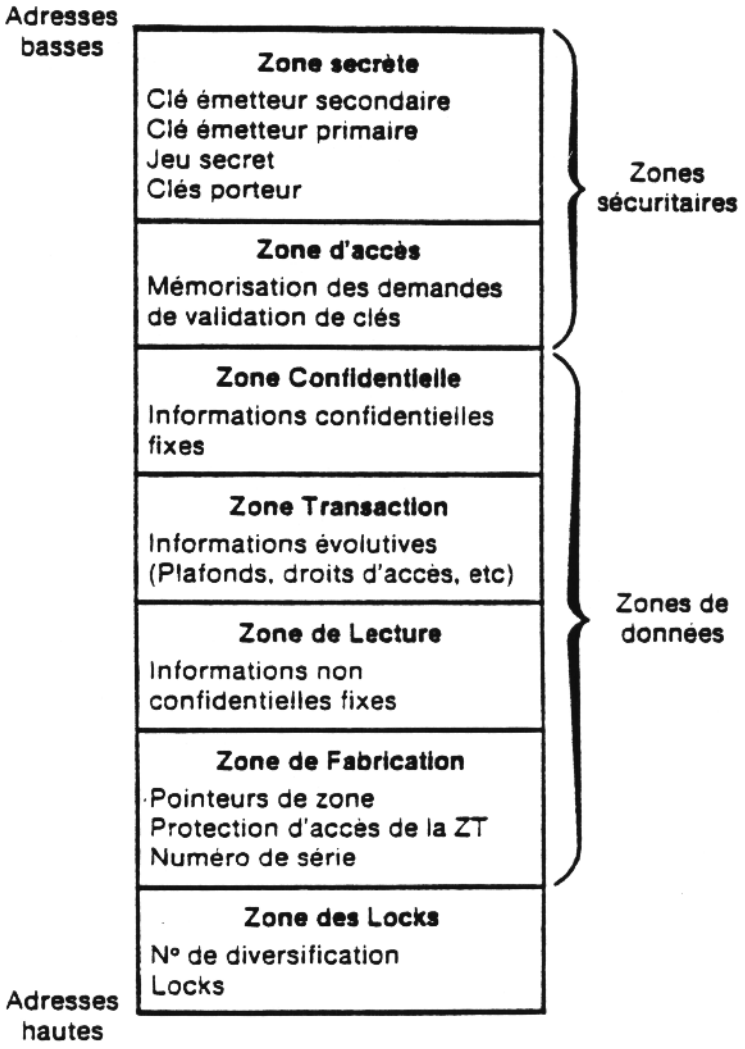

Figure 1.5 : Le contenu des 7 zones

1.4 Accessibilité d'une zone en lecture/écriture

Le microprocesseur s'interpose en permanence entre le monde extérieur et la mémoire PROM. Autrement dit, tout transfert d'informations, dans un sens comme un autre, fera toujours l'objet, de la part du monde extérieur, d'une requête ou ORDRE, envoyé au microprocesseur.

On dira qu'une zone est ACCESSIBLE EN LECTURE si le microprocesseur autorise, sous certaines conditions, et exécute le transfert d'informations, de la zone considérée vers le monde extérieur.

On dira qu'une zone est ACCESSIBLE EN ECRITURE si le microprocesseur autorise, sous certaines conditions, et exécute le transfert d'informations, du monde extérieur vers la zone considérée.

L'accessibilité d'une zone est implicite, non modifiable et fonction du contenu de la zone.

Le tableau ci-dessous présente l'accessibilité des zones d'une carte personnalisée.

	Accessibilité	
	En lecture	En écriture
Zone secrète	non	non
Zone d'accès	oui	non
Zone confidentielle	oui	non
Zone transaction	oui	oui
Zone de lecture	oui	non
Zone de fabrication	oui	non
Zone des locks	oui	oui

Tableau 1.2: Accessibilité des zones

La ZONE SECRETE contenant CLES et JEU SECRET n'est évidemment jamais accessible par le monde extérieur.
La ZONE D'ACCES peut être lue car il peut être intéressant de connaître le nombre de présentations de clés fausses et éventuellement détecter une tentative de fraude.

Les ZONES CONFIDENTIELLES, DE LECTURE et DE FABRICATION sont figées en leur contenu à la personnalisation. Elles ne peuvent donc qu'être lues.
Enfin, la ZONE TRANSACTION est accessible en lecture et en écriture.

1.5 La lecture

1.5.1 Zone en LECTURE PROTEGEE : BLOCAGE et RECYCLAGE d'une carte

Pour lire dans une zone dite en LECTURE PROTEGEE il est nécessaire de:

- PRESENTER UNE CLE, une parmi les trois mémorisées dans la Zone Secrète.
- Faire une DEMANDE DE VALIDATION de clé en lecture, à l'issue de laquelle la carte dit si la clé est bonne ou mauvaise.

Si la clé est bonne, la carte autorisera la lecture dans toutes les zones protégées en lecture (ZA, ZC ...)

Si la clé est mauvaise, afin d'éviter des tentatives frauduleuses de recherche itérative de clé, la carte se mettra elle-même dans l'ETAT BLOQUE, après 1 demande de validation d'une mauvaise clé de type 1 et 3 demandes de validation consécutives d'une mauvaise clé de type 2.

L'ETAT BLOQUE signifie que, provisoirement :

- Toute lecture dans une zone protégée en lecture est impossible, autrement dit la carte refusera toute présentation et demande de validation de clé.

- Seules les zones en lecture non protégée sont consultables.

Pour sortir la carte de cet état de blocage, il est nécessaire d'effectuer l'opération suivante, appelée RECYCLAGE :

- Présentation à la carte de la clé PORTEUR ET de la clé EMETTEUR PRIMAIRE.

- Demande de validation en lecture.

Si les deux clés sont bonnes, la carte est remise en fonctionnement normal. Si une des deux clés est mauvaise, la carte mémorise ce nouvel évènement et reste dans l'état bloqué.

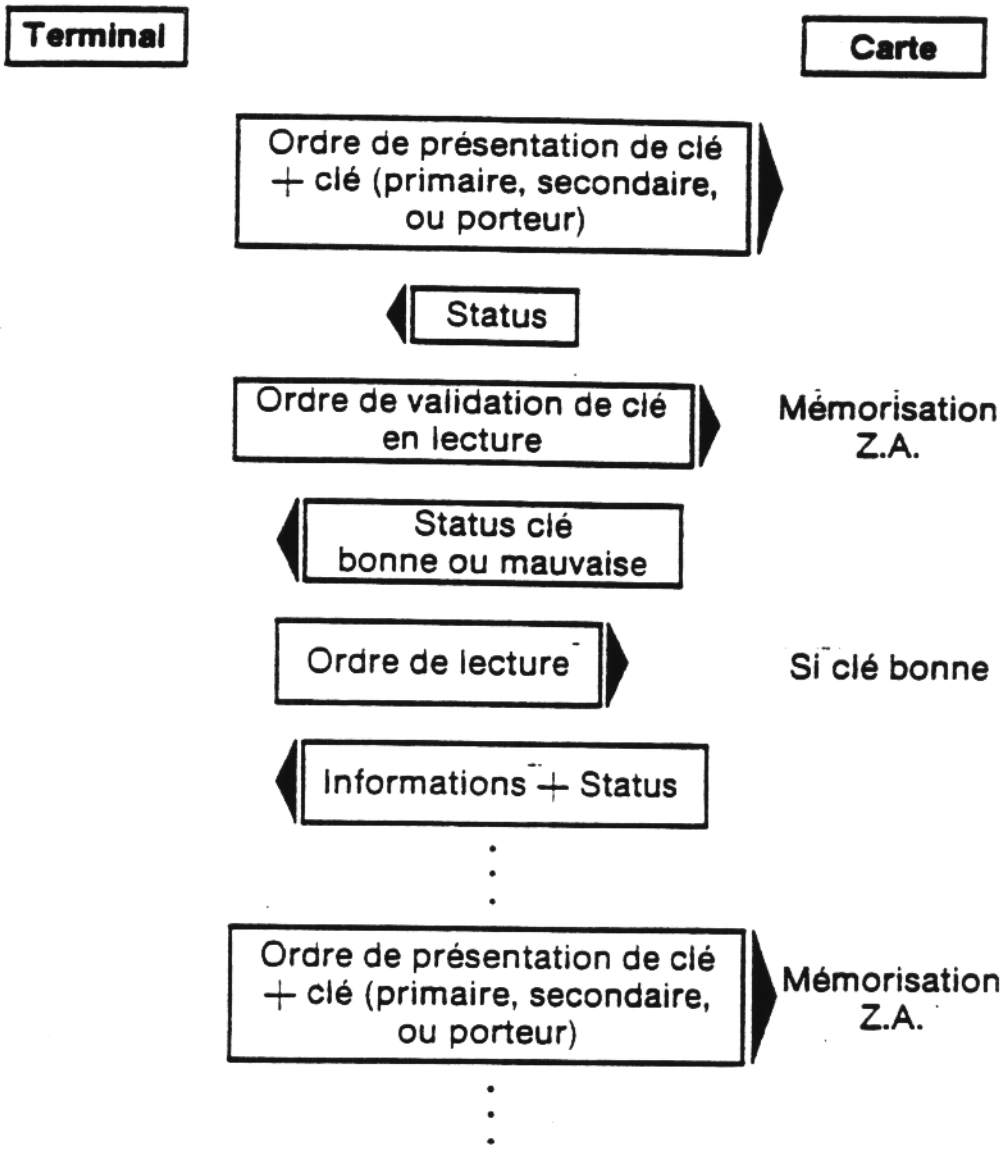

Figure 1.6 : Lecture dans une zone en LECTURE PROTEGEE

1.5.2 Zone en LECTURE LIBRE

Une zone est dite en LECTURE LIBRE s'il n'est pas nécessaire de faire une présentation et une demande de validation de clé en lecture pour lire cette zone. Pour ce faire, il suffit d'envoyer à la carte un ORDRE DE LECTURE.

On notera que la lecture dans une telle zone est possible même lorsque la carte est bloquée.

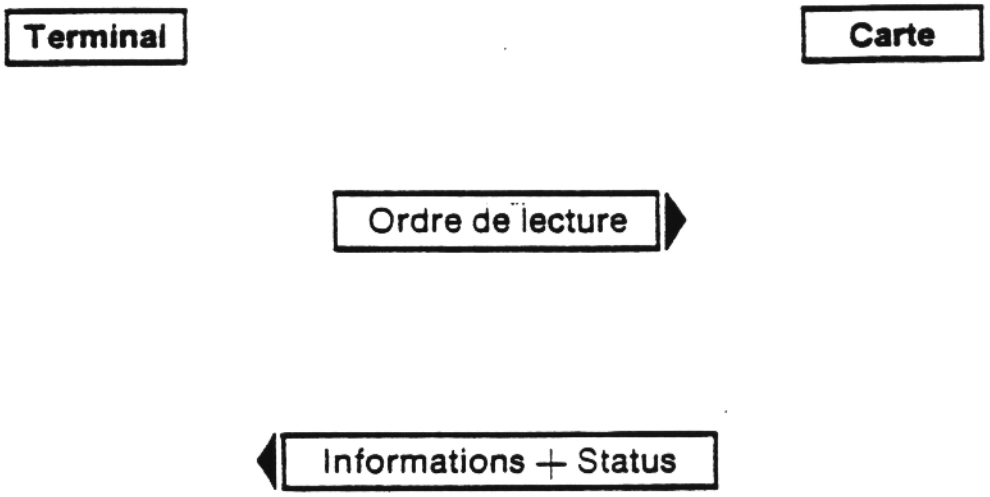

Figure 1.7 : Lecture dans une zone en LECTURE LIBRE

1.5.3 Récapitulatif des protections des zones en lecture.

La protection de la zone Transaction en lecture est spécifiée par le bit LP, situé dans un des mots de la Zone de Fabrication. Ce bit est positionné en phase de personnalisation, selon les besoins de l'application.

Zone	Protection	
Accès	Oui	
Confidentielle	Oui	
Transaction	* LP = 0 Oui	LP = 1 Non
Lecture	Non	
Fabrication	Non	
Locks	Non	

Tableau 1.3 : Protection des zones en lecture

1.6 L'écriture

1.6.1 Zone en ECRITURE PROTEGEE

Rappelons qu'à la fabrication du composant l'ensemble des bits de la mémoire PROM est au niveau logique 1. L'ECRITURE consiste à faire passer des bits du niveau logique 1 au niveau logique 0. Cette opération est irréversible.

1.6.1.1 Structure du mot mémoire

Un mot mémoire fait 32 bits. Les 32 bits sont répartis en deux groupes :

- 29 bits servant à mémoriser l'information proprement dite.
- 3 BITS SYSTEMES impliqués dans l'intégrité et la validité de l'information.

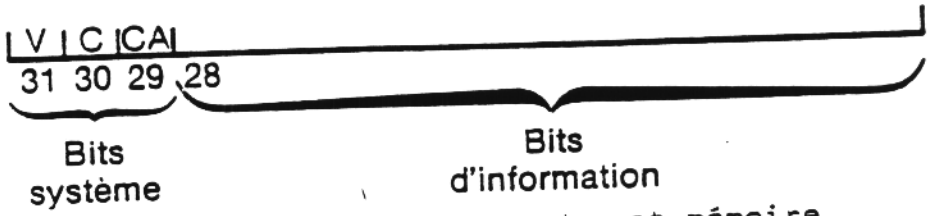

Figure 1.8 : Structure du mot mémoire

1.6.1.2 Les bits d'information

Comme leur nom l'indique, ils contiennent l'information écrite selon les besoins de l'application.

1.6.1.3 Les bits C, CA

Nous avons vu qu'il était possible de savoir "qui a écrit quoi". En particulier savoir si une information a été écrite sous la responsabilité de l'émetteur primaire, secondaire ou du porteur. Pour ce faire, les bits C, CA devront avoir les configurations suivantes :

		C	CA
Type 1	Emetteur primaire	1	1
	Emetteur secondaire	1	0
Type 2	Clé porteur, clé de fabrication	0	X

Tableau 1.4 : Signification des bits C, CA

On remarquera que dans le cas d'une validation sous clé type 2, le bit Ca n'est pas utilisé. Aussi, il peut être utilisé comme bit d'information et porte leur nombre à 30.

1.6.1.4 Le bit V

Nous avons vu que nous pouvons écrire des informations dans un ou plusieurs mots, et signifier qui avait écrit quoi à l'aide des bits C et C_A. Toutefois, il est important, lorsqu'on relit l'information, d'être certain que l'information n'a pas été dégradée, volontairement ou pas, et que celui qui l'a écrite s'est bien identifié. En effet, sur ce dernier point, n'importe qui peut positionner les bits C et C_A dans la configuration qu'il désire.

Le positionnement du bit V permet de répondre à cette double nécessité. Lorsque les bits d'information et les bits C et CA sont positionnés, on peut envoyer un ordre de validation en écriture qui consiste à :

- "identifier" qui a écrit l'information. Pour ce faire et préalablement à l'ordre de validation en écriture, une clé aura dû être présentée à la carte.
- Sur réception de l'ordre de VALIDATION en ECRITURE, le micro-calculateur compare le type de clé présentée (émetteur primaire, secondaire, porteur), avec le type de clé signifié par les bits C et CA.

Si les types sont différents, l'ordre de validation est abandonné.
Si les types concordent, et si la clé est bonne, le bit V du mot est positionné à 0.

Si la clé est mauvaise on retombe dans le même cas de figure que la lecture en zone protégée (trois essais pour clé type 2, un pour clé type 1).

Lorsque le bit V d'un mot est à 0, toute nouvelle tentative d'écriture ou de validation de ce mot sera refusé par la carte.

En conclusion, on dira que lorsqu'une zone est en ECRITURE PROTEGEE, la VALIDATION en ECRITURE d'un mot nécessite la PRESENTATION préalable de la CLE signifiée par les bits C, et CA. Par contre, il est toujours possible d'écrire sans présentation de clé préalable les bits informations et C, CA.
Cette opération d'écriture, tant que le mot n'est pas validé, peut être faite autant de fois que l'on veut, jusqu'à concurrence de nombre de bits restant au niveau 1. Cette propriété peut être utilisée dans le cas d'une consommation d'unités, de jetons etc...

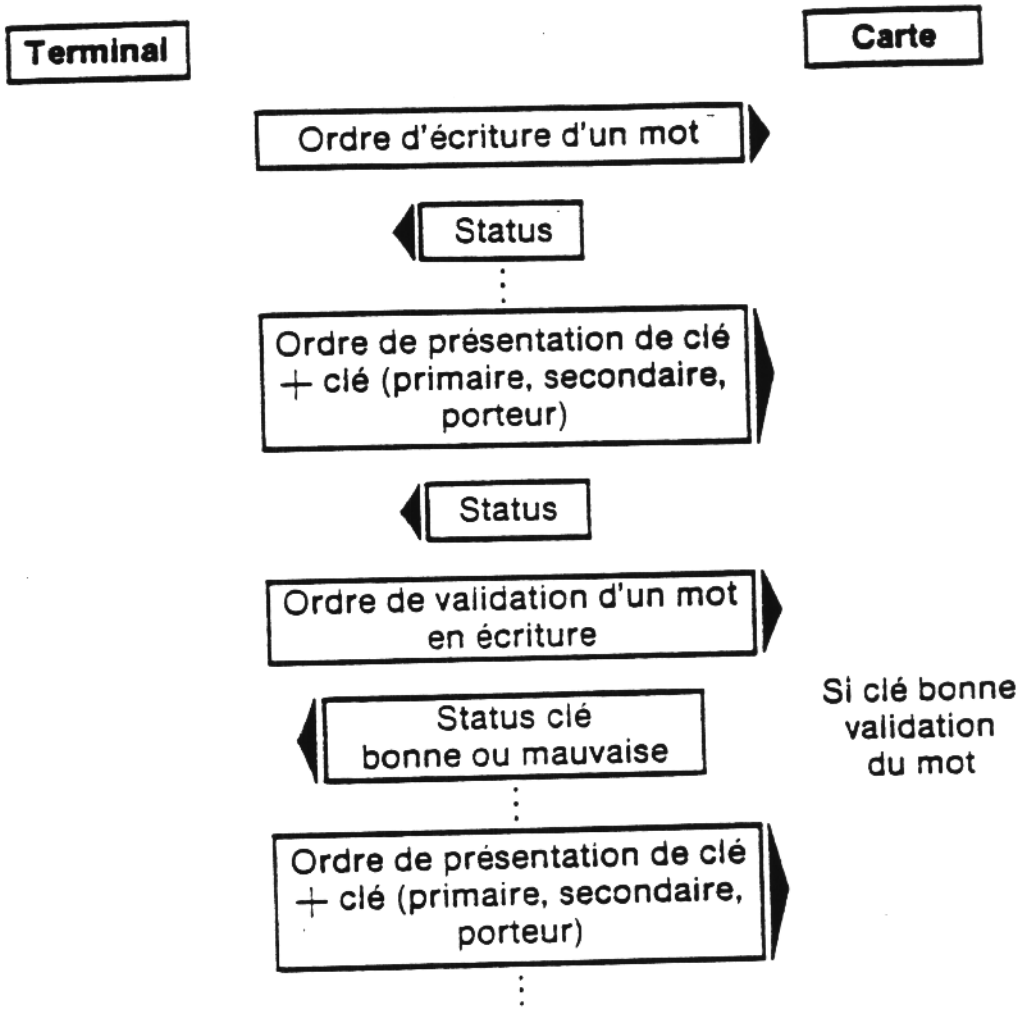

Figure 1.9 : Ecriture et Validation dans une zone en ECRITURE PROTEGEE

1.6.2 Zone EN ECRITURE LIBRE

La règle d'écriture est la même, on peut écrire dans un même mot tant qu'il n'est pas validé.
La validation d'un mot dans une telle zone ne requiert aucune présentation de clé, et il s'ensuit que les bits C,Ca peuvent être utilisés comme bits d'information.

