SPECIFICATION FONCTIONNELLE DE LA CARTE VIDEOTEX

CHAPITRE 1 : PRINCIPE D'UTILISATION DE LA MEMOIRE EPROM

1. Structure physique de la mémoire

   1.1 Affectation des zones
   1.2 Organisation mémoire

2. Description des zones "système"

   2.1 Zone de fabrication
   2.2 Zone des locks
   2.3 Zone CC
   2.4 Zone clé "émetteur"

3. Description de la zone porte-clés

   3.1 Bloc d'autorisation de type Abonnement
   3.2 Bloc d'autorisation de type Session

      a. Libre
      b. Contrôlée

   3.3 Bloc d'autorisation de type Consommation

CHAPITRE 2 : FONCTIONNALITES

1. RAZ

   1.1 Octets d'interface
   1.2 Octets complémentaires ou historiques

2. Ordres élémentaires

   2.1 Ordre de lecture
   2.2 Ordre d'écriture
   2.3 Ordre de marquage des locks
   2.4 Ordre de recherche sur argument
   2.5 Lecture d'un résultat

3. Ordres assurant la sécurité du système

3.1 Demande de calcul

3.1.1 Présentation générale
3.1.2 MODE = 00 calcul d'une combinaison d'accès
3.1.3 MODE = 01 télé-valorisation
3.1.4 MODE = 10 présentation de clé
3.1.5 MODE = 11 télé-écriture

3.2 Calcul de certificat

3.3 Calcul inverse

4. Compte rendu d'exécution des divers ordres

4.1 Erreurs "protocole"
4.2 Fin d'exécution

5. Cas d'enregistrement de IFZ

5.1 Type session
5.2 Type consommation

PRESENTATION

La carte VIDEOTEX se présente sous la forme d'une carte en plastique au format ISO conformément aux normes ISO 2894 et 3554.

Elle contient un microcalculateur monolithique, autoprogrammable, breveté par BULL.CP8, composé d'une mémoire non volatile permettant l'enregistrement de données à caractère secret ou confidentiel et de circuits associés assurant sa protection.

Le dialogue avec la carte s'effectue selon le protocole défini par la norme ISO relative aux cartes à microprocesseur.

De la famille des cartes porte-clés, la carte vidéotex offre un nouveau service : la consommation. Elle s'est également enrichie de fonctionnalités nouvelles telles que télé-écriture et certification. En outre, la fonction Vidéopass inversible (de la famille télépass) permet l'exploitation d'un parc de cartes "usager" à l'aide de cartes mères.

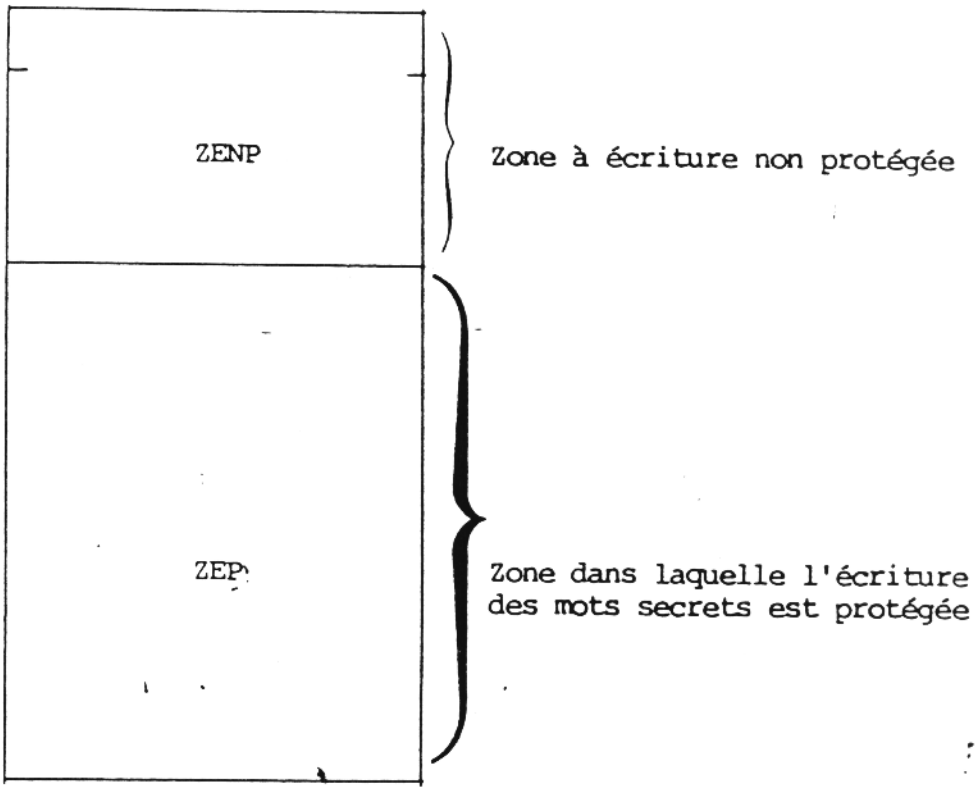
Les principes d'utilisation de la mémpire EPROM sont décrites au chapitre I du présent document. Les fonctionnalités faisant l'objet du chapitre II.

CHAPITRE I

PRINCIPES D'UTILISATION DE LA MEMOIRE EPROM

1 - STRUCTURE PHYSIQUE DE LA MEMOIRE

Les phases successives qui marquent la vie d'une carte (fabrication, personnalisation, utilisation) structurent la mémoire EPROM, banalisée à l'origine, en deux zones aux conditions d'accès différenciées.



1.1 Affectation des zones

- ZENP : zone de 10 mots à écriture non protégée, destinée à recevoir les informations de fabrication et une clé propre à l'émetteur.

- ZEP : zone à écriture protégée, destinée à recevoir les différents services accompagnés de leur clé d'où le nom de zone porte-clés qui lui est communément attribué.

1.2 Organisation mémoire

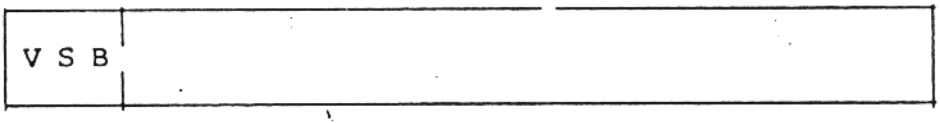
La carte VIDEOTEX fait partie d'une nouvelle génération de cartes pour lesquelles l'entité adressable est désormais l'octet.

De plus l'adressage devient relatif à la base 0.

Ainsi pour un numéro de composant duquel découle la taille EPROM dont ce composant dispose, il devient aisé de déterminer la zone d'adressage.

Ici la capacité de la mémoire EPROM est de 8 Kbits.
Elle est structurée en 256 mots de 32 cb.

Pour chaque mot les 3 cb de poids forts sont affectés aux bits "système" V, S et B. Ces bits conditionnent l'exploitation du mot par le microprocesseur de la carte.



- V = 1 : Le mot est non validé (1)

- V = 0 : le mot est validé

  - S = 0 : le mot est secret. La carte n'autorise pas la lecture externe d'un tel mot.

  - S = 1 : mot non secret dont la lecture est autorisée sans conditions.

    - B = 0 début de bloc

    - B = 1 mot courant dans le bloc

(1) à l'état vierge les bits sont à "1".

IMPRIME N° 740 C 102

2 - DESCRIPTION DES ZONES "SYSTEME"

2.1 Zone de fabrication

Elle est constituée des 4 mots de la partie supérieure de la ZENP ayant pour adresse 0, 4, 8 et C.

Adresse octet

	31				0
0	0 1	TESTO	N° SECRET LOT.	N° CHRONOLOGIQUE	CCE
4	0 1 1	N° CHRONOLOGIQUE SUITE			CCE
8	0 1 1	N° FABRICANT	N° DE DIVERSIFICATION		CCE
C	0 0	CLE DE FABRICATION			

Les mots dont les adresses sont 8 et C ainsi que le champ du premier mot contenant le numéro de secret de la carte lot, sont enregistrés en usine (MOTOROLA, EUROTECHNIQUE, etc...).

- N° de fabricant : il identifie l'encarteur (par exemple BULL/CP8) et par conséquent le mode de génération, propre à chacun des "encarteurs", des informations complémentaires.

Pour BULL/CP8 ces informations sont les suivantes :

- N° de secret : le numéro de secret identifie le secret de la carte "lot" utilisé pour générer la clé de fabrication.

- N° de diversification : le numéro est issu d'un compteur module 2^{15} incrémenté lors de chaque génération de clé de FAB. Le numéro est l'une des variables d'entrée servant à générer la clé de FAB.

- CCE : code correcteur d'erreur (1)

- Clé de FAB. : mot secret assurant la protection des composants (waffers) jusqu'à leur mise en exploitation, via l'"encarteur".

Le mot 1 et le demi mot de poids faible du mot 0 sont réservés pour l'enregistrement d'un numéro chronologique (numéro de série).

Ces informations de fabrication sont homogènes avec celles enregistrées dans les cartes B1 qui sont de la même génération.

Dans le cas de la carte VIDEOTEX seuls le numéro de série et le numéro de fabricant sont nécessaires, la clé de fabrication n'étant quant à elle pas exploitée.

2.2 Zone des locks

La zone des locks est constituée du dernier mot de la mémoire EPROM.

3FC				LU	LF	IV	TEST 1

LU : lock marquant l'entrée en exploitation d'une carte "utilisateur"

LF : lock marquant la fin de la phase de fabrication

IV : invalidation de la carte

2.3 Zone CC

Deux mots sont réservés aux enregistrements du code confidentiel :

CC1 : code fourni.
CC2 : code de remplacement pouvant être choisi par le porteur.

Ces deux mots précèdent le mot des locks.

0 0	CC2
0 0	CC1

Les codes sont cadrés à droite du mot et complétés sur leur gauche (poids forts) par des "zéros".

Exemple pour le code 5719

0	0	0	0	5	7	1	9

2.4 Zone clé émetteur

Cette zone constitue un espace privilégié destiné à recevoir un bloc d'autorisation particulier dont l'exploitation conditionnera la validation des mots secrets de la ZEP (zone à écriture protégée) soit par écriture directe soit par télé-écriture.

10	0 1 0	ORDRE						IDENTIFICATEUR D'AUTORISATION							IND.
14	0 1 1	0	N° EXPLOITATION INITIAL							TYPE		LG. FENETRE			
18	0 0	CLE SECRETE													
1C	0 0														
20	0 0														
24	0 0														

Les 6 mots ci-dessus constituent une en-tête de bloc d'autorisation. Le format de cette entête de bloc est commun aux divers types de blocs. Ces divers types de blocs sont possibles pour le bloc émetteur. Seule la clé de ce bloc peut être enregistrée sans protection (voir au § 3 la structure des divers blocs d'autorisation.

(1) Polynome de Hamming de la forme $X^5 + X^2 + 1$, référence "ERROR - CORRECTING CODE Second Edition WESLEY PETERSON ET E.J WELSON Jr MIT. PRESS CAMBRIDGE, Massachussets 02142". Est applicable sur 1 mot maximum. Le bit V est ignoré, on prend les bits précédents le CCE et on les complète à gauche par des zéros pour former une zone de 26 bits.

3 - DESCRIPTION DE LA ZONE PORTE-CLES

A l'exception du mot des locks et des mots CC1 et CC2 la ZEP (zone à écriture protégée) est destinée à recevoir des blocs d'autorisations donnant accès aux services correspondants.

