Bull CP8

Manuel d'utilisation
Systèmes d'exploitation
Famille SCOT - Cartes

Bull CP8
68, route de Versailles
BP 45
78430 LOUVECIENNES
FRANCE
Tél : 33 (1) 39 02 44 00
Fax : 33 (1) 39 02 44 02

Novembre 1991

Référence : TU 0208 F01

© Bull CP8 1991
Reproduction interdite

VOS REMARQUES SUR CE DOCUMENT / TECHNICAL PUBLICATIONS REMARKS FORM

TITRE / *TITLE*

Manuel d'Utilisation Famille SCOT - Cartes

N° REFERENCE / *REFERENCE No.:*

TU 0208 F01

DATE / *DATED*

Novembre 1991

ERREURS DETECTEES / *ERRORS IN PUBLICATION*

AMELIORATIONS SUGGEREES / *SUGGESTIONS FOR IMPROVMENT TO PUBLICATION*

▶ Vos remarques et suggestions sont attentivement examinées. Merci de les communiquer à Bull CP8.

▶ *Your comments are promptly investigated by qualified technical personnel and action is taken as required. Thank you for your sending to Bull CP8.*

DATE :.....

NOM / *NAME:*.....
SOCIETE / *COMPANY:*.....
ADRESSE / *ADDRESS:*.....

■ Envoyer ce document à :

■ *Send this sheet to:*

Bull CP8
Service Documentation Technique
68 route de Versailles
BP 45
78430 LOUVECIENNES FRANCE

AVANT-PROPOS

Ce manuel décrit l'utilisation des systèmes d'exploitation de la famille de cartes SCOT ; il est destiné aux concepteurs d'applications basées sur ces cartes.

Le chapitre 8 est réservé aux réalisateurs de la personnalisation des cartes.

La lecture du premier chapitre donne une vue d'ensemble du manuel et introduit à la lecture des autres chapitres. On y trouve en particulier un glossaire des termes spécifiques à la technologie des systèmes d'exploitation des cartes SCOT.

Les ordres exécutés par les systèmes d'exploitation sont décrits en détail dans le chapitre "JEU D'ORDRES". Cependant chaque système d'exploitation présente des spécificités pour certaines caractéristiques de ces ordres qui sont signalées.

Pour chaque modèle de la famille SCOT, une fiche cartonnée et mobile caractéristique est placée à la fin du manuel et peut être utilisée comme marque page en même temps qu'elle complète le texte.

En annexes, les ordres sont récapitulés sous forme de tables avec leurs caractéristiques :

- les performances,
- les cas d'erreur : mots d'état et mutisme,
- leur disponibilité en fonction des protections,
- les octets d'acquittement,

ainsi que l'accessibilité des différentes zones en fonction des protections.

A la fin de ce manuel figurent enfin des index permettant de retrouver facilement une information.

En début de manuel, le lecteur trouve une fiche de remarques qu'il peut compléter le cas échéant afin de la renvoyer à BULL CP8 pour collaborer à l'amélioration de la rédaction des Manuels Clients.

AVERTISSEMENT AU LECTEUR

Bull CP8, dans un souci constant d'améliorer ses produits, a fait évoluer en toute compatibilité les cartes de la famille SCOT, en y apportant des fonctions supplémentaires.

Les cartes SCOT 20 DES, SCOT 60 DES et SCOT 110 DES incorporent, comme leur nom l'indique, l'algorithme cryptographique D.E.S.. Ces cartes supportent toutes, deux zones de travail et certaines, des fonctions cryptographiques évoluées.

Note au personnalisateur de cartes

Attention, les restrictions suivantes sont imposées pour toutes les cartes SCOT TELEPASS et DES décrites dans ce manuel :

- *la clé émetteur 1A et la clé émetteur 1B ont une longueur fixe de deux mots (8 octets).*
- *le code porteur 2A (lorsqu'il existe) a une longueur limitée à un ou deux mots (4 ou 8 octets).*
- *le paramètre longueur dans l'ordre d'écriture des verrous a une longueur fixe égale à 2 octets.*
- *pour les cartes SCOT 50, la zone de lecture est obligatoire et doit comporter au moins un mot.*

SOMMAIRE

1	**GENERALITES**	**1**
1.1	Présentation du manuel	1
1.2	Présentation de la carte à microcalculateur	3
1.3	Définitions préalables	6
1.4	Liste des ordres exécutables	12
2	**FAMILLE SCOT**	**15**
2.1	Présentation de la famille SCOT	15
2.2	Description de la mémoire	18
2.3	Structure d'un mot	21
2.4	Partition de la mémoire	23
2.5	Phases de vie	27
3	**ACCES A LA CARTE**	**35**
3.1	Modes d'accès à la mémoire	35
3.2	Principe de lecture	37
3.3	Principe d'écriture	40
3.4	Principe d'effacement	44
4	**SECURITE DE LA CARTE**	**47**
4.1	Procédures de sécurité	47
4.2	Ressources cryptographiques	49
4.3	Gestion des clés, des codes et du jeu secret	52
4.4	Présentation de code ou de clé en clair	55
4.5	Presentation de clé chiffrée	56
4.6	Certification et authentification carte	57
4.7	Présentation de la zone d'accès	61
4.8	Gestion de la zone d'accès	64
5	**DIALOGUE CARTE - CAD**	**73**
5.1	Introduction	73
5.2	Déroulement d'un ordre	76
5.3	Eléments d'un ordre	78
5.4	Remise à zéro	82
5.5	Identification d'une carte	86

6	**JEU D'ORDRES**		**87**
6.1	Introduction		87
6.2	Lecture	: INS = B0h	89
6.3	Ecriture	: INS = D0h	92
6.4	Recherche d'un mot sur argument	: INS = A0h	96
6.5	Recherche du premier mot vierge	: INS = A0h	99
6.6	Recherche du premier mot non vierge	: INS = A8h	101
6.7	Lecture de résultat	: INS = C0h	103
6.8	Ecriture des verrous	: INS = 50h	108
6.9	Effacement de domaine	: INS = 0Eh	111
6.10	Demande de nombre aléatoire	: INS = C4h	114
6.11	Présentation en clair de clé ou code	: INS = 20h, 10h ou 30h	116
6.12	Présentation chiffrée de clé	: INS = 28h, 18h ou 38h	119
6.13	Validation de clé ou code en lecture	: INS = 40h	121
6.14	Validation en écriture	: INS = 70h	123
6.15	Calcul de certificat	: INS = 80h	125
6.16	Changement de code porteur	: INS = D2h	127
7	**OPERATIONS**		**129**
7.1	Lecture protégée		129
7.2	Ecriture protégée		131
7.3	Effacement		133
7.4	Déblocage d'une carte		135
7.5	Changement de code porteur		137
7.6	Recherche de mot		141
7.7	Identification de la carte		143
7.8	Certification		145
8	**PERSONNALISATION CARTE**		**147**
8.1	Introduction		147
8.2	Procédure de personnalisation des cartes		149
8.3	Calcul de clé de fabrication		151
8.4	Ecriture des pointeurs et calcul de CCR		154
8.5	Mise en place de la zone secrète et de la zone d'accès		156
8.6	Personnalisation des zones		162
ANNEXES			**164**
Annexe A -	Performances		164
Annexe B -	Mots d'état des systèmes d'exploitation de la famille SCOT		168
Annexe C -	Disponibilité des ordres en fonction des indicateurs		177
Annexe D -	Accessibilité des zones en fonction des protections		179
Annexe E -	Liste récapitulative des ordres		182
INDEX			
TABLE DES FIGURES			

- 1 -

GENERALITES

1 GENERALITES

1.1 Présentation du manuel

Ce manuel adopte certaines règles d'écriture décrites dans cette section.
Les mots ou expressions importants à repérer sont réunis dans un index alphabétique situé en fin de manuel.
Les figures, identifiées par des légendes, contiennent des schémas ou des exemples qui font l'objet d'une indexation séparée.

CONVENTION	SIGNIFICATION
::	Ce signe introduit une signification ou un ensemble de significations.
{ }	Ces signes encadrent un paramètre optionnel ou au choix.
MAJUSCULE	Les caractères ou mots imprimés en majuscules dans le texte ou dans les figures sont des intitulés propres à la famille SCOT.
minuscule	Les caractères ou mots minuscules, utilisés en dehors du texte, représentent une variable (indice ou paramètre) pouvant prendre plusieurs valeurs.
"chaîne"h	La lettre minuscule 'h' à la fin d'une chaîne, composée de caractères alphanumériques (lettres majuscules de A à F et/ou chiffres de 0 à 9), indique que cette chaîne est une valeur ou une adresse exprimée en base 16 (hexadécimale).
[LIBELLE]	Un libellé entre crochet signifie "contenu du mot pointé par l'adresse désignée par le libellé".
ETIQUETTE ::	{bit} {quartet} {mot} {adresse} une étiquette peut désigner une de ces 4 entités.
'P1P2'	Adresse telle que P1 = poids forts et P2 = poids faibles.

CONVENTION	SIGNIFICATION
[xx, yy]	Indication d'un intervalle bornes incluses. La disposition des crochets dans l'autre sens indique bornes exclues.

Exemple	Signification
LP	Bit LP, bit de la zone de fabrication.
TELEPASS	Fonction de calcul logico-mathématique.
V	Etiquette désignant le bit V, bit de validation.
EPi	Etiquette désignant le bit EPi (i = 1 ou 2).
AD2	Etiquette désignant l'adresse AD2, adresse du code porteur.
G(x) = $x^5 + x^2 + 1$	x est une variable.
BCh	Valeur hexadécimale BC.
[ADR]	Contenu du mot pointé par l'adresse ADR.
'P1P2' = 1050h	Adresse telle que P1 = 10h et P2 = 50h.
[200h, ADM[	Intervalle 200h inclus à ADM exclu.

Figure 1.1 - Exemples d'utilisation des conventions d'écriture.

1.2 Présentation de la carte à microcalculateur

La carte à microcalculateur est un système sécuritaire gestionnaire d'informations. Le microcalculateur contient en effet un programme appelé "Système d'exploitation" et une mémoire stockant des informations ; il peut aussi recevoir de l'extérieur ou émettre vers l'extérieur des données.
La carte est en fonctionnement uniquement lorsqu'elle est introduite dans un appareil, désigné dans ce manuel par le terme générique "CAD", qui communique avec elle.

Aspect physique de la carte

Une carte à microcalculateur, supportant les systèmes d'exploitation de la famille SCOT, a le format classique d'une carte de crédit, mais diffère dans sa composition :

- un support plastique aux normes ISO (norme 7816/1),
- un circuit imprimé jouant le rôle de connecteur,
- un microcalculateur constitué d'un composant monolithique et autoprogrammable.

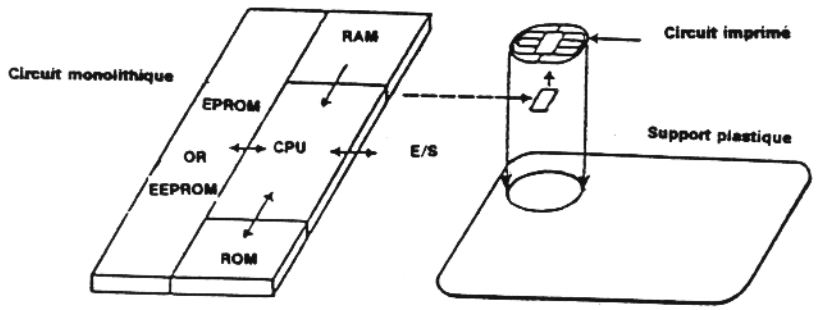

Figure 1.2 - Aspect physique de la carte

Remarque :

Le verso de la carte supporte parfois des pistes magnétiques dont l'utilisation est totalement indépendante de celle du microcalculateur.

Architecture

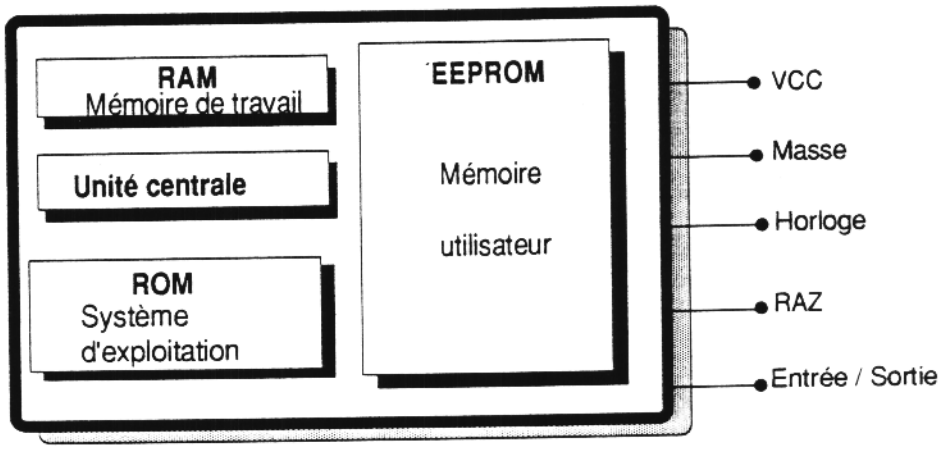

Figure 1.3 - Architecture du circuit monolithique.

Unité centrale
Unité de calcul arithmétique et logique contrôlant les échanges avec l'extérieur (Fréquence 3,57 Mhz pour 9600 bauds).

Mémoire de travail
Mémoire rapide, utilisée exclusivement par le système d'exploitation. Dès la mise hors tension, cette mémoire est effacée (mémoire RAM).

Système d'exploitation
Le système d'exploitation est inscrit dans une mémoire non modifiable (mémoire ROM).

Mémoire utilisateur
Cette mémoire contient les données. La mise hors tension n'efface aucune information (mémoire EEPROM ou EPROM). Dans la suite du manuel le mot "mémoire" désigne cette mémoire.

Connections vers l'extérieur

5 points de connexion (6 en technologie EPROM)

VCC	: tension élémentaire
Masse	: contact de masse
Horloge	: base de temps
RAZ	: initialisation
Entrée/Sortie	: échange des données
VPP	: tension de programmation (réservée technologie EPROM)

Remarque :

Les termes RAM, ROM, EEPROM, EPROM sont définis dans la section suivante.

Vie de la carte

La carte est fabriquée puis personnalisée puis utilisée : elle suit des étapes chronologiques, dites phases de vie, pour chacune de ces étapes un type d'acteur intervient.

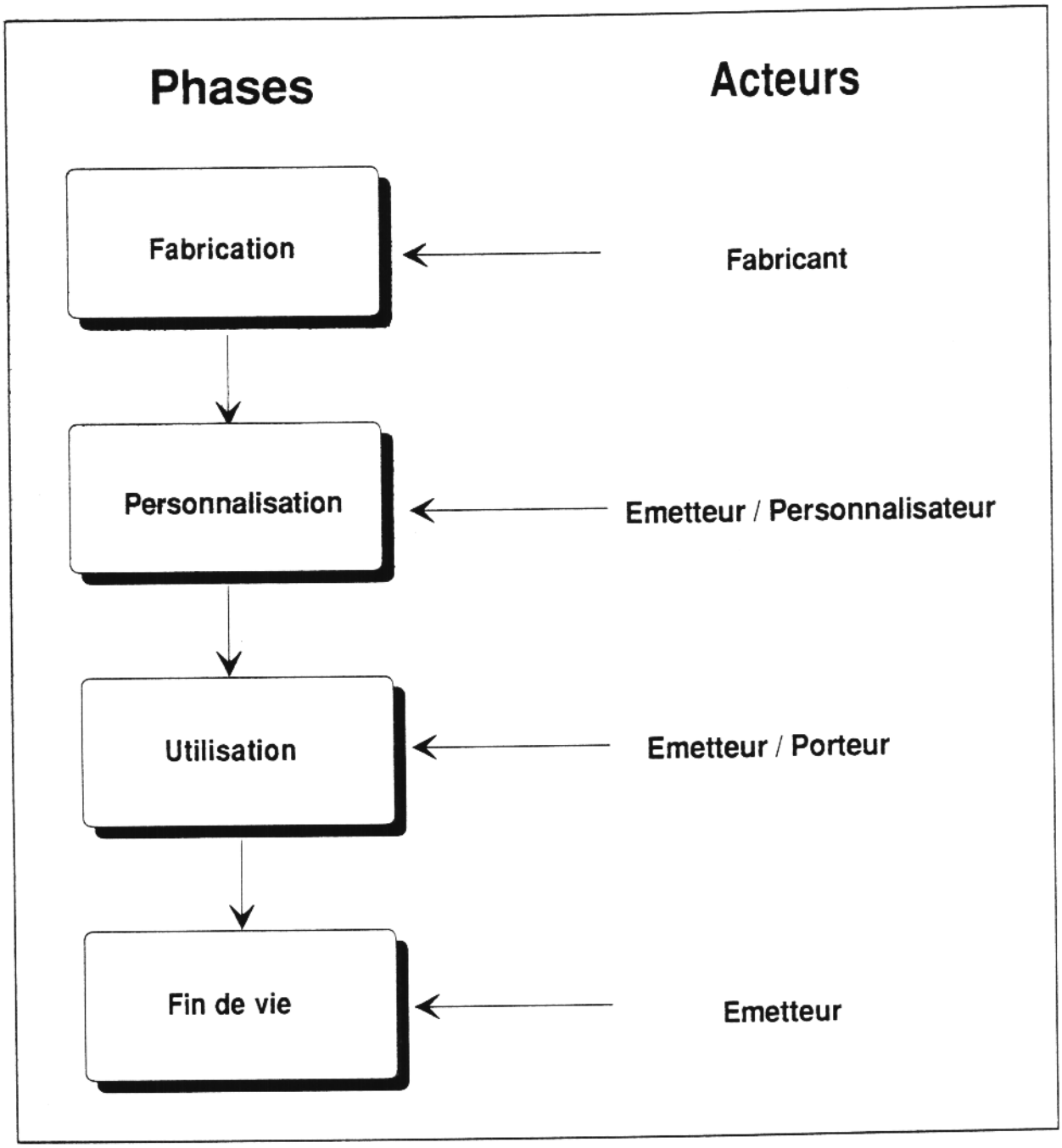

Figure 1.4 - Phases de vie de la carte.

1.3 Définitions préalables

Cette section rappelle les définitions de termes ou expressions utilisés dans ce manuel. Ils ne sont pas classés par ordre alphabétique mais en progressant du terme le plus général au terme le plus particulier. Dans le texte des définitions, les termes mis en valeur en gras sont eux-mêmes l'objet d'une définition dans cette section.

Définitions

Mémoire RAM

Mémoire vive à accès rapide. Utilisée comme mémoire de travail rapide, elle peut être lue, écrite et effacée à tout moment par le microcalculateur. Elle ne conserve pas l'information après la mise hors tension.