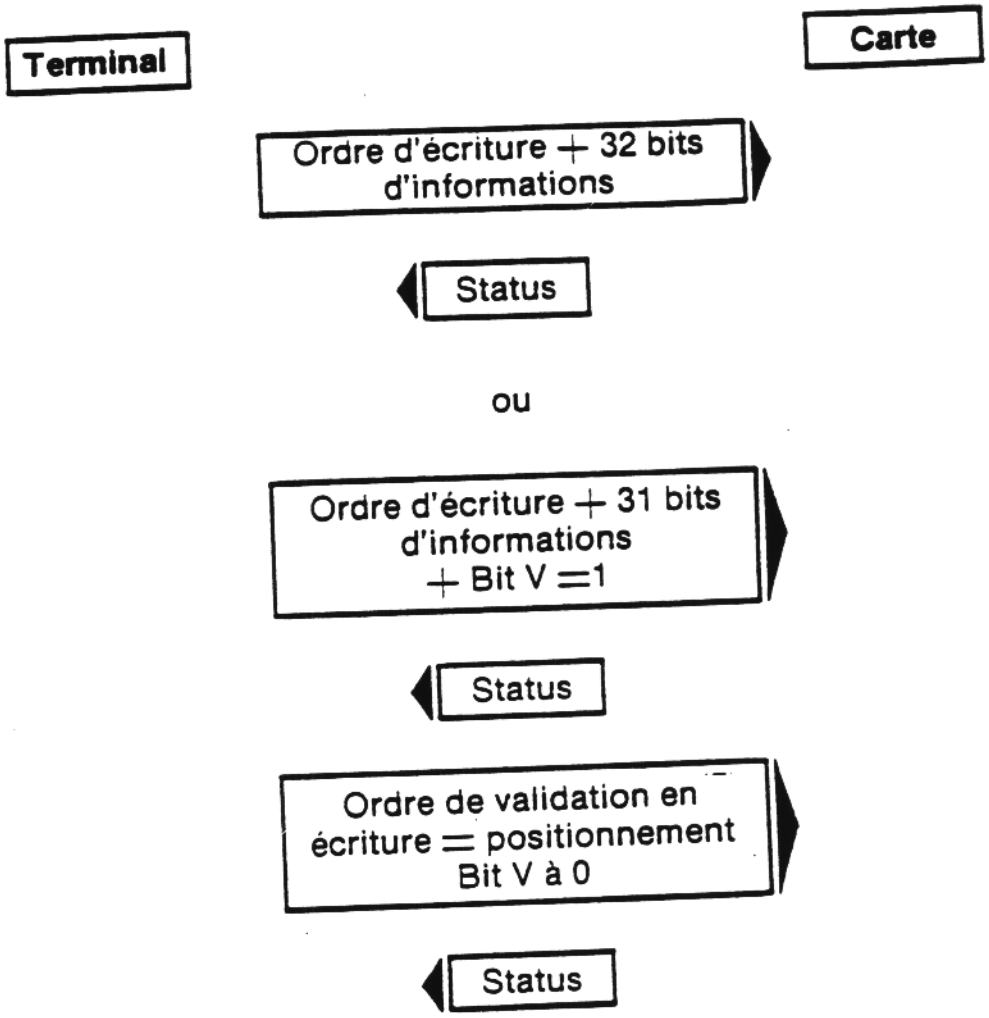

Figure 1.10 : Ecriture dans une zone en ECRITURE LIBRE

1.6.3 Récapitulatif des protections des zones en écriture.

Ce récapitulatif est simple, car seule la Zone Transaction est accessible en écriture. La protection de la Zone Transaction en écriture est spécifiée par le bit EP, situé dans un des mots de la Zone de fabrication. Ce bit est positionné en phase de personnalisation, selon les besoins de l'application.

EP	Protection de la ZT
1	Ecriture libre
0	Ecriture protégée

Tableau 1.5 : protection des zones en écriture

1.7 Blocage et Recyclage d'une carte

La figure ci-dessous résume les différentes manières de bloquer et recycler une carte.

Ce principe est vrai pour les demandes de validation de clé en lecture et en écriture.

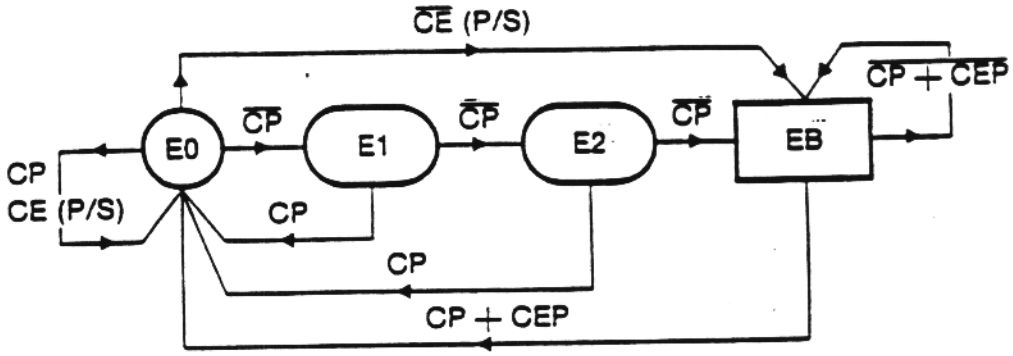

Figure 1.11: blocage et recyclage

E0	:	Carte non bloquée; fonctionnement normal
E1	:	Etat 1 erreur
E2	:	Etat 2 erreurs
EB	:	Etat bloqué; recyclage nécessaire
CP	:	présentation et demande de validation d'une clé porteur bonne
CE	:	présentation et demande de validation d'une clé émetteur bonne
$\overline{CP}$	:	présentation et demande de validation d'une clé porteur mauvaise
$\overline{CE}$	:	présentation et demande de validation d'une clé émetteur mauvaise
CP+CEP	:	Recyclage avec clés bonnes
$\overline{CP+CEP}$	:	Recyclage avec clé(s) mauvaise(s)

1.8 La fonction TELEPASS

Le programme MASQUE 4 est capable de réaliser une fonction logico-mathématique. Cette fonction est symbolisée sur la figure ci-dessous.

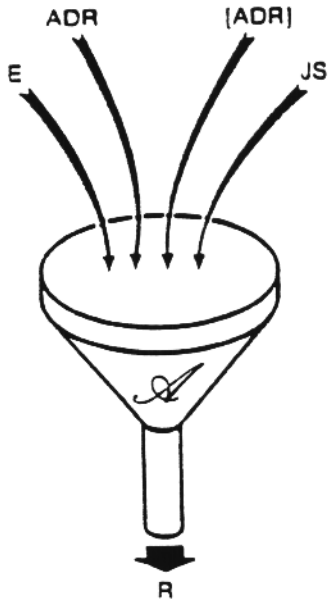

Figure 1.12 : La fonction TELEPASS

La fonction TELEPASS peut également être formulée comme suit :

$$R = F (E, ADR, (ADR), S)$$

Avec:

E = nombre aléatoire de 48 bits.
ADR = adresse d'un mot situé dans une des zones accessible en lecture (ZA, ZC, ZT, ZL, ZF)
E et ADR sont envoyés à la carte.

Et :
S = Jeu secret mémorisé dans la Zone Secrète
(ADR) = Contenu du mot pointé par ADR
S et (ADR) sont des données internes à la carte.

Propriétés:
- Le Résultat R,sur 64 bits, variera si un seul des paramètres change.
  Si par exemple, on fait exécuter à une même carte deux fonctions TELEPASS avec deux E différents, toutes choses égales par ailleurs, on obtiendra deux R différents.
- La fonction TELEPASS est un algorithme à clé secrète. Cette clé secrète est le Jeu Secret, dont il est impossible de connaître la valeur, étant mémorisé dans la Zone Secrète.
- La fonction TELEPASS est non réversible : connaissant R, il est impossible de retrouver E, ADR, (ADR) ou S.

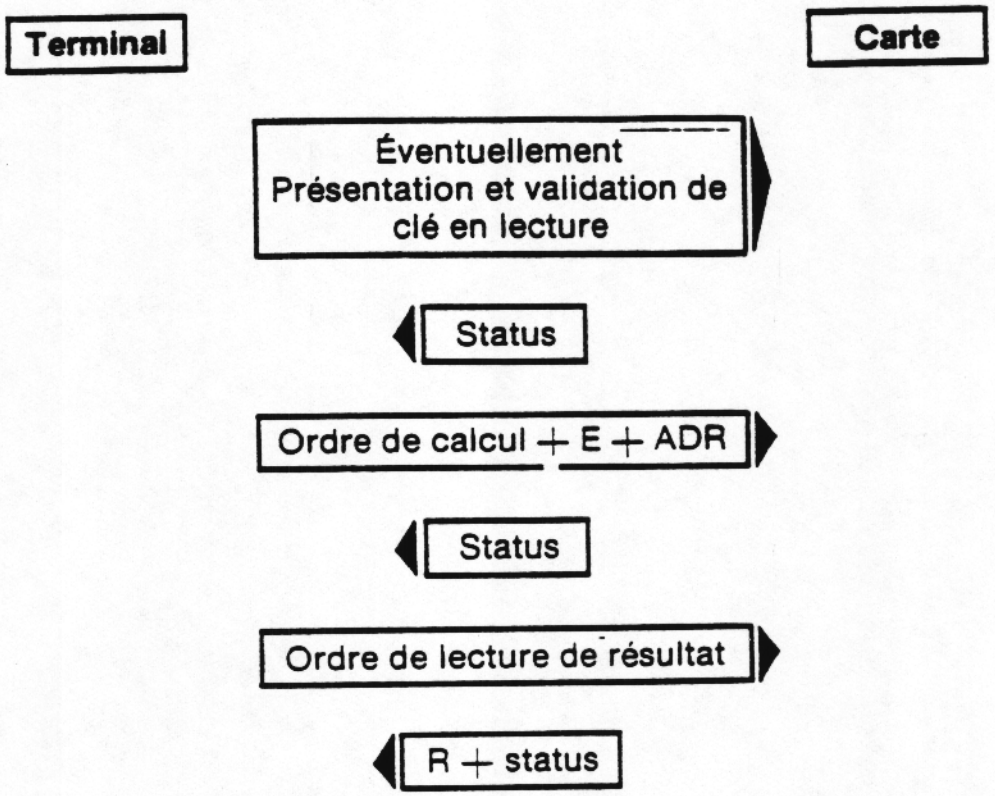

Figure 1.13 : Scénario d'exécution de la fonction TELEPASS

2. ETUDE DETAILLEE DES DIFFERENTES ZONES

2.1 Expression de l'adresse d'un mot

Chacun des 256 mots de la mémoire PROM est accessible via une adresse. Cette adresse est un nombre multiple de 8;
8 car l'adresse pointe en fait sur un quartet (4 bits) et un mot est constitué de 8 quartets.

Toutes les adresses seront exprimées en hexadécimal. L'adresse du premier mot est 200.

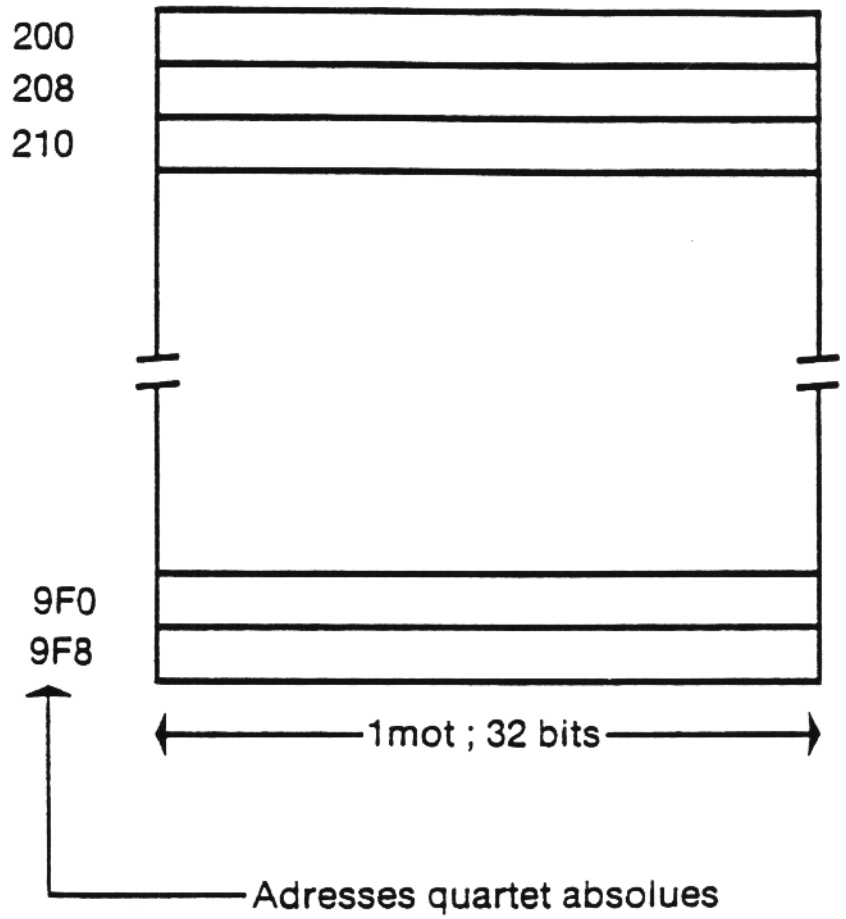

Figure 2.1 : Adressage des mots

2.2 La ZONE SECRETE

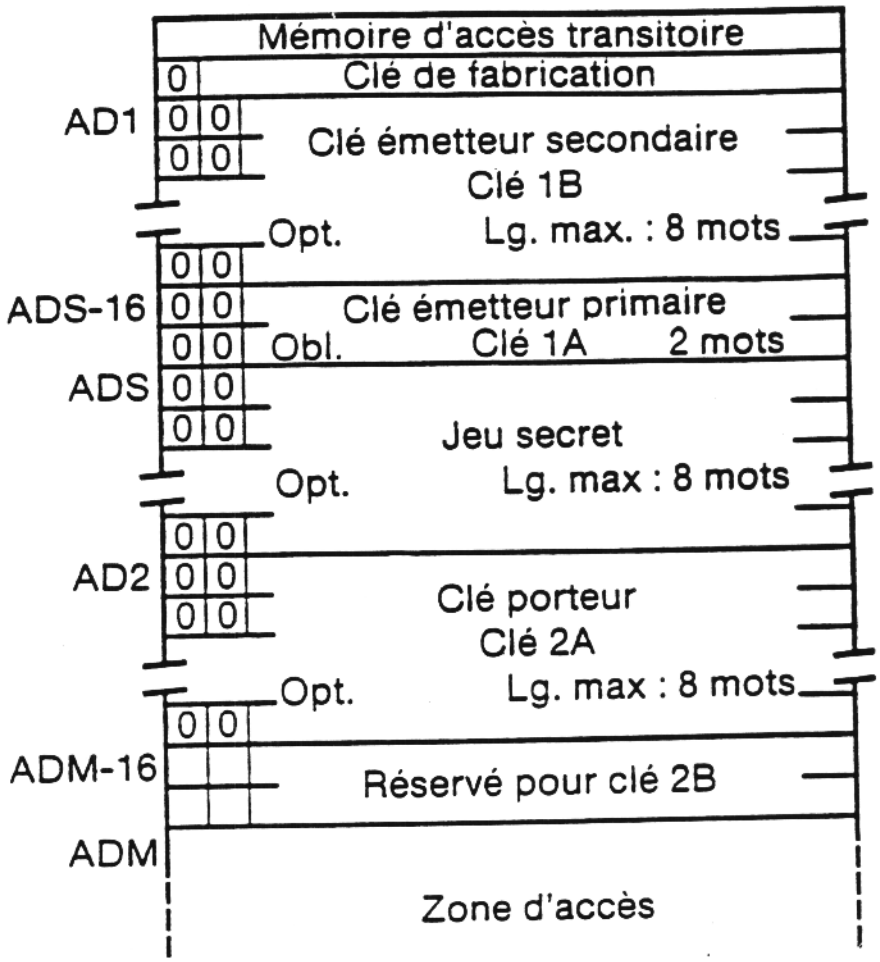

Figure 2.2 : La zone secrète

2.2.1 Les deux premiers mots de la mémoire

Jusqu'à présent, ils ont été volontairement ignorés car leur contenu ne joue aucun rôle dans une carte personnalisée; par contre, ils sont importants en phases de FABRICATION et de PERSONNALISATION.

Le mot d'adresse 200 est utilisé pour les premiers tests du composant et joue le rôle provisoire de zone d'accès lorsqu'elle n'existe pas encore.

Le mot d'adresse 208, écrit en phase de FABRICATION, contient la clé de FABRICATION, NECESSAIRE en phase de PERSONNALISATION à la validation en écriture des différents mots. C'est donc le premier niveau de protection d'accès en écriture de la mémoire.

2.2.2 La clé EMETTEUR SECONDAIRE ou CLE 1B

- La présence de la clé 1B est OPTIONNELLE, l'utilisation d'une carte par un émetteur secondaire n'étant pas systématique.

- Sa longueur est variable, de 1 à 8 mots maximum.

- Elle est inscrite dans la mémoire durant la phase de personnalisation.

- Le programme M4 connait l'adresse de cette clé grâce au pointeur AD1 situé en ZF.

- Les bits V et C sont à 0, ce qui signifie que les mots ont été validés en écriture après présentation d'une clé de type 1 soit la clé de fabrication.