Les blocs d'autorisations peuvent être de trois types différents. Le choix du type est effectué par l'émetteur en fonction de l'utilisation qui sera faite de ce bloc d'autorisation, de manière à offrir le meilleur service possible.

3.1 Bloc d'autorisation de type abonnement

Chaque bloc d'autorisation est composé de **6 mots validés consécutifs.**

V S B

0 1 0	X X X X X	IDENTIFICATEUR D'AUTORISATION (24 cb)		IND.
0 1 1	0	N° EXPLOITATION INITIAL	MOD = F	LG. FENETRE
0 0	CLE SECRETE			
0 0				
0 0				
0 0				

- Le bit B dans le cas d'un mot validé non secret permet à la carte de rechercher aisement un début de bloc.
  La combinaison V, S, B = 0, 1, 0 est réservée à ce type de mot.

- Identificateur d'autorisation (24 cb) : c'est par l'intermédiaire de cet identificateur d'autorisation que l'on accède au bloc d'autorisation, en cours d'exploitation, spécifique au service émis.

- N° exploitation initial (12 cb) : caractérise le début de validité de l'abonnement (en jours par exemple).

- TYPE : doit ici identifier le type "taxation à l'abonnement" et doit avoir dans ce cas la valeur 1111.

- Largeur fenêtre (12 cb) : donne la durée de validité de l'abonnement.

- CLE : cette clé de 128 cb dont les bits V et S sont à zéro permet de délivrer la combinaison d'accès K lorsque toutes les conditions sont réunies pour que le calcul de cette dernière soit effectué.

3.2 Bloc d'autorisation de type session

a) Session libre

Chaque bloc d'autorisation en mode session est composé d'au moins 7 mots validés et consécutifs.

0 1 0 X X X X X	IDENTIFICATEUR D'AUTORISATION							
0 1 1 0	N° EXPLOITATION INITIAL			MOD = N.MOTS	0 0 0 0	LG. FENETRE		
0 0 0 0 0 0 0 0	CLE SECRETE							
0 1 1 0	C	IFZ	V MAX	0	1	1 0	DU1	DEPL1
0 1 1 0	DU2		DEPL2					

NB. MOTS

- Identificateur d'autorisation (24 cb) : identique au mode taxation à l'abonnement (3.1).

- N° exploitation initial (12 cb) : identique au mode taxation à l'abonnement (3.1).

- TYPE : donne ici le nombre de mots attribués à la zone inscriptible. Destinée à recevoir les enregistrements correspondants aux ouvertures de sessions.

  0000 < NB. MOTS < 1111

- Largeur fenêtre (12 cb) : donne la durée de validité du service souscrit sur les 8 bits de poids faible, les poids forts devant être à "0" afin d'interdire DEPL > FFH (taille du champ déplacement d'une session).

- Clé : identique au mode taxation à l'abonnement (3.1).

- Zone inscriptible : cette zone comprend ½ mot d'ouverture de zone inscriptible et offre la possibilité d'enregistrer une session par demi mot.

- ½ mot d'ouverture :

  - C (1 cb) conditionne le mode d'enregistrement des sessions. En mode libre C = 1.

  - IFZ (3 cb) indicateur fin de zone interdit l'exploitation de la zone si ≠ 111 et permet de poursuivre la recherche au-delà de ce bloc.

  - VMAX (8 cb) prédétermine le nombre d'unités de valeur à consommer pour l'ensemble des sessions inhérentes au bloc.

- ([2 x NB mots] - 1) SESSIONS

  - Hormis le ½ mot d'ouverture de la zone inscriptible chaque demi mot est réservé à l'enregistrement d'une session.

  - Du (4 cb) : durée ou nb d'unités de valeurs attribué à la session.

IMPRIME N° 740 C 102

- DEPL (8 cb) : différence calculée entre le n° d'exploitation diffusé et le n° d'exploitation initial enregistré.

- Chaque session possède 4 bits "système" nécessités par les demis-mots de gauche qui ne doivent pas perturber le système d'exploitation V, S, B, = 0, 1, 1.
  A ces 3 bits déjà connus vient s'ajouter le bit E qui joue le rôle pseudo bit V pour chaque session. Ce bit est géré par la carte.

b) Session contrôlée

Chaque bloc d'autorisation en mode session est composé d'au moins 7 mots validés et consécutifs.

0 1 0	N° ORDRE	IDENTIFICATEUR D'AUTORISATION (24 cb)					
0 1 1 0	N° EXPLOITATION INITIAL		TYPE	0 0 0 0	LG. FENETRE		
0 0							
0 0	CLE SECRETE						
0 0							
0 0							
0 1 1 0	C	IFZ	V MAX	0	1 1 0	DU1	DEPL1
0 1 1 0	DU2		DEPL2	0	1 1 0	DU2	DEPL2
0							
0							
0							

NB. MOTS

- N° ordre (5cb) : donne le rang du bloc d'autorisation pour un identificateur d'autorisation donné.

- Identificateur d'autorisation (24 cb) : identique au mode taxation à l'abonnement (3.1).

- N° d'exploitation initial (12 cb) : identique au mode taxation à l'abonnement (3.1).

- TYPE : identique à 3.2 a).

- Longueur fenêtre (12 cb) identique à 3.2 a).

- Clé : identique à 3.1

- Zone inscriptible : cette zone comprend ½ mot d'ouverture de zone inscriptible et offre la possibilité d'enregistrer une session par demi-mot.

- ½ mot d'ouverture :

  - C (1 cb) caractérise le mode d'enregistrement des sessions.

  - En mode contrôlé C = 0

  - IFZ : identique à 3.2 a)

  - VMAX : identique à 3.2 a)

- [[2 x NB_mots] - 1] SESSIONS

  - Du : identique à 3.2 a)

  - DEPL : identique à 3.2 a)

NOTA : Les mots composant la zone inscriptible doivent être prévalidés lors de l'enregistrement du bloc d'autorisation afin de prémunir l'émetteur contre tout enregistrement de session qui ne serait pas contrôlé par lui.

3.3 Bloc d'autorisation de type consommation

Chaque bloc d'autorisation est composé d'au moins 7 mots validés et consécutifs.

V S B					
0 1 0	N° ORDRE	IDENTIFICATEUR D'AUTORISATION			
0 1 1 0	N° EXPLOITATION INITIAL		TYPE = 0	LG. FENETRE	
0 0 0 0 0 0 0 0	CLE SECRETE				
0 1 1 0	X	IFZ	N.EV	NM/EV	ZV
0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 ZC 0 1 1 0 1 1 0 1 1 0 1 1	RUF		EV N EV.1		
0 1 1 0 1 1 0 1 1			EV.0		

- N° ordre (5 cb) : identique au mode session contrôlé (3.2 b).

- Identificateur d'autorisation (24 cb) : identique au mode taxation à l'abonnement (3.1).

- TYPE : doit ici identifier le type taxation à la consommation (TYPE = 0).

- Numéro d'exploitation initial (12 cb) : identique au mode abonnement (3.1).

- LG fenêtre : identique au mode abonnement (3.1).

- Clé : identique au mode abonnement (3.1).

- Zone inscriptible : cette zone comprend 1 mot d'ouverture et l'espace mémoire alloué à la consommation dont l'exploitation est fonction du mot d'ouverture.

- Mot d'ouverture :

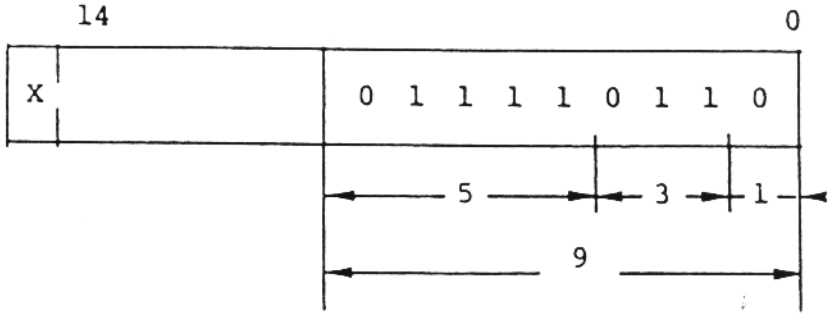
  - IFZ : identique à 3.2 a).

  - NEV : nombre d'entités valorisables (1 à 15). La zone de consommation comprend un nombre entier d'entités valorisables. Une entité constitue la plus petite partie de la zone de consommation qu'il est possible de mettre en service (voir ZV).

  - NM/EV : nombre de mots par entité (1 à 15). Chaque mot supporte 24 unités
    NEV.NM/EV définit la taille (en mots) de la zone consommable.

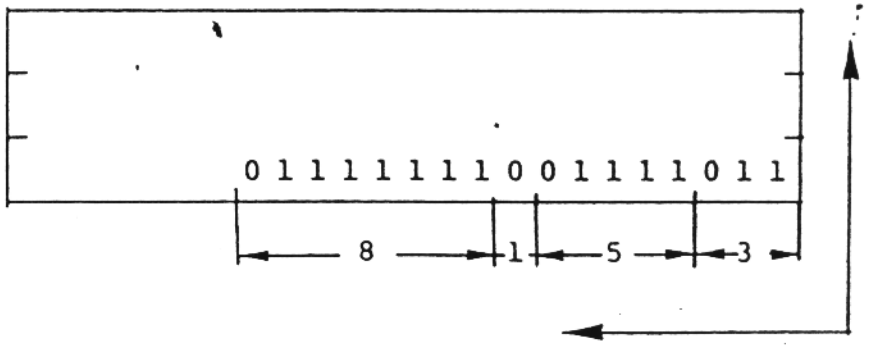
  - ZV : Zone de valorisation. Cette zone contient les indicateurs de mise en service relatifs à chacune des entités valorisables (max = 15). Un indicateur de mise en service est actif à "0". Le bit de rang 0 de ZV correspond à l'entité 0 de la zone de consommation.
    L'indicateur actif de rang le plus élevé correspond au nombre d'entités valorisables ouvertes.

L'écriture par télé-valorisation dans la zone ZV se fait de la droite vers la gauche. L'enregistrement d'un seul bit suffit à la mise en service d'une ou plusieurs entités et caractérise une valorisation. Le déplacement entre deux "zéros" définit le nombre d'entités mises en service lors d'une valorisation.



- ZC : (Zone de consommation).
La zone de consommation est constituée de N. entités valorisables, chacune de ces entités étant elle-même constituée d'un nombre de mots (NM/EV) choisi par le bloc.
Le rôle de la zone de consommation est de recevoir l'enregistrement du nombre d'unités à payer pour accéder au service désiré.
La consommation se fait à partir de la fin de zone (première entité en service) vers son début (dernière entité mise en service).
A chaque accès un seul bit est "grillé" dans la zone de consommation. Ainsi l'espace entre 2 bits à zéro représente le nombre d'unités consommées lors de l'accès considéré.

Ex. :



CHAPITRE II

FONCTIONNALITES

IMPRIME Nº 740 C 102

La carte peut être sollicitée soit par une remise à zéro (RAZ) soit par un ordre.

Toute session sera initialisée par une RAZ à la suite de laquelle des ordres élémentaires pourront être exécutés.

Les ordres élémentaires sont partagés en 2 catégories :

- Les ordres entrant pour lesquels les données transitent du terminal vers la carte et entrent dans la carte.
- Les ordres sortant pour lesquels les données transitent de la carte vers le terminal et sortent de la carte.