Mémoire ROM

Mémoire non volatile accessible uniquement en lecture.

Dans le cadre des cartes de la famille SCOT, cette mémoire contient le **système d'exploitation**.

Mémoire EEPROM ou EPROM

Mémoire non volatile, accessible en lecture et écriture, modifiable par le microcalculateur. Elle conserve l'information après la mise hors tension.

La spécificité de la mémoire EPROM est qu'elle ne peut être écrite qu'une seule fois.

Dans le cadre des cartes de la famille SCOT, cette mémoire est dédiée à la mémoire utilisateur.

Système d'exploitation (Masque)

Programme constituant l'intelligence de la carte. Il est inscrit en mémoire **ROM**, il est ineffaçable et inaccessible de l'extérieur. Ce programme offre au concepteur d'applications un ensemble de commandes appelées **ordres** afin d'assurer la gestion de la mémoire utilisateur.

Le terme masque était utilisé primitivement pour désigner ce programme parce qu'il est, au sens propre, masqué dans la mémoire ROM. Dans ce manuel l'expression "**Système d'exploitation**" est utilisée ou parfois le terme "Carte" désignant globalement la carte avec son **système d'exploitation**.

CAD (Card Accepting Device)

Terme générique employé dans ce document pour désigner tout appareil permettant de communiquer avec la carte.

Ordre

Fonctionnalité élémentaire du **système d'exploitation**. Un **ordre** est dit :

ENTRANT lorsque l'échange s'opère dans le sens extérieur vers la carte,
SORTANT quand l'échange s'opère dans le sens carte vers l'extérieur.

Fonction TELEPASS

Algorithme cryptographique **TELEPASS** utilisé, dans le cadre du fonctionnement d'une carte, pour chiffrer certaines informations.

Fonction D.E.S.

Algorithme cryptographique **D.E.S.** (Data Encryption Standard) utilisé, dans le cadre du fonctionnement d'une carte, pour chiffrer certaines informations.

Mot

Elément de la mémoire constitué de 32 bits adressables par quartets (4 bits). L'**adresse** d'un mot est donc un multiple de 8.

Adresse

Valeur hexadécimale, représentée par un nombre en hexadécimal ou un libellé, désignant l'emplacement d'un **mot** dans une **zone** de la mémoire.

Pointeur

Adresse du premier **mot** d'une **zone** de la mémoire.

Zone

Ensemble de plusieurs **mot**s soumis à un même type de gestion.

Fabrication

Période d'élaboration en plusieurs étapes de la carte.

Etapes exécutées par le constructeur :

- fabrication de l'ensemble **ROM**, **RAM**, et **EEPROM** (ou **EPROM**),
- écriture dans la mémoire (**EEPROM** ou **EPROM**) d'un ensemble d'informations caractéristiques de la fabrication.

Etapes exécutées par l'encarteur :

- assemblage des trois éléments (encartage) :
  - circuit monolithique,
  - bouton de contact (points de connexion),
  - support plastique.
- écriture dans la mémoire (**EEPROM** ou **EPROM**) d'un ensemble d'informations propres à la carte et caractéristiques du type d'application (prépersonnalisation).

Personnalisation

Période d'inscription en mémoire des informations caractéristiques de l'application et de l'**utilisation** finale : en particulier **pointeurs** et informations secrètes.

Utilisation

Période de disponibilité de la carte pour un usager pour des services déterminés dans le cadre d'une application.

Invalidation

L'invalidation d'une carte consiste à la déclarer définitivement inutilisable par le **porteur**.

L'application met une carte au rebut en positionnant un **verrou** particulier dit "**verrou** d'invalidation". La carte est alors inutilisable sauf pour être expertisée (lue).

Verrou

Elément logique à deux états :

- **verrou** non positionné,
- **verrou** positionné.

L'état positionné, irréversible, indique la fin d'une **phase de vie de la carte**.

Clé

Information secrète, propre à chaque carte, enregistrée en **mémoire** et dont elle conditionne l'accès.

Porteur

Personne, titulaire final de la carte à microcalculateur personnalisée, utilisatrice de cette carte dans le cadre d'une application.

Code porteur

Information secrète, propre à chaque carte, enregistrée en **mémoire**, conditionnant l'**utilisation** de la carte par son propriétaire (ou **porteur**).

Jeu secret

Information secrète, propre à chaque carte, enregistrée en mémoire, utilisée par le **système d'exploitation** pour la **certification** et pour le **chiffrement des clés**.

Certification

Action permettant d'assurer la présence et l'intégrité d'une information dans la mémoire au bon emplacement.

Chiffrement

Action de codage d'un message de telle façon que seul le destinataire de ce message peut déchiffrer ce message.

Authentification

Vérification de l'habilitation d'une carte ou d'un **CAD**.

Protections

Ensemble des indicateurs et informations secrètes (**code porteur**, **jeux secrets**, **clés**), servant à gérer la sécurité de l'échange des données entre le **CAD** et la carte. Le qualificatif "protégé" est utilisé chaque fois qu'une action est soumise à l'un de ces éléments de protection.

Phase de vie de la carte

Avant qu'une carte soit utilisée par un **porteur**, elle passe par certaines étapes. L'ensemble de ces étapes, y compris la période d'**utilisation**, est désigné par l'expression "Vie de la carte". Les étapes sont appelées "Phases de vie de la carte".

Zone secrète

Zone de la mémoire du microcalculateur dans laquelle sont inscrites divers **codes**, **clés** et **jeu secret** utilisés en interne par la carte. Cette **zone** est rigoureusement impossible à lire de l'extérieur que ce soit par voie physique ou voie logique.

Zone d'accès

Zone de la mémoire du microcalculateur dans laquelle sont mémorisés les résultats de validation de **clé** (ou de validation de **code**) en lecture ou en écriture. La carte comptabilise les tentatives d'accès, échec ou réussite, et provoque le **blocage** en cas d'erreurs répétées (tentative de fraude).

Zone confidentielle

Zone de la mémoire du microcalculateur dans laquelle sont mémorisées des informations permanentes gérées par l'application.

Zone de transactions

Zone de la mémoire du microcalculateur dans laquelle sont mémorisées des informations gérées par l'application : données administratives, médicales....

Zone de lecture

Zone de la mémoire du microcalculateur dans laquelle sont mémorisées des informations permanentes et non confidentielles.

Zone de fabrication

Zone de la mémoire du microcalculateur dans laquelle sont mémorisées des informations de services :

- numéro de série de la carte,
- numéro d'application,
- **pointeurs** des **zones**,
- **verrous**.

Zone de travail

Zone de la mémoire du microcalculateur, évolutive dans le temps, dont les **protections** sont paramétrables. La **zone de transactions** est une **zone** de travail ; la **zone confidentielle** peut être par option définie comme une deuxième **zone** de travail.

Blocage

Le blocage d'une carte consiste à empêcher les présentations exhaustives de **clés** ou **code**.

La carte autorise un certain nombre d'erreurs successives lors de tentatives d'accès protégé, le blocage de la carte se produit lorsque ce nombre d'erreurs est atteint.

Saturation

La carte est saturée lorsque la **zone d'accès** est remplie. La carte peut fonctionner encore pour tous les accès non protégés.

Mutisme

Comportement de la carte qui ne répond pas aux interrogations du **CAD**.

1.4 Liste des ordres exécutables

Cette section donne la liste et la fonction des ordres disponibles dans le système d'exploitation de la famille SCOT.

Des opérations, composées d'une séquence particulière d'ordres, sont également citées.

Ces ordres et opérations sont décrits en détail dans les chapitres "JEU D'ORDRES" et "OPERATIONS".

Ordres

Lecture

Lecture d'un ou plusieurs octets de la mémoire (256 au maximum).

Ecriture

Ecriture d'un mot de la mémoire.

Recherche d'un mot sur argument

Recherche, à partir d'une adresse donnée, d'un mot dont les 16 bits de poids forts sont égaux à l'argument.

Recherche du premier mot vierge

Recherche, à partir d'une adresse donnée, du premier mot dont aucun bit n'est positionné.

Recherche du premier mot non vierge

Recherche, à partir d'une adresse donnée, du premier mot dont au moins un bit est positionné.

Lecture de résultat

Fourniture au CAD du résultat d'un ordre exécuté précédemment :

- résultat de remise à zéro : adresse de fin de mémoire et caractéristiques de la carte,
- fonction TELEPASS ou D.E.S. : résultat du calcul de certificat,
- recherche sur argument : adresse du mot contenant l'argument donné et son contenu,
- recherche du premier mot vierge ou recherche du premier mot non vierge : adresse et contenu du mot trouvé.

Ecriture des verrous

Positionnement à 0 d'un ou plusieurs verrous dans la zone des verrous (incluse dans la zone de fabrication).

Effacement de domaine

Remise à l'état vierge d'une partie de la mémoire (disponible sur certains modèles de la famille SCOT).

Demande de nombre aléatoire

Envoi d'un nombre unique par la carte au CAD (disponible sur certains modèles de la famille SCOT).

Présentation en clair de clé ou code

La clé (ou le code) présentée est comparée terme à terme avec la clé (ou le code) correspondante stockée en zone secrète. Le résultat de la comparaison est mémorisé par la carte.

Présentation chiffrée de clé

Le résultat du chiffrement de clé est déchiffré par la carte et comparé terme à terme avec une valeur prédéterminée. Le résultat de la comparaison est mémorisé par la carte (disponible sur certains modèles de la famille SCOT).

Validation de clé ou code en lecture

Positionnement d'un bit de la zone d'accès en fonction du résultat de la présentation de la clé (ou du code) puis fourniture du résultat au CAD.

Validation en écriture

Ecriture du bit dit de validation du mot.

Calcul de certificat

Calcul algorithmique effectué à partir de données aléatoires fournies par le CAD et de données caractéristiques d'un mot de la carte et mémorisation du résultat.

Changement de code porteur

Remplacement du code porteur par un nouveau code porteur dans la mémoire (disponible sur certains modèles de la famille SCOT).

Opérations

Lecture protégée

Lecture de données dans une zone de la mémoire soumise à une vérification d'un droit de lecture.

Ecriture protégée

Ecriture de données dans une zone de la mémoire soumise à une vérification d'un droit d'écriture.

Effacement

Effacement dans une zone de la mémoire soumise à une vérification d'un droit d'effacement.

Déblocage d'une carte

Remise en accès d'une carte bloquée.

Changement de code porteur

Remplacement du code porteur enregistré en mémoire par une nouvelle valeur (opération disponible sur certains modèles de la famille SCOT).

Recherche de mot

Recherche en mémoire d'un mot donné.

Identification de la carte

Identification d'une carte dans la famille et de ses caractéristiques.

Certification

Assurance de la présence au bon emplacement et de l'intégrité d'une information dans la mémoire.

FAMILLE SCOT

2 FAMILLE SCOT

2.1 Présentation de la famille SCOT

La famille SCOT réunit des systèmes d'exploitation compatibles sur des composants offrant différentes tailles et types de mémoire.

Cette famille est entièrement renouvelée mais compatible avec les anciens modèles.

Circuits monolithiques

La gamme des circuits monolithiques est composée de :

SPOM24, SPOM21, SPOM11

offrant des tailles de mémoire différentes effaçables ou non effaçables.

Famille SCOT

Référence modèle	SCOT 10	SCOT 20 DES	SCOT 50	SCOT 60 DES	SCOT 100	SCOT 110 DES
Circuit	SPOM11	SPOM11	SPOM24	SPOM24	SPOM21	SPOM21
Capacité ROM	6 ko	6 ko	3 ko	3 ko	6 ko	6 ko
Capacité PROM	8 ko EPROM	8 ko EPROM	1 ko EEPROM	1 ko EEPROM	3 ko EEPROM	3 ko EEPROM
Algo crypto	T	D	T	D	T	D
Zones de travail	1	2	1	2	1	2
Changement code porteur	1	1	1	n + 1	1	n + 1

T indique l'algorithme TELEPASS
D indique l'algorithme D.E.S.

Evolution de la famille SCOT

Nouveautés

- D.E.S.
- Demande de nombre aléatoire
- Présentation chiffrée de clé émetteur
- Changement de code porteur
- Deuxième zone de travail

Particularités

- Clé émetteur 1B sur 2 mots fixes
- Code porteur 2A sur 1 ou 2 mots fixes
- Ordre d'écriture des verrous : paramètre longueur = 2 octets
- Zone de lecture obligatoire pour le système d'exploitation SCOT 50

Adresses de la mémoire

L'adresse de début est dans tous les cas = 200h.

Taille des mémoires

L'adresse de fin de mémoire est variable suivant la taille de cette mémoire.

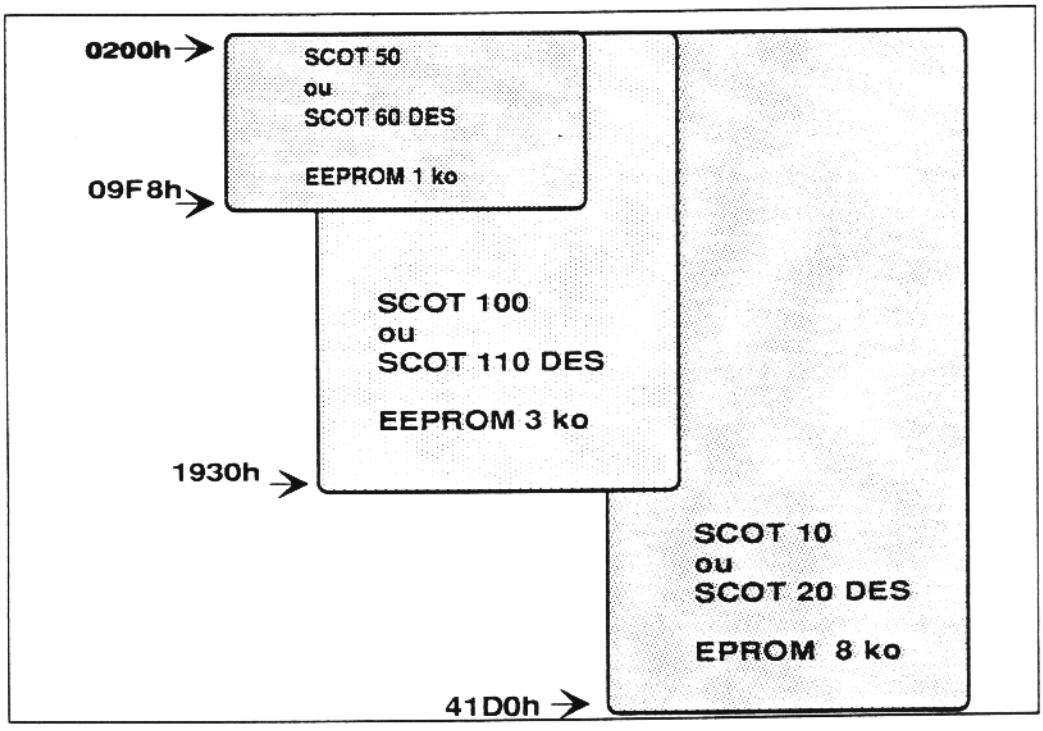

Figure 2.1 - Comparatif des mémoires des cartes SCOT.

Ordres disponibles pour chaque modèle de carte

	Modèles SCOT					
Ordres	**10**	**20 DES**	**50**	**60 DES**	**100**	**110 DES**
Demande de nombre aléatoire		**OUI**				**OUI**
Présentation chiffrée de clé		**OUI**				**OUI**
Effacement			**OUI**	**OUI**	**OUI**	**OUI**
n changements de code porteur				**OUI**		**OUI**
Tous autres ordres	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**

Identification du modèle de carte

Une remise à zéro suivie de l'ordre "Lecture de résultat" permet d'identifier le modèle de carte par la reconnaissance des informations suivantes :

- la taille de la mémoire,
- le nombre de zones de travail,
- les protections de la zone confidentielle, si elle existe,
- le type d'algorithme cryptographique.

2.2 Description de la mémoire

La mémoire est divisée en 6 zones distinctes. Chaque zone a un rôle particulier et une taille différente définie à la conception de l'application.

Zones de la mémoire

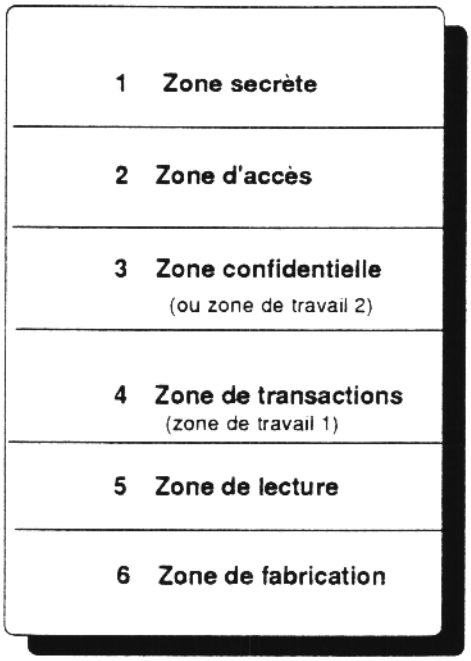

Figure 2.2 - Partition de la mémoire.

Caractéristiques de chaque zone

- taille
- contenu
- accessibilité (non modifiable) :

  - lecture libre
  - lecture protégée
  - lecture interdite

  - écriture libre
  - écriture protégée
  - écriture interdite

  - effacement protégé
  - effacement interdit

Zone secrète

Cette zone contient toutes les informations secrètes :

- clés
  - clé de fabrication,
  - clé émetteur 1A,
  - clé émetteur 1B,
- codes porteur
  - code porteur 2A,
  - code porteur 2B,
- jeu secret.

Zone d'accès

Cette zone reçoit l'enregistrement de toutes les tentatives d'accès à la carte par des clés ou des codes.

Zone confidentielle ou Zone de travail 2

Option : 1 zone de travail

La zone confidentielle n'est pas une zone de travail, elle contient des informations inscrites en phase de personnalisation, non évolutives dans le temps.

Option : 2 zones de travail

La zone confidentielle est alors une zone de travail (zone de travail 2) et contient des informations évolutives dans le temps.

Zone de transactions dite Zone de travail (1)

Zone contenant les informations propres à l'application. C'est la plus grande zone de la mémoire. Son contenu est évolutif dans le temps.

Zone de lecture

Zone totalement libre à la lecture. Elle contient des informations fixes non confidentielles.

Zone de fabrication

Zone totalement libre à la lecture.

Elle contient des informations figées :

- les pointeurs de zones
- le numéro de série
- le numéro d'encarteur
- les types de protection d'accès à la (ou les) zone(s) de travail

et des informations non figées :

- les verrous.