- Pour une application donnée, toutes les cartes peuvent avoir la même clé 1B, ou chacune sa clé propre, dans ce cas la clé est dite DIVERSIFIEE.

  Cette clé est une valeur binaire, choisie arbitrairement ou calculée selon les spécifications propres à l'émetteur secondaire.

- Elle est utilisée par l'émetteur secondaire pour ouvrir l'accès en lecture aux zones protégées en lecture (ZA, ZC, ZT si CF) et pour valider en écriture les informations qu'il désire écrire en ZT.

2.2.3 La clé EMETTEUR PRIMAIRE ou CLE 1A

- La présence de la CLE 1A est OBLIGATOIRE.

- Sa longueur fixe est de 2 mots.

- Elle est inscrite dans la mémoire durant la phase de personnalisation.

- La programme M4 connait l'adresse de cette clé grace au pointeur ADS (ADS-16) situé en ZF.

- Les Bits V et C sont à 0 ce qui signifie que les 2 mots ont été validés en écriture après présentation d'une clé de type 2, soit la clé de fabrication.

- Pour une application donnée, toutes les cartes peuvent avoir la même clé 1A, ou chacune sa clé propre, dans ce cas la clé est dite DIVERSIFIEE.
Cette clé est une valeur binaire, choisie arbitrairement ou calculée selon les spécifications propres à l'émetteur primaire.

- Elle est utilisée par l'émetteur primaire pour ouvrir l'accès en lecture aux zones protégées en lecture (ZA, ZC, ZT si LP=0), et pour valider en écriture les informations qu'il désire écrire en ZT.
Enfin, elle est nécessaire au recyclage de la carte lorsqu'elle est bloquée.

2.2.4 Le JEU SECRET ou JS

- La présence du Jeu secret est optionnelle, la fonction TELEPASS d'une carte n'étant pas nécessairement activée.

- Sa longueur est variable, de 1 à 8 mots maximum.

- Il est inscrit dans la mémoire durant la phase de personnalisation.

- Le programme M4 connait l'adresse du jeu secret grâce au pointeur ADS situé en ZF.

- Les bits V et C sont à 0, ce qui signifie que les mots ont été validés en écriture après présentation d'une clé de type 2, soit la clé de fabrication.

- Pour une application donnée, toutes les cartes peuvent avoir le même JS, ou chacune son propre secret, dans ce cas le Jeu Secret est dit DIVERSIFIE.

- Ce jeu secret est une valeur binaire, choisie arbitrairement ou calculée selon la spécification d'un ou des deux émetteur(s)

2.2.5 La CLE PORTEUR ou CLE 2A

- La présence de la clé 2A est OPTIONNELLE, certaines applications ne nécessitant pas l'identification du porteur.

- Sa longueur est variable de 1 à 8 mots.

- Elle est inscrite dans la mémoire durant la phase de personnalisation.

- Le programme M4 connait l'adresse de cette clé grâce au pointeur AD2 situé en ZF.

- Les bits V et C sont à 0, ce qui signifie que les mots ont été validés en écriture après présentation d'une clé de type 2, soit la clé de fabrication.

- Pour une même application, toutes les cartes peuvent avoir la même clé 2A ou chacune sa clé 2A propre, dans ce cas elle est dite diversifiée.

  Cette clé est une valeur binaire, choisie arbitrairement ou calculée selon les spécifications d'un ou des deux émetteur (s).

- Cette clé est en général connue du porteur et correspond au code confidentiel des cartes à piste.

- Exemple

Supposons le code confidentiel 4590, tel qu'il serait saisi sur un clavier par le porteur. Il pourra être mémorisé en BCD sous la forme suivante.

Représentation interne à la carte en binaire:

```
VC
0001 0010 0101 0100 0011 1111 1111 1111
  4    9    5    0    padding à 1
```

Soit en hexadécimal : 12 54 3F FF

2.2.6 La seconde CLE PORTEUR ou CLE 2B

La carte CP8 masque 4 offre au porteur la possibilité d'affecter à sa carte une nouvelle clé porteur ou clé 2B choisie par lui-même, remplaçant définitivement celle inscrite pendant la phase de personnalisation, à savoir la clé 2A.

- Pour ce faire, une zone doit être réservée en phase de personnalisation.

- Sa longueur fixe est de 2 mots.

- Le programme M4 connait l'adresse du premier des 2 mots grâce au pointeur ADM (ADM - 16) situé en ZF.

- Ces deux mots, vierges à la fin de la phase de personnalisation, seront écrits durant la vie de la carte, lorsque le porteur désirera changer son code porteur.

  On notera que la nouvelle clé inscrite dans ces deux mots ne sera effectivement prise en compte que lorsque le bit LU sera positionné à 0. Cela étant, les deux mots seront "rattachés" fonctionnellement à la Zone Secrète.

2.3 La ZONE D'ACCES

La Zone d'Accès est utilisée par le programme M4 pour mémoriser :

- Les résultats possibles d'une demande de validation en lecture d'une clé de type 1 ou 2 à savoir:
  Clé type 1 ou 2 bonne.
  Clé type 1 fausse.
  Clé type 2 fausse. (trois tentatives possibles)

- Les résultats possibles d'une demande de validation de clé en écriture:
  Clé type 1 fausse.
  Clé type 2 fausse (trois tentatives possibles).

Le cas clé 1 ou 2 bonne n'est pas mémorisé en Zone d'Accès, mais par le biais du positionnement du bit V à 0 du mot à valider.

L'ensemble des mots de la Zone d'Accès est divisé logiquement en fenêtres d'accès de 4 bits. Les différentes valeurs prises par ces fenêtres sont les suivantes :

fenêtres d'accès normales	1111	fenêtre vierge
	0111	1 clé type 1 ou 2 bonnes
	0011	2 "
	0001	3 "
	0000	4 "
fenêtres d'erreur	1011	clé type 2 fausse, 1er essai
	1001	" , 2ème essai
	1000	" , 3ème essai carte bloquée
	1110	clé type 1 fausse, carte bloquée.

Dynamiquement cela se passe comme suit :
Soit une Zone d'Accès de 3 mots, tous vierges.

```
                              1 mot
                    <------------------------------------>
                  1 fenêtre
                    <-->
                    1111 1111 1111 1111 1111 1111 1111 1111
ADM
3 MOTS              1111 1111 1111 1111 1111 1111 1111 1111
                    1111 1111 1111 1111 1111 1111 1111 1111
```

Figure 2.3.1 : La zone d'accès

Après une première demande de validation en lecture d'une clé type 1 ou 2 correcte, la zone d'accès deviendra :

```
  ADM               0111 1111 1111 1111 1111 1111 1111 1111
3 MOTS              1111 1111 1111 1111 1111 1111 1111 1111
                    1111 1111 1111 1111 1111 1111 1111 1111
```

Figure 2.3.2 : La zone d'accès

La fenêtre soulignée est la dernière fenêtre active.

Après une seconde demande :

```
  ADM               0011 1111 1111 1111 1111 1111 1111 1111
3 MOTS              1111 1111 1111 1111 1111 1111 1111 1111
                    1111 1111 1111 1111 1111 1111 1111 1111
```

Figure 2.3.3 : La zone d'accès

..... Après une cinquième demande :

```
  ADM               0000 0111 1111 1111 1111 1111 1111 1111
3 MOTS              1111 1111 1111 1111 1111 1111 1111 1111
                    1111 1111 1111 1111 1111 1111 1111 1111
```

Figure 2.3.4 : La zone d'accès

Supposons maintenant qu'une demande de validation en lecture (ou écriture) soit faite après présentation d'une clé type 2 fausse; une fenêtre d'erreur est alors ouverte.

ADM	0000 0111 1011 1111 1111 1111 1111 1111
3 MOTS	1111 1111 1111 1111 1111 1111 1111 1111
	1111 1111 1111 1111 1111 1111 1111 1111

Figure 2.3.5 : La zone d'accès

Remarque : les trois bits de la précédente fenêtre active sont perdus.

Une deuxième tentative avec une clé type 2 fausse est réalisée.

ADM	0000 0111 1001 1111 1111 1111 1111 1111
3 MOTS	1111 1111 1111 1111 1111 1111 1111 1111
	1111 1111 1111 1111 1111 1111 1111 1111

Figure 2.3.6 : La zone d'accès

Si, à la troisième tentative, la clé présentée est bonne, la fenêtre d'erreur redevient fenêtre d'accès normale.

ADM	0000 0111 0001 1111 1111 1111 1111 1111
3 MOTS	1111 1111 1111 1111 1111 1111 1111 1111
	1111 1111 1111 1111 1111 1111 1111 1111

Figure 2.3.7 : La zone d'accès

Remarque : Le grillage du premier bit de la fenêtre aurait également eu lieu après présentation d'une bonne clé au deuxième essai.

Supposons maintenant que nous avons fait trois demandes de validation d'une clé type 2 fausse, nous avons :

ADM	0000 0111 0001 1000 1111 1111 1111 1111
3 MOTS	1111 1111 1111 1111 1111 1111 1111 1111
	1111 1111 1111 1111 1111 1111 1111 1111

Figure 2.3.8 : La zone d'accès

La carte est BLOQUEE.

Après un recyclage, nous aurons :

ADM	0000 0111 0001 1000 0111 1111 1111 1111
3 MOTS	1111 1111 1111 1111 1111 1111 1111 1111
	1111 1111 1111 1111 1111 1111 1111 1111

Figure 2.3.9 : La zone d'accès

Après une demande de validation d'une clé type 1 fausse et un recyclage, nous aurons :

ADM	0000 0111 0001 1000 0111 1110 0111 1111
3 MOTS	1111 1111 1111 1111 1111 1111 1111 1111
	1111 1111 1111 1111 1111 1111 1111 1111

Figure 2.3.10 : La zone d'accès

- Il est possible, en lisant la Zone d'Accès, de compter le nombre de blocages, et d'en déterminer l'origine (blocage par clé type 1 ou 2).
- La durée de vie d'une carte est limitée par la dimension de sa Zone d'Accès. Lorsque l'octet de poids faible du dernier mot de la zone d'accès devient "non vierge", la carte est dite SATUREE
- La Zone d'Accès doit faire obligatoirement 1 mot minimum, (même s'il ne doit jamais être utilisé) et peut aller jusqu'à 64 mots maximum.

2.4 La ZONE CONFIDENTIELLE

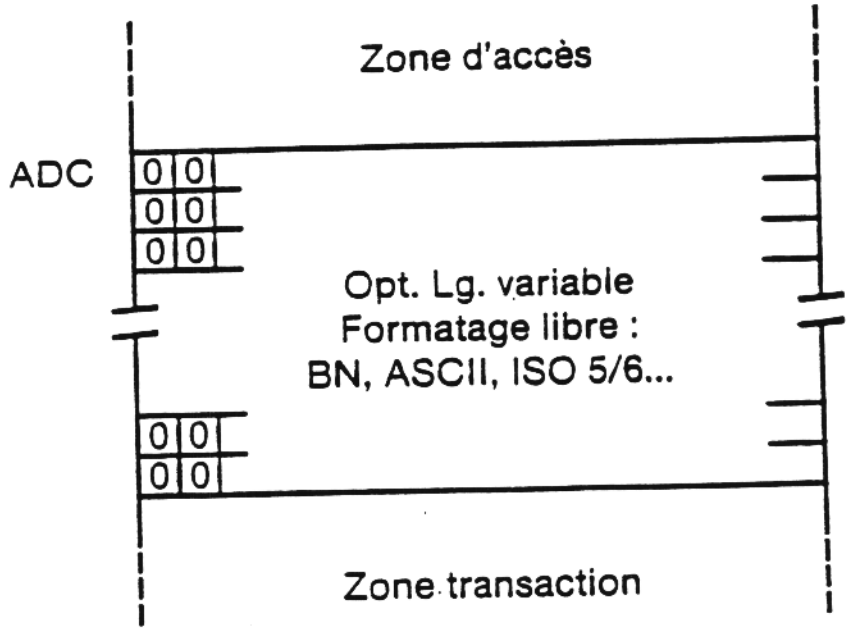

Figure 2.4 : La zone confidentielle

- La Zone Confidentielle est OPTIONNELLE et de taille VARIABLE.
- Lorsqu'elle existe, elle est définie et écrite pendant la phase de personnalisation.
- L'information stockée dans cette zone peut être de tous types: BCD, binaire pur, ISO5, ISO6, ASCII, CCR etc ... Elle est formatée de la manière qu'on le désire.
- Seule doit être respectée la règle de positionnement des bits V et C.
- Le programme M4 connait l'adresse du premier mot de la Zone Confidentielle grâce au pointeur ADC situé dans la ZF.

Exemple

Soit l'information "BULL CP8" écrite dans une Zone Confidentielle de 2 mots, implantée à l'adresse 300.
L'information est codée en ASCII:

300	3	4	25	54	C4
308	3	C	43	50	38

L'information est encadrée. On remarquera que le deuxième "L" est "à cheval" sur les deux mots (code 4C souligné).

" B "	=	42
" U "	=	55
" L "	=	4C
" L "	=	4C
" C "	=	43
" P "	=	50
" 8 "	=	38

2.5 La ZONE TRANSACTION

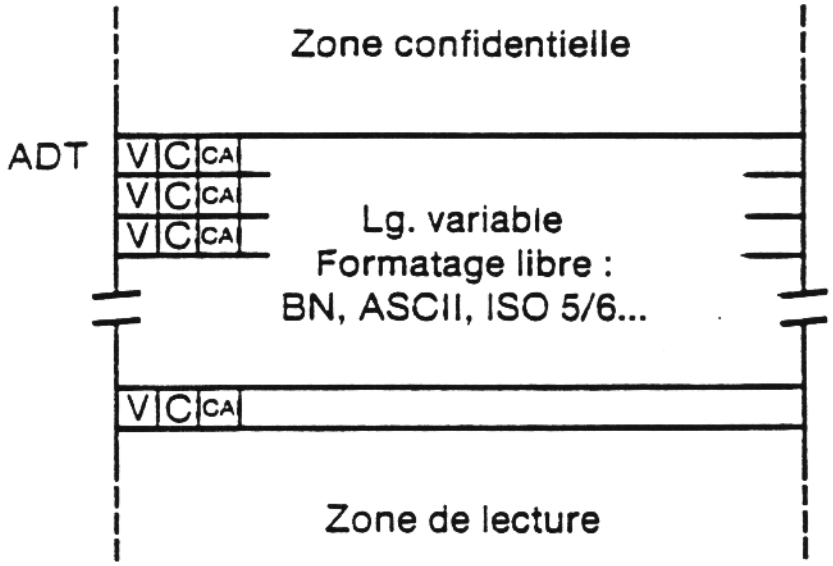

Figure 2.5 : La zone transaction

La Zone Transaction est OPTIONNELLE et de taille VARIABLE. (toutefois, une carte CP8 sans Zone Transaction est rare). La Zone Transaction est vierge en fin de phase de personnalisation.

Durant la vie de la carte, des informations seront écrites dans cette zone. Leur codification, comme pour la ZC, est indifférente au fonctionnement de la carte : BCD , binaire pur, ISO5, etc ... De même, la manière dont elles sont organisées est à la discrétion du concepteur.

Toutefois, en fonction des règles de protection d'accès de la ZT, les bits V, C, CA devront être correctement positionnés.

Le programme M4 connait l'adresse du premier mot de la zone transaction grâce au pointeur ADT situé dans la ZF.

2.6 La ZONE de LECTURE

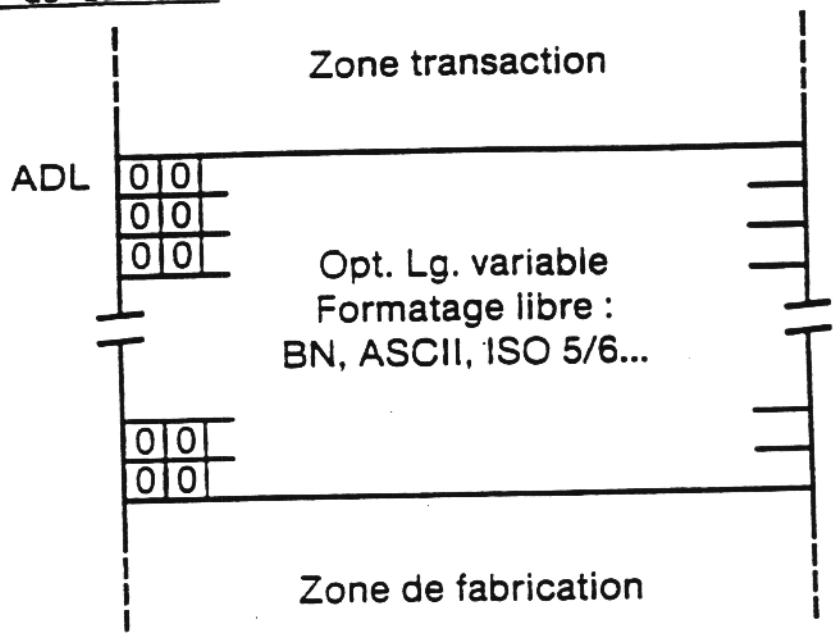

Figure 2.6 : La Zone de lecture

Identique en son principe à la Zone Confidentielle, exepté qu'elle est en lecture libre.

2.7 La Zone de FABRICATION

adresse	V	C	Zone de lecture			
9C0	0	0	Mot réservé			
9C8	0	0	ADL	CCR	ADT	CCR
9D0	0	0	ADC	CCR	ADM	CCR
9D8	0	0	AD2	CCR	ADS	CCR
9E0	0	0	Type d'application		0 0 1 0 0 0 0 EP LP 0 0	CCR
9E8	0	0	AD1	CCR	N° encarteur	CCR
9F0	0	0	N° de série			CCR

Figure 2.7 : La zone de fabrication

- La présence de cette zone est OBLIGATOIRE.
- Sa dimension est FIXE. Cette zone est écrite dans sa majeure partie durant la phase de personnalisation.
- Elle contient principalement l'ensemble des pointeurs définissant la dimension et l'implantation des différentes zones et clés vues précédemment ainsi que le type de protection d'accès de la Zone Transaction.

2.7.1 Les pointeurs

2.7.1.1 Principe de calcul des pointeurs

Nous avons vu que chaque mot avait une adresse multiple de 8. Par exemple, l'adresse du premier mot de la CLE 1B est 210 (en hexadécimal).
Le pointeur correspondant à ce mot est AD1. AD1 ne vaudra pas 210, mais 42 soit la valeur réelle de l'adresse, divisée par 8. Cela est vrai pour tous les autres pointeurs.

2.7.1.2 Les CCR

A chaque pointeur est associé un CCR de 5 bits permettant la détection d'une éventuelle destruction de l'information.