Les divers ordres peuvent être différenciés en 2 grandes classes :

- Les ordres standards : ces ordres sont nécessaires à toutes les cartes ou ne sont pas alloués à la sécurisation du système :
  - ECRITURE
  - LECTURE
  - MARQUAGE DES LOCKS
  - RECHERCHE SUR ARGUMENT
  - LECTURE DU RESULTAT.
- Les ordres assurant la sécurité du système : ce sont les ordres qui permettent à un émetteur de carte de contrôler leur utilisation et à l'usager de bénéficier des services pour lesquels il a acquis des droits.
  - calcul de combinaison d'accès
  - calcul de clé de validation des mots secrets ou identification du porteur (PIN)
  - télé-valorisation
  - télé-écriture
  - calcul de certificat
  - fonction inverse (réservée aux cartes mères)

IMPRIME N° 740 C 102

1 - RAZ

Une RAZ appliquée sur la carte entraîne une réponse de cette dernière sous forme d'un train de 11 octets dont la première partie (4 octets) se rapporte à l'interface de la carte et conditionne le mode d'échanges entre cette carte et le terminal, la seconde (7 octets) caractérise l'application, conformément au paragraphe "structure des échanges de la norme ISO".

1.1 Octets d'interface

TS = 3F H

TO = 67 H

TB = 35 H

TC = 02 H

1.2 Octets complémentaires ou historiques

Ces octets permettent à l'utilisateur :

- d'identifier la carte en présence,
- de connaître la phase de vie dans laquelle la carte est entrée.

1.2.1 Mot des caractéristiques MEMOIRE UTILISATEUR

MCM	0	0	0	0	0	0	1	0

Dans cet octet est codé un numéro de composant. A ce numéro sont associées les caractéristiques de la mémoire utilisateur.

- TYPE de la mémoire : EPROM
- Taille de la mémoire : 8Kbits

1.2.2 Mot des caractéristiques fonctionnelles (MCF)

Dans cet octet est rangé un code fonction auquel sont associés une classe d'instruction et un jeu d'ordres spécifiques.

Cet octet s'exploite en complément du précédent. A partir de MCF = 10 H nous avons affaire à une nouvelle génération de cartes pour laquelle l'adressage devient relatif (ad. début = 0) avec pour unité d'adressage l'octet.

Pour la carte VIDEOTEX l'octet MCF pourra prendre l'une parmi deux valeurs possibles suivant que la carte est destinée à un usage standard (carte fille) ou qu'elle est destinée à assurer le contrôle du système d'exploitation (carte mère).

MCF	0	0	0	1	0	0	1	0	carte "fille

ou

MCF	0	0	0	1	0	0	1	1	carte "mère"

A ces 2 codes fonction (12 H et 13 H) est associé un jeu d'ordre spécifique identifié par AC (code classe d'instruction).

ORDRE	MNEMO	CODE (Hexa)
LECTURE	LEC	BO
ECRITURE + VALIDATION	ECR	DO
ECRITURE DES LOCKS	LOC	50
RECHERCHE SUR ARGUMENT	RSA	AO
DEMANDE DE CALCUL	DDC	10
DEMANDE DE RESULTAT	DDR	20
CERTIFICATION	CER	80
* DEMANDE DE CALCUL INVERSE	DDCI	88

* interdite lorsque MCF = 12 H (carte fille)

1.2.3 Mots des extensions EXH et EXB

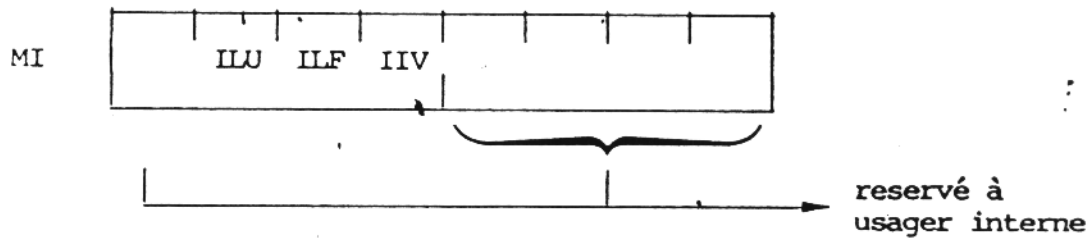
Ces deux octets font leur apparition avec cette nouvelle génération de cartes pour lesquelles MCF identifie les fonctionnalités de base dont est dotée la carte en présence. Ces fonctionnalités peuvent être étendues lors de la réalisation d'autres masques. Dans ce cas, le code fonction demeure inchangé et on utilise les octets EXH et EXB pour identifier ces diverses extensions, chacune des extensions se voyant attribuer un bit particulier de EXH, EXB. On notera à l'occasion qu'une extension constitue une entité indivisible.

Pour le cas qui nous occupe, les octets d'extensions sont tous deux nuls (inutilisés).

EXH = 00
EXB = 00

1.2.4 Mot des indicateurs

Dans cet octet sont rangés les indicateurs qui conditionnent la mise en oeuvre des fonctionnalités offertes par la carte. C'est le cas des locks qui jalonnent les diverses phases de vie de la carte.



ILU : Présence du lock utilisateur. Dès la prise en compte de ce lock la carte a pour code fonction MCF = 12 H et dispose du jeu d'ordres associé (fonction "vidéopass" inverse inhibée).

ILF : Présence du lock de fabrication. En absence de LU le jeu d'ordres disponible est celui correspondant au code fonction MCF = 13 H.

IIV : Carte invalide. Sa présence interdit l'exécution des fonctions :

- écriture directe
- télé-écriture
- télé-valorisation
- certification
- calcul inverse

NOTA : l'exploitation des droits en cours, des divers services, demeure possible.

1.2.5 Mot d'état ME1 et ME2

Ce sont les mots d'état caractérisant la phase fin de tous les ordres. Lors de la RAZ ces mots d'état auront pour valeur 90 et 00. Lors de l'exécution les divers ordres, ME1 et ME2 pourront prendre différentes valeurs (voir § 4.2).

IMPRIME N° 740 C 102

2 - ORDRES ELEMENTAIRES

2.1 Ordre de lecture (B0)

Les octets A1-A2 de la phase d'intialisation de l'ordre donnent l'adresse logique (octet) à partir de laquelle L octets seront lus.

NOTA : Si L = 0 la longueur du message d'infos lues sera de 256 octets.

La lecture ne sera toutefois possible que si l'adresse communiquée lors de la phase d'initialisation de l'ordre est une adresse mot (multiple de 4 octets) et que si ce mot appartient au champ de mémoire EPROM.

Dans le cas contraire la carte devient sourde et muette.

Le contenu réel des mots secrets (mots dont les bits V et S sont à zéro) est remplacé par des zéros.

2.2 Ordre d'écriture (D0)

Les octets A1-A2 de la phase d'initialisation donnent l'adresse du mot à écrire

- L = 4. L'entité d'écriture est le mot.

- L'adresse pointe un mot (adresse multiple de 4 octets).

Si cette condition n'est pas satisfaite la carte se manifeste par un mutisme.

- Le mot adressé n'est pas validé (V = 1). Dans le cas contraire, le bit ER est positionné dans ME2.

L'écriture d'un mot s'exécute en 2 phases :

- une phase d'écriture de 31 bits de données,

- une phase validation si le bit V est prépositionné à "0" dans les données transmises à la carte.

S'il n'y a pas modification du contenu d'un octet à écrire, l'écriture n'est pas effective (gain de temps).

A la suite de chaque écriture effective, il y a contrôle de cette écriture, en cas d'échec la carte interrompt l'écriture et signale cette erreur en positionnant le bit ER de ME2 à 1.

IMPRIME N° 740 C 102

- Dans la zone à écriture non protégée (ZENP) tous les mots sont à écriture libre.

- Dans la zone à écriture protégée (ZEP) les mots secrets ne peuvent être validés que sous contrôle de l'émetteur.

Une sollicitation préalable de cette dernière (voir § 3.1.2) donnera un résultat exploitable comme code confidentiel d'accès.

Si ce code est correct, la validation est réalisée sinon l'indicateur CF (MEl) est positionné.

En phase utilisation LU = 1 l'écriture de mots secrets est interdite.

2.3 Présentation d'un ordre de marquage des locks (50).

Les paramétres A1-A2 ne sont pas significatifs.

L = 4 obligatoirement les locks proprement dits sont situés dans le 3ème octet de la zone des LOCKS (CII 1.2.2).

L'écriture dans la zone des locks se fait comme une écriture standard avec contrôle sur chacun des octets. Il est impératif que toute modification de ce mot soit opéré en conformité avec son contenu initial par exemple :

Pour écrire le lock	LF	DF	
Pour écrire le lock	LU	9F	(LF + LU)
Pour écrire le bit d'invalidation	IV	8F	(LF + LU + IV)

Seules exceptions aux règles d'écriture :

- Le bit V n'interdit pas ici un nouvel accès.

- Rendre le mot secret ne nécessite pas l'utilisation de la clé émetteur.

2.3 Recherche sur argument (A0)

La recherche sur argument permet d'accéder rapidement à un mot en mémoire EPROM dont le contenu est connu.

- Les octets A1-A2 de la phase initialisation de l'ordre contiennent l'adresse du mot (multiple de 4 octets) à partir de laquelle la recherche s'exécutera.

- L = 4 obligatoirement.

- Si depuis l'adresse indiquée jusqu'à l'adresse supérieure de la mémoire le profil recherché n'est pas rencontré, la carte positionne l'indicateur argument absent de ME2.

2.5 Lecture du résultat (20)

Les paramètres A1-A2 ne sont pas significatifs, la longueur est impérativement égale à 8.

Cet ordre doit suivre un ordre de recherche sur argument ou un ordre mettant en oeuvre la fonction "VIDEOPASS".

- Faisant suite à une recherche sur argument le résultat lu est le suivant :

Profil du mot	ad mot	ad mot + 8 *

* Dans le cas de recherche d'un début de bloc cette adresse est mémorisée par la carte et pointe donc la clé qui est utilisable pour effectuer des calculs de certificats s'ils suivent cette lecture de résultat. En effet, cet indicateur est remis à jour par tout ordre autre que lecture du résultat ou certification.

- Faisant suite à un ordre mettant en oeuvre la fonction VIDEOPASS les 8 octets lus contiennent le résultat obtenu après calcul, si ce résultat est lisible.

La lecture d'un résultat n'est possible qu'une seule fois, le renouvellement de cette lecture se traduisant par un résultat nul. Il en est de même pour une lecture illicite de résultat.

3 - ORDRES ASSURANT LA SECURITE DU SYSTEME

Il s'agit d'une manière générale des ordres qui permettent sous contrôle de clés secretes (fonction VIDEOPASS) :

- Au porteur de la carte de fournir la combinaison K permettant à un instant donné d'accéder à un service .
- A l'émetteur de personnaliser une carte ou de lui délivrer des droits nouveaux.

3.1 Demande de calcul (10)

3.1.1 Présentation générale

L'ordre "demande de calcul" est spécifique à la famille des cartes de contrôle d'accès dont le code classe d'instructions est "AC".

Cet ordre est paramétrable. Quatre MODES d'exploitation sont possibles :

- Calcul d'une combinaison d'accès
- Télé-valorisation
- Présentation de clé
- Télé-écriture

Quel que soit le mode d'exploitation l'ordre "demande de calcul" se présentera comme suit.

3.1.1.1 Phase initialisation

Les paramètres A1-A2 ne sont pas significatifs en tant qu'adresse. Seul le bit de poids fort de A1 est utilisé pour indiquer à la carte qu'elle est autorisée à utiliser la tension de programmation (VPP).

Plus communément nous appelerons ce bit indicateur d'autorisation d'écrire (I.A.E.).

L = 14 déc.