Droits d'accès

Droits d'accès aux différentes zones			
	Effacement	**Lecture**	**Ecriture**
Zone secrète	interdit	interdite	interdite
Zone d'accès	interdit	protégée	interdite
Zone confidentielle *(option 1 zone de travail)*	interdit	protégée	interdite
Zone confidentielle (Zone de travail 2) *(option 2 zones de travail)*	L'application définit les droits d'accès à cette zone		
Zone de transactions (Zone de travail 1)	L'application définit les droits d'accès à cette zone.		
Zone de lecture	interdit	libre	interdite
Zone de fabrication	interdit	libre	interdite sauf verrous

2.3 Structure d'un mot

Les zones de la mémoire accessibles en écriture sont constituées de mots eux-mêmes partageables en quartets (4 bits) adressables directement.

Mot

Un mot est composé de 32 bits dont les 3 bits de poids forts peuvent être réservés.

Les 3 bits système sont utilisés pour la gestion de la protection en écriture.

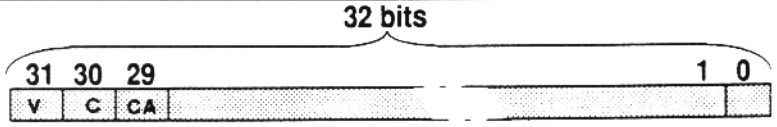

Figure 2.3 - Aspect d'un mot de la mémoire.

Mode d'écriture dans un mot

L'écriture d'un bit est irréversible, elle consiste à positionner un bit.

Un bit **non positionné** est à 1 et peut être positionné à 0.

Un bit **positionné** est à 0 et ne peut plus être positionné à 1 par écriture.

Exemple de positionnement de bits

Profil existant : 11110000

Profil présenté : 10110001

Résultat obtenu : 10110000

Le dernier bit, déjà positionné, ne peut pas être changé.

Figure 2.4 - Exemple de positionnement de bits.

Mode d'adressage d'un mot

Un mot est constitué de 8 **quartets** adressables individuellement. L'adresse d'un mot est donc par définition l'adresse de son premier quartet.

L'adresse d'un mot est toujours un nombre multiple de 8.

Bits système

Bit: Bit V de validation

Positionner ce bit signifie que le contenu du mot est validé et le mot ne peut plus être réinscrit.

Bit C et Bit CA : bits liés

Indiquent quelle autorité a validé un mot (détaillé dans la section "Principe d'écriture" du chapitre "ACCES A LA CARTE").

Taille utile d'un mot

Lorsque les 3 bits système sont utilisés, la taille utile d'un mot est : **29 bits.**

2.4 Partition de la mémoire

Cette section donne le détail de la partition de la mémoire pour chaque modèle de carte.

Cartes SCOT

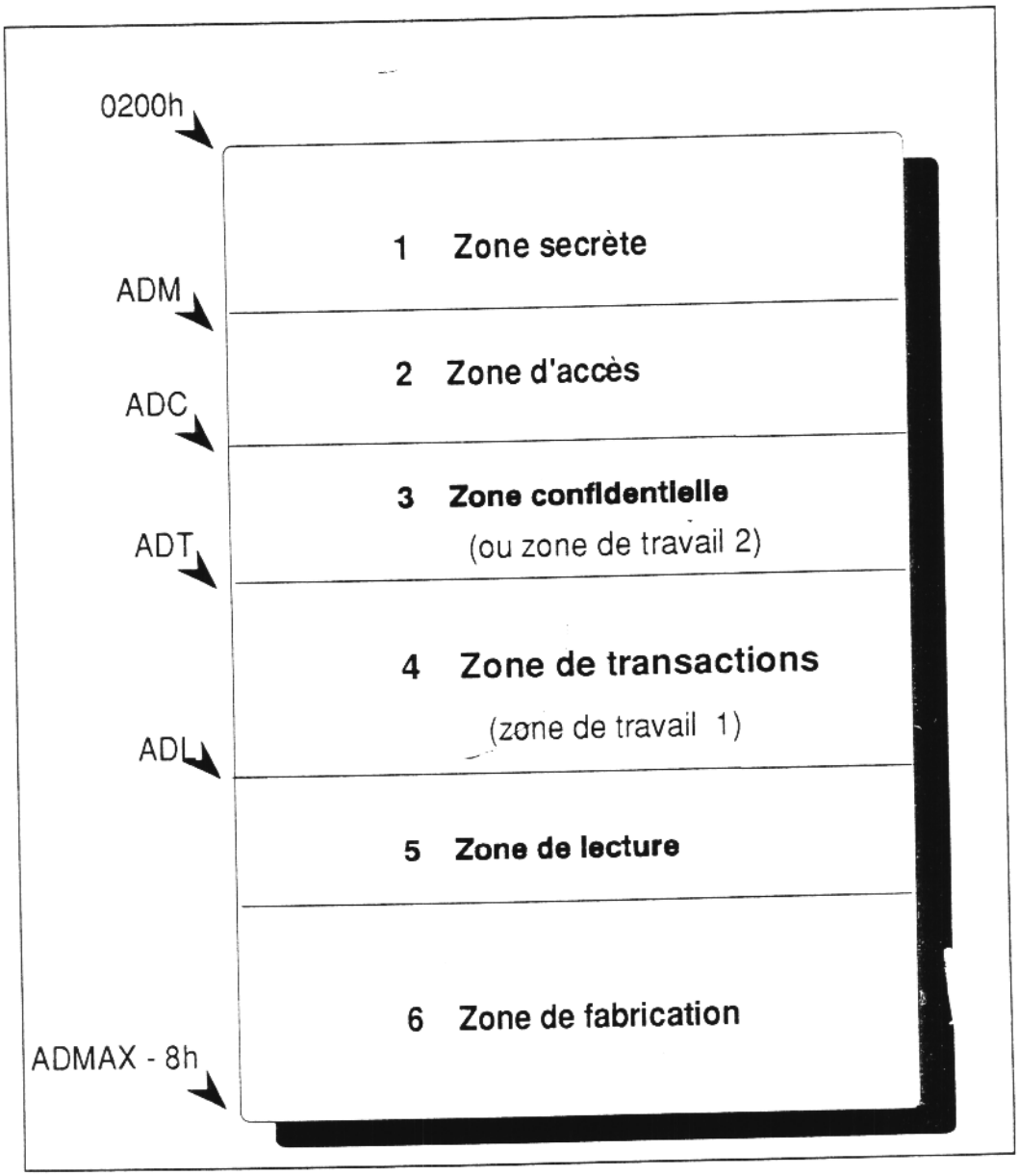

Figure 2.5 - Zones et adresses des zones des cartes SCOT.

Notations utilisées dans les schémas des mémoires

Adressés (16 bits)

AD1 : adresse de début de la clé 1B
ADS : adresse de début du jeu secret
AD2 : adresse de début du code porteur 2A
ADM : adresse de début de zone d'accès
ADC : adresse de début de zone confidentielle
ADT : adresse de début de zone de transactions (zone de travail)
ADL : adresse de début de zone de lecture
ADMAX - 8h : adresse du dernier mot de la mémoire

Bytes

RUF : espace réservé à une utilisation future (à laisser à 1)
CCR : code correcteur d'erreur (5 bits) excluant le bit de poids fort de chaque demi mot (non géré par le système d'exploitation)
N : numéro d'identification de lot de cartes (6 bits), utilisé par le personnalisateur
I : numéro de diversification de secret (8 bits), utilisé par le personnalisateur (propre à chaque carte)
Numéro de série : propre à chaque carte (25 bits)
Numéro d'encarteur : identificateur du fabricant de la carte (11 bits)
Type d'application : identificateur de l'application de la carte (14 bits)

Verrous

LU relatif à l'utilisation des codes porteur (1 bit)
LC relatif à la personnalisation (1bit)
LF relatif à la fabrication (1bit)
IV relatif à l'invalidité de la carte (1 bit parmi 2 au choix)

Indicateurs

La signification des indicateurs ECi (2 bits) est donnée dans la section "Principe d'effacement" du chapitre "ACCES A LA CARTE".

EC1 : indicateur de protection d'effacement de la zone de travail 1
EC2 : indicateur de protection d'effacement de la zone de travail 2

Pour les indicateurs LPi et EPi (1 bit), la valeur 1 signifie non protégée, la valeur 0 signifie protégée.

LP1 : indicateur de protection en lecture de la zone de travail 1
LP2 : indicateur de protection en lecture de la zone de travail 2
EP1 : indicateur de protection en écriture de la zone de travail 1
EP2 : indicateur de protection en écriture de la zone de travail 2

IA : indicateur d'algorithme (IA = 1 pour TELEPASS ; IA = 0 pour D.E.S.)
Z2 : indicateur du nombre de zones de travail (Z2 = 1 pour une seule zone de travail ; Z2 = 0 pour 2 zones de travail)

Partition détaillée de la mémoire : éléments communs

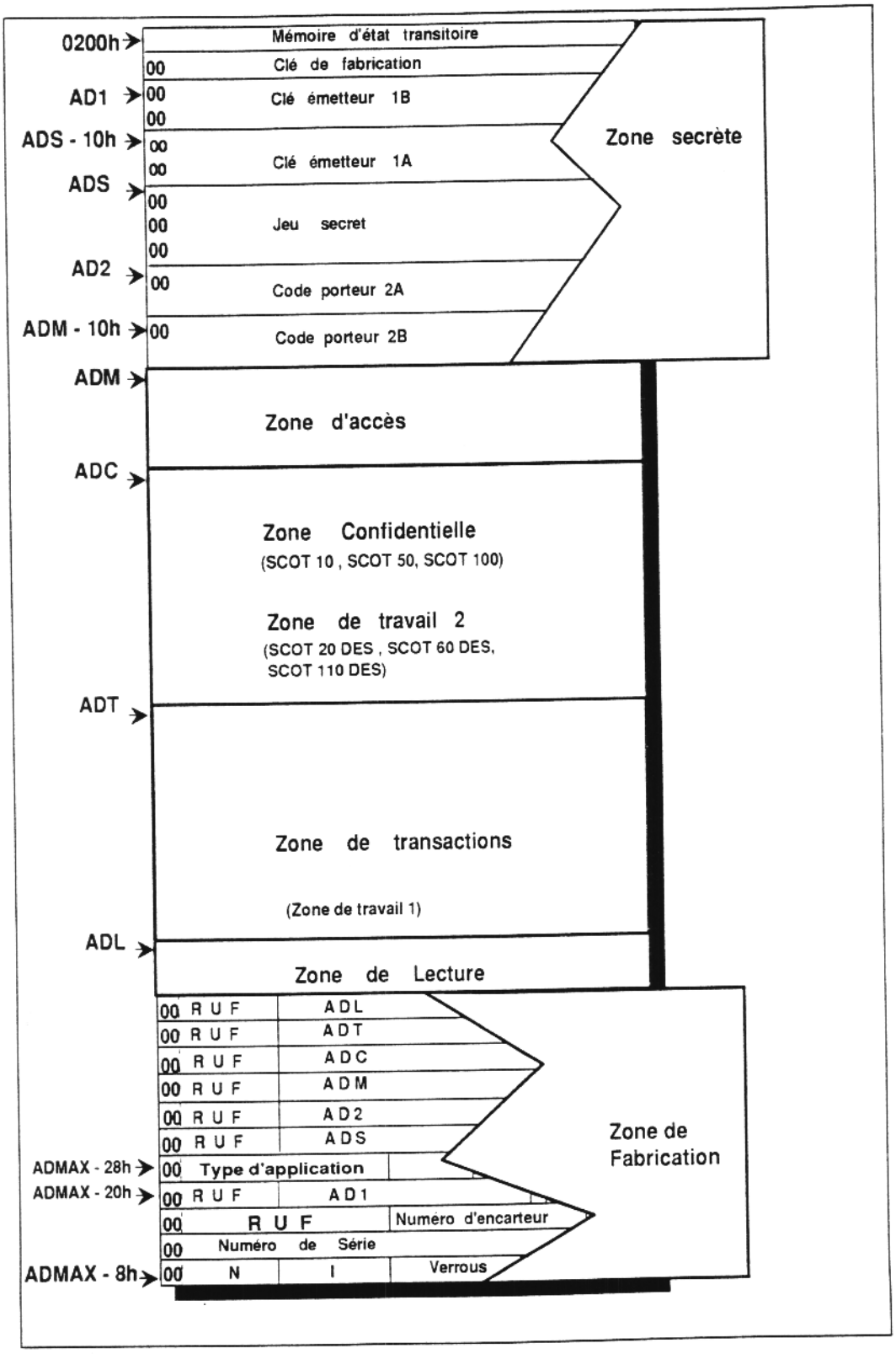

Figure 2.6 - Partition de la mémoire des cartes SCOT.

Partition de la zone de fabrication pour chaque modèle

La zone de fabrication est différente suivant les modèles.

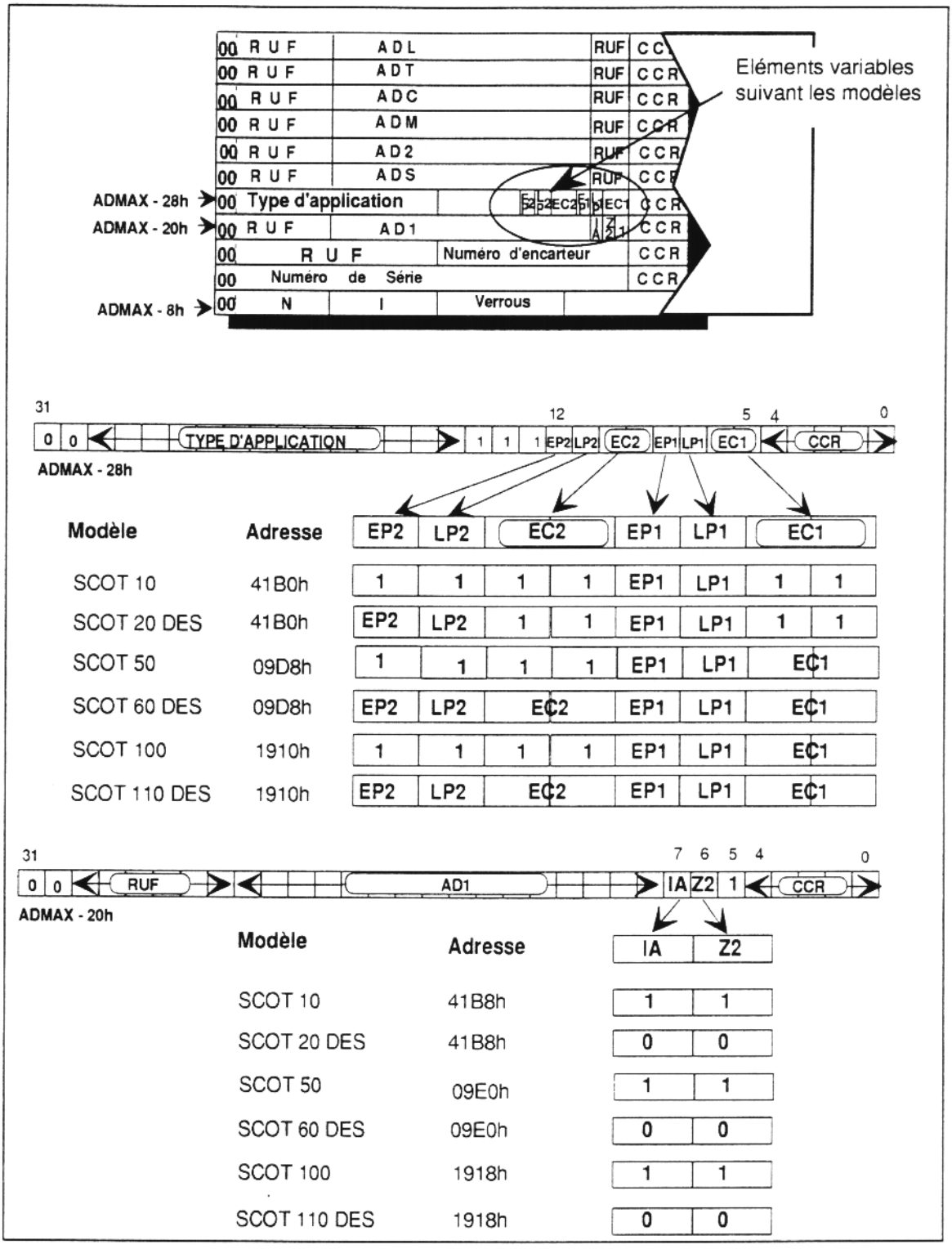

Figure 2.7 - Partitions de la zone de fabrication suivant les modèles.

2.5 Phases de vie

La mémoire est gérée différemment suivant les phases de vie. Cette section décrit les phases de vie.

Délimitation des phases de vie

La fin d'une phase de vie est concrétisée par le positionnement d'un verrou.

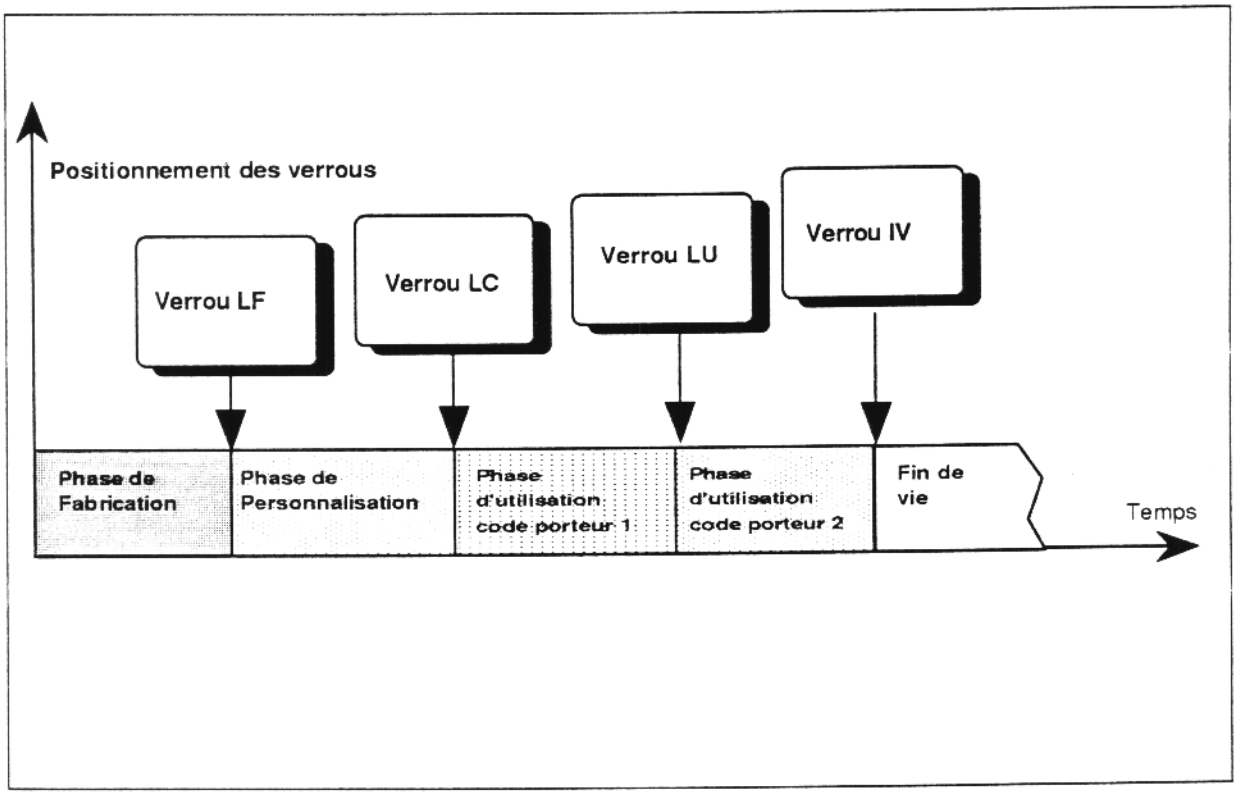

Figure 2.8 - Schéma des phases de vie et positionnement des verrous.