Ce CCR est le reste de la division polynomiale du contenu du champ à contrôler par le polynôme générateur $G(x)=x^7+x^2+1$

Les CCR sont écrits en même temps que les pointeurs, en phase de personnalisation.
Ils ne sont en aucun cas controlés par la carte elle-même.
Seules les applications mettant en oeuvre la carte CP8, pourront, si elles le désirent, les contrôler afin de s'assurer de l'intégrité des pointeurs.

2.7.1.3 Le pointeur de la Zone de Lecture : ADL

Ce pointeur pointe le premier mot de la Zone de Lecture.
Si la zone est absente, ADL=9C0. Il tient dans un champ de 9 bits.

2.7.1.4 Le pointeur de la Zone Transaction : ADT

Ce pointeur pointe le premier mot de la Zone Transaction.
Il tient dans un champ de 9 bits.

2.7.1.5 Le pointeur de la Zone Confidentielle : ADC

Ce pointeur pointe sur le premier mot de la Zone Confidentielle.
Si la zone est absente, ADC=ADT. Il tient dans un champ de 9 bits.

2.7.1.6 Le pointeur de la Zone d'Accès : ADM

Ce pointeur pointe sur le premier mot de la Zone d'Accès.
Il tient dans un champ de 9 bits.

2.7.1.7 Le pointeur de la Clé 2A : AD2

Ce pointeur pointe le premier des mots contenant la clé 2A.
Il tient sur un champ de 9 bits.

2.7.1.8 Le pointeur du Jeu Secret: ADS

Ce pointeur pointe le premier des mots contenant le Jeu Secret.
Si le jeu secret est absent, ADS=AD2. Il tient sur un champ de 11 bits.

2.7.1.9 Le pointeur de la clé 1B : AD1

Le pointeur pointe sur le premier des mots contenant la clé 1B.
Si la clé 1B est absente, AD1=ADS-16
Il tient sur un champ de 9 bits.

2.7.2 Le type d'application

Le type d'application sert à identifier l'application dans le cadre de laquelle est utilisée une carte.
Cette information est à la "discrétion" du concepteur.
Remarque: toutes les cartes n'appartenant pas aux applications bancaires ont les deux bits de poids forts du type d'application systématiquement positionnées à 0 (Cette opération est faite par BULL CP8).

2.7.3 EP, LP

Ces 2 bits déterminent le niveau de protection de la zone Transaction.

EP	LP	Protection de la ZT
1	1	Ecriture et lecture libres
1	0	Ecriture libre, lecture protégée
0	1	Ecriture protégée, lecture libre
0	0	Ecriture et lecture protégées

Tableau 2.1 : Protection de la ZT

2.7.4 Le numéro d'encarteur

Ce numéro sert à identifier l'encarteur du composant
BULL CP8 : 1
PHILIPS : 2
Il tient sur un champ de 11 bits. Le CCR associé est calculé sur les 11 bits.

2.7.5 Le numéro de série

Le numéro de série de la carte est un nombre binaire de 25 bits.
Le CCR associé est calculé sur ce champ de 25 bits.
Il est affecté par BULL CP8 en phase de PRE-PERSONNALISATION

2.8 La ZONE des LOCKS

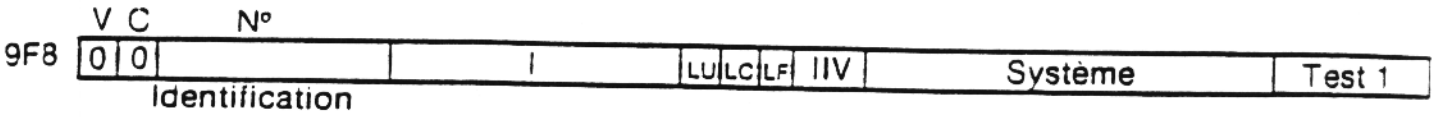

Figure 2.8 : La zone des Locks

Cette zone est constituée par le dernier mot de la mémoire PROM. Elle contient les LOCKS, bits indiquant la phase de vie de la carte, et des informations nécessaires au calcul de la Clé de Fabrication, lors de la phase de Personnalisation.

2.8.1 Les Locks

Les Locks (LU,LC,LF,IIV) sont un ensemble de bits indiquant la phase de vie de la carte, ou plus précisément, du composant CP8. Comme dans les autres bits de la mémoire, ils sont initialement au niveau logique 1. Positionner un Lock consiste à le faire passer au niveau logique 0. Cet état est irréversible. Cela est possible grâce l'ordre d'écriture des Locks.

2.8.1.1 Le lock LF

Lors de la fabrication du composant, le fabricant (Motorola ou Eurotechnique) inscrit dans la PROM les informations telles que la clé de fabrication, le pointeur AD1, le numéro d'identification etc...
A l'issue de cette phase le Lock LF est positionné à 0 et le composant est dit FABRIQUE.

2.8.1.2 Le lock LC

Le composant étant encarté, la mémoire PROM va être logiquement divisée en zones, et pour certaines d'entre elles les informations y seront écrites.

Cette phase est appelée PHASE de PERSONNALISATION.

A l'issue de cette phase, le lock LC est positionné à 0 et la carte est dite PERSONNALISEE.

Une telle carte peut-être mise en service.

2.8.1.3 Le lock LU

Nous avons vu que durant la phase d'utilisation de la carte, le porteur a la possibilitéé de modifier le code porteur initial.

Pour cela un nouveau code porteur ou CLE 2B est inscrit dans la zone réservée à cet effet (ADM-16).

Le programme considèrera le contenu de cette zone comme le nouveau code porteur seulement lorsque le lock LU sera positionné à 0.

2.8.1.4 Le lock IIV

Ce lock est en fait constitué de 2 bits.
Lorsqu'un des deux bits, ou les deux, est (sont) positionné(s) à 0, la carte est dite INVALIDEE.

Les ordres d'écriture et d'activation de la fonction TELEPASS seront refusés. Seuls les accès en lecture seront encore possibles. Ces locks sont positionnés lorsque l'on veut empêcher l'utilisation d'une carte si celle-ci est en liste noire, saturée en accès etc...

2.8.2 Numéro d'identification et I

Ces informations sont inscrites par le fabricant.
Elles sont utilisées pour le calcul de la clé de fabrication.
Le numéro d'identification est un champ de 7 bits, et le I un champ de 8 bits.

Ci dessous sont détaillés les mots 9C8 à 9F0 de la ZF avec pour chaque mot:
- la représentation binaire
- la représentation hexadécimale.
- les champs pointeur, CCR etc... et leur valeur propre.

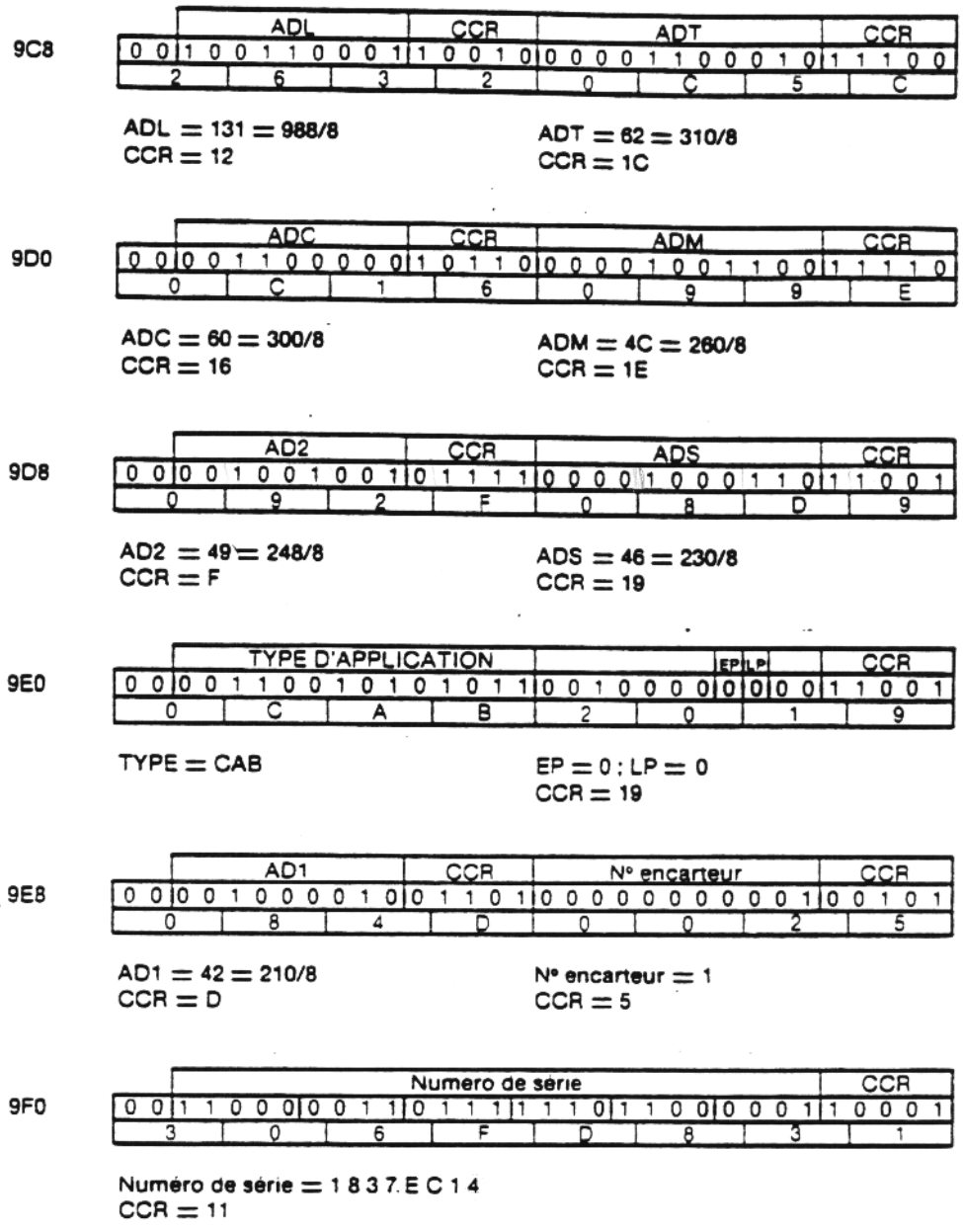

Figure 2.10 : détails d'une ZF

2.9 Mapping détaillé d'une PROM

Ci-dessous est présenté le format de la mémoire de la carte d'initiation CPB Masque 4.

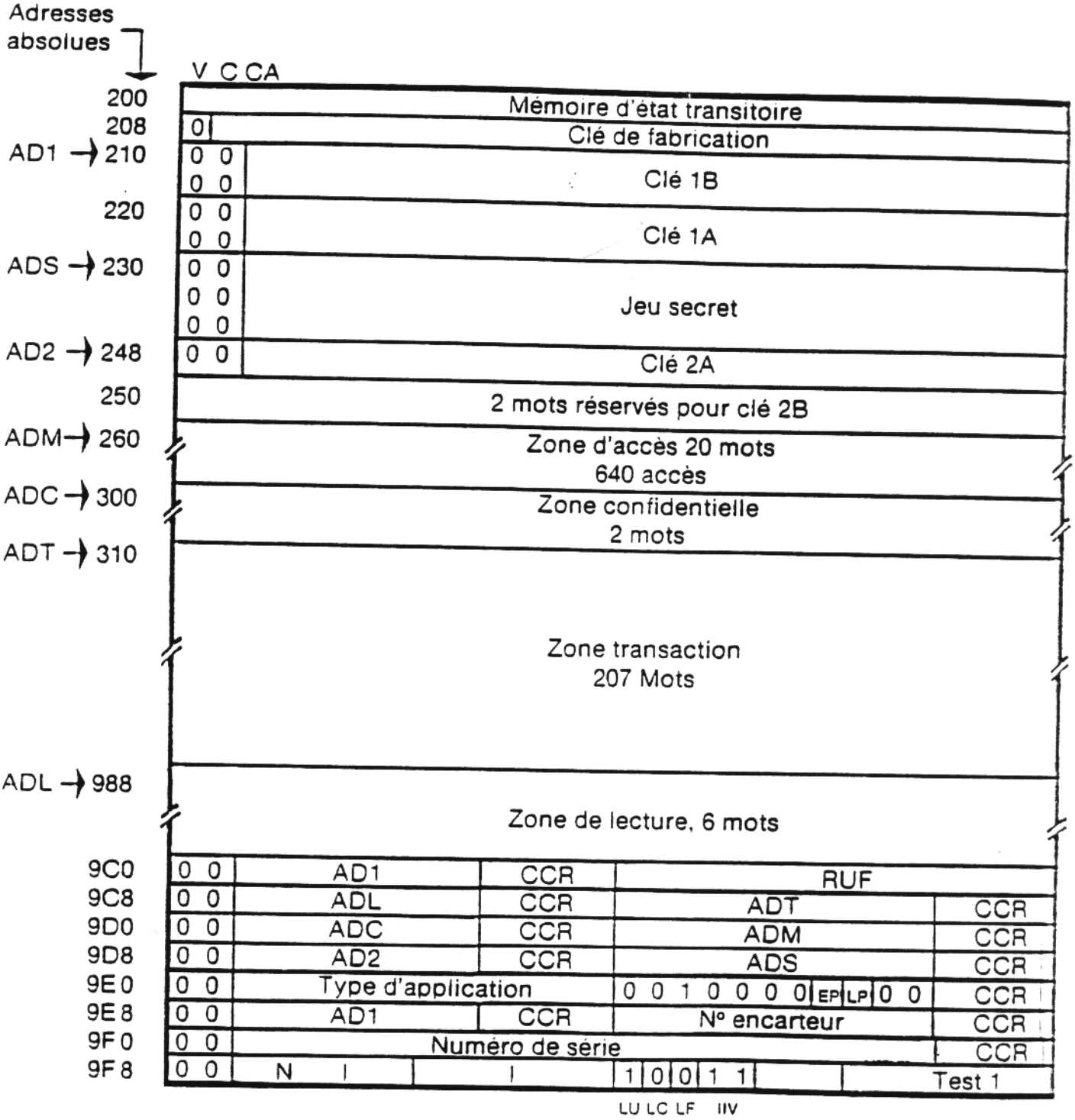

Figure 2.9 : Mapping détaillé d'une PROM

2.10 Accessibilité et protection des zones

Le tableau ci-après résume l'accessibilité et la protection des différentes zones d'une carte CP8 MASQUE 4 personnalisée.

		Accessible en lecture		Non accessible en lecture	Accessible en écriture		Non accessible en écriture
		Lecture protégée	Lecture libre		Écriture protégée	Écriture libre	
Zone secrète		•	•	V	•	•	V
Zone d'accès		V	•	•	•	•	V
Zone confidentielle		V	•	•	•	•	V
Zone transaction	LP = 0	V	•	•	—	—	—
	LP = 1	•	V	•	—	—	—
	EP = 0	—	—	—	V	•	•
	EP = 1	—	—	—	•	V	•
Zone de lecture		•	V	•	•	•	V
Zone de fabrication		•	V	•	•	•	V
Zone des locks		•	V	•	•	V	•

V = vrai ; • = faux ; — = sans objet

Tableau 2.2 : Accessibilité et protection des Zones d'une Carte personnalisée.

3. ELEMENTS DU DIALOGUE CARTE - TERMINAL

Nous avons vu au chapitre 1 que le dialogue CARTE-TERMINAL s'effectuait au moyen d'ordres tels que :

- écriture, lecture
- présentation et validation de clé
- activation de la fonction TELEPASS
- lecture de résultat

Le présent chapitre présente la nature des informations échangées, leur format, ainsi que le protocole d'échange.

3.1 L'ordre RAZ (remise à zéro)

Avant d'exécuter un quelconque ordre, le composant doit s'initialiser et spécifier au TERMINAL ses caractéristiques propres. Tel est l'objet de l'ordre RAZ.
(on remarquera, que l'ordre RAZ n'est pas un ordre au sens stricte du terme, car il est activé "hardwarement" par un signal appliqué sur le contact RAZ).

A l'issue de cette RAZ, le composant MASQUE 4 envoie au TERMINAL 9 octets :

- 4 octets dits "système".

- 5 octets dits "application".

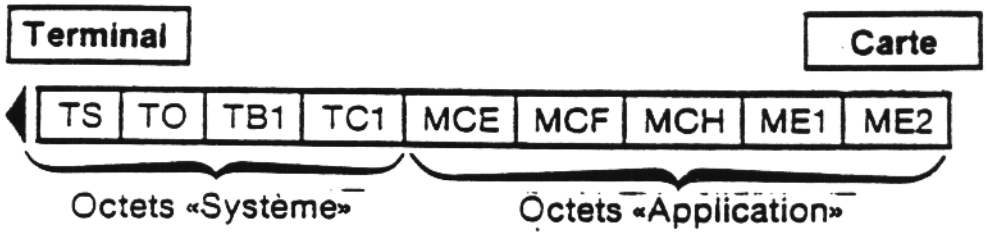

Figure 3.1 : Octets rendus à la RAZ

3.1.1 Octets Systèmes

TS=3F : Spécifie que les données échangées seront transférées poids forts en tête, avec une parité paire, et que la fréquence d'horloge à fournir à la carte est 3.579545 Mhz.

TO=65 : Spécifie la présence ou l'absence des octets système TA1, TB1, TC1, TD1, et le nombre d'octets caractérisant l'application.

TB1=33 : Définit la tension et l'intensité de courant maximum de programmation.

TC1=10
ou 64 : Définit l'intervalle de temps minimum séparant l'émission par le TERMINAL, de deux caractères. (10 si Carte non bloquée, 64 si Carte bloquée).

Tels sont les 4 octets système envoyés par la carte à l'issue d'une RAZ.(Toutefois, dans la pratique les coupleurs CP8 gérant le dialogue élémentaire renvoient l'octet TS complémenté, et rajoutent deux octets supplémentaires: TA1 = 11 et TD1 = 00 .)

3.1.2 Octets Application

Ces octets permettent à l'utilisateur:

- d'identifier la carte en présence
- de connaitre la phase de vie dans laquelle elle se trouve
- d'avoir un compte rendu exact de la dernière fenêtre active de la zone d'accès

3.1.2.1 MCE : Mot des Caractéristiques PROM

MCE = 1 Composant fabriqué par MOTOROLA
= 2 Composant fabriqué par EUROTECHNIQUE

3.1.2.2 MCF : Mot des Caractéristiques Fonctionnelles

Ce numéro de MASQUE définit une Classe d'Instruction, BC, et un jeu d'ordres spécifique.

MCF = 4 numéro de masque

3.1.2.3 MCH : Mot "CHRONOLOGIQUE"

Cet octet indique la phase de vie où se trouve la carte ainsi que le niveau de protection de la zone transaction. On remarquera que dans MCH, l'information est exprimée en "logique positive", alors que dans la carte elle est exprimée en logique négative. Ainsi, si dans la zone de fabrication EP=0, le bit image correspondant IEP dans MCH est égal à 1.