IMPRIME N° 740 C 102

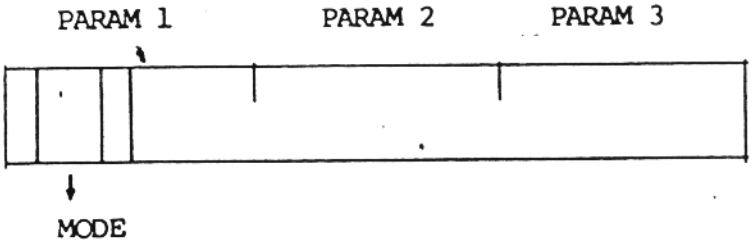
3.1.1.2 Phase exécution

Les 14 octets de données, échangés du terminal vers la carte durant la phase active de l'ordre, sont partagés en 3 champs :

- Un champ référence de 3 octets : c'est à partir de cette référence que la carte recherche le bloc d'autorisation désiré dans l'espace mémoire autorisé.

- Un champ paramètres de 3 octets dans lequel les bits 5 et 6 de l'octet PARAM 1 code le mode d'exploitation de l'ordre et définit le contenu des paramètres proprement dits.

- Un champ de 8 octets de données : le contenu de ce champ est totalement indépendant du service utilisé et peut être généré (par l'émetteur) de manière totalement aléatoire. C'est ce nombre qui changeant à chaque accès interdit la réutilisation d'une combinaison d'accès K et protège l'émetteur contre les utilisations illicites de services.



3.1.1.3 Phase fin

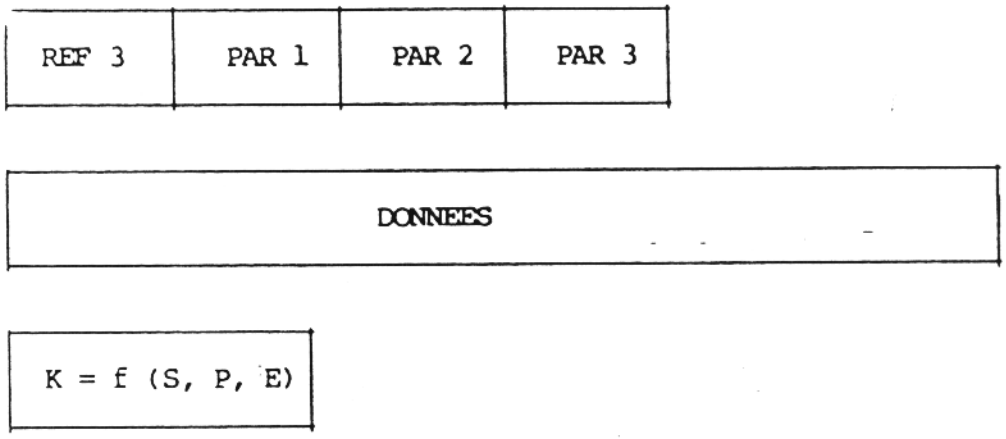
Le contenu des mots ME1, ME2 constitue le compte rendu d'exécution. Les indicateurs contenus par ME1 et ME2 sont définis au paragraphe 4.2 du présent chapitre.

IMPRIME N° 740 C 102

En conclusion :

Une combinaison K (8 octets) est calculée en activant la fonction "VIDEOPASS" qui exploite comme éléments d'entrée

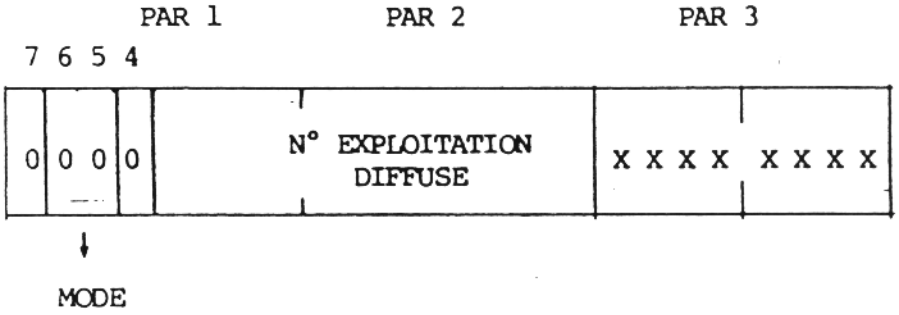
- La clé secrete (128 cb) du bloc d'autorisation (S)
- Le champ de paramètre plus l'octet REF 3 du champ référence (P)
- Le champ de données (8 octets) qui constitue le champ de données à chiffrer ou à déchiffrer (E).



3.1.2 MODE = 00 : Calcul d'une combinaison d'accés

Il s'agit d'une demande de calcul courante s'adressant à un bloc de type ABONNEMENT, SESSION LIBRE, SESSION CONTROLEE ou CONSOMMATION, conduisant à la fourniture d'une combinaison d'accès K. En fonction du type de bloc exploité, le champ des paramètres prend des significations différentes. De même le traitement du bloc est particulier à chaque type.

3.1.2.1 Type abonnement



Les 2 octets de paramètres 1 et 2 sont exploités tels quels pour effectuer le contrôle de validité du bloc lors de l'accès considéré.

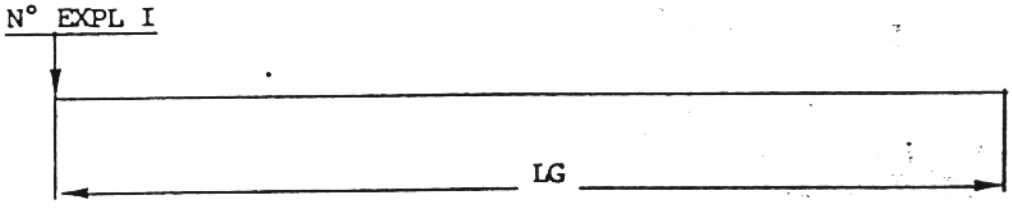
(1) N° EXPL I $\leqslant$ N° EXPL D $<$ N° EXPL I + LG

Les bits 4 et 7 du quartet de poids fort de PAR 1 doivent être positionnés à "0" par le diffuseur (prestataire de service).

N° EXPL I : numéro d'exploitation initial

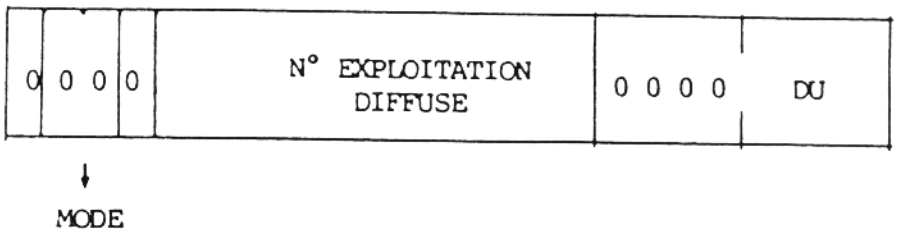
N° EXPL D : numéro d'exploitation diffusé (émis)

LG : largeur fenêtre définissant la période de validité exprimé par un nombre sans unité particulière bien que l'unité de temps soit la plus communément utilisée.



IMPRIME N° 740 C 102

3.1.2.2 Type_session_libre_



Le cas est identique au précédent avec la particularité que l'octet PARAM 3 contient la durée (nombre de numéros) pour laquelle la session si elle doit être enregistrée sera valide.

Il est impératif que le quartet de poids fort de PARAM 3 soit positionné à "0" par le diffuseur.

Le premier contrôle qu'effectue la carte est le contrôle exprimé par l'équation (1) précédente ; s'il est réalisé avec succès, 2 autres contrôles suivent.

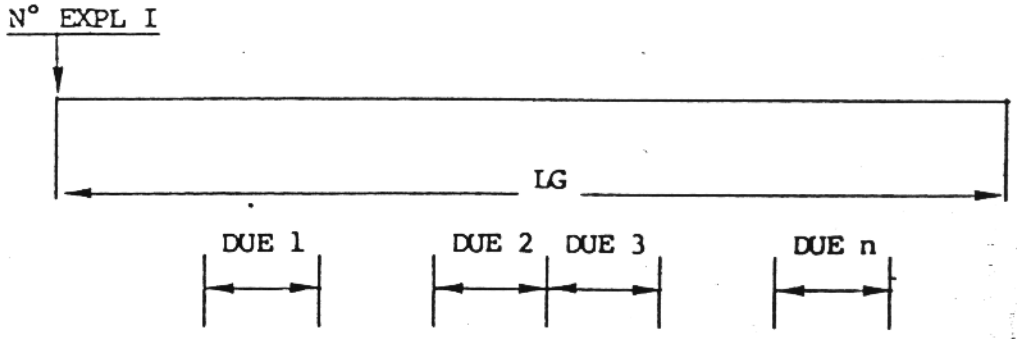
(2) $DEPL\ E_i \leqslant DEPL\ D < DEPL\ E_i + DUE_i$

$DEPL\ E_i$: déplacement enregistré dans la session de rang i.

DEPL D : déplacement calculé à l'aide du paramètre d'entrée (paramètres diffusés ou émis) avec DEPL D = N° EXPL D - N° EXPL I

DUE_i : durée enregistrée dans le champ correspondant de la session de rang i. Ce champ définit la période de validité de la session.

(3) $\sum_{i=1}^{i=n} DUE_i \leqslant VMAX$



IMPRIME N° 740 C 102

Si aucune des sessions enregistrées ne peut satisfaire le DEPL D, la carte enregistrere une nouvelle session si :

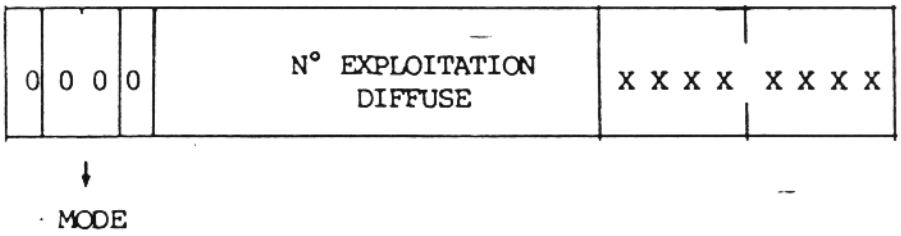
- Elle est autorisée à le faire (I.A.E. = 1).

- La place est disponible pour le faire (dans la zone inscriptible).

$$- \quad \sum_{i=1}^{i=n} DUE_i + DUD \leqslant VMAX$$

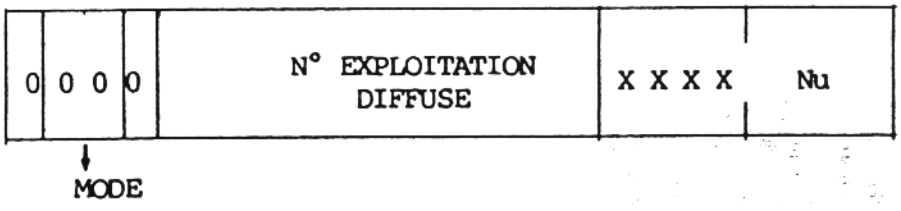
Après enregistrement de la session le nombre n des sessions enregistrées est incrémenté,
DEPL D fournissant DEPL E_n et
DUD fournissant DUE_n

3.1.2.3 Type_session_contrôlée_



Ce cas est identique au type abonnement pour ce qui concerne le contenu des 3 octets de paramètres.
Le traitement effectué par la carte est identique à celui du mode session libre excepté lorsque l'ouverture d'une nouvelle session est nécessaire. Cette ouverture ne pouvant être réalisée qu'en mode télé-valorisation sous "contrôle" de la clé émetteur.