Disposition des verrous

La disposition des verrous dans le dernier mot de la mémoire est la suivante :

LU (bit 15)	**LC** (bit 14)	**LF** (bit 13)	**IV** (bit 12)	**IV** (bit 11)

Phase de fabrication

Au cours de cette phase, sous le contrôle du fabricant, la carte est :

- **encartée**
  les 3 éléments physiques de la carte sont assemblés :

  - microprocesseur,
  - support plastique carte,
  - connecteur.

- **prépersonnalisée**
  inscription des informations suivantes :

  - clé de fabrication,
  - type d'algorithme cryptographique,
  - nombre de zones de travail,
  - numéro de série,
  - type d'application,
  - protections de lecture et écriture relatives à la zone confidentielle et à la zone de transactions,
  - pointeur AD1.

Cette phase est close par le positionnement d'un **verrou de fabrication (LF)**.

Phase de personnalisation

Au cours de cette phase, sous le contrôle de l'émetteur, sont inscrits en mémoire :

- les clés émetteur,
- le jeu secret,
- le code porteur,
- les pointeurs,
- des données propres à l'application, en particulier en zone de lecture et en zone confidentielle si elle existe.

Cette phase est close par le positionnement d'un **verrou de personnalisation (LC)**.

Durant cette phase, la mémoire est protégée en écriture par la clé de fabrication.

Phase d'utilisation

Au cours de cette phase, toutes les zones prennent leur identité et la carte est utilisée normalement par son porteur. Pour certains modèles de carte, le code porteur peut être changé, par le porteur lui-même, une ou plusieurs fois.

Accès à la mémoire

L'accès à la mémoire est protégé selon un protocole particulier à l'aide des clés ou codes inscrits en phase de personnalisation.

Le **verrou d'utilisation (LU)** marque la fin de la possibilité de changer de code porteur :

- fin d'utilisation du premier code porteur (cas d'un seul changement de code possible),

- fin d'utilisation de l'avant-dernier code porteur (cas de plusieurs changements de code possibles).

Cette phase est close par le positionnement d'un **verrou d'invalidation (IV)**.

Fin de vie

La fin de vie de la carte intervient lorsque la carte est selon les cas :

- saturée (la zone d'accès est saturée),
- invalidée.

Elle ne peut être utilisée que pour des lectures.

L'invalidation de la carte est matérialisée par le positionnement d'un **verrou d'invalidation (IV)**.

En réalité cette fin de vie peut intervenir n'importe quand durant la vie de la carte.

Remarque

La suite de ce manuel, excepté le chapitre "PERSONNALISATION", décrit le fonctionnement de la carte en phase d'utilisation.

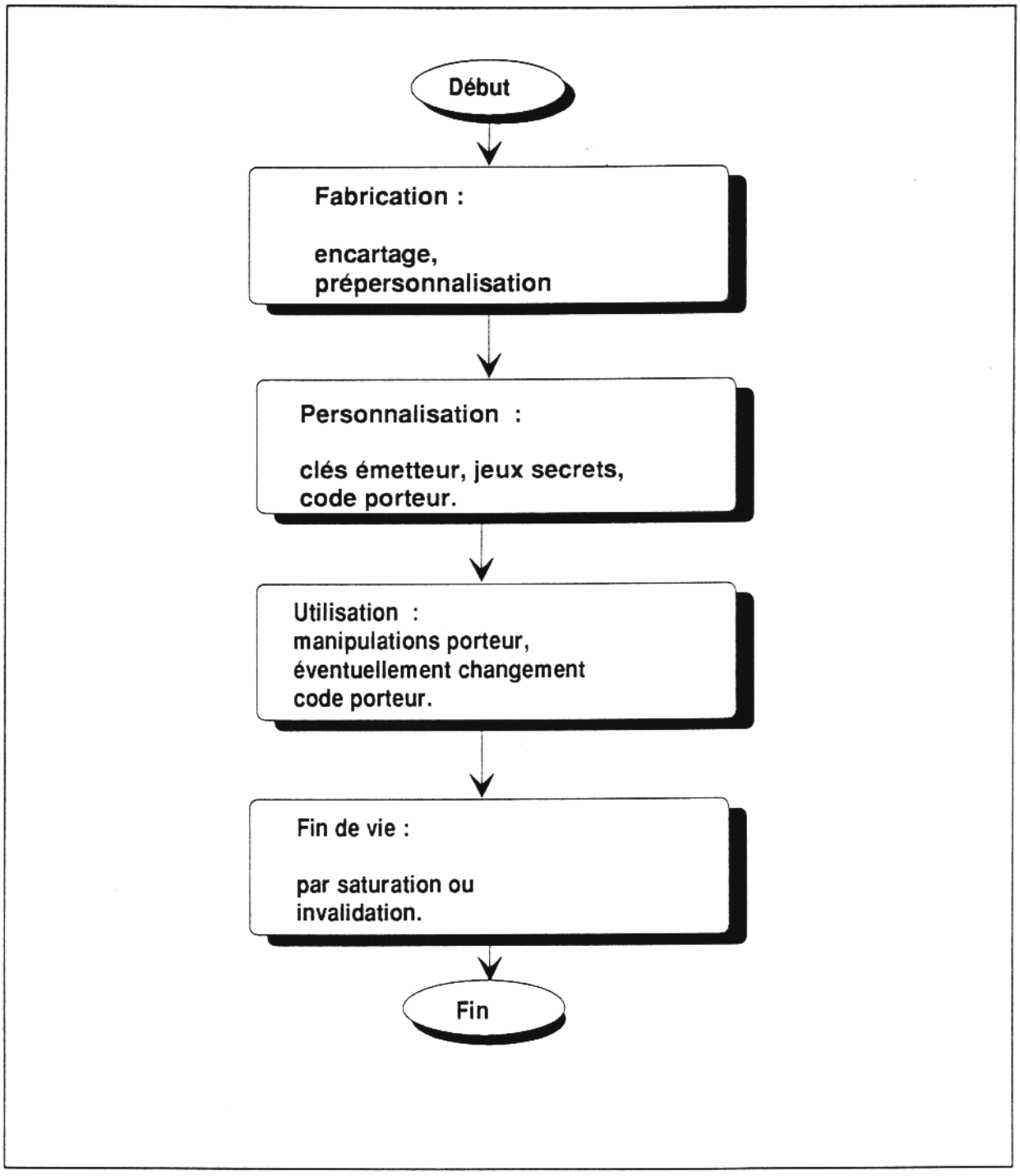

Figure 2.9 - Diagramme de la "Vie d'une carte".

Aspect de la mémoire pendant les différentes phases de vie

Pendant les phases de vie de la carte, certaines caractéristiques de la mémoire évoluent. Les figures suivantes mettent en valeur pour chaque phase les informations importantes.

Phase de fabrication

AD1	Adresse de la clé émetteur 1B.
Numéro d'encarteur	Numéro propre au fabricant.
Numéro de série	Numéro identifiant la carte dans une série.
N et I	Informations qui permettent en phase de personnalisation de retrouver la clé de fabrication. Chaque carte a une clé de fabrication propre.
LF	Verrou qui une fois positionné marque la fin de la phase de fabrication.

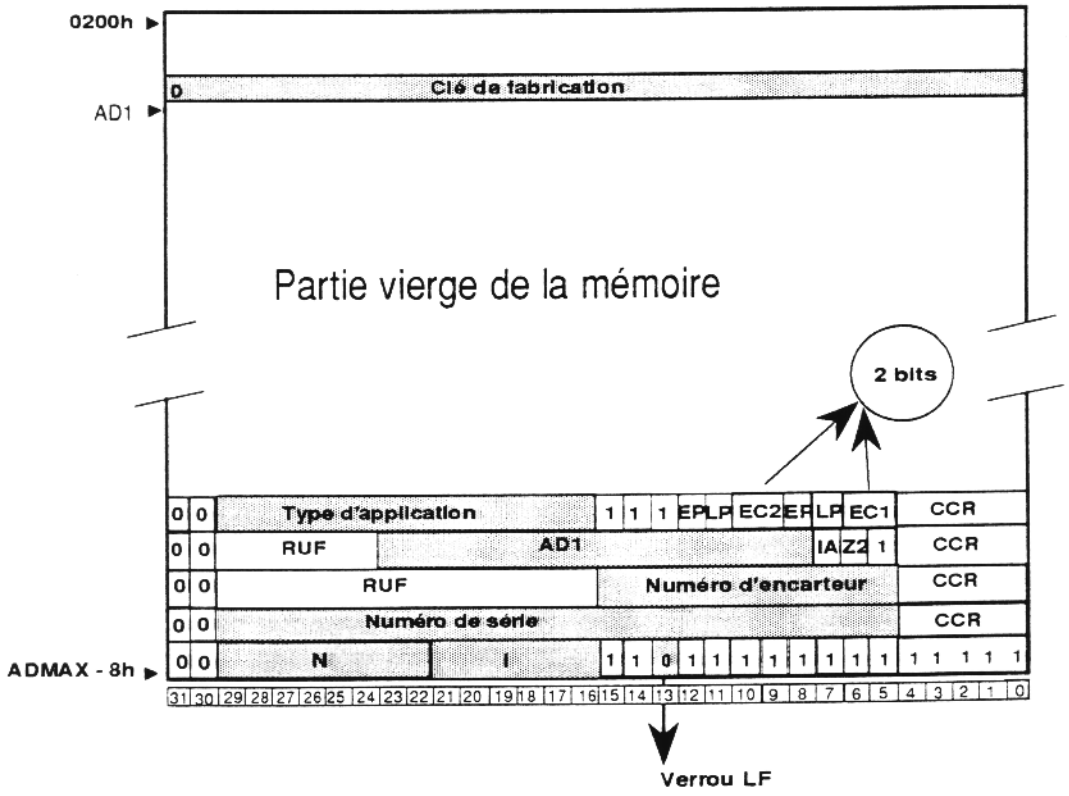

Figure 2.10 - Eléments de la mémoire spécifiques de la phase de fabrication.

Phase de personnalisation

Cette phase détermine la destination de la carte. Toutes les clés et les pointeurs sont écrits.

LC Verrou qui, une fois positionné, marque la fin de la phase de personnalisation.

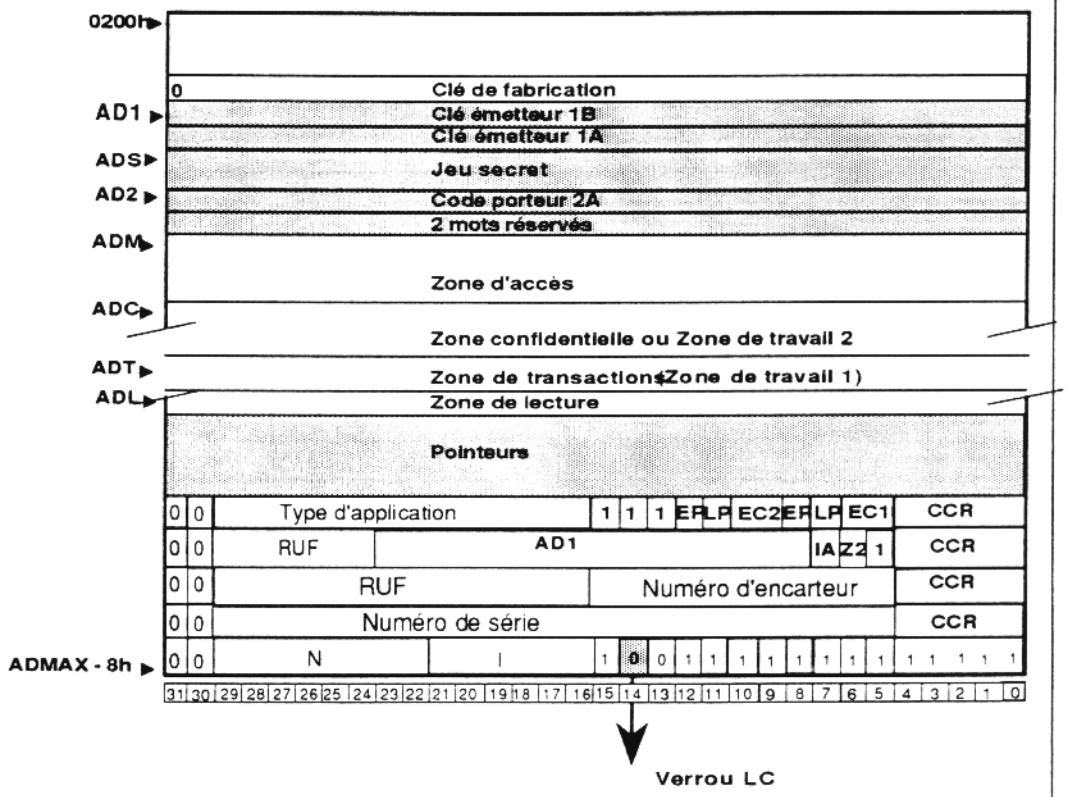

Figure 2.11 - Eléments de la mémoire spécifiques de la phase de personnalisation.

Phase d'utilisation

La **zone confidentielle** n'évolue que si l'option deux zones de travail est adoptée.

La **zone de transactions** évolue.

LU Verrou qui, une fois positionné, signale la fin de la possibilité de changer de code porteur.

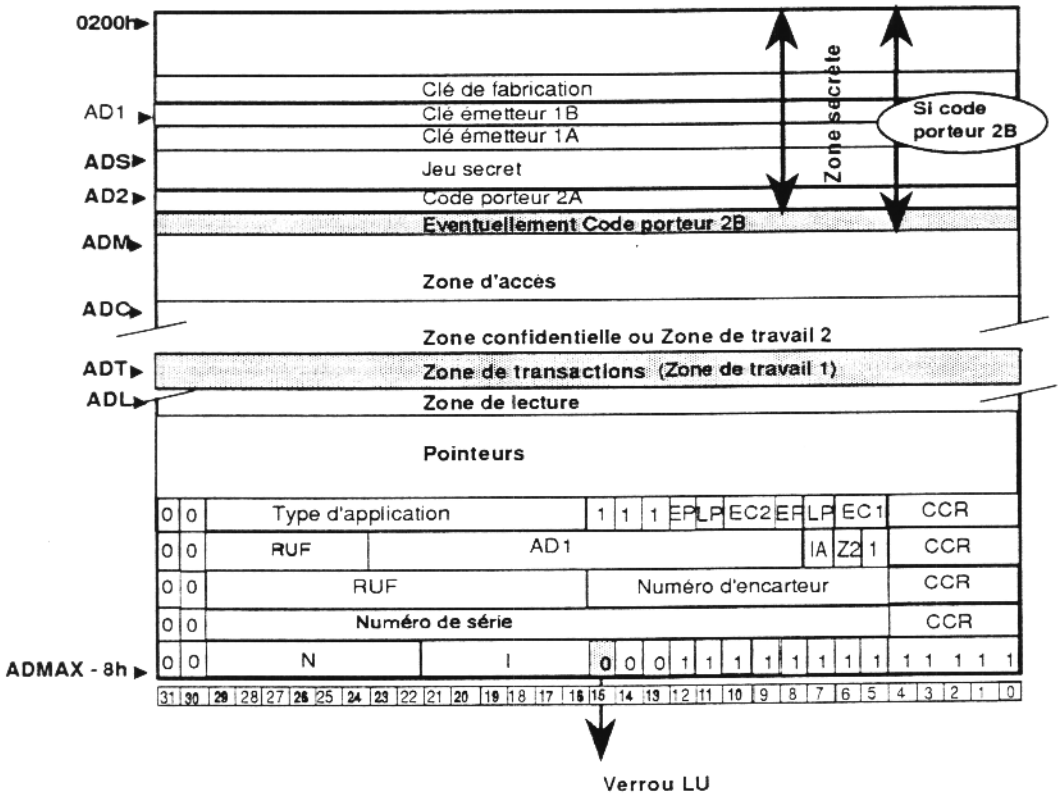

Figure 2.12 - Eléments de la mémoire spécifiques de la phase d'utilisation.

Fin de vie

IV Verrou qui, une fois positionné, signale la fin de vie de la carte.

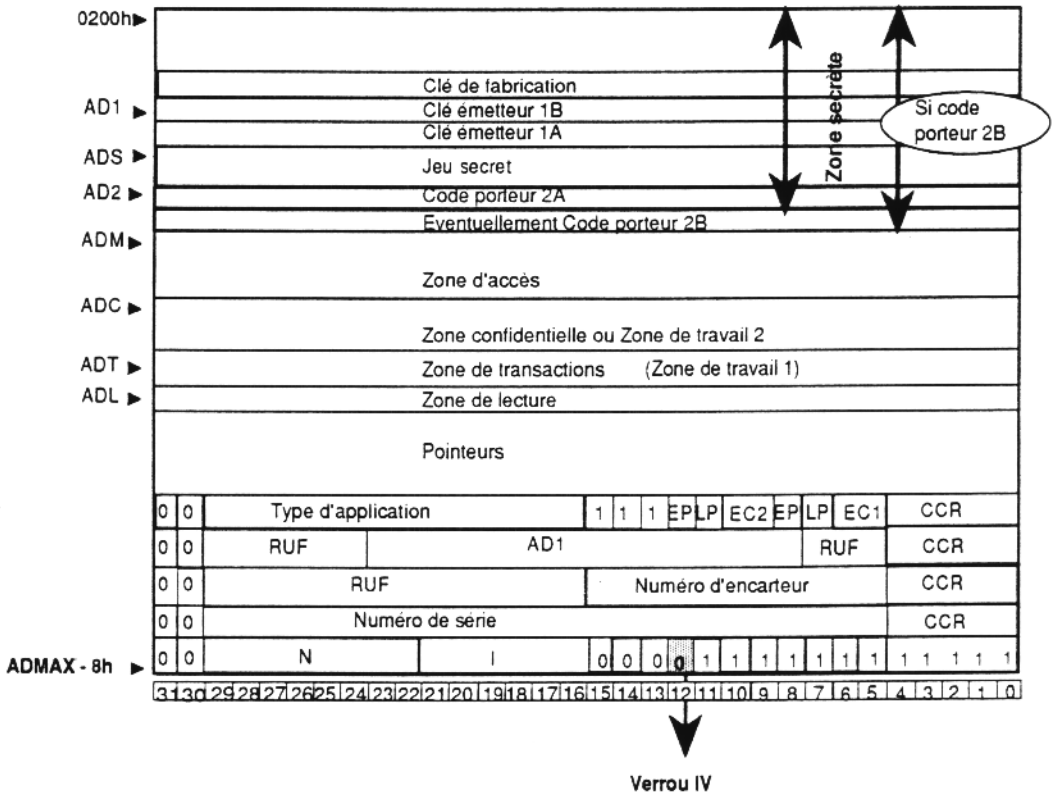

Figure 2.13 - Eléments de la mémoire spécifiques de la fin de vie.