	ILU	ILC	ILF	IIV	IEP	ILP	O	O
Bits	7	6	5	4	3	2	1	0

Figure 3.2 : MCH

ILP = 1 La zone transaction est en lecture protégée
(LP = 0 en ZF)
ILP = 0 La zone transaction est en lecture libre
(LP = 1 en ZF)

IEP = 1 La zone transaction est en écriture protégée
(EP = 0 en ZF)
IEP = 0 La zone transaction est en écriture libre
(EP = 1 en ZF)

IIV = 1 La carte est invalidée (locks IV différents de 11)
IIV = 0 La carte n'est pas invalidée (locks IV = 11)

ILF = 1 La carte est fabriquée (lock LF = 0)
ILF = 0 La carte n'est pas "fabriquée"(lock LF = 1)

ILC = 1 La carte est personnalisée (lock LC = 0)
ILC = 0 La carte n'est pas personnalisée (lock LC=1)

ILU = 1 Clé 2B active (lock LU = 0)
ILU = 0 Clé 2A (s'il y en a une) active (lock LU = 1)

Exemple : - si une carte est juste fabriquée, MCH = 20
- si une carte est personnalisée, avec une ZT protégée en lecture et en écriture, MCH = 6C

3.1.2.4 ME1, ME2 : Compte-rendu d'exécution

Ce sont les deux derniers octets rendus lors de la RAZ, mais également à la fin de tous les ordres.

ME1 = 90 fin normale
= 6X fin anormale

ME2 : ME2 n'est significatif que si ME1 = 90

	IF	IT	IE2	IE1	CCF	CF		ER
Bits	7	6	5	4	3	2	1	0

Figure 3.3 : ME2

ER = 1 : erreur déclarée par la carte, à la suite de laquelle elle deviendra muette à la réception du prochain ordre, quelqu'il soit. Dans ce cas, seule une nouvelle RAZ permettra de réinstaurer le dialogue.

CF = 1 : Clé fausse, suite à une demande de validation de clé.

CCF : CCF n'a de sens que si CF = 1 et suite à une tentative de recyclage "malheureux".

CCF = 1 la clé 2 était mauvaise
CCF = 0 la clé 2 était bonne, autrement dit la CLE 1 A était fausse.

ER, CF et CCF seront positionnés après l'exécution d'un ordre

IE1 = 1: la dernière fenêtre active de la zone d'accès est en position 1 erreur (1011).

IE2 = 1: la dernière fenêtre active de la zone d'accès est en position 2 erreurs (1001).

IT = 1: la carte est bloquée. (1XX0)

IF = 1: la zone d'accès est saturée, l'octet de poids faible du dernier mot de la zone est différent de FF.

Exemple:
Une Carte en fonctionnement normal rendra ME2 = 00.
Une Carte bloquée rendra ME2 = 40.
Une Carte saturée rendra ME2 = 80.

3.2 Principe général de déroulement d'un ordre

Un ordre est exécuté en 3 phases:

- Initialisation
- Exécution
- Fin

3.2.1 Initialisation

Lors de l'initialisation, le terminal envoie à la carte 5 octets, décomposés comme suit:

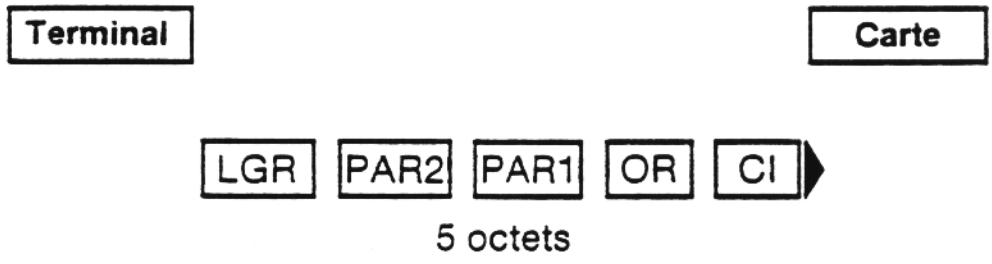

Figure 3.4 : initialisation d'un ordre

- CI = BC; classe d'instruction de la carte MASQUE 4.
- OR (ou CODOP) = code hexadécimal de l'ordre à exécuter (le bit de poids faibles est toujours à 0).

  Exemple : OR = B0 pour l'ordre de lecture standard

- PAR1 (ou A1), PAR2 (ou A2) = adresse quartet de lecture ou d'écriture.

  Exemple : lorsqu'on veut lire le mot d'adresse 9F0, alors PAR1 = 09 et PAR 2 = F0.

- LG = longueur en octets des données à transférer pendant la phase d'exécution, dans un sens comme dans l'autre, entre la carte et le terminal. LG est toujours inférieure ou égale à 20 (soit 32 en décimal).

  Exemple : si on veut lire 2 mots, LG=08.

3.2.2 Exécution d'un Ordre

3.2.2.1 L'octet d'acquittement

La carte acquitte la réception des 5 octets en renvoyant un octet d'acquittement.

Dans cet octet, la carte spécifiera le mode d'échange des données, ainsi que la nécessité ou pas de la tension de programmation Vpp.

On distingue deux modes d'échange, compte-tenu de la longueur des données à transférer. La carte a une capacité de stockage de l'information limitée, liée à la dimension de sa RAM. Ainsi, si les données sont nombreuses, elle "cadencera" le transfert des données : c'est le MODE ASSERVI. Dans le cas contraire, l'ensemble des données est transféré d'un seul bloc, c'est le MODE SIMPLE.

Dans chacun de ces deux cas, SIMPLE et ASSERVI, la carte peut demander la présence du Vpp, afin de pouvoir écrire (suite à un ordre d'écriture par exemple) ou pas. Pour ce faire, l'octet d'acquittement ACQ aura les formats suivants.

ACQ	M. simple	M. asservi
$\overline{Vpp}$	OR	$\overline{OR}$
Vpp	OR + 1	$\overline{OR + 1}$

NOTA : L'ordre envoyé par le terminal doit avoir toujours le bit de poids faible libre.

Tableau 3.1 : formats de l'octet d'acquittement ACQ

3.2.2.2 Transfert de DONNEES et exécution de l'ordre

A la suite de l'envoie de l'octet ACQ, un transfert de DONNEES peut avoir lieu si nécessaire et la carte exécute l'ordre proprement dit. Les DONNEES échangées seront les mots lus ou écris dans la Carte, les clés, les données d'entrée ou le résultat R de la fonction TELEPASS.

3.2.2.3 Fin de l'ordre : ME1, ME2

L'ordre étant exécuté, la carte envoie les deux octets ME1, ME2 tels que:

ME1 = 90
ME2 = 6E la classe d'instruction envoyée n'est pas BC
= 6D ordre envoyé inconnu.

Tous les autres cas d'erreurs (par exemple tentative de lecture dans une zone inaccessible en lecture) se traduiront par un mutisme de la carte.
Pour réinstaurer le dialogue, il sera nécessaire de refaire un RAZ.

3.3 Ordre Entrant, ordre Sortant

On distingue deux classes d'ordres.

On dit qu'un ordre est ENTRANT si les DONNEES sont échangées dans le sens TERMINAL --> CARTE.

L'ordre d'ECRITURE est un ordre ENTRANT.

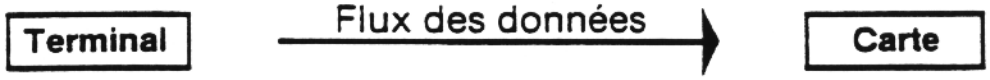

Figure 3.5 : Sens d'échange des données pendant un ordre ENTRANT

Inversement, on dit qu'un ordre est SORTANT si les DONNEES sont échangées dans le sens CARTE --> TERMINAL.

L'ordre de LECTURE est un ordre SORTANT.

Lorsqu'aucune donnée n'est échangée, l'ordre correspondant est assimilé à un ordre ENTRANT.

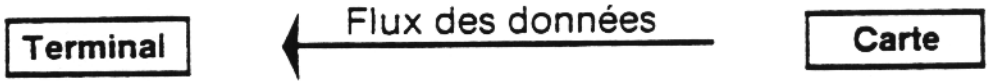

Figure 3.6 : Sens d'échange des données pendant un ordre SORTANT

Les paragraphes ci-dessous donnent des exemples de dialogue en fonction du type d'ordre, entrant ou sortant, et du mode d'échange (on supposera que le Vpp n'est jamais nécessaire, le lecteur pouvant facilement imaginer le dialogue dans le cas contraire).

3.3.1 Ordre entrant, mode simple

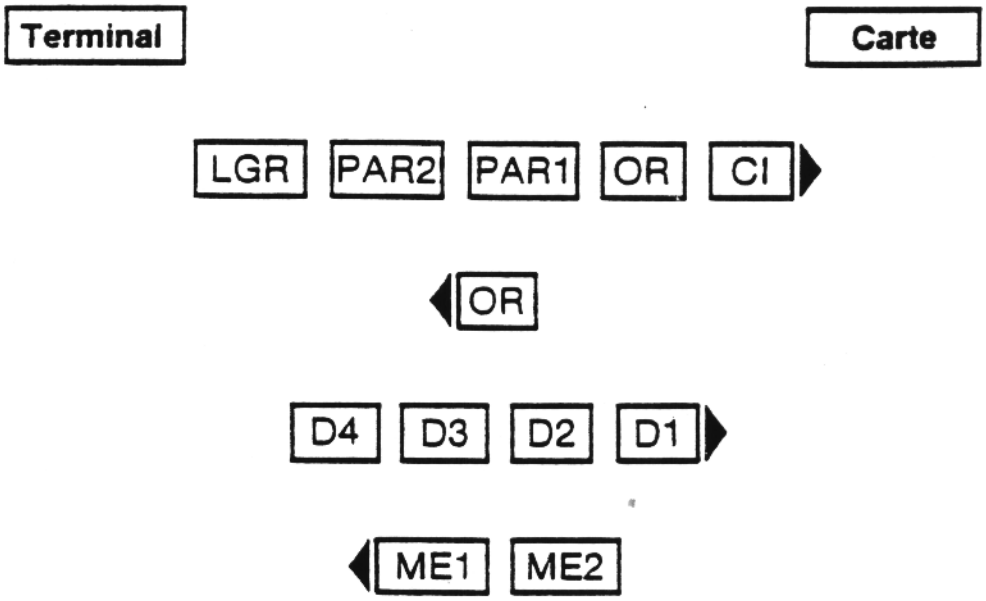

Figure 3.7 : Déroulement d'un ordre entrant, mode simple

Dans les cas où l'ordre est incompatible avec les règles de fonctionnement de la carte la carte est muette.
Le mutisme d'une carte est détecté par les coupleurs, considérant que si au bout d'un certain temps la carte ne répond pas elle est considérée comme MUETTE. L'information correspondante "remonte" en général au niveau du programme applicatif.

3.3.2 Ordre entrant, mode asservi

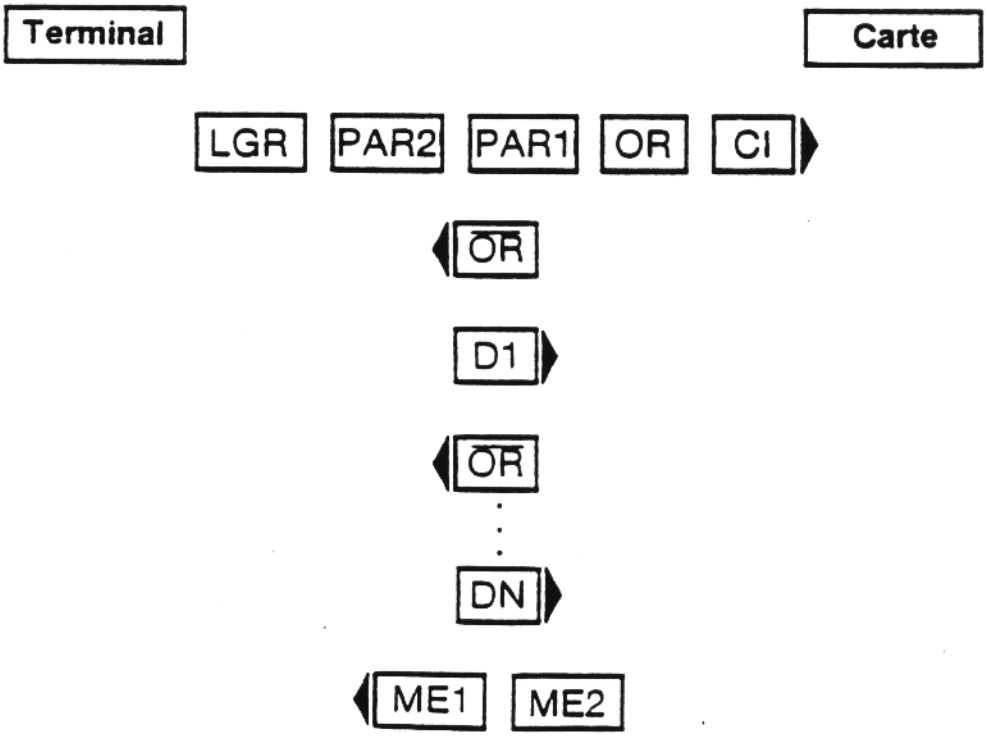

Figure 3.8 : déroulement d'un ordre entrant mode asservi

3.3.3 Ordre sortant, mode simple

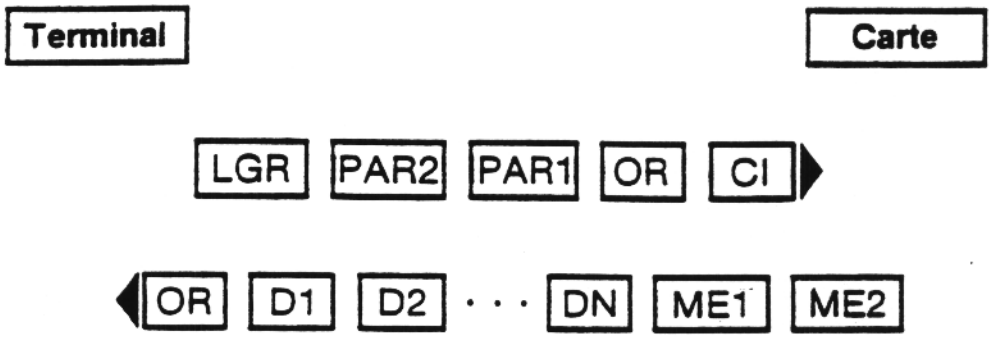

Figure 3.9 : déroulement d'un ordre sortant , mode simple

Remarque : Il n'existe pas d'ordre sortant, mode asservi.

4. ORDRES ELEMENTAIRES MASQUE 4 : MISE EN OEUVRE

Ce chapitre présente de façon détaillée, pour chaque ordre:

a) le but de l'ordre

b) la fonction exécutée

c) les conditions générales d'emploi de cet ordre

d) l'initialisation

e) ce que la carte renvoie

f) un ou plusieurs exemple(s)

convention: Comme dans le reste de l'ouvrage, l'ensemble des valeurs numériques, données, etc ... est exprimé en hexadécimal.

L'ensemble des exemples peut être reproduit avec la carte INITIALISATION CP8 MASQUE 4.

4.1 PRESENTATION D'une CLE : OR = 20 ou 10, ou 30.

TYPE : ENTRANT MODE : SIMPLE Vpp : non.

a) But

Cet Ordre est utilisé lorsqu'on désire:
- lire dans les Zones en LECTURE PROTEGEE
- valider en écriture un mot écrit dans une zone en ECRITURE PROTEGEE.

b) Fonction exécutée

La carte mémorise le type de clé grâce au code de l'ordre employé:

- 20; la clé présentée sera une clé type 2 soit la CLE de FABRICATION, la CLE 2A, ou la CLE 2B.
- 10; la clé présentée est la CLE 1A, clé type 1.
- 30; la clé présentée est la CLE 1B, clé type 1.