3.1.2.4 Type_consommation



Le quartet de poids faible du champ des paramètres donne le nb d'unités à consommer (0 à 15). Cette consommation sera effectuée dans la zone des entités valorisables ouvertes après contrôle de validité habituel représenté par l'équation (1).

L'organigramme suivant met en évidence et résume les différents contrôles effectués lors d'une demande de calcul d'une combinaison d'accès (MODE = 00) et ce en fonction du type de bloc en présence.

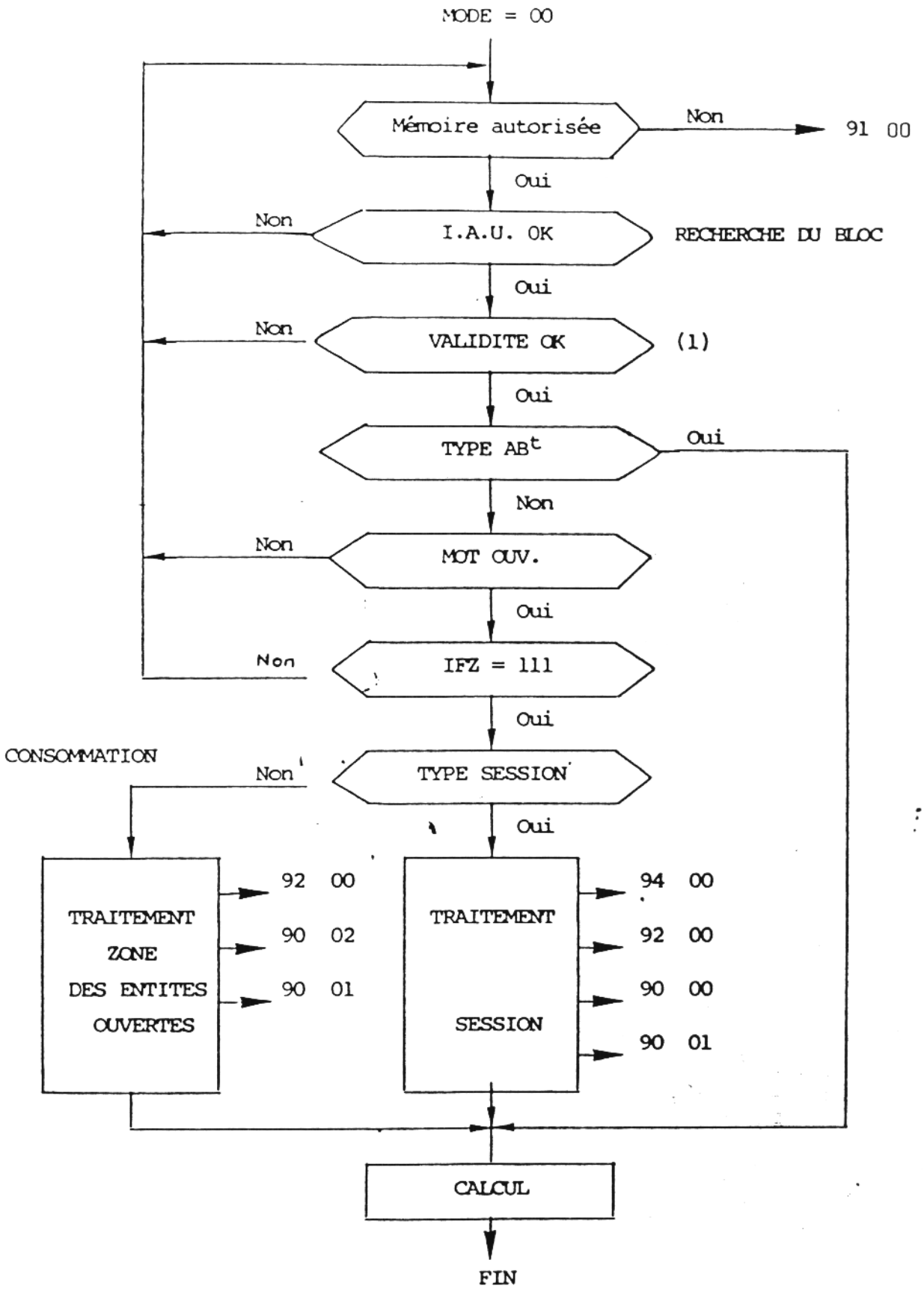
On voit apparaitre également le rôle important alloué à l'indicateur IFZ qui permet de chainer sur un autre bloc (avec même identificateur d'autorisation) et donc de mettre hors service un bloc devenu inexploitable.

L'exploitation d'un bloc s'effectue en 4 phases :

- Recherche du bloc d'autorisation
- Contrôle de la validité du bloc
- Traitement inhérent au type de bloc
- Calcul de la combinaison d'accès.

Les diverses phases comportent des tests conditionnels à l'issue desquels le traitement peut être interrompu. Les diverses sorties qui en résultent sont classées suivant l'ordre dans lequel ces tests sont effectués.
Pour chacune d'entre elles est affecté aux mots d'état, un contenu qui la caractérise et qui permet de l'identifier.

CALCUL D'UNE COMBINAISON D'ACCES



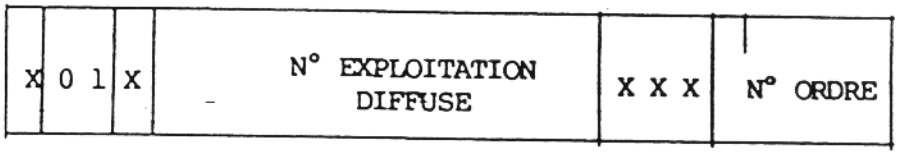
3.1.3 Mode = 01 : Télé-valorisation

Le mode de paramétrage de l'ordre demande de calcul est utilisé pour ouvrir sous contrôle de l'émetteur via la clé du même nom, des droits nouveaux, relatifs à des blocs d'autorisation déjà existants.

Ces blocs ne peuvent être que de 2 types :

- TYPE session contrôlée
- TYPE consommation

3.1.3.1 TYPE session contrôlée



Le contenu des 3 octets de paramètres diffusés doit être tel que représenté ci-dessus.

L'objet du calcul ici n'est pas de fournir une combinaison d'accès mais un résultat qui soit exploitable pour ouvrir une session.

La recherche du bloc d'autorisation à télé-valoriser s'effectue sur l'identificateur d'autorisation et le numéro d'ordre associé. Puis le calcul est effectué. Le résultat obtenu (K = K7, K6 ... K0) doit satisfaire la cohérence prédéterminée suivante :

K7, K6, K5, K4 = K3, K2, K1, K0

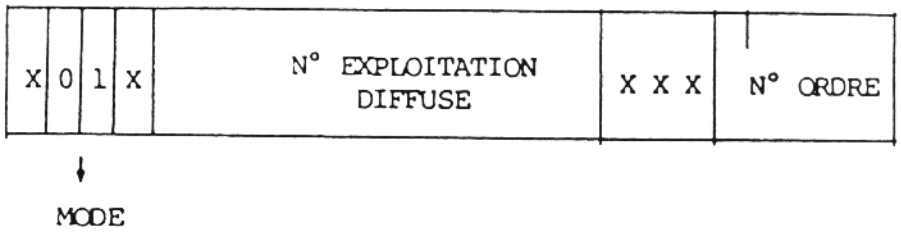
Cette cohérence étant établie, la carte utilisera les octets K2, K1, K0 comme champ des paramètres.

Ces paramètres doivent alors satisfaire les même exigences que ceux délivrés par le diffuseur dans le cas de session libre (§ 3.2.2).

L'organigramme qui suit met en évidence le rôle du n° d'ordre dans le cas de télé-valorisation qui seul permet d'éviter un bloc hors service.

IMPRIME N° 740 C 102

3.1.3.2 TYPE_CONSOMMATION



L'exécution se déroule suivant le même principe que dans le cas du type session contrôlée, jusqu'à l'obtention du résultat de calcul qui doit satisfaire la même règle de cohérence.

Cette première cohérence étant établie une seconde spécifique au type consommation devra être établie qui consiste à vérifier l'égalité du contenu initial de ZV (ZVI) et le contenu des octets K2 et K1. Cette condition est nécessaire pour éviter de rejouer une combinaison d'entrée. K0 contient alors dans son quartet des poids faible le nombre d'entités à ouvrir.

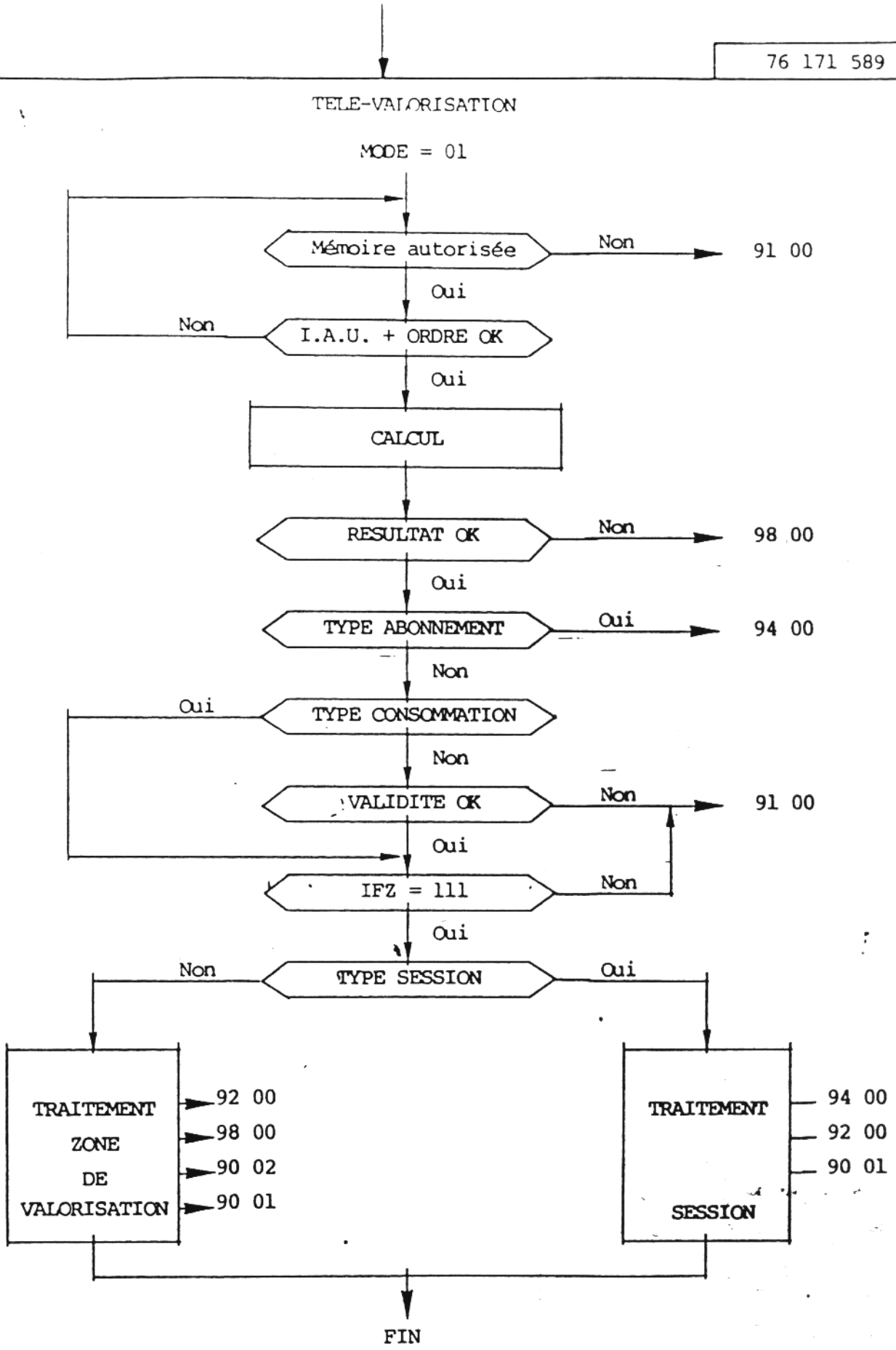
L'organigramme suivant relatif au mode télé-valorisation met en évidence les particularités de ce mode.