- 3 -

ACCES A LA CARTE

3 ACCES A LA CARTE

3.1 Modes d'accès à la mémoire

Le système d'exploitation gère la mémoire. L'application a accès à la mémoire par l'intermédiaire du système d'exploitation au moyen des ordres.

Accès à la carte

L'application accède à la mémoire principalement par :

- lecture : lecture d'un octet ou d'un domaine,

- écriture et validation : écriture d'un mot et de son bit V,

- effacement : effacement d'un mot ou d'un domaine,

Ces trois types d'accès sont régis par des règles précises décrites dans les sections suivantes de ce chapitre.

Il est possible aussi d'effectuer :

- des recherches : recherche d'un mot dans une zone,

- des écritures de verrou,

- des calculs de certificat : obtenir la certification d'une information écrite en mémoire,

- des présentations de clé : envoyer une clé à la carte pour qu'elle la compare avec la clé mémorisée en zone secrète,

- des validations de clé : connaître la validité d'une clé présentée,

- des demandes de nombre aléatoire...

Réponse de la carte

Le système d'exploitation renvoie au CAD une réponse qui suivant les cas est constituée :

- de données et de deux 'mots d'état' ou STATUS (2 octets),

- des deux mots d'états seulement.

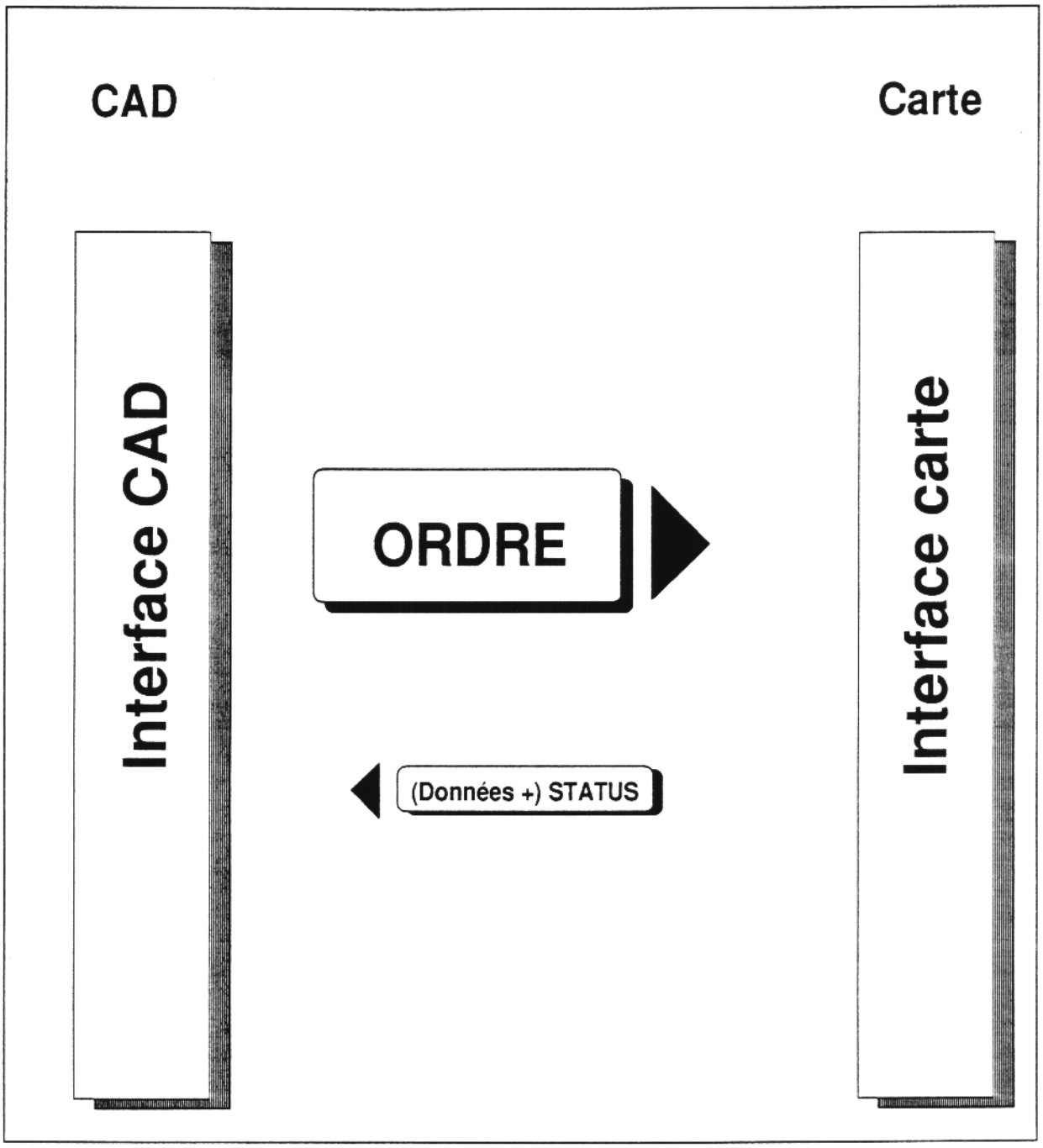

Figure 3.1 - Moyen d'accès à la carte.

3.2 Principe de lecture

La lecture en mémoire obéit à certaines règles décrites dans cette section.

La lecture s'effectue sur un ou plusieurs octets.

Lecture

La lecture en mémoire est, suivant les zones, libre, protégée ou interdite :

Libre	**Protégée**	**Interdite**
Zone de fabrication Zone de lecture	Zone confidentielle Zone de transactions Zone d'accès	Zone secrète

Protections de lecture des zones de travail

Les zones de travail sont contrôlées ou non en lecture par des clés ou des codes.

Les indicateurs LPi précisent si les zones sont protégées ou non :

- l'indicateur LP1 pour la zone de travail 1,

- l'indicateur LP2 pour la zone de travail 2 (si elle existe).

Rappel de la structure des indicateurs de protection.

EP2 1 bit	**LP2** 1 bit	EC2 2 bits	EP1 1 bit	**LP1** 1 bit	EC1 2 bits

Ces indicateurs sont dans un mot de la zone de fabrication.

Signification des indicateurs LPi

LPi = 1 lecture libre
LPi = 0 lecture protégée par clé ou code

Mise en oeuvre de la lecture

Lecture libre

La lecture libre en mémoire s'effectue par un simple ordre de lecture.

Le CAD demande la lecture d'une zone définie de la mémoire, le système d'exploitation lui envoie le résultat de la lecture.

Lecture protégée

La protection est un "droit de lecture" vérifié par le système d'exploitation. Ce "droit de lecture" est matérialisé par une clé ou un code.

La séquence "lecture protégée" est composée des 3 ordres successifs :

- présentation d'une clé ou d'un code,

- validation de clé ou de code en lecture,

- lecture de données.

Résultat de validation bon

Si le résultat de la validation est bon, la lecture transfère le contenu de la partie de la mémoire demandée au CAD.

L'autorisation de lecture demeure valable pour d'autres lectures jusqu'à l'occurrence d'un des événements tels que :

- mise hors tension de la carte,
- présentation d'une clé ou d'un code.

Résultat de validation faux

Si le résultat de la validation est faux, la lecture n'a pas lieu.

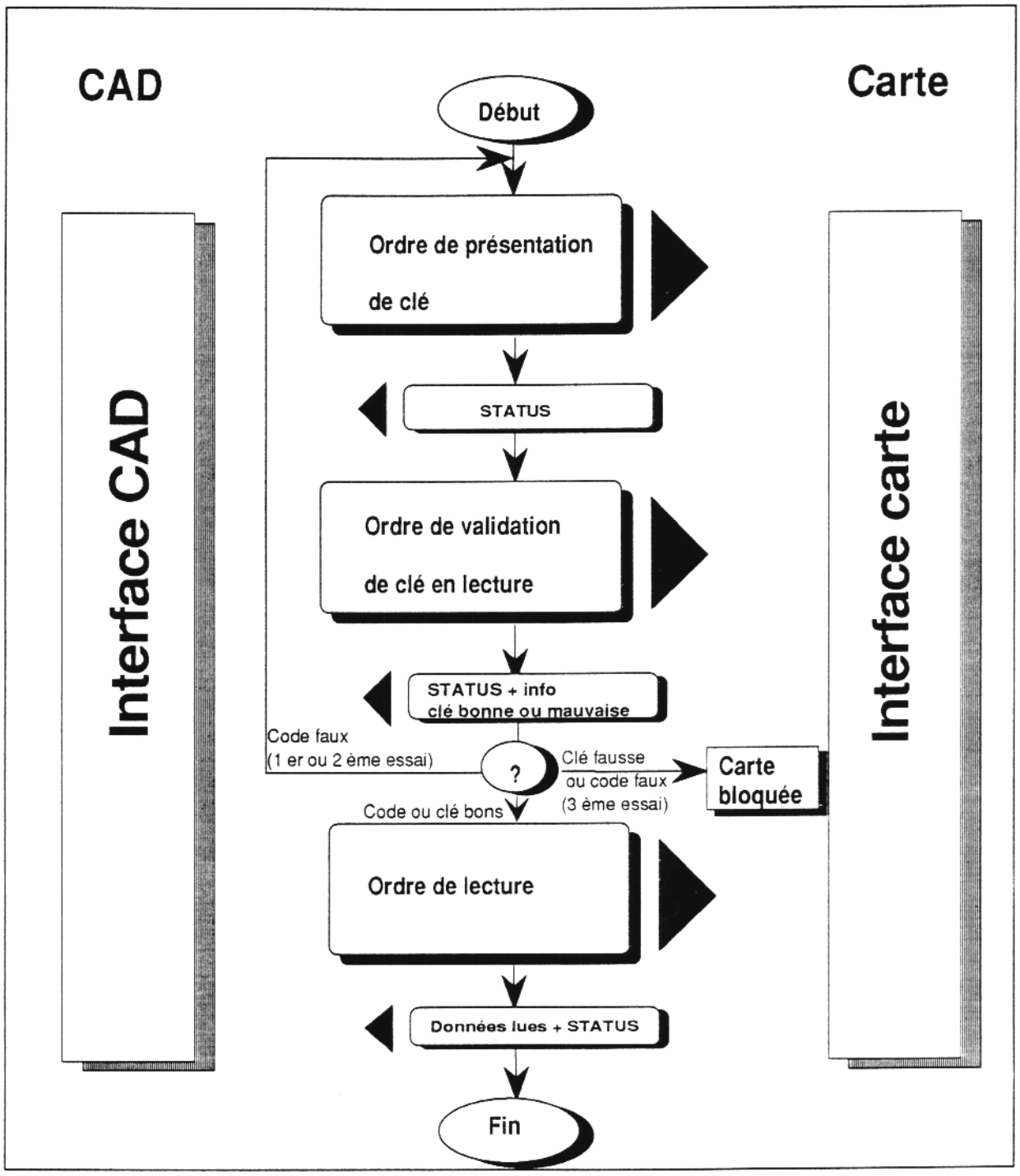

Figure 3.2 - Diagramme de la "Lecture protégée".

3.3 Principe d'écriture

De la même façon que la lecture, l'écriture en mémoire obéit à certaines règles décrites dans cette section. A la différence de la lecture, l'écriture agit toujours sur un mot complet.

Ecriture

L'écriture en mémoire est, suivant les zones, libre, protégée ou interdite.

Libre ou protégée (défini en personnalisation)	Les zones de travail
Interdite	Toutes les autres zones

Protections d'écriture

L'écriture s'effectue en deux temps :

- écriture des 31 bits d'information
- validation par l'écriture du bit V (bit de poids fort).

Les zones de travail sont protégées en écriture par des clés ou des codes. Cette protection intervient au moment de la validation.

Les indicateurs EPi précisent si ces zones sont protégées en écriture ou non :

- l'indicateur EP1 pour la zone de travail 1,

- l'indicateur EP2 pour la zone de travail 2 (si elle existe).

Rappel de la structure des indicateurs de protection.

EP2 1 bit	LP2 1 bit	EC2 2 bits	**EP1** 1 bit	LP1 1 bit	EC1 2 bits

Ces indicateurs sont dans un mot de la zone de fabrication.

Signification des indicateurs EPi

EPi = 1 écriture libre
EPi = 0 écriture protégée par clé ou code

Rappel de la structure d'un mot d'une zone en écriture protégée

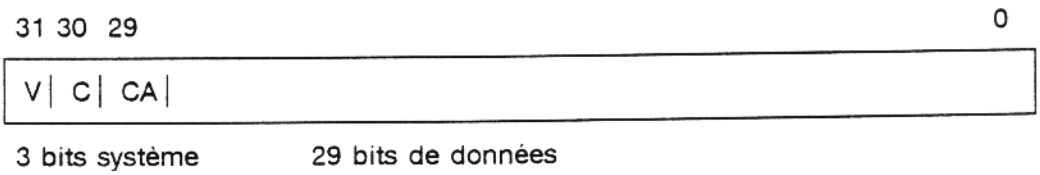

Figure 3.3 - Rappel : aspect du mot standard protégé en écriture.

Mise en oeuvre de l'écriture libre

L'écriture libre en mémoire s'effectue par un simple ordre d'écriture.

Le CAD demande l'écriture de 32 bits dans un mot défini de la mémoire, et dans ce cas, les bits C et CA sont des bits de données.

Une validation d'écriture peut être demandée bien que la clé (ou le code) ne soit pas vérifiée, elle positionne alors le bit V dans le mot.

Mise en oeuvre de l'écriture protégée

L'écriture dans une zone protégée en écriture est toujours possible, mais la validation n'a lieu qu'après présentation d'un code ou d'une clé correct.

La séquence "écriture protégée" est composée des 3 ordres successifs :

- écriture directe du mot (31 bits),
- présentation de la clé (ou code) adéquate,
- validation de l'écriture (écriture du bit V).

L'application transmet 31 bits (bits 0 à 30) dont les bits C et CA indiquent quelle autorité (signifiée par la clé ou le code) doit écrire le bit V :

Type de clé	Nom de clé à présenter	Bit C	Bit CA
Type 1	Clé émetteur 1A Clé émetteur 1B	1 1	1 0
Type 2	Code porteur ou Clé de fabrication	0	X

La notation X, dans ce tableau, indique que la valeur est indifféremment 1 ou 0.

Validation de l'écriture

Au moment de valider le mot :

- le système d'exploitation vérifie par l'analyse des bits C et CA, que l'autorité demandant la validation est bien habilitée dans cette zone ;

- si le résultat de la présentation de clé (ou code) était correct, signifiant que la clé (ou le code) était bonne, le bit V du mot considéré est alors positionné. Le mot est alors validé.

A partir de ce moment, toute nouvelle tentative d'écriture ou de validation de ce mot est refusée par la carte.

L'autorisation d'écriture, ainsi acquise, demeure valable pour d'autres écritures jusqu'à l'occurrence d'un des événements tels que :

- mise hors tension de la carte,
- présentation d'une clé.

Abandon de validation

La validation est abandonnée si :

- l'analyse des bits C et CA n'est pas satisfaisante
ou
- la clé (ou le code) est mauvaise.

Remarque :

La présentation de clé (ou code) peut servir à plusieurs validations successives de même type (bits C et CA identiques).

Exemple

L'écriture protégée de 10 mots de même type peut se faire par une séquence telle que :

10 écritures
1 présentation de clé (ou code)
10 validations d'écriture.

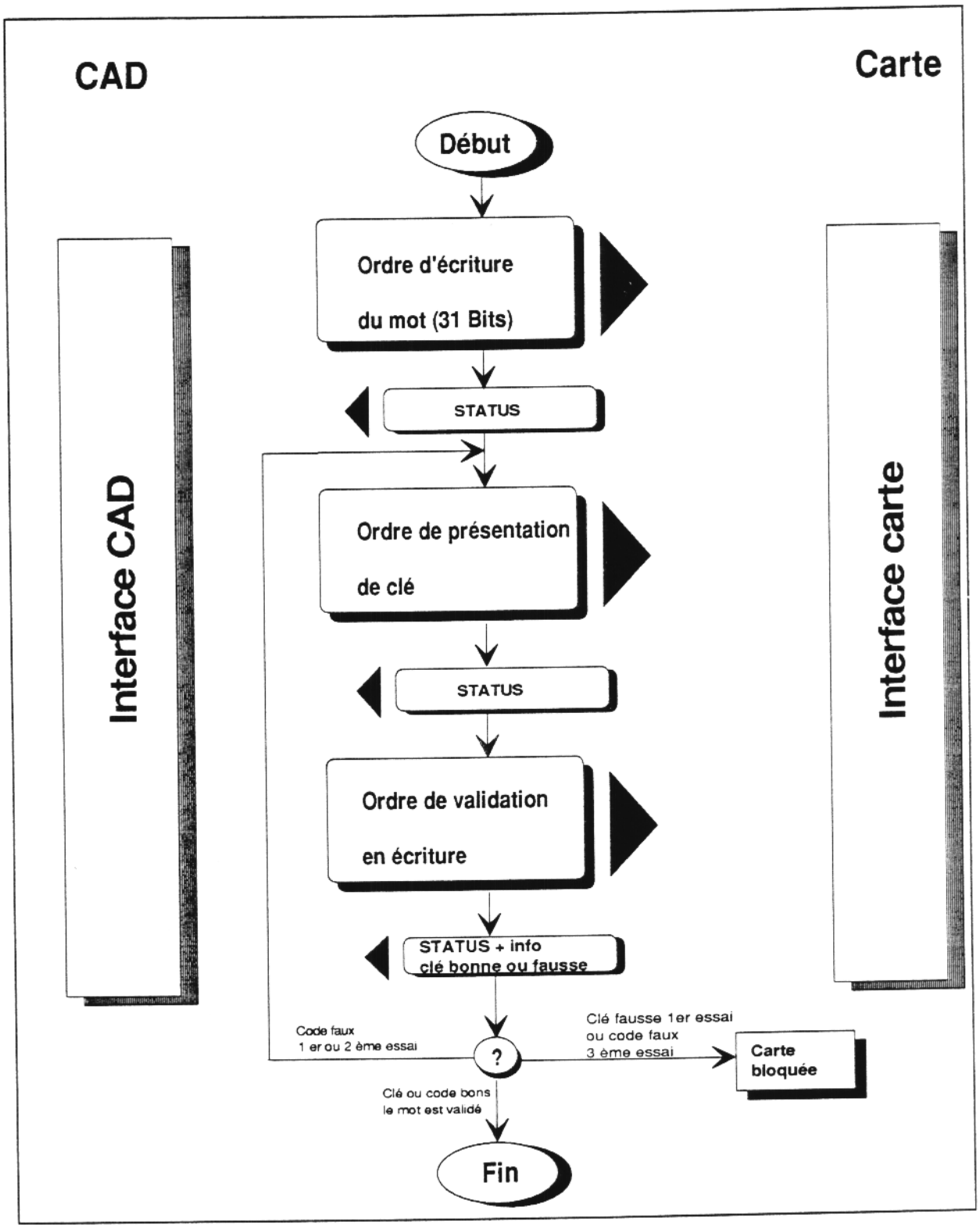

Figure 3.4 - Diagramme de l'"Ecriture protégée".