Au fur et à mesure de la réception de la clé, la carte compare terme à terme les octets reçus aux octets de la clé correspondante stockée en ZONE SECRETE. Le résultat de la comparaison est mémorisé, mais non communiqué à l'issue de cet ordre.

c) Conditions d'emploi

Une carte étant sous tension, on peut successivement présenter des clés différentes. C'est la dernière clé présentée qui sera prise en compte lors de la première demande de validation (en écriture ou en lecture) suivant l'ordre de présentation.
La mise hors tention d'une carte "annule" le résultat de la présentation d'une clé. Lors de la mise sous tention suivante, il sera nécessaire de présenter à nouveau une clé, si besoin est.

d) Initialisation

```
CI       = 8C
OR       = 20  : présentation d'une clé 2 ie,
                 CLE 2A, CLE 2B, CLE de FABRICATION
         = 10  : présentation de la CLE 1A
         = 30  : présentation de la CLE 1B
PAR 1    = 00
PAR 2    = 00
LG       = longueur de la clé en octets
DONNEES = clé au format interne à la carte.
```

e) La carte renvoie :

ME1, ME2

Exemples

* présentation de la CLE 2A

```
CI       =   BC
OR       =   20
PAR1     =   00
PAR2     =   00
LG       =   04
DONNEES  =   12 54 3F FF   (représentation hexadécimale de 4950 en
                            BCD au format interne).
```

La Carte renvoie:

```
ME1      =   90
ME2      =   00
```

* présentation de la CLE 1A:

```
CI       =   BC
OR       =   10
PAR1     =   00
PAR2     =   00
LG       =   08
DONNEES  =   3A AA AA AA 3A AA AA AA
```

La Carte renvoie:

```
ME1      =   90
ME2      =   00
```

4.2 VALIDATION de CLE en LECTURE: OR = 40

TYPE : ENTRANT MODE : SIMPLE Vpp : oui

a) But

Cet ordre est utilisé, suite à une présentation de clé :

- Pour lire dans les zones en LECTURE PROTEGEE (ZA, ZC, ZT si LP = 0).
- Pour recycler une carte bloquée.

b) Fonction exécutée

En fonction du résultat de la comparaison effectuée lors de la présentation de clé, la carte grille un bit dans la zone d'Accès,et fournit le résultat au TERMINAL.

c) Conditions d'emploi

Une clé doit préalablement avoir été présentée à l'aide d'un des ordres 20, 10 ou 30.
Dans le cas contraire, le résultat de la validation est le même que si l'on validait une clé 2 fausse, d'où risque de blocage.

d) Initialisation

CI = BC
OR = 40
PAR1 = 00
PAR2 = 00
LG = 00
DONNEES = aucune

e) La carte renvoie

ME1 = 90
ME2 = 00 clé bonne
= 14 clé type 2 fausse, première tentative
= 24 clé type 2 fausse, deuxième tentative
= 44 clé type 2 fausse, troisième tentative, ou clé type 1 fausse. Carte bloquée.

f) Exemples:

* Validation de la clé 2A

CI = BC
OR = 40
PAR1 = 00
PAR2 = 00
LG = 00
DONNEES = aucune

la carte renvoie:

ME1 = 90
ME2 = 00

* Validation d'une mauvaise clé type 2, premier essai: même initialisation

La carte renvoie:

ME1 = 90
ME2 = 14

4.3 LECTURE : OR = B0

TYPE : SORTANT MODE : SIMPLE Vpp : non

a) But

Lire dans une zone Accessible en lecture, qu'elle soit en LECTURE PROTEGEE ou PAS.

b) Fonction exécutée

Lecture, à une adresse quartet donnée, d'un ou plusieurs octets.

c) Conditions d'emploi

- Lecture dans une zone en LECTURE LIBRE:
  aucune.
- Lecture dans une zone en LECTURE PROTEGEE:
  il faudra préalablement avoir présenté une clé parmi les trois disponibles (ordre 10, 20 ou 30), et avoir eu un résultat positif à la demande de validation de clé en lecture (ordre 40).

d) Initialisation

CI = BC
OR = B0
PAR1 = poids forts de l'adresse quartet de début de lecture.
PAR2 = poids faibles de l'adresse quartet de début de lecture.
LG = nombre d'octets à lire.
DONNEES = aucune.

remarque: Si on veut lire un nombre entier de mots à partir d'un début de mot, l'adresse quartet de lecture sera un multiple de 8, et LG sera de la forme (N * 4), avec N = nombre de mots à lire. Ceci est la méthode la plus couramment utilisée.

e) La carte renvoie

Les octets lus qui constituent les données et ME1, ME2

f) Exemples

- Lecture des 2 premiers mots de la ZONE de LECTURE, à l'adresse 988:

```
CI       =  BC
OR       =  BO
PAR1     =  09
PAR2     =  88
LG       =  08
DONNEES  =  aucune
```

La carte renvoie:

mot d'adresse 988				mot d'adresse 990				ME1	ME2
33	05	06	11	35	54	52	41	90	00

- Lecture de 5 octets à partir de l'adresse quartet 988:

```
CI       =  BC
OR       =  BO
PAR1     =  09
PAR2     =  88
LG       =  05
DONNEES  =  aucune
```

La Carte renvoie :

					ME1	ME2
50	61	13	55	45	90	00

4.4 ECRITURE : OR = D0

TYPE : ENTRANT MODE : ASSERVI Vpp : oui

a) But

Positionner à 0 les bits d'un mot se trouvant dans une zone en ECRITURE PROTEGEE ou PAS.

b) Fonction exécutée

La carte, en fonction de la configuration binaire fournie en données, positionne à 0 les bits désirés.
On ne peut écrire que dans 1 mot à la fois.

c) Conditions d'emploi

- L'écriture est irréversible : tout bit à 0 ne peut revenir à son état initial 1.
- On ne peut pas écrire dans un mot validé.
- Si la zone n'est pas en ECRITURE PROTEGEE, le bit V peut être positionné à 0 au moment de l'écriture. Si la zone est en ECRITURE PROTEGEE, le bit V na peut être positionné à 0 qu'avec l'ordre de VALIDATION en ECRITURE.

d) Initialisation

CI = BC
OR = D0
PAR1 = poids forts de l'adresse quartet d'écriture
PAR2 = poids faibles de l'adresse quartet d'écriture
LG = 04
DONNEES = 32 bits du mot à écrire.

Remarque: l'adresse d'écriture est nécessairement une adresse multiple de 8

e) La carte renvoie

ME1, ME2

f) Exemples

Supposons que nous ayons à griller des bits 2 par 2, à des instants différents, à partir du premier mot de la zone Transaction (les bits V et C ne seront pas positionnés à 0)

- grillage des 2 premiers

```
CI       =  BC
OR       =  D0
PAR1     =  03
PAR2     =  10
LG       =  04
DONNEES  =  CF FF FF FF

La carte renvoie  :  ME1  =  90
                     ME2  =  00
```

- grillage des 2 suivants

```
CI       =  BC
OR       =  D0
PAR1     =  03
PAR2     =  10
LG       =  04
DONNEES  =  F3 FF FF FF

La carte renvoie  :  ME1  =  90
                     ME2  =  00
```

- grillage des 2 suivants

```
CI       =  BC
OR       =  D0
PAR1     =  03
PAR2     =  10
LG       =  04
DONNEES  =  FC FF FF FF

La carte renvoie  :  ME1  =  90
                     ME2  =  00
```

A ce moment, le mot d'adresse 0310 aura la valeur:
C0 FF FF FF.

4.5 VALIDATION en ECRITURE : OR = 70

TYPE : ENTRANT MODE : SIMPLE Vpp : oui

a) But

Positionner à 0 le bit V d'un mot situé dans une zone en ECRITURE PROTEGEE ou pas.
Le mot étant validé en écriture, aucune écriture dans ce mot ne sera possible.

b) Fonction exécutée

- Validation dans une ZONE PROTEGEE en ECRITURE

La carte contrôle si le type de clé présentée précédemment concorde avec les deux bits C, CA du mot à valider :
Si oui, en fonction du résultat de la comparaison effectuée lors de la présentation de clé, elle valide le mot, c'est-à-dire positionne le bit V à 0, ou grille un bit en zone d'accès si la clé est fausse.
Si non, elle arrête l'exécution de l'ordre.

- Validation dans une zone NON PROTEGEE en ECRITURE

La carte positionne le bit V du mot à valider à 0, sans aucun autre type de contrôle.

c) Conditions d'emploi

- Si la zone est PROTEGEE en ECRITURE, il faut avoir préalablement PRESENTE une clé (ordres 20, 10 ou 30)

- On ne peut pas valider un mot déjà validé.

d) Initialisation

CI = BC
OR = 70
PAR1 = Poids forts de l'adresse quartet du mot à valider
PAR2 = Poids faibles de l'adresse quartet du mot à valider.
LG = 0
DONNEES = aucune

Remarque :
- l'ordre de validation en écriture ne permet la validation que d'un mot à la fois.
- l'adresse quartet du mot à valider est nécessairement une adresse multiple de 8.

e) La carte renvoie

ME1 = 90
ME2 = 00 clé bonne
= 14 clé type 2 fausse, première tentative
= 24 clé type 2 fausse, deusième tentative
= 44 clé type 2 fausse, troisième tentative, ou clé type 1 fausse. La carte est bloquée.

f) Exemple

* Valider le mot écrit dans l'exemple fournit dans l'ordre d'écriture.

CI = BC
OR = 70
PAR1 = 03
PAR2 = 10
LG = 00
DONNEES = aucune

Remarque : On aura pris soin d'avoir préalablement présenté la clé 1B, les bits C, CA étant respectivement égaux à 1, 0.

La carte renvoie:
ME1 = 90
ME2 = 00

4.6 ACTIVATION de la FONCTION TELEPASS : OR = 80 *

TYPE : ENTRANT MODE : ASSERVI Vpp : non.

a) But

Comme son nom l'indique.

b) Fonction exécutée

Réception des données externes, calcul algorithmique et stockage du résultat R, qui sera fourni sur ORDRE de LECTURE DE RESULTAT.
Rappelons que la fonction Télépass est telle que :
R = F (E, ADR, (ADR), JS)

c) Condition d'emploi

Le mot à certifier doit être dans une zone accessible en lecture.
Si la zone est PROTEGEE en LECTURE, il est nécessaire d'avoir préalablement PRESENTE ET VALIDE une clé en lecture.

d) Initialisation

CI = BC
OR = 80
PAR1 = 00
PAR2 = 00
LG = 08
DONNEES = 6 octets constituant E, suivis des 2 octets constituant ADR.

e) La carte renvoie

ME1, ME2

f) Exemple

Soit la fonction TELEPASS à faire éxécuter en pointant sur le mot d'adresse 9C8 avec E = AB CD FF 00 00 00

- Initialisation

CI = BC
OR = 80
PAR1 = 00
PAR2 = 00
LG = 08
DONNEES = AB CD EF 00 00 00 09 C8

La carte renvoie:
ME1 = 90
ME2 = 00

* Appelée également ORDRE HABILITATION ou ORDRE DE CALCUL.

4.7 LECTURE de RESULTAT : OR = C0

TYPE : SORTANT MODE : SIMPLE VPP : non

a) But

Comme son non l'indique.

b) Fonction exécutée

La carte envoie au TERMINAL le R de 64 bits de la fonction TELEPASS.

c) Condition d'emploi

Avoir préalablement effectué l'ordre d'ACTIVATION DE LA FONCTION TELEPASS.

d) Initialisation

CI = BC
OR = C0
PAR1 = 00
PAR2 = 00
LG = 08
DONNEES = aucune.

e) La carte renvoie

Les 8 octets constituant le résultat R, suivis de ME1, ME2

f) Exemple

Lecture du R de l'exemple précédent

Initialisation

CI = BC
OR = C0
PAR1 = 00
PAR2 = 00
LG = 08
DONNEES = aucune

La carte renvoie

R = A8 FF 3F F9 5E D6 C8 0C
ME1 = 90, ME2 = 00

4.8 ECRITURE des LOCKS : OR = 50

TYPE : ENTRANT MODE : SIMPLE Vpp : oui.

a) But

Positionner à 0 le ou les locks situé(s) dans la zone des locks.

b) Fonction exécutée :

Positionnement d'un ou plusieurs locks.

c) Condition d'emploi

Aucune

d) Initialisation

CI = BC
OR = 50
PAR1 = 00
PAR2 = 00

DONNEES = 2 octets D1 et D2 :

D1: masque des locks à positionner ; le (ou les) bit(s) correspondant au lock à positionner doit être à 0.

D1 :	LU	LC	LF	IV	IV	1	1	1
bits	7	6	5	4	3	2	1	0

D2 : FF.

e) la carte renvoie

ME1, ME2.

f) Exemple

Positionner le lock LU

- Initialisation

CI = BC
OR = 50
PAR1 = 00
PAR2 = 00
LG = 02
DONNEES = 7F FF

- La carte renvoie

ME1 = 90
ME2 = 00

4.9 RECYCLAGE d'une CARTE

Le recyclage consiste à:

- présenter à la carte bloquée la CLE 2 A (ou CLE 2 B) suivie de la clé 1A avec l'ordre 20
- faire une demande de validation en lecture (OR=40)

Si les 2 clés sont bonnes, la carte est RECYCLEE.
Si une des 2 clés, ou les 2 clés, elle (sont) mauvaise(s) une nouvelle fenêtre de blocage est ouverte en ZA et la carte reste bloquée.

- Exemple

Recycler une carte telle que:

CLE 2A (ou B) = 12 54 3F FF
CLE 1A = 3A AA AA AA
= 3A AA AA AA

* Présentation de la clé de Recyclage

Initialisation.

CI = BC
OR = 20
PAR1 = 00
PAR2 = 00
LG = 0C
DONNEES = 12 54 3F FF 3A AA AA AA 3A AA AA AA

La carte renvoie
ME1 = 90
ME2 = 00

* Demande de validation en lecture

Initialisation

CI = BC
OR = 40
PAR1 = 00
PAR2 = 00
LG = 00
DONNEES = aucune

La carte renvoie
ME1 = 90
ME2 = 00

La carte est recyclée.

4.10 CHANGEMENT du CODE PORTEUR

Cette opération n'est possible que si 2 mots vierges ont été réservés en PERSONNALISATION à l'adresse ADM - 16.
Les opérations à effectuer sont:

a) Présentation de la clé 2A (OR=20).

b) Ecriture à partir de l'adresse ADM - 16, de la nouvelle clé sur 1 ou 2 mots, en prenant soin de positionner le bit C à 0, le bit CA faisant partie des bits d'information (OR=D0).

c) Relecture (OR=B0) du ou des mots pour contrôler si l'écriture s'est bien passée. Aucune validation de clé en lecture n'est nécessaire ces 2 mots étant en LECTURE LIBRE.

d) Validation en écriture du ou des 2 mots (OR=70).

e) Positionnement à 0 du lock LU (OR=50).

Remarque: La clé sera constituée par le ou les mots validés.

Exemples de clé sur 1 mot:
ADM - 16 12 54 3F FF
ADM - 8 FF FF FF FF

ADM - 16 3F FF FF FF
ADM - 8 FF FF FF FF

Exemples de clé sur 2 mots:
ADM - 16 1A 54 3F F0
ADM - 8 3F FF FF FF

ADM - 16 12 54 3F FF
ADM - 8 13 65 4F FF

4.11. Conditions d'utilisation d'une carte CP8

La réalisation de certaines actions (ex: lecture en zone protégée en lecture), sera ou ne sera pas possible compte-tenu de l'état de la carte. Les logiciels d'applications mettant en oeuvre la carte CP8 devront donc connaître l'état des cartes présentées sur les lecteurs afin de les accepter, les rejeter et décider si telle ou telle opération est réalisable ou pas.
Pour ce faire, ils testeront en particulier les octets MCH et ME2 rendus par la carte lors de la RAZ.

4.11.1 MCH

MCH précise la "phase de vie" dans laquelle se trouve la carte.

4.11.1.1 ILF

Toutes les cartes vendues par BULL CP8 sont "Fabriquées". Autrement dit, ILF doit toujours être égal à 1.

4.11.1.2 ILC

Si ILC = 0, la carte n'est pas personnalisée;
Si ILC = 1, la carte l'est . Un logiciel de personnalisation acceptera et traitera les cartes non personnalisées (pour les personnaliser); un logiciel "d'utilisation" de la carte fera l'inverse.

4.11.1.3 ILU

Si ILU = 1, la CLE 2B est active. Si ILU = 0, elle ne l'est pas, CLE 2A active.
Un logiciel offrant la fonctionnalité "changement de code porteur" testera ce bit pour savoir si elle est réalisable ou pas: ou ne peut pas changer 2 fois le code porteur ...

4.11.1.4 IIV

Si IIV = 1, la carte est INVALIDEE. Lorsqu'une carte est invalidée, on peut:
- Lire toutes les zones non protégées, en lecture.
- Lire les zones anciennement protégées en lecture, moyennant une validation en lecture (OR=40) préalable. (la présentation d'une clé n'est pas nécessaire).

On ne peut plus:

- Ecrire (OR=DO)
- Valider un mot en écriture (OR=70)
- Faire une fonction TELEPASS (OR=80 et OR=CO)

4.11.1.5 IEP, ILP

IEP et ILP indiquent à l'application si la présentation d'une clé est nécessaire avant la validation en lecture ou en écriture lors d'accès en zone transaction.

4.11.2 ME2

ME2 est une représentation de la dernière fenêtre active de la zone d'accès.
Le tableau ci-après présente les actions qu'il est possible ou pas de réaliser, selon que la carte est:

- En fonctionnement normal, ME2=00
- Saturée, ME2=80
- Bloquée, ME2=40
- Dans l'état "1/2 faux code(s)", ME2=10 ou 20

On remarquera que certaines actions impliquent la mise en oeuvre d'une séquence d'ordres élémentaires. Si une action "interdite" sur le tableau est toutefois réalisée, la carte deviendra "MUETTE" à la réception d'un des ordres de la séquence, mais pas nécessairement au premier.

exemple:

Lorsqu'on veut lire une zone protégée en lecture, il faut:
- Présenter une clé (OR=20, 10 ou 30)
- Valider la clé en lecture (OR=40)
- Lire (OR=80)

Si la carte est saturée, la présentation de clé sera acceptée, mais la carte deviendra muette à la réception de l'ordre de validation.

ME2 à la RAZ / Actions	00	Carte saturée 80	Carte bloquée 40	Carte 1/2 faux code(s) 20 / 10
Lecture en Zone en LECTURE LIBRE BO	oui	oui	oui	oui
Lecture en Zone en LECTURE PROTÉGÉE (20 / 10 / 30) + 40 + B0	oui	non	non	oui si 20
				non si 10 ou 30
Écriture DO	oui	oui	oui	oui
Validation en Écriture en Zone en ÉCRITURE LIBRE 70	oui	oui	oui	oui
Validation en Écriture en zone en ÉCRITURE PROTÉGÉE (20 / 10 / 30) + 70	oui	non	non	oui si 20
				non si 10 ou 30
Fonction TELEPASS avec ADR pointant dans une zone en LECTURE LIBRE 80 + CO	oui	oui	oui	oui
Fonction TELEPASS avec ADR pointant dans une zone en ÉCRITURE PROTÉGÉE (20 / 10 / 30) + 40 + 20 + CO	oui	non	non	oui si 20
				non si 10 ou 30
Écriture des locks 50	oui	oui	oui	oui
Recyclage 20 + 40	non	non	oui	non

oui = action possible

non = la carte deviendra MUETTE

TABLEAU 4.1: Conditions d'utilisation selon ME2

4.11.3 Cas de mutisme d'une carte

On dit qu'une carte est muette si elle ne renvoie aucune information après:
- Une RAZ
- La réception d'une séquence d'initialisation d'ordre.

La liste des cas de mutisme qui suit n'est pas exhaustive. Toutefois les cas les plus fréquents sont décrits.

Une carte est MUETTE si:

- Le composant est "hors service". Ce cas de mutisme est détecté dès la RAZ, la carte n'envoyant pas les octets "SYSTEME" et "APPLICATION".

- Le paramètre LG en initialisation est mauvais.
  exemple: LG n'est pas égal à 4 en écriture (OR=D0)

- Tentative de lecture ou d'écriture dans une zone inaccessible en lecture et/ou écriture.
  exemple: lecture ou écriture en ZS
  écriture en ZC

- Tentative de lecture dans une zone en lecture protégée sans présentation de clé préalable (40); de même pour la validation en écriture.

- Tentative d'écriture ou de validation de mots déjà validés.

- Non prise en compte de l'état de la carte fournis par ME2.

D'une manière générale, une carte est muette après une action incompatible avec son mode de fonctionnement.

4.11.4 RAZ de la Carte

On effectuera un RAZ de la carte:
- Pour instaurer un dialogue avec une carte
- Quand, en cours d'utilisation:
  . la carte est bloquée (voir TS)
  . le bit ER de ME2 est positionné à 1 à l'issue de l'exécution d'un ordre.
  . la carte est muette.

Dans ces trois cas, la RAZ ne sera effectuée que si on désire poursuivre les échanges avec la carte. Dans le cas contraire, elle n'est pas obligatoire.