L'ordre des phases d'exploitation du bloc est modifié :

- Recherche du bloc d'autorisation
- Calcul
- Contrôle de la validité du bloc
- Traitement inhérent au type du bloc pour ouverture des droits

Il s'en suit que l'ordre, dans lequel les différentes erreurs peuvent survenir, est modifié également.

Lors de l'exécution d'une demande de calcul en mode télé-valorisation, il n'y a pas accès au service, la combinaison K n'étant pas calculée à la suite de l'ouverture de droits.



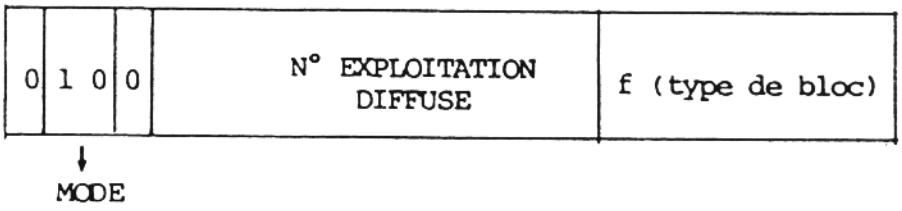
	P.C.	DESSIN NO:	FOLIO	REV.
Bull	A	76 171 589	38	A

IMPRIME Nº 740 C 102

3.1.4 Mode = 10 : Présentation de clé

Le troisième mode de paramétrage de la "demande de calcul" ne s'adresse qu'au bloc émetteur qui permet d'en contrôler l'exploitation dans les buts suivants :

- présentation de clé d'écriture,
- identification du porteur.



Le contenu du 3ème octet des paramètres est fonction du type du bloc émetteur. Ce contenu est identique à celui pris par chacun des blocs en mode calcul de combinaison d'accès.

soit : pour abonnement X X X X X X X X

pour session libre 0 0 0 0 DU

pour session contrôlée X X X X X X X X

pour consommation X X X X NU

Le résultat de calcul sera obtenu lorsque le traitement particulier au type du bloc émetteur aura été réalisé sans incident.

On remarque ainsi que le cas de bloc émetteur de type consommation permet par la présence de sa zone de consommation et sa mise en service progressive de contrôler les tentatives d'accès faites dans ce mode, l'on reconstitue par ce biais une pseudo zone de contrôle.
On notera d'ailleurs que pour renforcer la sécurité, une consommation nulle est alors interdite.

3.1.4.1 Présentation d'une clé d'écriture

Ce cas d'utilisation correspond au besoin de protéger les écritures des diverses clés associées aux services qui sont enregistrés au cours de la personnalisation de la carte et uniquement lors de cette opération soit lorsque ILU = 0.

Pour être utilisé en tant que clé d'écriture le résultat de calcul doit satisfaire la règle de cohérence habituelle K7, K6, K5, K4 = K3, K2, K1, K0.

3.1.4.2 Identification du porteur (ON-LINE)

Cette opération pourra être effectuée lorsque la phase de vie de la carte correspond à la phase d'exploitation marquée par la présence de ILU.

Dans ce cas d'utilisation le champ des 8 octets de données du message d'entrée subit un traitement particulier en 2 étapes.

- au niveau du terminal

Le champ de données émis par le diffuseur est partagé en 2 champs égaux.

CH 1 diffusé	CH 2 diffusé

Le champ 2 est modifié par le code client (CCE) saisi au clavier du terminal par application d'un OU exclusif.

Le message d'entrée ainsi modifié est transmis à la carte à la suite des champs de référence et paramètres.

CH 1 diffusé	CH 2 diffusé ⊕ CCE

- au niveau carte

La carte effectue une opération similaire mais cette fois avec le code client interne, en service (CCI = CC1 ou CC2).

De manière à obtenir avant calcul le champ de données ci-dessous.

CH 1 diffusé	CH 2 diffusé ⊕ CCE ⊕ CCI

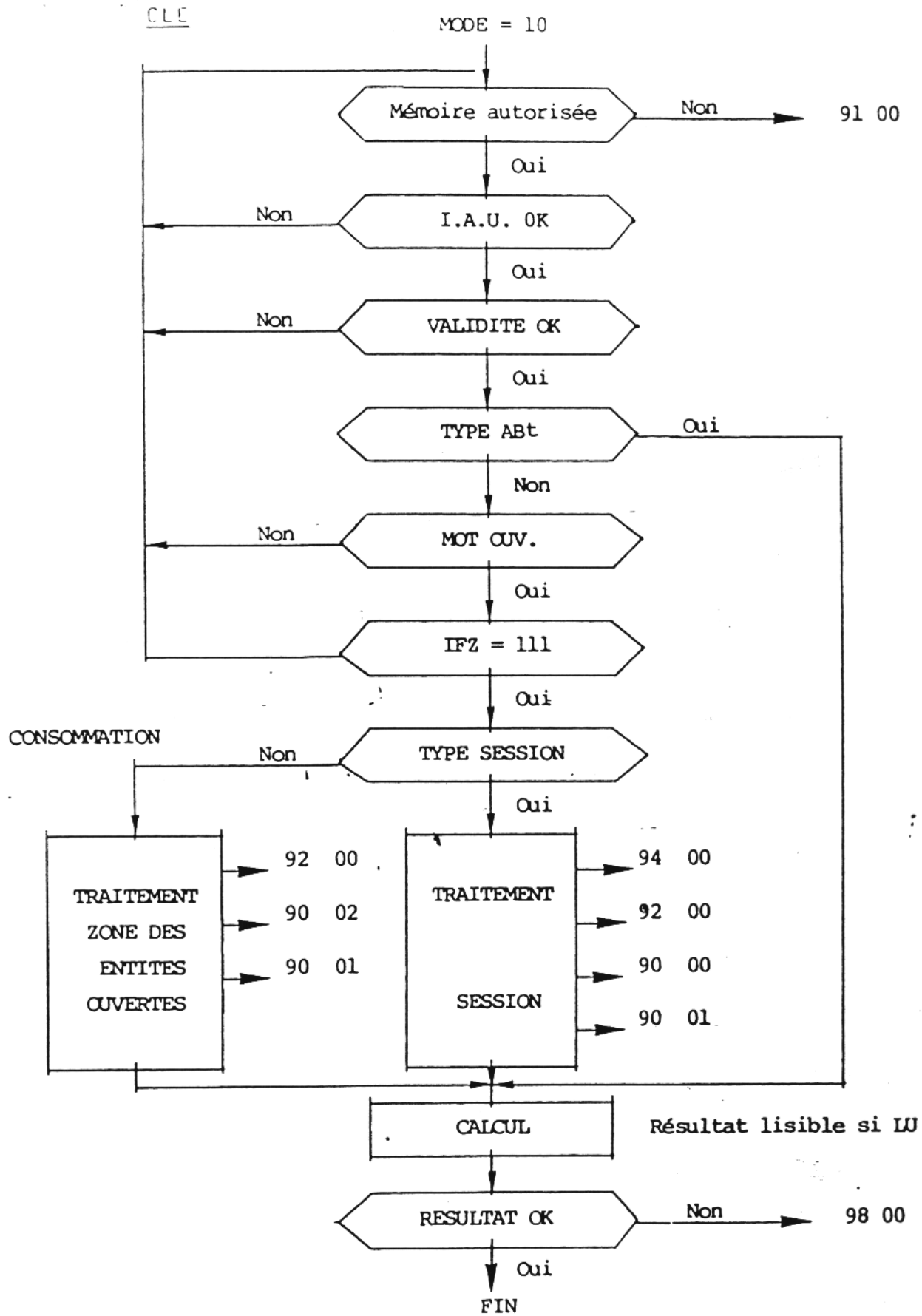
Si donc CCI = CCE, participe au calcul le message initialement diffusé. Le résultat de calcul est celui attendu par l'émetteur. Dans le cas contraire le code client sera reconnu faux, l'émetteur pourra répeter l'opération ou abondonner la sesssion en cours.

On notera que si le contrôle du code client est effectué au central, ce code n'est toutefois pas connu de celui-ci.

L'organigramme qui suit est tout à fait comparable à celui relatif au mode 00 à l'exception faite de l'espace mémoire autorisé qui est ici réduit à la ZENP.

IMPORTANT

L'autorisation d'écrire devra être gérée comme en mode 00 en fonction du type du bloc émetteur.



3.1.5 Mode = 11 : Télé-écriture

Le quatrième et dernier mode de paramétrage de la "demande de calcul" ne s'adresse également qu'au bloc émetteur qui permettra de déchiffrer le champ des 8 octets de données chiffrées émises par l'émetteur. L'opération se déroule comme suit :

0	1	1	0	N° EXPLOITATION DIFFUSE	f (type de bloc)

MODE

Le champ des paramètres et les traitements relatifs au code client d'une part et au type de bloc d'autre part sont identiques à ceux réalisés pour le MODE 10.

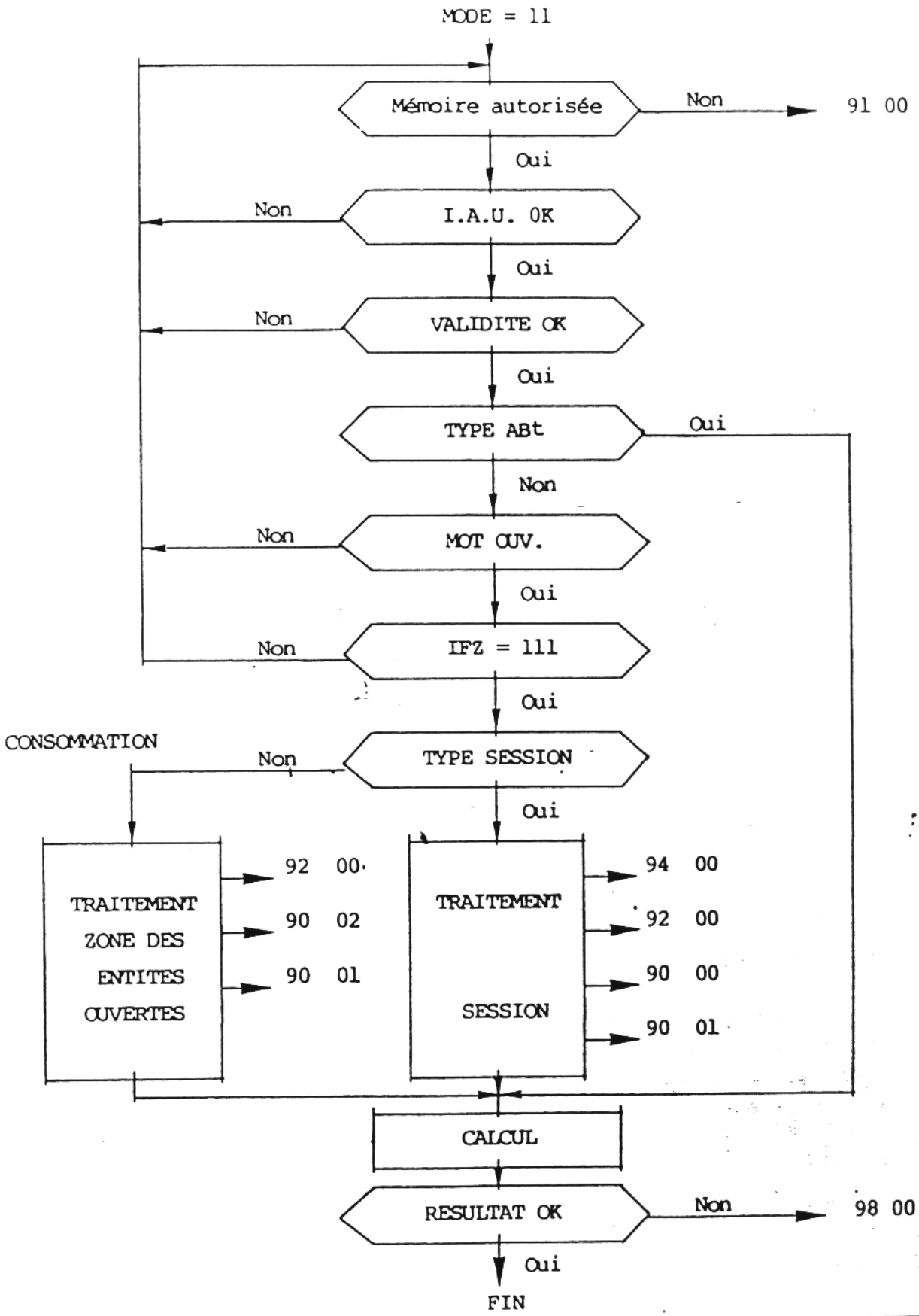
Le résultat de calcul est partagé par la carte en 3 champs. Les 2 premiers champs de 16 cb chacun doivent avoir des contenus égaux (règle de cohérence pour ce mode). Si c'est le cas, ce contenu constitue l'adresse d'un mot dans lequel seront enregistrées les données contenues dans le 3ème champ (32 cb) du résultat.