3.4 Principe d'effacement

De la même façon que la lecture et l'écriture, l'effacement en mémoire obéit à certaines règles décrites dans cette section. L'effacement, s'effectue sur un ou plusieurs mots.

Effacement

L'effacement en mémoire est interdit ou protégé.

Les seules zones autorisées à l'effacement sont les zones de travail.

Protections d'effacement

Les zones de travail sont contrôlées en effacement par des clés ou des codes.

Les indicateurs ECi précisent les conditions d'effacement dans ces zones :

- l'indicateur EC1 pour la zone de travail 1,

- l'indicateur EC2 pour la zone de travail 2 (si elle existe).

Rappel de la structure des indicateurs de protection.

EP2 1 bit	LP2 1 bit	**EC2** 2 bits	EP1 1 bit	LP1 1 bit	**EC1** 2 bits

Ces indicateurs sont dans un mot de la zone de fabrication.

Signification des indicateurs ECi

ECi	=	11	effacement interdit
ECi	=	10	effacement protégé par le code porteur actif
ECi	=	01	effacement protégé par la clé 1B
ECi	=	00	effacement protégé par la clé 1A

Mise en oeuvre de l'effacement

L'effacement nécessite un droit d'effacement acquis par la présentation puis la validation d'une clé ou code correct.

La séquence "effacement protégé" est composée des 3 ordres successifs :

- présentation de l'élément de protection (clé ou code) en adéquation avec le type de protection de la zone à effacer (indicateur ECi),

- validation de lecture,

- effacement du domaine demandé.

Résultat de validation bon

Si le résultat de la validation est bon, l'effacement du domaine demandé est effectué dans la mémoire.

Le droit d'effacement, ainsi acquis, demeure valable jusqu'à l'occurrence d'un des événements :

- mise hors tension de la carte,

- présentation d'une clé ou d'un code.

Résultat de validation faux

Si le résultat de la validation est faux, l'effacement n'a pas lieu.

Remarque :

La présentation de clé (ou du code) peut servir à plusieurs effacements successifs sur des espaces non jointifs de même type comme l'exemple le montre.

Exemple

L'effacement de 3 domaines de même type peut se faire par une séquence telle que :

1 présentation de clé (ou du code)
1 validation de lecture ou écriture
3 effacements.

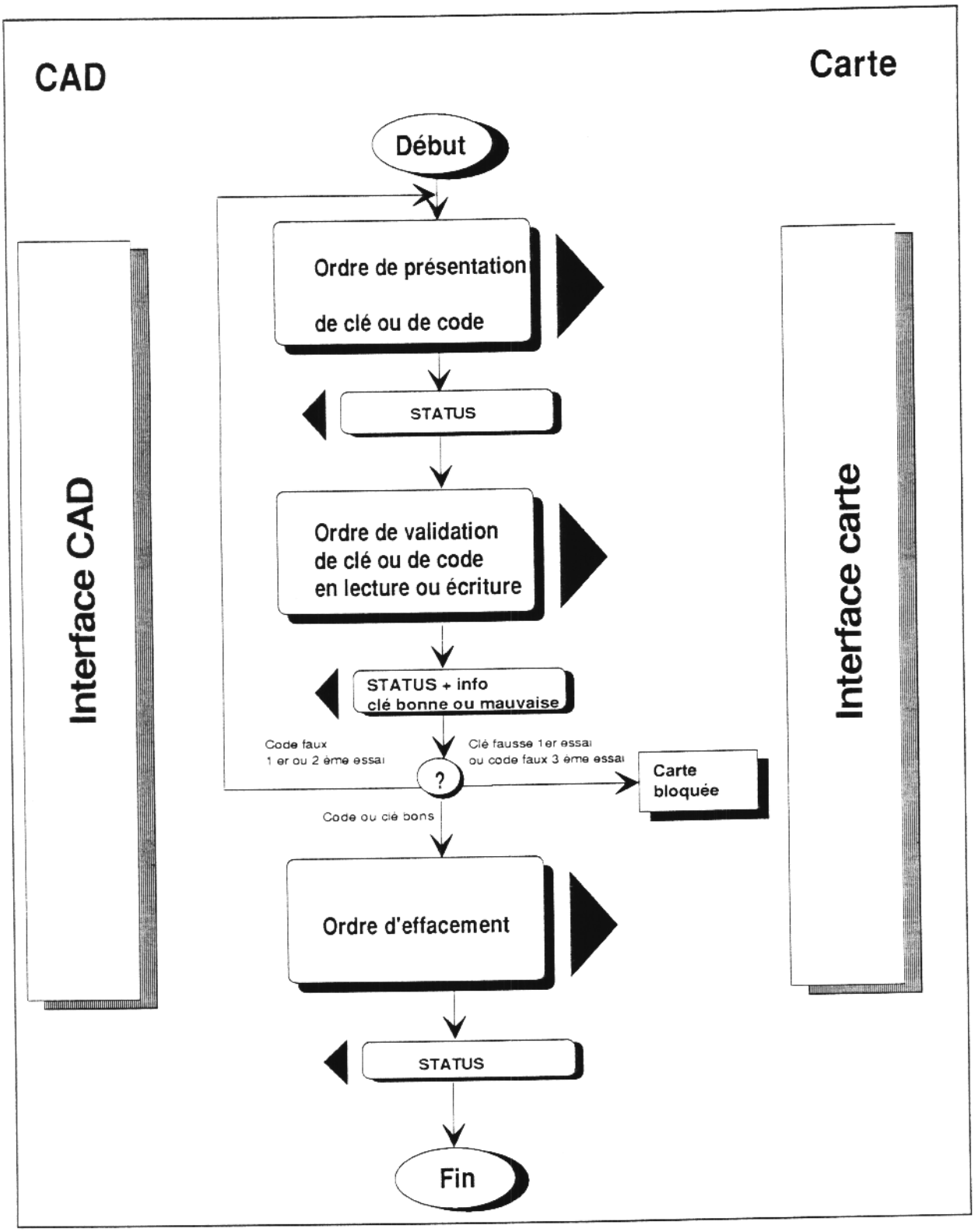

Figure 3.5 - Diagramme de l'"Effacement".

- 4 -

SECURITE DE LA CARTE

4 SECURITE DE LA CARTE

4.1 Procédures de sécurité

Cette expression "Procédures de sécurité" réunit l'ensemble des mécanismes sécuritaires et les éléments utilisés pour assurer la sécurité des données enregistrées sur la carte.

Mécanismes sécuritaires

Présentation de clé ou code

Calcul de certificat

Gestion de la zone d'accès

Protection des zones de la mémoire

Eléments de sécurité

Clés

Codes

Jeu secret

Verrou

Bit de validation

Indicateurs de protection en lecture

Indicateurs de protection en écriture

Indicateurs de protection en effacement

Algorithme (D.E.S., TELEPASS)

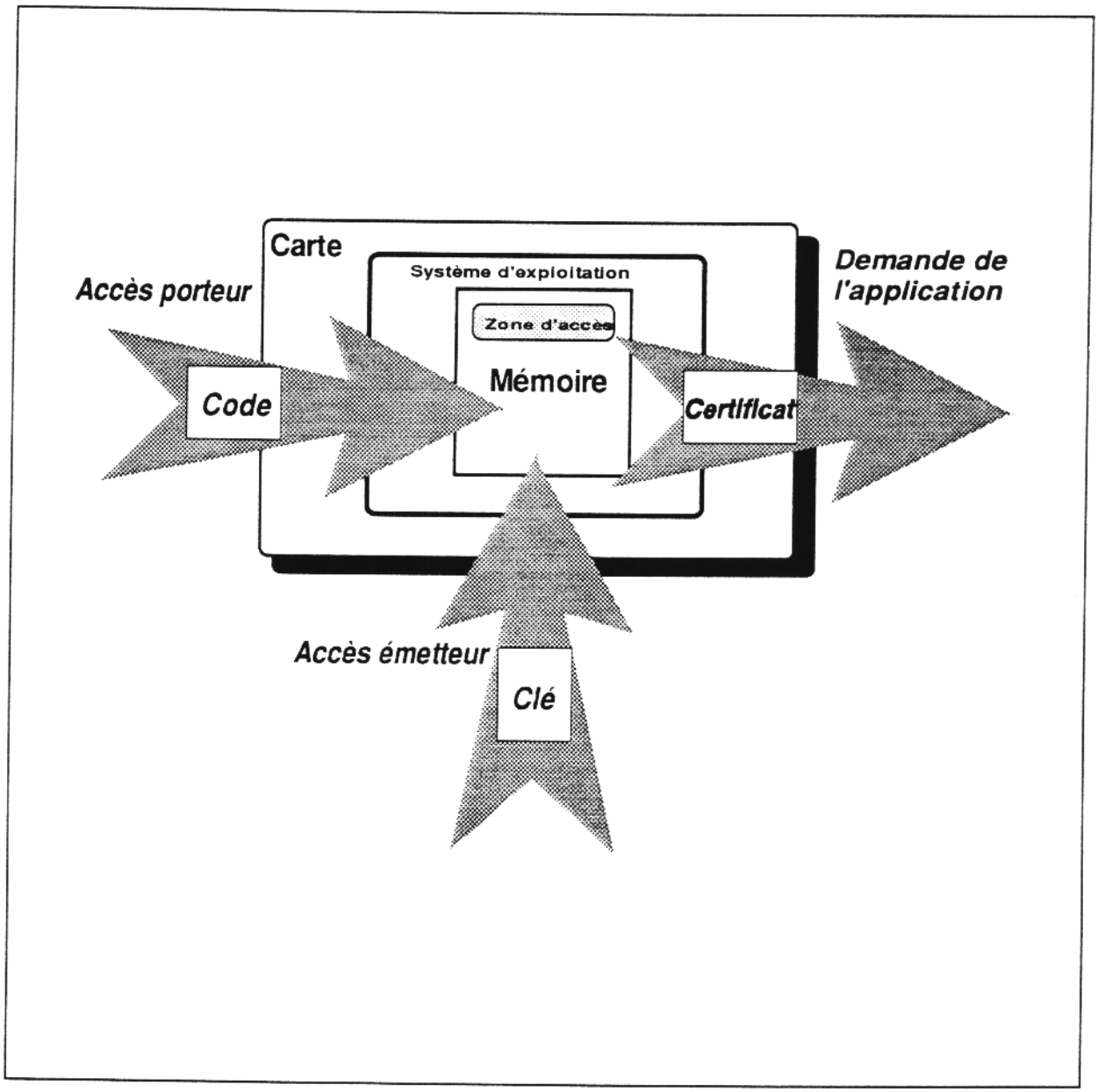

Figure 4.1 - Schéma synthétique des mécanismes sécuritaires.

4.2 Ressources cryptographiques

La cryptographie consiste à coder une information de telle manière qu'elle soit déchiffrable par le destinataire et l'émetteur seulement.

L'action de coder l'information est mise en oeuvre par un algorithme dit cryptographique.

Algorithmes cryptographiques

Les algorithmes utilisés par la famille SCOT sont :

- algorithme TELEPASS,

- algorithme D.E.S..

Ce sont des fonctions logico-mathématiques qui font correspondre à un ensemble de paramètres d'entrée un résultat.

Algorithme TELEPASS

Il peut être formulé ainsi : **R = F (E, ADR, [ADR], S)**

R	résultat obtenu
F	fonction

Paramètres d'entrée :

E	message d entree (48 bits ; eventuellement nombre aleatoire)
ADR	adresse d'un mot contenu dans une des zones accessibles en lecture (16 bits)
[ADR]	contenu du mot situé à l'adresse ADR (32 bits)
S	jeu secret mémorisé dans la zone secrète (96 bits).

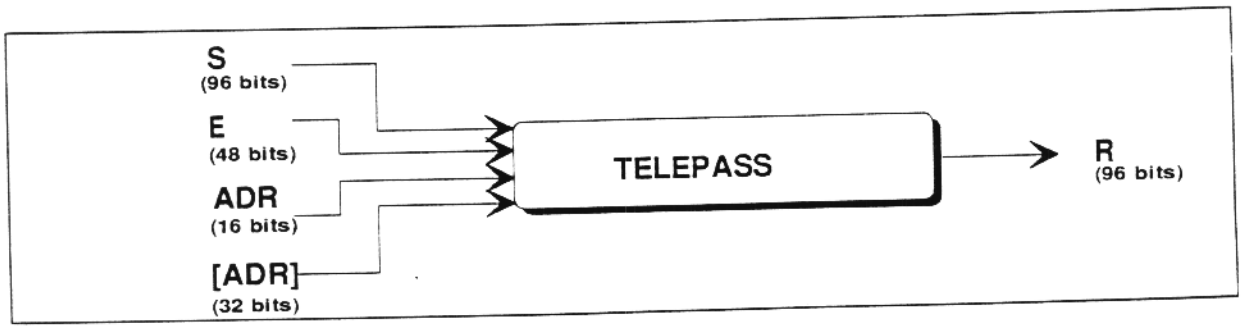

Figure 4.2 - Représentation de l'"Algorithme TELEPASS".

Algorithme D.E.S.

D.E.S. signifie Data Encryption Standard :

système de chiffrement de données défini par IBM, basé sur l'existence de clés uniques conduisant à environ 10^{18} combinaisons.

Cette fonction est bijective.

Elle peut être formulée ainsi :

R = F (E, CLE)

R	résultat (64 bits)
F	fonction dans son sens direct
E	message d'entrée (64 bits)
CLE	nombre secret utilisé par D.E.S. (64 bits)

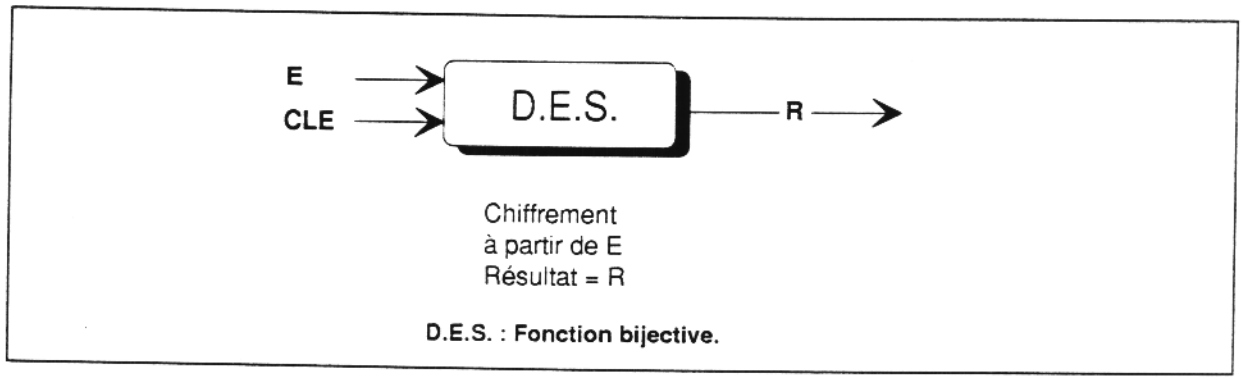

Figure 4.3 - Représentation de l'"Algorithme D.E.S.".

Application à la carte

Mise en oeuvre de TELEPASS

L'algorithme est présent dans la carte, il est utilisé pour la certification (voir la section "Certification et authentification carte" de ce chapitre).

R = F (E, ADR, [ADR], S)

Paramètres envoyés à la carte	Paramètres présents dans la carte
E et ADR	[ADR] et S

Mise en oeuvre de D.E.S.

La notation **CLE** de la fonction D.E.S., ne désigne pas une clé au sens clé émetteur, mais un nombre secret qui, en l'occurrence pour le CAD et la carte, est le jeu secret.

Dans le CAD, l'algorithme D.E.S. est présent dans le sens inverse :

$E = F^{-1}$ (R, CLE)

il est utilisé pour le chiffrement des clés : clés utilisées pour l'accès à la mémoire de la carte.

En résumé, les clés sont chiffrées dans le CAD par D.E.S. avec CLE (jeu secret).

Dans la carte, l'algorithme est présent dans le sens direct :

R = F (E, CLE)

il est utilisé pour le déchiffrement des clés et pour la certification (voir les sections suivantes).

En résumé, les clés sont déchiffrées dans la carte par D.E.S. avec CLE (jeu secret).

Attention

Le système d'exploitation ne délivre aucun résultat de calcul de D.E.S. à l'extérieur de la carte.

Paramètre envoyé à la carte	Paramètre présent dans la carte
E	CLE

4.3 Gestion des clés, des codes et du jeu secret

Les clés, les codes et le jeu secret jouent un rôle primordial dans la vie de la carte. Suivant les phases de la vie de la carte, certaines clés ou codes sont utilisées pour protéger l'accès à la carte. Le jeu secret intervient dans les chiffrements.

Clés et codes utilisés

Nom de la clé ou du code	Présence	Taille
Clé émetteur **1A**	obligatoire	2 mots
Clé émetteur **1B**	facultative	2 mots
Code porteur **2A**	facultative	1 ou 2 mots
Code porteur **2B**	obligatoire	1 ou 2 mots
Clé de déblocage **concaténation** de Clé **1A** et Code **2A** ou **2B**	obligatoire	3 ou 4 mots

Jeu secret

Le jeu secret est constitué de 3 mots (96 bits) inscrits en phase de personnalisation dans la zone secrète de la carte.

Utilisation par TELEPASS : les 3 mots sont utilisés.