5. CYCLE DE VIE D'UNE CARTE

Le cycle de vie d'une carte, de sa "naissance" à sa "mort" est le suivant:

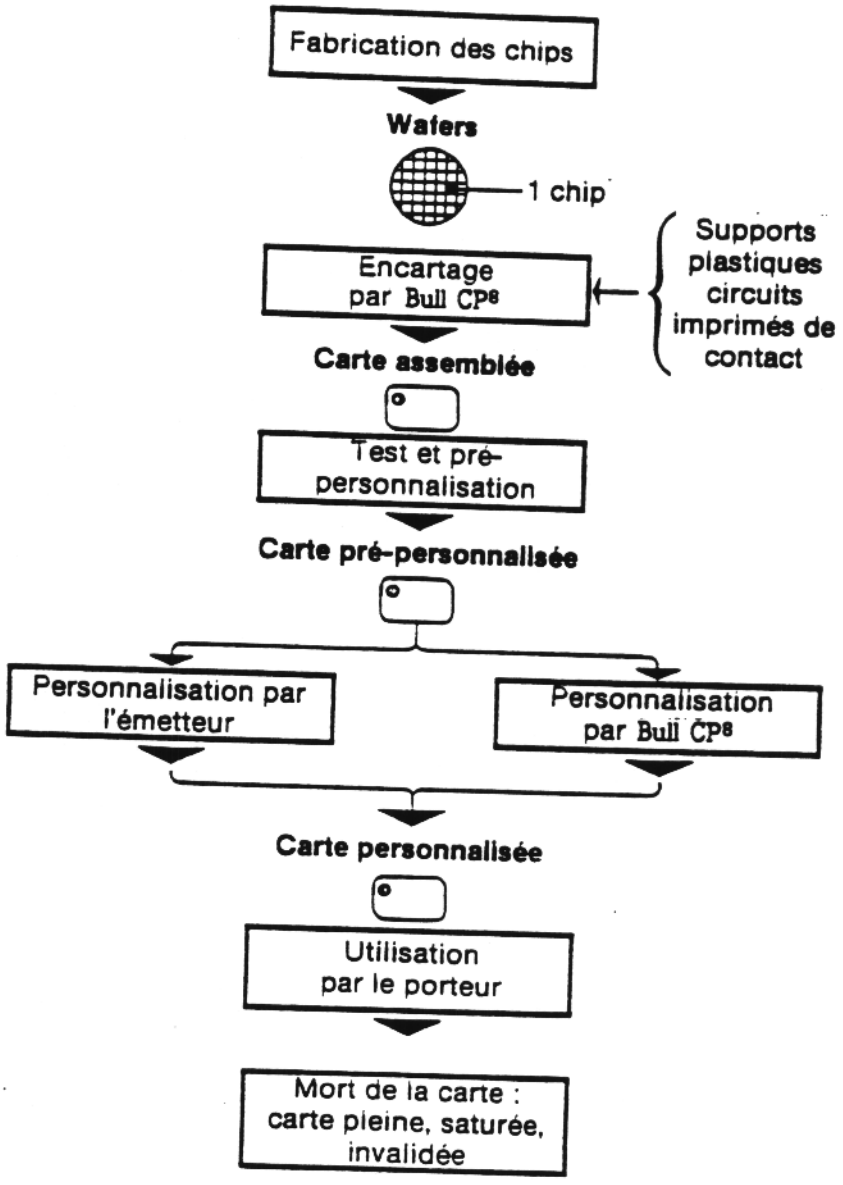

Figure 5.1 : Cycle de vie d'une carte CP8

5.1 La fabrication du composant

Cette étape consiste à :

- Fabriquer l'ensemble micro-processeur, RAM, ROM, PROM, etc.

- Implanter par masque dans la ROM le programme de la carte, définissant ainsi ses spécificités fonctionnelles.

- Ecrire dans la mémoire PROM :
  . la clé de fabrication (clé type 2). Le principe de calcul de la clé F est exposé au paragraphe 5.4
  . le pointeur AD1 et le numéro d'encarteur
  . le numéro d'identification et le I.

- Positionner le lock LF à 0. A partir de ce moment, la mémoire est protégée de la manière suivante :

  . lecture LIBRE

  . écriture PROTEGEE ; ainsi, la validation d'un mot en écriture nécessitera la présentation préalable de la clé F (ordre 20). Autrement dit, la mémoire est protégée par la clé F.

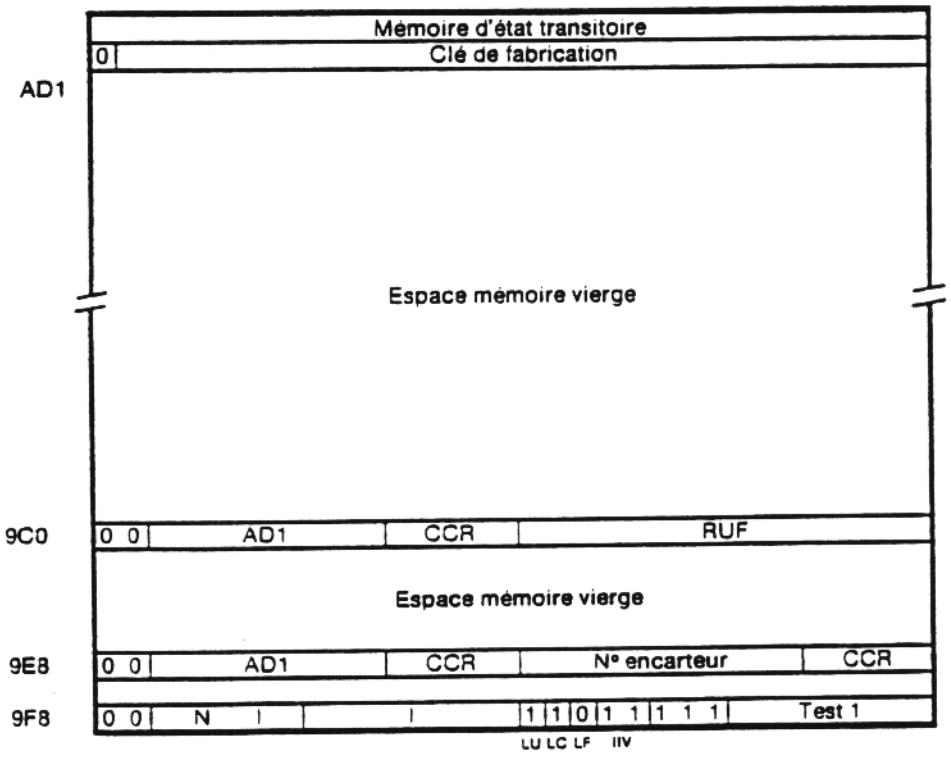

Figure 5.2 : Etat mémoire à la fin de la Fabrication

5.2 Encartage

La figure ci-dessous résume le processus d'encartage.

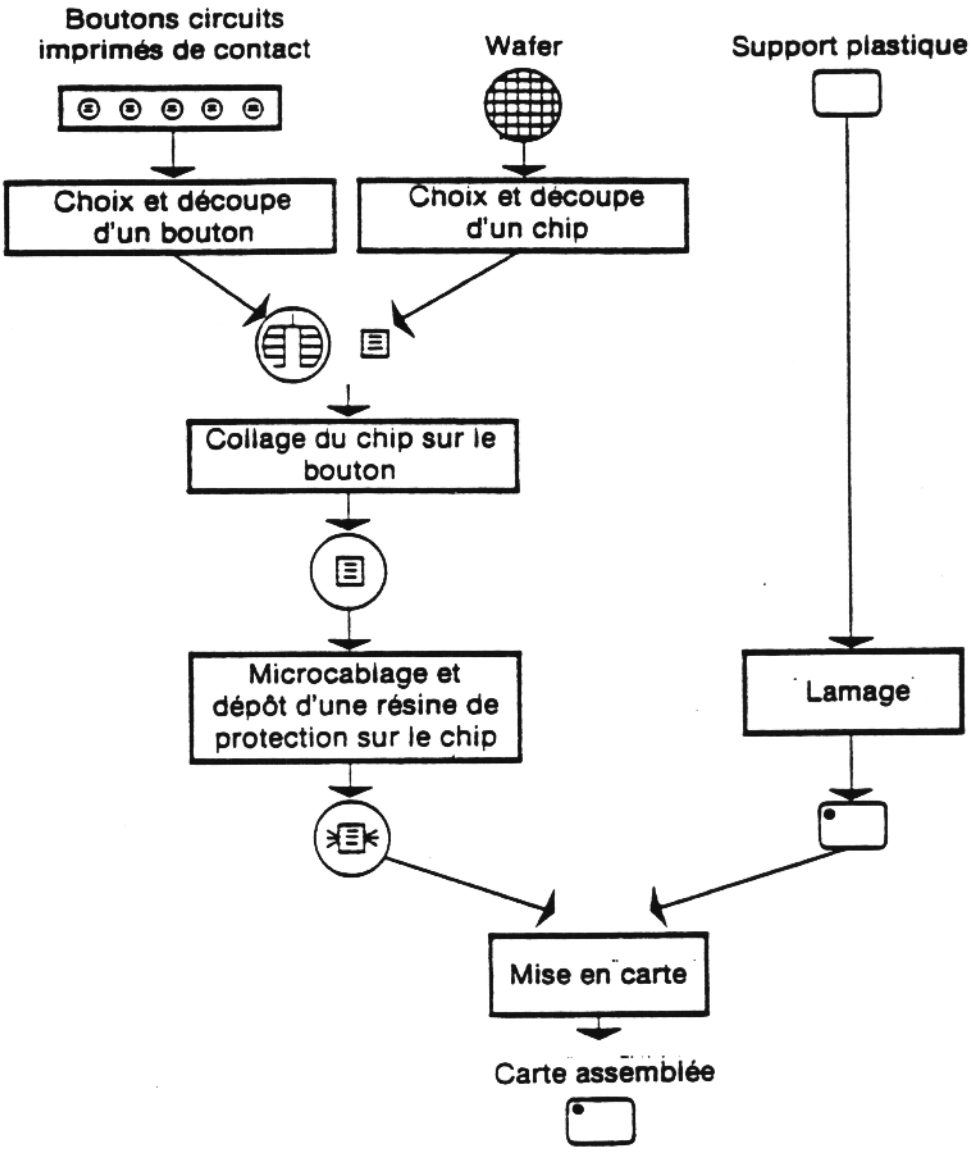

Figure 5.3 : Procédure d'encartage

5.3 Tests et Pré-Personnalisation

Cette étape consiste à tester le chip implanté sur le support plastique.

Par ailleurs, au cours de ce test sont écrits :
- Le numéro de série.
- Les deux bits de poids forts du type d'application.

Des cartes peuvent être fournies en l'état, la personnalisation étant réalisée par l'émetteur.

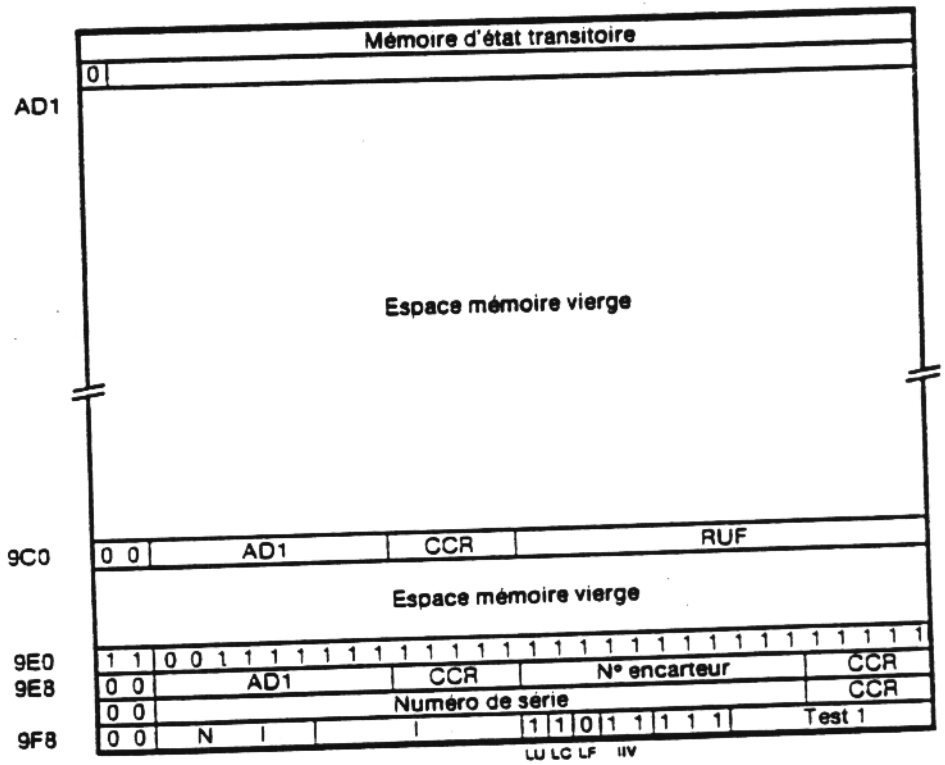

Figure 5.4 : état mémoire pré-personnalisée

5.4 La personnalisation

La PERSONNALISATION consiste à ECRIRE et VALIDER en ECRITURE, dans une carte PRE-PERSONNALISEE, en fonction du caractère intrinsèquement obligatoire ou optionnel de chaque zone et des besoins de l'application:

- Les clés et jeu secret.
- Les données de la zone confidentielle
- Les données de la zone de lecture
- Les données de la zone de fabrication:
  . pointeurs de zones
  . CCR
  . bits EP, LP type d'application

et enfin, positionner le lock LC à 0.

5.4.1 Calcul de la clé de fabrication

Rappelons que la mémoire d'une carte pré-personnalisée est:
- en lecture libre
- en écriture protégée par la clé de Fabrication, clé type 2.

Autrement dit, la validation en écriture (OR=70) ne peux être réalisée qu'après présentation (OR=20) de la clé de Fabrication, inscrite durant la phase de fabrication du composant.

Cette CLE DE FABRICATION, tant en phase de fabrication qu'en phase de personnalisation, est calculée par une carte spéciale, dite CARTE LOT, à laquelle on fait exécuter une fonction TELEPASS, avec des données d'entrée externes propres au résultat désiré. Les CARTES LOT sont identifiées par un NUMERO DE CARTE LOT.

L'ensemble des opérations suivantes doit être effectué dans l'ordre ci-dessous décrit, que le calcul soit réalisé automatiquement par programme ou "artisanalement" avec un lecteur, un papier, un crayon et une gomme...

- Lecture dans la carte à personnaliser des 16 bits de poids forts du mot d'adresse 9F8, contenant le numéro d'identification et le I. Le NI doit être égal au numéro de la carte lot fournie avec les cartes pré-personnalisée.

- Formatage des données d'entrée externes de la fonction TELEPASS à faire exécuter par la carte lot.

- Formatage du R obtenu, afin d'obtenir la clé de fabrication au format interne carte.

5.4.1.1 Lecture du NI et du I dans la carte à personnaliser

Lire le mot d'adresse 09F8 dans la carte à personnaliser, et extraire les 16 bits de poids forts.

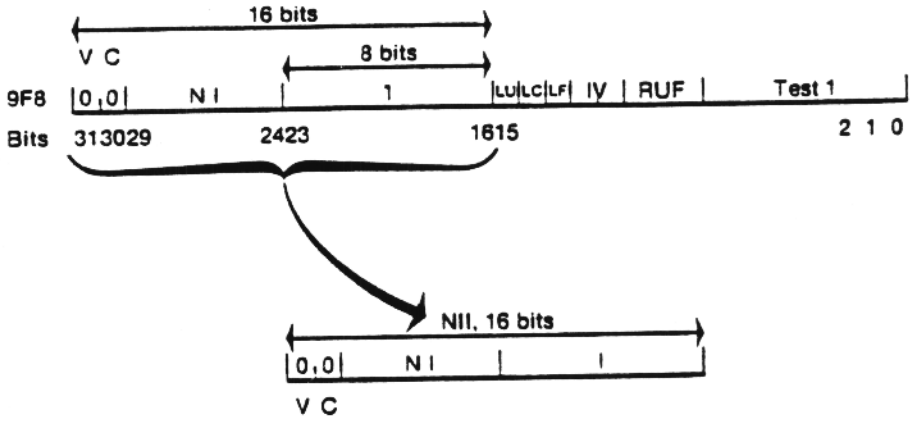

Figure 5.5: Lecture et prélèvement du n° d'identification et du I

5.4.1.2 Formatage des données externes de la fonction TELEPASS à faire exécuter par la carte lot

Les 64 bits de données d'entrée externes de la fonction TELEPASS seront formatées comme ci-après :

- Le E de 48 bits:

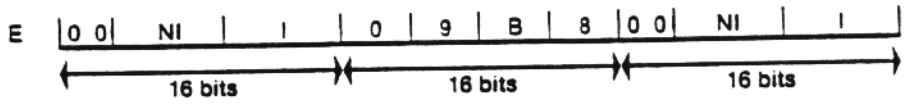

Figure 5.6 : E pour Carte lot

0988 = valeur héxadécimal

- Le ADR de 16 bits

ADR = 0988
ADR pointe sur un mot de la zone de lecture de la carte lot. Ce mot contient, cadrés à droite, le n° de carte lot auquel est associé un CCR.

5.4.1.3 Calcul définitif de la clé de Fabrication

Faire exécuter à la Carte Lot une fonction TELEPASS (OR=80 et CO) avec les 64 bits de données d'entrée externes au format décrit ci-dessus.

Le résultat R de 64 bits de la fonction TELEPASS peut être considéré comme deux champs R1 et R2, de 32 bits chacun.

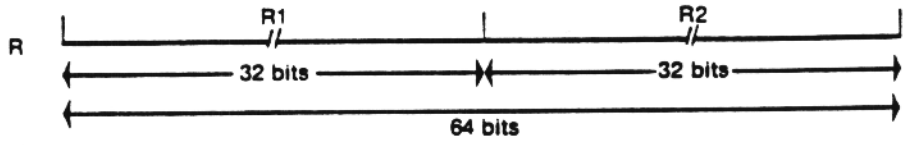

Figure 5.7 : R de carte lot

La Clé de Fabrication sur 32 bits est calculée de la manière suivante:
CF = (R1 + R2) * 7FFFFFFF

avec + : "ou exclusif"
* : "et"

ou en clair:
"ou exclusif" des deux champs R1 et R2, et forçage à 0 du bit de poids forts.
Les 32 bits ainsi obtenus pourront être présentés à la carte à personnaliser, en utilisant l'ordre 20.

5.4.2 Méthode de DIVERSIFICATION des CLES EMETTEUR et JEU SECRET

Pour un ensemble de cartes donné, la DIVERSIFICATION a pour objectif que chaque carte ait un JEU SECRET et des CLES EMETTEUR qui lui soient propres.

Jeu Secret et Cles Emetteur seront des valeurs calculées, en fonction d'un paramètre spécifique à chaque carte:
ce pourrait être, par exemple, le numéro de série de la carte.