La télé-écriture permet d'écrire ou de modifier le contenu de tout mot non validé, elle permet aussi à l'émetteur de modifier un mot validé dont la configuration des bits systèmes est 0 1 1 1 mais dans ce cas la modification des bits S et B est interdite.

Comme pour chacun des 3 modes précédents, l'organigramme qui suit met en évidence les différentes phases du traitement du bloc d'autorisation utilisé (émetteur ici) et les indicents qui peuvent survenir en cours de traitement par ordre de priorité.

IMPRIME N° 740 C 102

TELE-ECRITURE



	P.C.	DESSIN NO:	FOLIO	REV
Bull	A	76 171 589	44	A

IMPRIME N° 740 C 102

DEMANDE DE CALCUL

MODE	BLOC ADRESSE	CLE UTILISEE POUR LE CALCUL	CONDITIONS D'UTILISATION	LECTURE DU RESULTAT AUTORISE	OBSERVATIONS
00	bloc qcq	Clé du bloc adressé		Oui	
01	bloc qcq	Clé émetteur		Non	- pour ouvrir une session controlée - pour ouvrir des EV à la consommation
10	bloc émetteur	Clé émetteur	$\overline{LU}$	Non	- pour validation d'écriture (mot secret)
		Clé émetteur + CC	LU	Oui	- Contrôle du CC ON LINE - Ecriture protégée interdite
11	bloc émetteur	Clé émetteur	$\overline{LU}$	Non	- télé-écriture carte mère
		Clé émetteur + CC	LU	Non	- télé-écriture carte fille obligatoire pour mots secrets

3.2 Calcul de certificat (80).

Nous avons vu précédemment l'ordre "demande de calcul" et ses divers modes de paramètrage qui permettent de gérer les services spécifiques à cette carte. D'autres services peuvent être créés qui ne répondent pas aux critères qu'exigent les précédents. Le calcul de certificat est dans ce cas nécessaire afin de sécuriser les services qui seront alors exploités à l'aide des ordres standards.

3.2.1 Phase initialisation:

Les paramètres A1-A2 donnent l'adresse du mot à certifier.

L = 8 obligatoirement.

3.2.2 Phase active : exécution de l'ordre

Les paramètres A1-A2 (adresse) sont chargés dans les 2 octets de poids forts du champ de 8 octets de données. Le calcul de certificat répond à l'équation suivante :

$$C = f(E, S, PI)$$

dans laquelle

- C est le résultat sur 64 cb,
- E le champ des données et d'adresse de PI,
- PI un paramètre interne du format d'un mot dont l'adresse est communiquée par A1-A2.
- S la clé secrète d'une en-tête de bloc tel que défini au chapitre I, qu'il s'agisse d'une carte fille ou d'une carte mère.
  Seule restriction, cette clé secrète ne peut appartenir à la ZENP (réservée à la clé émetteur).

NOTA : Cet ordre nécessite impérativement d'être précédé d'une recherche sur argument. Cet argument doit être caractéristique du début de bloc dont on veut exploiter la clé pour certifier.

Par ailleurs, le type de bloc n'a aucune importance, le contenu du mot paramètre n'étant pas exploité dans ce cas.

Après tout ordre différent de calcul de certificat ou lecture du résultat, une nouvelle recherche sur argument est nécessaire.

3 - CALCUL INVERSE (88)

C'est par cet ordre qui leur est strictement réservé que les cartes mères permettent à un émetteur ou prestataire de services de contrôler et gérer avec une sécurité maximale les services offerts.

D'une manière générale, cette fonction est "inverse" par rapport à celle utilisée, pour un ordre donné, dans la carte "utilisateur".

L'ordre "demande de calcul" que nous avons vu précédemment, quel que soit son mode de paramètrage exploite la fonction déchiffrement pour calculer :

- Une combinaison d'accès
- Les paramètres de télé-valorisation
- Une clé d'écriture
- l'adresse et le contenu du mot à télé-écrire

Dans ce cas, il est nécessaire que la carte mère permette de chiffrer le champ de données qui sera exploité par les cartes "utilisateur".

Par contre, lors d'un "calcul de certificat" le résultat fourni par une carte "utilisateur" constitue un chiffrement des données d'entrée. Dans ce second cas, la carte mère n'intervient que pour effectuer le contrôle du résultat, pour cela 2 solutions sont possibles :

- Comparaison : La carte mère exécute le même calcul et le contrôle sera effectué par une simple comparaison des 2 résultats.
- Calcul inverse : comme dans le premier cas on utilise le calcul inverse mais cette fois pour déchiffrer.

On notera que lorsque l'exploitation du système exige un chiffrement et un déchiffrement ils sont toujours effectués dans cet ordre et c'est donc toujours la carte chiffre qui effectue le premier calcul.

3.1 Phase initialisation de l'ordre

- Les paramètres A1-A2 donnent l'adresse de la clé à utiliser. Cette adresse ne peut être relative qu'à un mot de la zone porte-clés (ZENP)
- L = 12 (déc.) obligatoirement.

IMPRIME N° 740 C 102

3.2 Phase active : exécution de l'ordre

La carte reçoit les 12 octets de données constitués d'un premier champ E de 8 octets contenant les données à chiffrer ou à déchiffrer selon le cas et d'un second champ P de 4 octets contenant les paramètres de calcul.

3.3 Structure des blocs de contrôle

Les clés secrêtes qui donc ont pour rôle de contrôler le système d'exploitation, peuvent être chargées dans la zone parte-clés de la carte mère selon des critères propres à chaque émetteur. Cependant pour harmoniser les systèmes qui environnent et exploitent ces cartes mères, nous préconisons de donner au bloc de contrôle la structure suivante :

V S B

0 1 0	X D I	X X	IDENTIFICATEUR D'AUTORISATION	IND.
0 0				
0 0			CLE SECRETE	
0 0				
0 0				

Avec :

- Identificateur d'autorisation : identificateur d'autorisation du service.

- IND : indice de la clé du service. Cet indice permet à l'émetteur de changer la clé du service par application des critères qui lui sont propres et de poursuivre l'exploitation des cartes dans lesquelles ce service a été chargé avant qu'intervienne ce changement.

- I : Cet indicateur a pour vocation d'indiquer à quel type de calcul cette clé est dévolue. Calcul inverse ou direct.

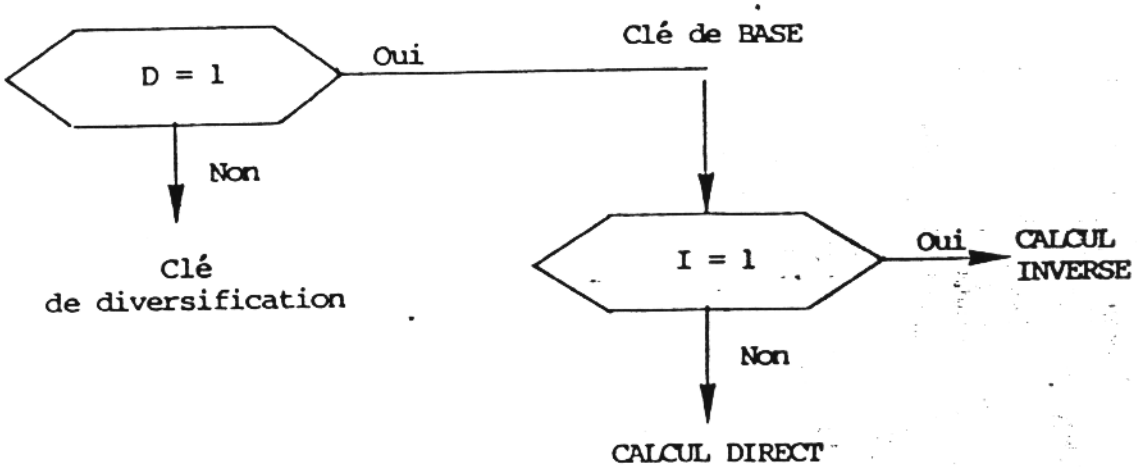
I = 0 : Clé "directe" signifie que la clé est exploitable de manière identique à la clé correspondante des cartes filles "utilisateur" par exemple pour vérifier un certificat par la éthode de comparaison.

I = 1 : Clé "inverse" signifie que cette clé est exploitable en complémentarité de la clé correspondante des cartes "utilisateur" qui sont supposées toujours posséder des clés directes.
Par exemple, dans le cas de contrôle de certificat utilisant le calcul inverse. Cette clé permet de déchiffrer un certificat qui est en fait un chiffrement réalisé par la carte "utilisateur".

- D : Indicateur de diversification.

D = 1 : Clé non diversifiée.
Certains services exigent que la clé associée soit identique dans toutes les cartes "utilisateur". C'est le cas de la télé-diffusion à laquelle l'ensemble des porteurs doit pouvoir accéder en même temps.

D = 0 : clé diversifiée.
D'autres services et particulièrement le bloc émetteur exigent pour obtenir une sécurité accrue d'utiliser une clé diversifiée (différente pour chacune des cartes usager). Dans ce cas, la clé est celle qui permet à la carte mère, de calculer le paramètre de diversification de la clé de base contenue dans le bloc de contrôle ayant le même identificateur mais avec toutefois l'indicateur D = 1.
L'analyse des indicateurs D et I pour un identificateur donné peut se faire comme suit :



3.4 Mise en oeuvre des fonctions directe et inverse

Principes :

- Chaque clé secrete "Vidéopass" est décomposée en 16 clés élémentaires d'un octet.

- De même chaque paramètre est décomposé en 4 paramètres élémentaires d'un octet.