Utilisation par D.E.S. : seulement 64 bits sont utilisés comme le montre le tableau représentant les octets utiles de chacun des 3 mots.

Jeu secret	Octet 1	Octet 2	Octet 3	Octet 4
Mot 1		X	X	X
Mot 2		X	X	X
Mot 3		X	X	

Diversification

Pour une application donnée, toutes les cartes peuvent avoir la même clé 1A ou bien chacune sa propre clé ; dans ce dernier cas, la clé 1A est dite "diversifiée". Ceci est aussi valable pour la clé 1B, le jeu secret et le code 2A.

Mode de présentation des clés et des codes

La présentation des clés ou des codes est utilisée pour protéger les accès à la mémoire de la carte.

Une présentation de clé ou de code étant faite, l'occurrence d'une nouvelle présentation de clé ou code annule la présentation précédente.

La présentation peut se faire de deux manières :

- en clair pour les clés et les codes,
- chiffrée pour les clés.

Le mode de présentation n'est pas imposé par le système d'exploitation.

Présentation en clair

La clé (ou le code) est présentée en clair lorsque sa valeur est transmise telle quelle sans aucun codage.

Présentation chiffrée (réservée aux modèles SCOT 20 DES et SCOT 110 DES)

Seules les clés émetteur et les clés de déblocage peuvent être chiffrées.

La clé est présentée chiffrée lorsque sa valeur est cryptée par un programme dit "module de sécurité" (unité de chiffrement avec l'algorithme D.E.S.) avant d'être transmise.

Nombre de tentatives de présentations de clé ou code

~~Le nombre d'essais de clé ou code au-delà duquel la carte reste bloquée~~ est :

un seul essai de clé émetteur ou de clé de déblocage,

trois essais de code porteur.

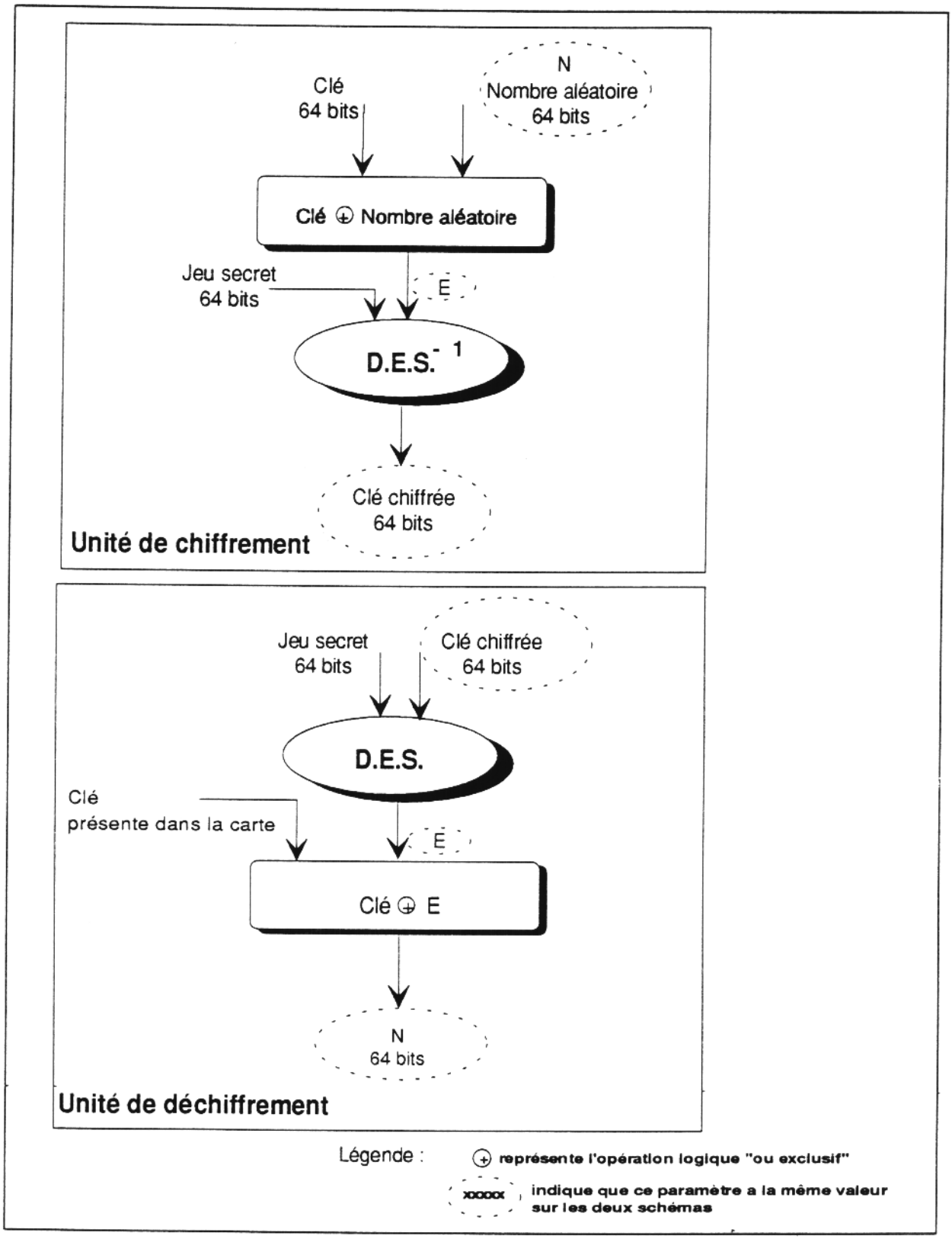

Figure 4.4 - Représentation du chiffrement.

4.4 Présentation de code ou de clé en clair

Présenter un code ou une clé en clair signifie faire reconnaître par la carte la validité d'un code ou d'une clé sans les chiffrer avant de les transmettre.

Mode de présentation

Le code ou la clé transmis est comparé au code ou à la clé présents en mémoire et le résultat de la comparaison est mémorisé par l'unité de calcul.

Sur le schéma ci-dessous, la clé peut être remplacé par le code porteur, la procédure de présentation est identique.

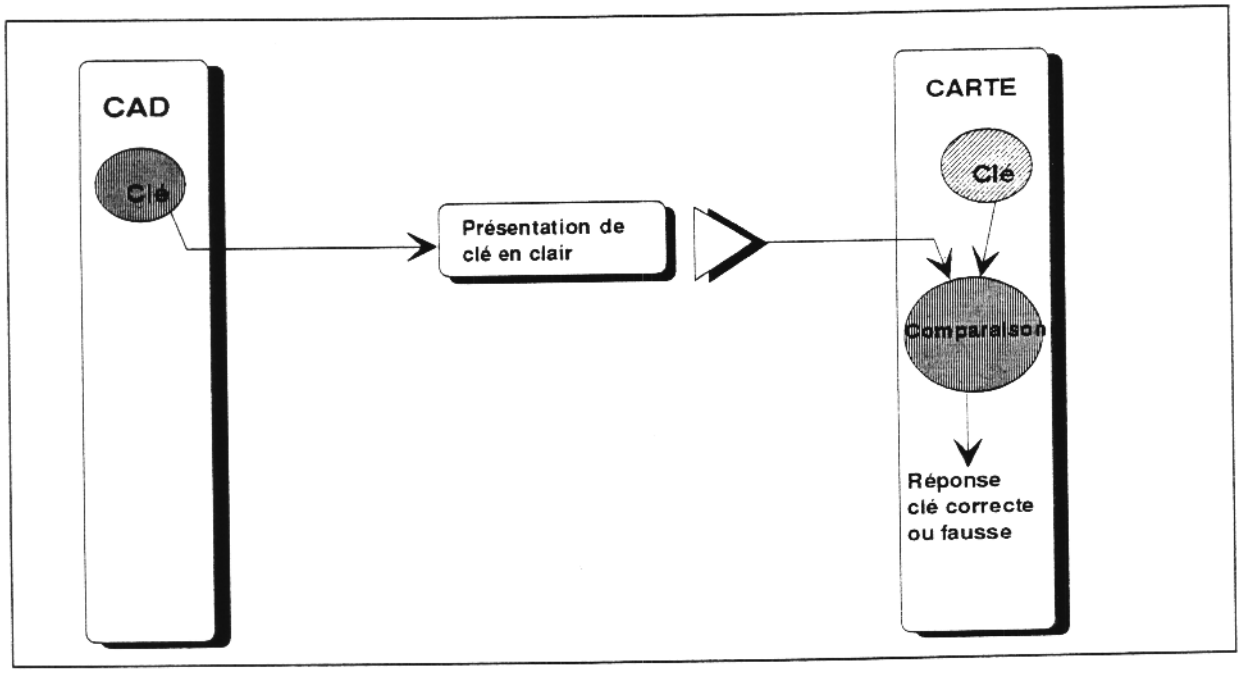

Figure 4.5 - Schéma de la présentation de clé en clair.

Remarque :

Les codes porteur sont toujours présentés en clair.

4.5 Présentation de clé chiffrée

Présenter une clé chiffrée signifie faire reconnaître par la carte la validité d'une clé qui a été chiffrée avant de la transmettre.

Mode de présentation

Le résultat du chiffrement est transmis à la carte qui déchiffre et le résultat est comparé à la clé présente en mémoire. Le résultat de la comparaison est mémorisé par l'unité de calcul.

Le nombre aléatoire est utilisé pour toutes les présentations de clé chiffrée d'une même session (mise sous tension). Toutefois, si une présentation de clé erronée se produit, une nouvelle demande de nombre aléatoire est nécessaire pour les présentations suivantes de clé chiffrée.

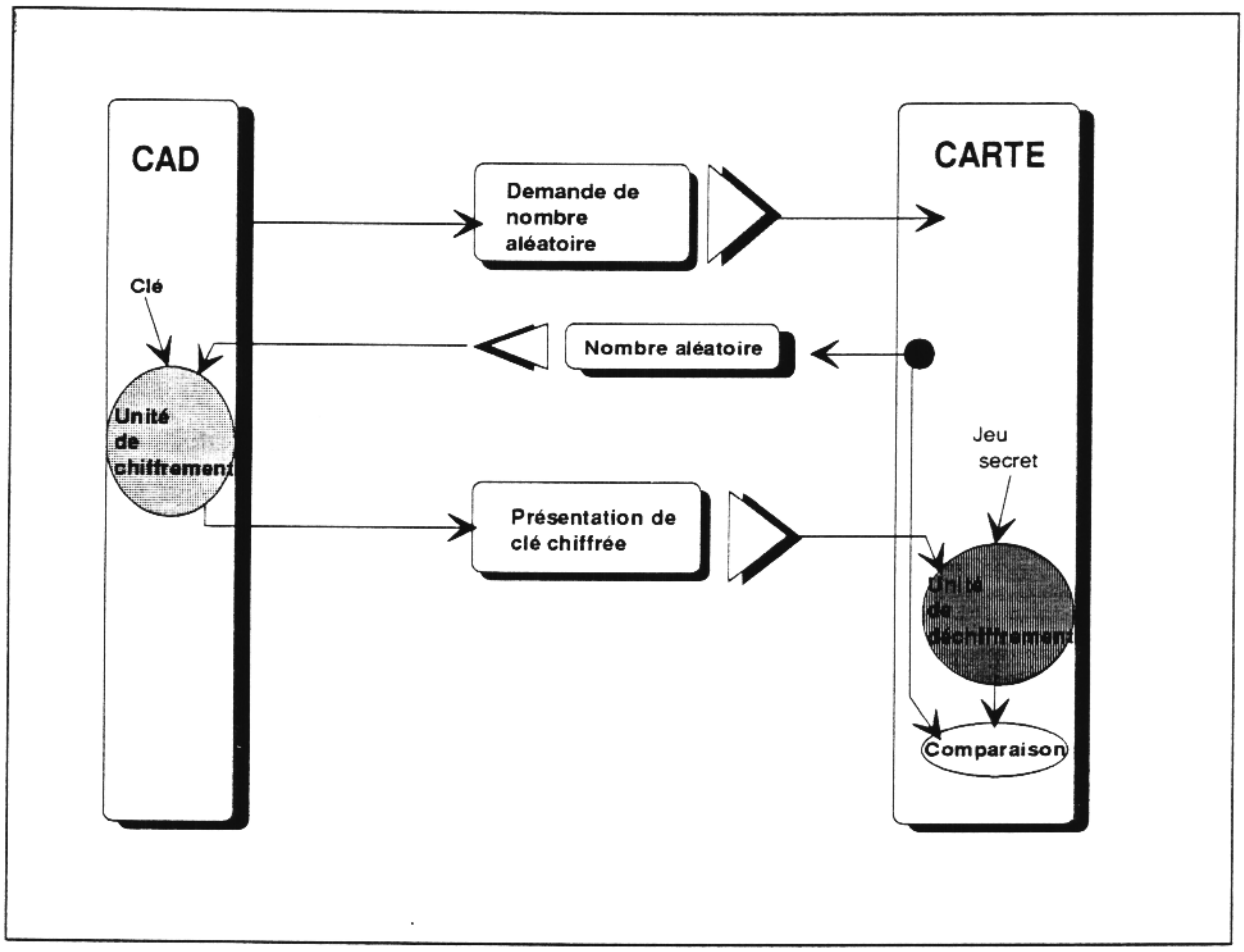

Figure 4.6 - Schéma de la présentation de clé chiffrée.

4.6 Certification et authentification carte

La certification est une preuve de la carte sur une information contenue dans celle-ci.

L'authentification carte consiste à vérifier que la carte a été émise par l'autorité supposée.

La certification et l'authentification mettent en oeuvre la fonction "Calcul de certificat" qui utilise un calcul cryptographique qui est suivant les cas :

- algorithme D.E.S.,
- algorithme TELEPASS.

Certificat

Un certificat est le résultat R (64 bits) d'un calcul cryptographique effectué dans la carte prenant en compte :

- un message d'entrée fourni par le CAD : comprenant un nombre E et une adresse ADR d'un mot (deux derniers octets du message d'entrée) ;
- le jeu secret S et le contenu du mot [ADR],

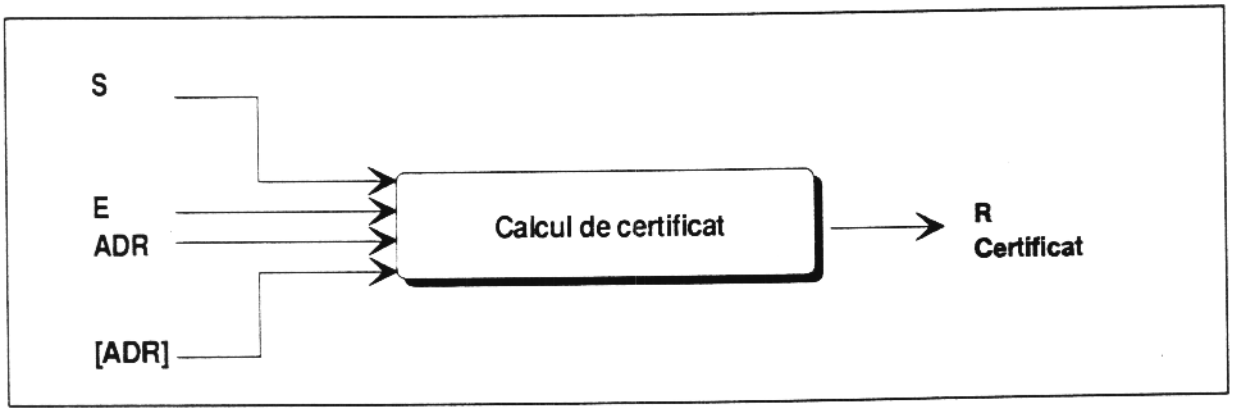

Figure 4.7 - Représentation du calcul de certificat.

Certification d'un mot

La certification d'un mot (32 bits) est une preuve qu'une information donnée à une adresse donnée n'a pas été altérée.

Le contrôle de cette preuve peut être réalisée par le CAD, c'est le contrôle du certificat.

Authentification d'une carte

Pour prouver que la carte en présence est habilitée, le CAD envoie un nombre aléatoire (48 bits) comme message d'entrée d'un calcul de certificat assurant l'unicité de chaque certificat et empêchant la fraude.

Le contrôle du certificat par le CAD conclut l'authentification de la carte en présence.

Contrôle de certificat

Un calcul analogue à celui effectué dans la carte est exécuté dans le CAD afin de comparer les deux résultats.

Le CAD n'utilise alors que des paramètres mémorisés dans sa mémoire, en particulier il est capable de calculer le jeu secret de la carte.

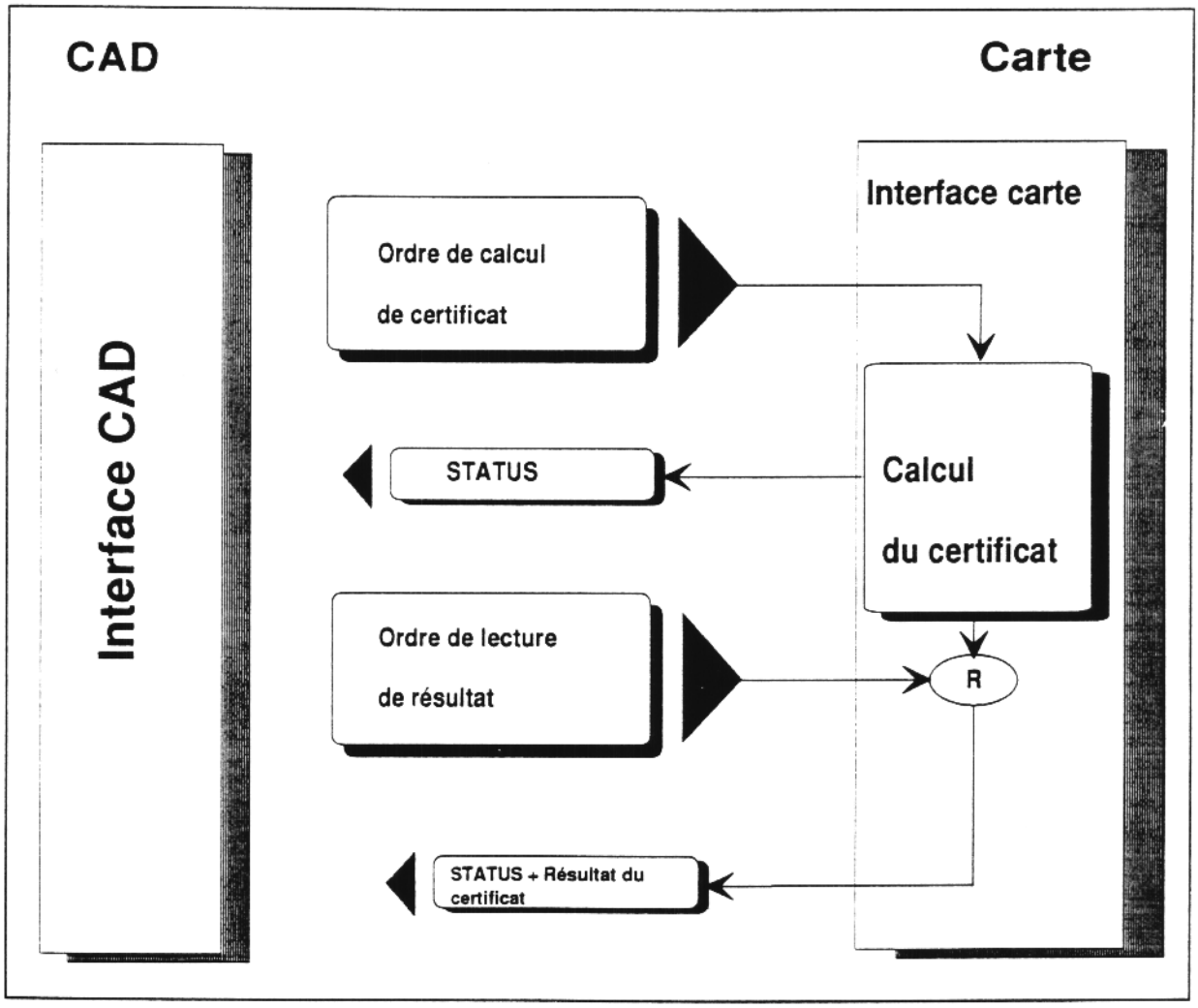

Figure 4.8 - Diagramme général de la certification.