Par ailleurs, le calcul de ces valeurs pourra être réalisé grâce à la fonction TELEPASS d'une carte CP8.
Les cartes dédiées à ce calcul sont appelées CARTE MERE et il s'en suit que les cartes dont on calcule le Jeu Secret et les Clés seront appelées CARTES FILLES.

Ainsi, une carte mère sera caractérisée par:
- Un JEU SECRET MERE, connu du seul émetteur habilité à personnaliser des cartes, pour une application donnée.

- Des mots situés en Zone Transaction (ou autre), servant à différencier les résultats R, l'un donnant une CLE 1A, l'autre une CLE 1B, etc ...

Ainsi, chaque CLE et JEU SECRET d'une carte fille donnée sera fonction:

- De la carte elle-même, au travers du numéro de série.
- D'une carte mère, au travers de JEU SECRET MERE et de mots situés dans sa zone Transaction.

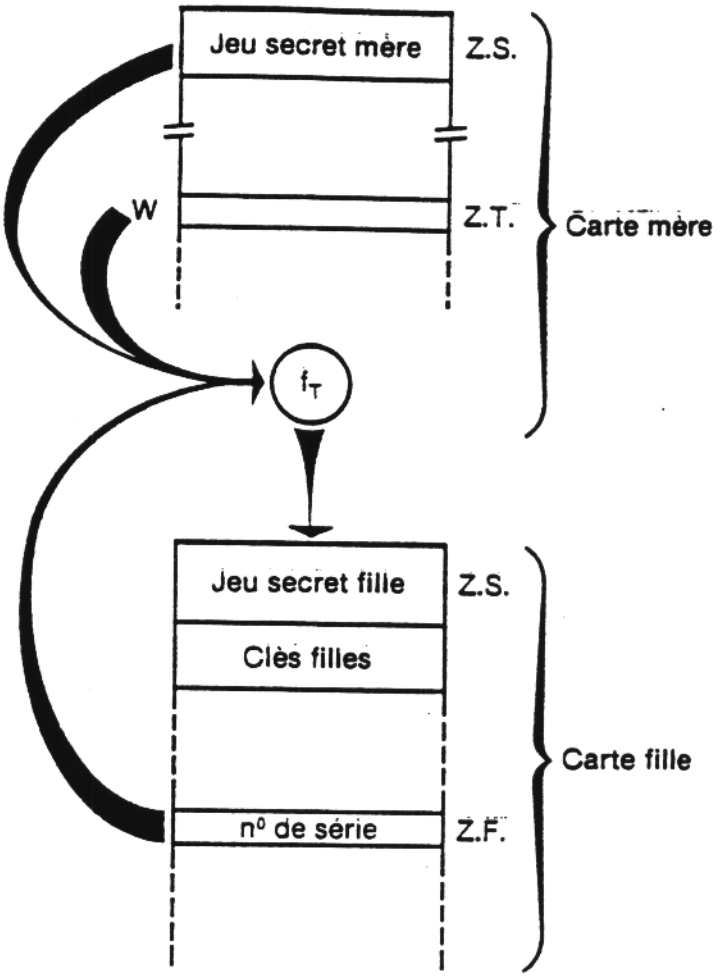

Figure 5.8 : Principe général de DIVERSIFICATION

Le calcul des CLES ou du JEU SECRET d'une carte fille sera effectué de la manière suivante:

- Lecture dans la carte fille des 11 bits constituant le n° d'ENCARTEUR et des 26 bits du n° de série
- Formatage des données d'entrée externes de la fonction TELEPASS à faire exécuter à la carte mère.
- Formatage du R obtenu afin de générer le JEU SECRET et les CLES définitives.

5.4.2.1 Lecture du n° d'encarteur et du n° de série de la carte à personnaliser

Le N° d'ENCARTEUR se trouve dans le mot d'adresse 9E8.

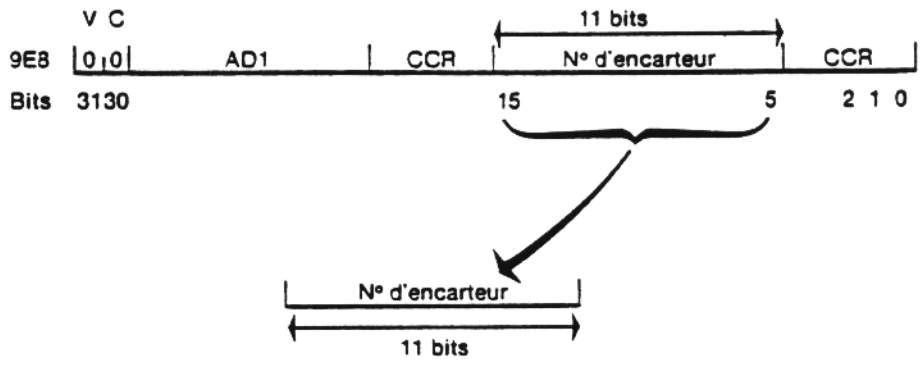

Figure 5.9: Lecture et prélèvement du N° d'ENCARTEUR

Le N° de série se trouve dans le mot d'adresse 9F0.

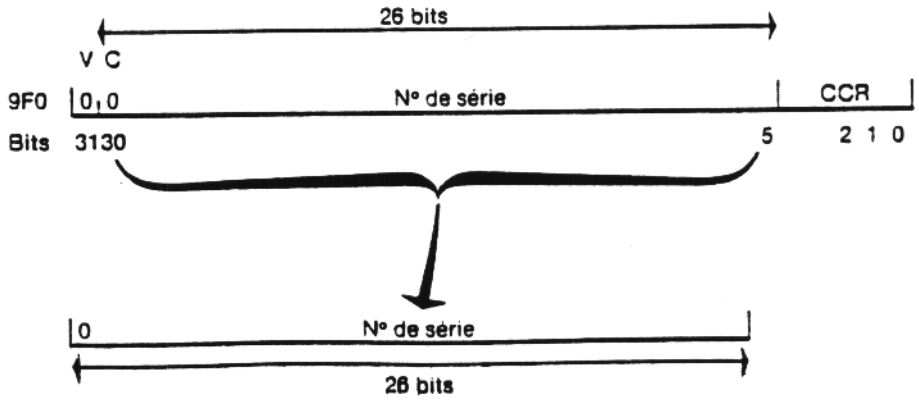

Figure 5.10 : Lecture et prélèvement du N° de série

5.4.2.2 Formatage des données d'entrée externes de la fonction TELEPASS à faire exécuter par la carte mère

Les 64 bits de données d'entrée externes de la fonction TELEPASS seront formatés comme ci-après :

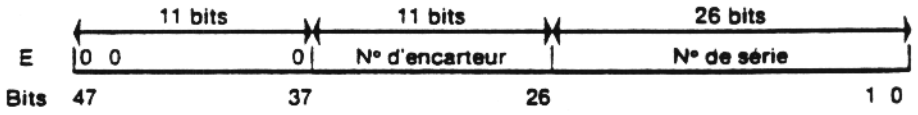

Figure 5.11: E pour carte mère

- Le ADR de 16 bits

ADR = 0888 si calcul du jeu SECRET FILLE
ADR = 0890 si calcul de la clé 1A FILLE
ADR = 0898 si calcul de la clé 1B FILLE
ADR = 08A0 si calcul de la clé 2A FILLE

Dans chacun des cas, ADR pointe sur un des mots de la Zone Transaction de la carte mère.
Les contenus de chaque mot sont différents les uns des autres, et choisis arbitrairement.
Ces mots sont souvent désignés symboliquement par WI, avec:

Wo pour l'adresse 0888
W1 pour l'adresse 0890
W2 pour l'adresse 0898
W3 pour l'adresse 08A0

5.4.2.3 Calcul définitif

Faire exécuter à la carte mère une fonction TELEPASS avec les 64 bits de données d'entrée au format décrit ci-dessus.

Le résultat R de 64 bits de la fonction TELEPASS peut être considéré comme deux champs R1 et R2, de 32 bits chacun.

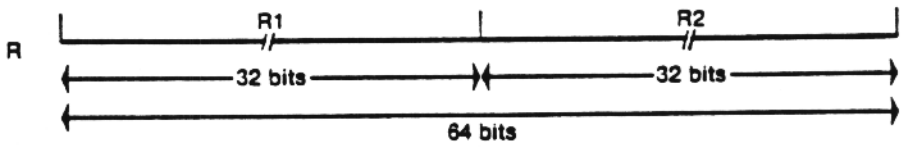

Figure 5.12: R de la carte mère

Le JEU SECRET de 3 mots est constitué de la manière suivante:

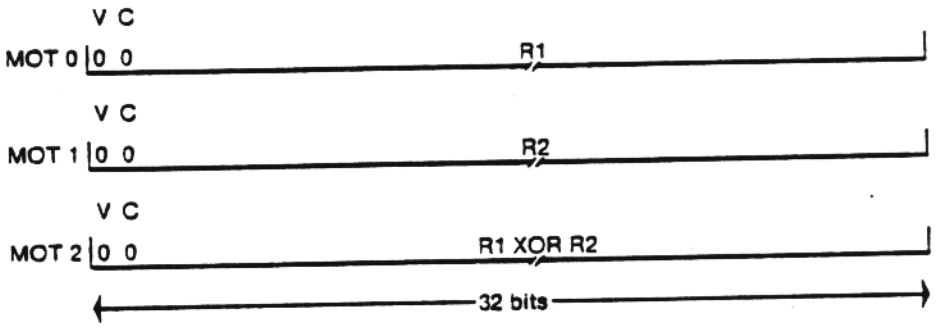

Figure 5.13: le JEU SECRET

On notera que les 2 bits de poids forts de chaque champ sont perdus, au profit des bits V et C.

Les CLES 1A/B de 2 mots sont constituées de la manière suivante:

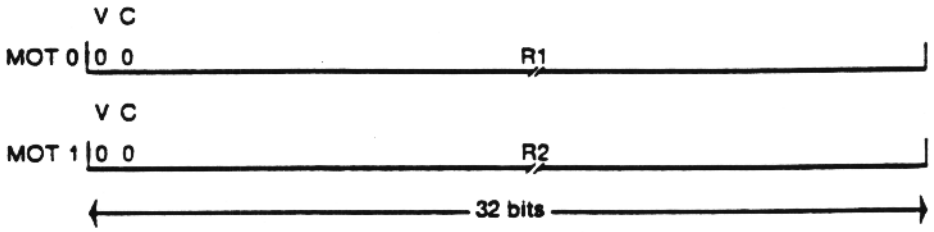

Figure 5.14: les CLES 1A/B

On notera que les 2 bits de poids forts de chaque champs sont perdus, au profit des bits V et C.

5.5 Schémas de principe d'une chaine de personnalisation

5.5.1 Sans diversification

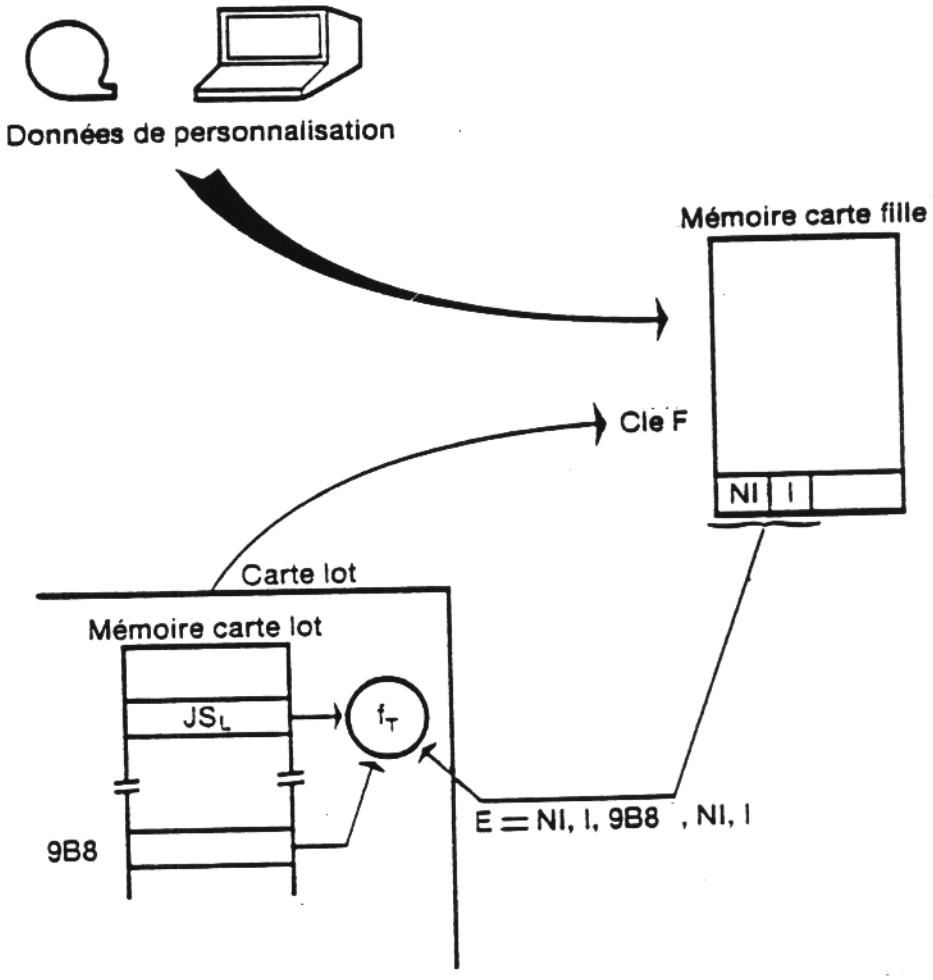

Figure 5.15: personnalisation sans diversification

5.5.2 Avec diversification

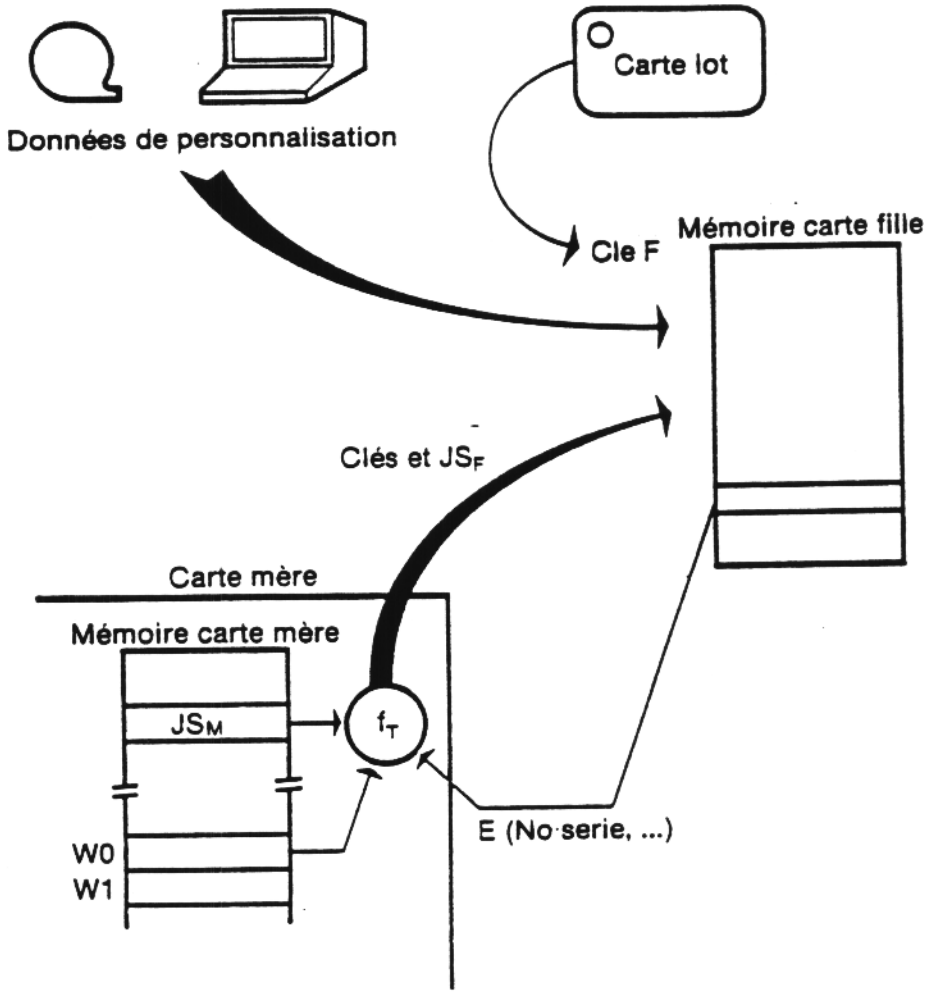

Figure 5.16: personnalisation avec diversification

5.6 Cycle de vie, clés et locks

La figure ci-après présente quelles sont les différentes clés actives selon les phases de vie d'une carte.

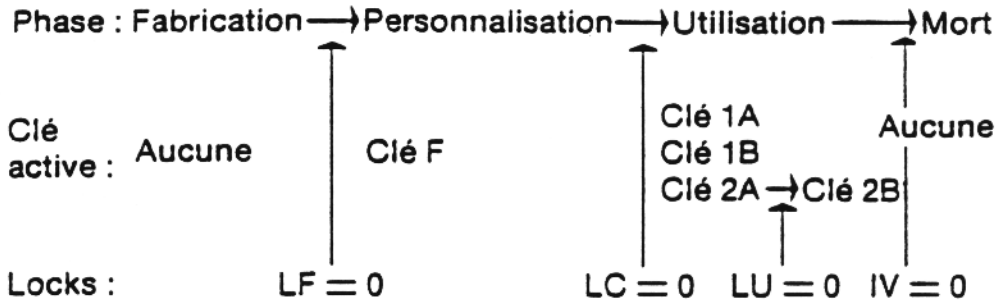

Figure 5.17: Cycle de vie, clés et locks

ANNEXE 1 : ORDRES ELEMENTAIRES MASQUE 4

T	ORDRE	CI	OR	A1	A2	LG	DONNEES
S	Lecture	BC	B0	PF @ de lecture	Pf @ de lecture	Nb. d'octets à lire	/
E	Ecriture	BC	D0	PF @ d' écriture	Pf @ d' écriture	04	Mot à écrire
E	Présentation Clé 2	BC	20	00	00	LG. clé en octets	Clé 2
E	Présentation Clé 1 A/B	BC	10 / 30	00	00	LG. clé en octets	Clé 1 A/B
E	Validation Clé en lecture	BC	40	00	00	00	/
E	Validation clé en écriture	BC	70	PF @ de validation	Pf @ de validation	00	/
E	Ordre de calcul télépass	BC	80	00	00	08	E, ADR
S	Lecture du résultat	BC	C0	00	00	08	R
E	Écriture des locks	BC	50	00	00	02	Masque, FF