- Chaque chiffrement ou déchiffrement est le résultat R (64 bits) d'un calcul Vidéopass appliqué sur une donnée d'entrée E mettant en oeuvre une clé secrete S et un paramètre P. Ce paramètre selon le cas peut être interne ou externe à la carte.

$$R = f(E, S, P)$$

$$\text{ou } R = f^{-1}(E, S, P)$$

- La fonction f^{-1} est obtenue en associant à la fonction f une clé secrete S et un paramètre P dont l'ordre des éléments qui les composent, est inverse à celui utilisé pour la fonction directe.
La notation f^{-1} implique donc que la clé et le paramètre utilisés soient ainsi constitués.

- Chaque résultat fourni par une fonction directe ou inverse devra voir ses 2 demis champs RH et RL croisés pour fournir le champ d'entrée à la fonction inverse (de contrôle).

  La figure ci-après met en lumière tous les principes évoqués précédemment.
  Considérons que ce qui est contenu dans le cercle représente la fonction contenue dans la carte "utilisateur" (rappelons que f peut aussi bien représenter selon le cas la fonction chiffrement que la fonction déchiffrement et f-1 son inverse).
  Considérons par ailleurs les 4 points particuliers marqués 1 à 4 d'un cycle complet de calcul et contrôle (excepté le contrôle par comparaison). Nous avons alors la possibilité d'évoquer toutes les fonctions demandées à la carte.

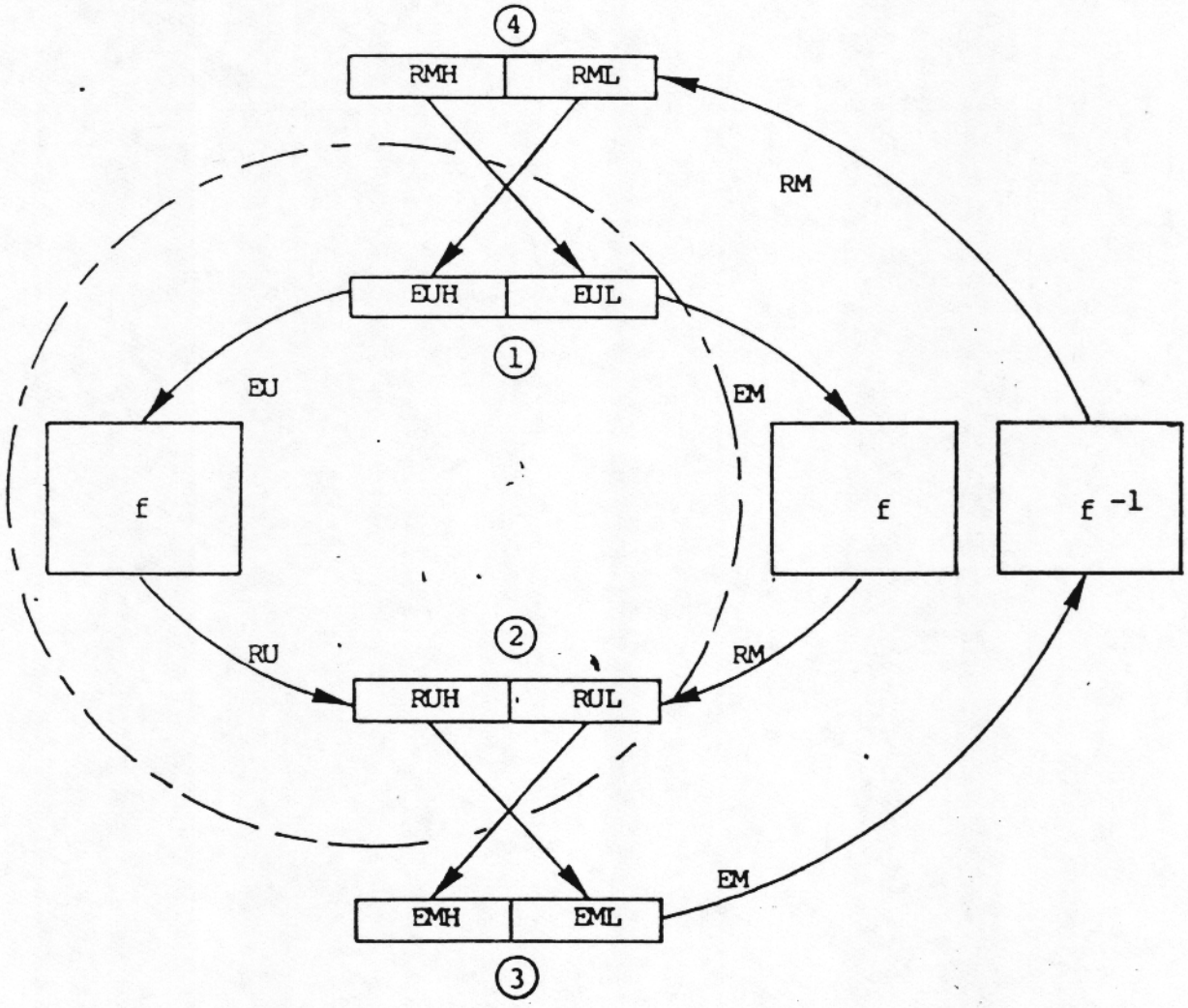
- Quel que soit la finalité d'un résultat de calcul (combinaison d'accés, paramètres de télé-valorisation, adresse et données de télé-écriture) ce résultat est prédeterminé par le système de contrôle.

- Le cycle démarrera en (2) on passera en (3) puis en (4) pour fournir l'entrée 1 chiffrée, à la carte "utilisateur" qui déchiffrera pour exploiter la combinaison (2) de départ.

IMPRIME N° 740 C 102

- Contrôle de certificat

Cette fois le cycle demarrera en (1) le champ E étant constitué d'un nombre aléatoire et d'une adresse, puis on bouclera la boucle pour revenir en (1) et effectuer le contrôle.



IMPRIME Nº 740 C 102

4 - COMPTE RENDU D'EXECUTION DES DIVERS ORDRES

4.1 Erreurs "Protocole" ME1 = 6X

Pour signaler une erreur protocole détectée par la carte lors de la reception des octets de la phase initialisation de l'ordre

- 6F : Erreur protocole sans précision
- 6E : Erreur sur le code classe d'instruction (CLA)
- ED : Erreur sur l'ordre
- 67 : Erreur sur la longueur.

4.2 Erreurs d'exécution

Fin d'exécution de l'ordre ME1 = 9X.

ME1	1	0	0	1	CF	ERM	DAO	AA

Lorsque X = 0 l'exécution de l'ordre s'est déroulée sans indicent.

Si X est différent de 0 une anomalie a été rencontrée en cours d'exécution.

CF : - La clé d'écriture calculée ou non à l'aide dela clé secrete du bloc émetteur a été reconnue fausse lors de la validation d'un mot secret par écriture directe ou lors d'une télé-écriture.

- Non vraissemblance ou cohérence des paramètres obtenus après exécution d'une demande de calcul en mode télé-valorisation d'une session ou d'une zone de validation.

ERM : Erreur mode. Le mode choisi pour accéder à un service n'est pas conforme avec le type de bloc relatif au service.

- Autorisation d'enregistrement (I.A.E. = 1) d'une session en mode libre alors que le bloc nécessite un mode contrôlé ou vis-versa.

- Tentative de télé-valorisation d'un bloc de type abonnement.

D.A.O. : Demande d'Autorisation d'Ouverture (autorisation donnée à la carte d'utiliser VPP).

a) Il n'y avait pas I.A.E. sur l'ordre exécuté

- Pour enregistrer une session libre ou contrôlée.

- Pour ouvrir des entités en ZV.

- Pour consommer en Zone de consommation.

- Pour écrire IFZ.

b) Il y avait I.A.E. lors de l'exécution de l'ordre

- L'autorisation d'écrire a été utilisée pour écrire IFZ (voir cas d'écriture de IFZ § 5).
  Dans ce cas la carte effectue une nouvelle demande d'autorisation d'ouverture pour accéder à un éventuel autre bloc d'autorisation identique.

AA : Peut prendre 2 significations distinctes :

a) Bloc d'autorisation absent :

- Cet indicateur est positionné si, après recherche dans l'espace mémoire autorisé pour l'accès considéré, aucun bloc n'a pus remplir totalement les conditions d'accès suivantes :

  . Identificateur d'autorisation *

  . Période de validité

IMPRIME N° 740 C 102

. Structure de l'entité de bloc
(6 mots consécutifs validés)

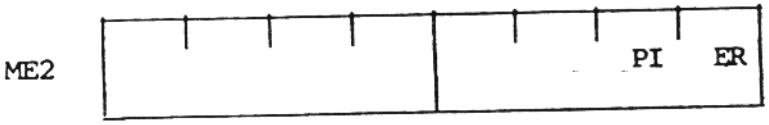
. Présence du demi-mot d'ouverture
pour les blocs de type autre
qu'abonnement

. Le demi-mot d'ouverture est présent
mais IFZ = 111

b) Argument absent

Lors d'une recherche sur argument le profil recherché (4 octets) n'a pas été rencontré.

ME2 n'est significatif que si ME1 = 90



PI : Place Insuffisante :

Cet indicateur ne concerne que les blocs de type consommation.

Il est positionné sur les évènements suivants :

- Tentative de consommation (même nulle) alors qu'aucune entité n'a été ouverte dans ZV (pas de droits).
- Place insuffisante parmi les entités ouvertes pour satisfaire l'accès alors que toutes les entités valorisables (NEV) n'ont pas été ouvertes.
- Place insuffisante en ZV pour satisfaire la demande d'ouverture d'entités demandée en trop grand nombre par rapport à celui des entités valorisables restant à ouvrir.

ER : Erreur déclarée par la carte à la suite de laquelle elle devient muette. Cet indicateur est positionné dans les cas suivants :

- Echec en écriture.(défaut mémoire ou VPP défaillant).
- Tentative d'écriture sur un mot déjà validé.

* Le numéro d'ordre est associé à l'identificateur d'autorisation en cas de télé-valorisation (mode = 00).

IMPRIME N° 740 C 102

5 - CAS D'ENREGISTREMENT DE IFZ (indicateur fin de zone)

Cet indicateur n'est utilisé que par les blocs d'autorisation auquels est associée une zone incriptible.

5.1 IFZ dans le cas de blocs de Type Session

Pour les blocs de type session le positionnement de l'indicateur IFZ survient :

- Lorsque l'ouverture d'une session, libre ou contrôlée, s'avère nécessaire et que toute la zone inscriptible associée au bloc est consommée.
- Lorsque l'enregistrement d'une nouvelle session engendre un dépassement de VMAX.
- Lorsque la structure d'un début de session ne présente pas la configuration requise 0110 et que le bit B ou le bit E (pseudo bit V) est à zéro. Ces cas correspondent à un débordement de zone.
- Ou lorsque la durée à enregistrer au cours d'une ouverture de session est plus grande que la période de validité résiduelle.

5.2 IFZ dans le cas de blocs de type consommation

Pour ce type de bloc IFZ est positionné :

- Lorsque la place, en zone de consommation, est insuffisante pour satisfaire la demande alors que toutes les entités valorisables sont en service.
- Lorsqu'un début de mot de la zone de consommation ouverte présente une configuration de ses bits "systèmes" différente de X 1 1 X.
- Lorsque la zone de consommation déborde de la zone porte-clés.

NOTA : Après avoir enregistré IFZ, la carte positionne à nouveau l'indicateur DAO (ME 1). Ceci permet à la carte de chaîner sur un éventuel autre bloc d'autorisation identique à l'occasion d'un nouvel accès.

IMPRIME Nº 740 C 102