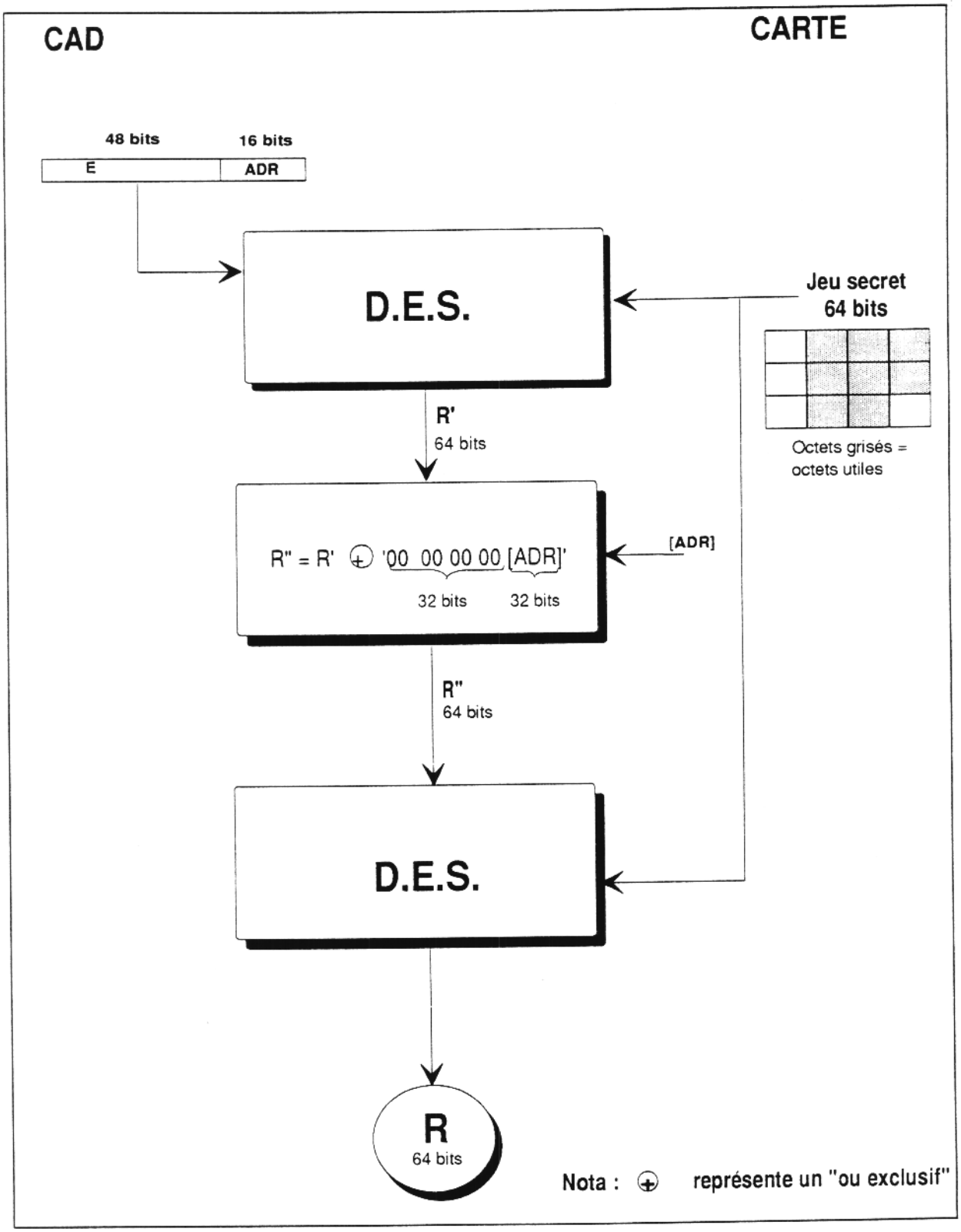

Figure 4.9 - Diagramme du calcul de certificat D.E.S..

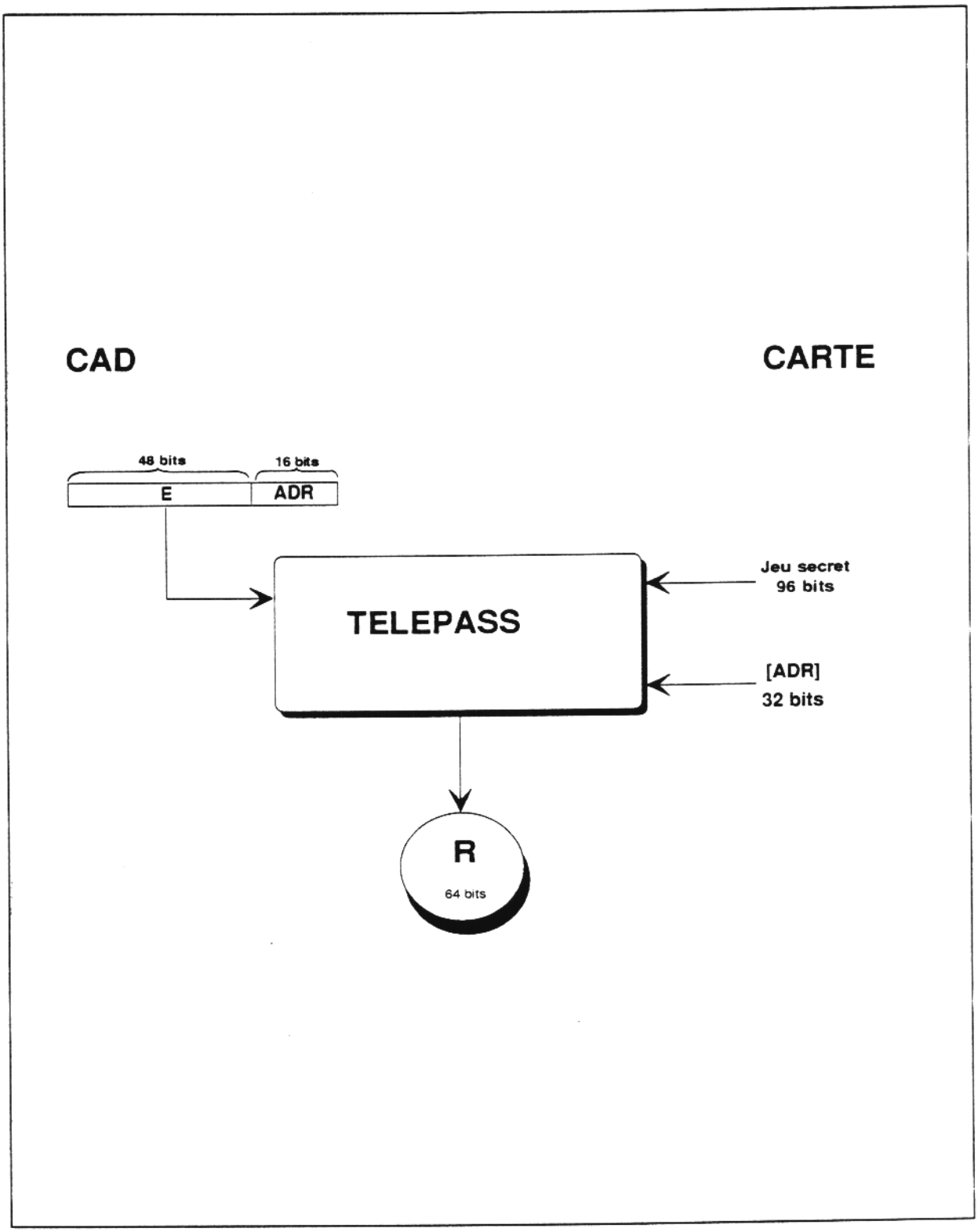

Figure 4.10 - Diagramme du calcul du certificat TELEPASS.

4.7 Présentation de la zone d'accès

Elément essentiel du système anti-fraude, la zone d'accès garde la trace de tous les accès protégés à la carte. Son fonctionnement est interne au système d'exploitation. Toutefois, l'application peut lire la zone d'accès pour vérifier les différentes actions effectuées sur la carte.

Structure de la zone d'accès

La zone d'accès est la zone de la mémoire comprise entre l'adresse ADM (incluse) et l'adresse ADC (exclue).

Les mots de cette zone n'ont pas de bits système (voir section "Structure d'un mot" du chapitre "FAMILLE SCOT").

Chaque mot est constitué de 8 quartets dits "fenêtres".

Au départ de la phase d'utilisation de la carte, la zone d'accès est vierge (tous les bits sont à 1).

Fenêtre courante

La gestion de la zone d'accès est organisée autour du concept de fenêtre.

La fenêtre courante est la fenêtre active à un moment donné :

- au début de la phase d'utilisation c'est la première fenêtre de la zone d'accès,

- au cours de l'exploitation de la carte, la fenêtre courante est la fenêtre qui précède la première fenêtre vierge.

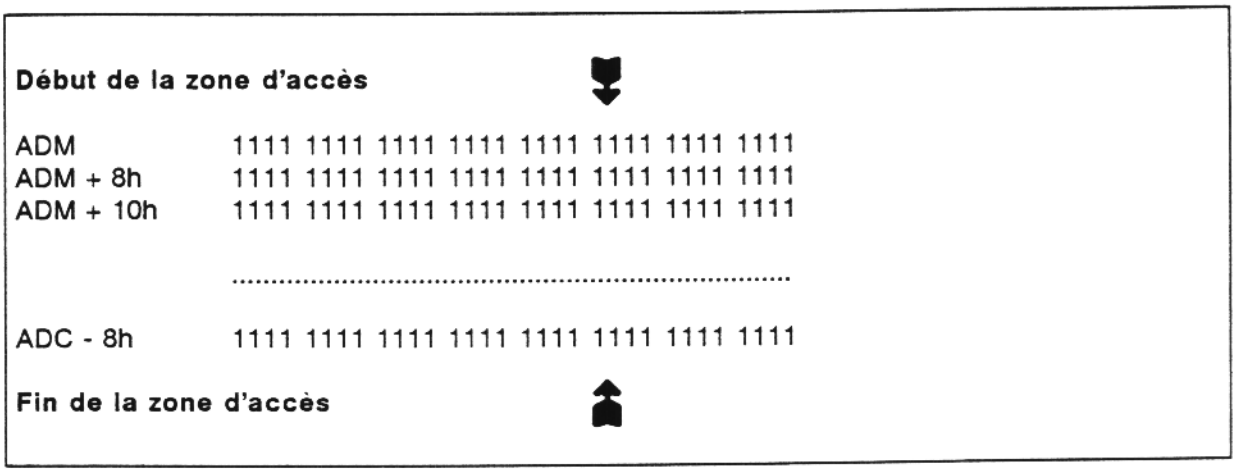

Figure 4.11 - Schéma de la zone d'accès au début de la phase d'utilisation.

Mode d'écriture dans la zone d'accès

Le système d'exploitation écrit dans la zone d'accès en positionnant un bit à 0 dans une fenêtre.

Lorsque toutes les fenêtres sont utilisées la zone est dite pleine ;

elle peut être recyclée dans certaines conditions pour les modèles :

- SCOT 50 et SCOT 60 DES
- SCOT 100 et SCOT 110 DES ;

elle ne peut pas être recyclée pour les modèles :

- SCOT 10 et SCOT 20 DES

et la carte est saturée.

4.8 Gestion de la zone d'accès

Cette section décrit l'utilisation et le codage des fenêtres de la zone d'accès par le système d'exploitation.

Etat des fenêtres

Le tableau ci-dessous décrit les différents états possibles d'une fenêtre.
Dans ce tableau la notation X désigne un bit dont la valeur est 1 ou 0.

Etat de la fenêtre	**Profil binaire correspondant**
Vierge	1111
Pleine	0000
En accès	0XXX
1ère clé ou code correct	0111
2ème clé ou code correct	0011
3ème clé ou code correct	0001
4ème clé ou code correct	0000
En erreur	10X1
1ère erreur code porteur	1011
2ème erreur code porteur	1001
En blocage	1XX0
3ème erreur code porteur	1000
1ère erreur clé 1A, clé 1B ou clé de déblocage	1110

Début de la zone d'accès

ADM	**1111** 1111 1111 1111 1111 1111 1111 1111
ADM + 8h	1111 1111 1111 1111 1111 1111 1111 1111
	.....
ADC - 8h	1111 1111 1111 1111 1111 1111 1111 1111

Fin de la zone d'accès

La zone d'accès est vierge. La fenêtre courante est dans le 1er quartet du mot situé à l'adresse ADM, elle est vierge.

La carte est opérationnelle.

Début de la zone d'accès

ADM	1111 1111 1111 1111 1111 1111 1111 1111
ADM + 8h	1111 1111 1111 1111 1111 1111 1111 1111
	.....
ADM + YYh	0000 0111 1000 **0111** 1111 1111 1111 1111
	.....
ADC - 8h	1111 1111 1111 1111 1111 1111 1111 1111

Fin de la zone d'accès

La fenêtre courante est dans le 4ème quartet du mot situé à l'adresse ADM + YYh, elle est en accès.

La carte est opérationnelle.

Début de la zone d'accès

ADM	1111 1111 1111 1111 1111 1111 1111 1111
	.....
ADM + YYh	0000 0111 1000 0111 **1110** 1111 1111 1111
	.....
ADC - 8h	1111 1111 1111 1111 1111 1111 1111 1111

Fin de la zone d'accès

La fenêtre courante est dans le 5ème quartet du mot situé à l'adresse ADM + YYh, elle est en blocage.

La carte est bloquée.

Figure 4.12 - Exemples de l'état de la zone d'accès.

Gestion des fenêtres

A l'occurrence d'une validation, le système d'exploitation trouve la fenêtre active par la recherche de la dernière fenêtre non vierge ; selon les cas, il positionne un bit de la fenêtre courante ou passe à la fenêtre suivante.

Carte en fonctionnement : la fenêtre active est en accès, en erreur code porteur ou pleine

Les possibilités classées (3 cas) sont présentées dans les tableaux suivants.

1er cas : validation avec clé correcte (code porteur ou clé émetteur)

Fenêtre courante et suivante avant validation	Fenêtre modifiée et suivante ou nouvelle après validation
1111 1111 0111 1111 0011 1111 0001 1111	0111 1111 0011 1111 0001 1111 0000 1111
1011 1111 1001 1111	0011 1111 0001 1111
0000 1111	0000 0111 nouvelle fenêtre

2ème cas : validation avec code porteur incorrect

1111 1111 0XXX 1111	1011 1111 0XXX 1011 nouvelle fenêtre
1011 1111 1001 1111	1001 1111 1000 1111

3ème cas : validation avec clé émetteur incorrecte

1111 1111 0111 1111 0011 1111 0001 1111	1110 1111 0111 1110 nouvelle fenêtre 0011 1110 nouvelle fenêtre 0001 1110 nouvelle fenêtre
1011 1111 1001 1111	mutisme de la carte mutisme de la carte
0000 1111	0000 1110 nouvelle fenêtre

Début de la zone d'accès

ADM	1111 1111 1111 1111 1111 1111 1111 1111
ADM + 8h	1111 1111 1111 1111 1111 1111 1111 1111
ADM + 10h	0000 0111 1110 0111 **1011** 1111 1111 1111
	.....
ADC - 8h	1111 1111 1111 1111 1111 1111 1111 1111

Fin de la zone d'accès

La fenêtre courante, dans le 5ème quartet du mot situé à l'adresse ADM + 10h, est en erreur.

La succession de validations qui ont écrit dans les 5 fenêtres non vierges telles que

0000 0111 1110 0111 1011 est :

4 validations réussies	0000fenêtre pleine
1 validation réussie	0111fenêtre en accès
1 échec de validation (clé émetteur 1A, abandon de la fenêtre courante) nouvelle fenêtre	1110fenêtre en blocage
1 validation avec clé de déblocage réussie	0111fenêtre en accès
1 validation échouée (code porteur 1er essai, abandon de la fenêtre courante) nouvelle fenêtre	1011fenêtre en erreur

Figure 4.13 - Exemple de l'état de la zone d'accès après validation de clés.

Mutisme de la carte

La carte n'accepte pas de présentation de clé émetteur à la suite d'une présentation erronée de code porteur.

ADM + YYh 0000 0111 0011 **1001** 1111 1111 1111 1111

La fenêtre courante est dans le 4ème quartet du mot situé à l'adresse ADM + YYh, elle est en erreur.
Une tentative de validation de clé émetteur dans ce cas conduit au mutisme de la carte.
Seule une validation de code porteur est acceptable.
La carte est restée en erreur.

Figure 4.14 - Exemple de mutisme (validation de clé émetteur).

Carte bloquée : la fenêtre active est en blocage

La carte étant bloquée, la fenêtre courante peut avoir un des deux profils suivants :

- 1000 blocage à la suite de 3 erreurs de code porteur,

- 1110 blocage à la suite d'une erreur clé émetteur.

Seule la présentation de la clé de déblocage permet de débloquer la carte. Cette présentation peut conduire à deux cas :

Clé de déblocage correcte

Une nouvelle fenêtre en accès est ouverte et la carte est débloquée.

Fenêtre courante et suivante avant validation	**Fenêtre modifiée et nouvelle fenêtre après validation**
1000 1111	1000 0111 nouvelle fenêtre
1110 1111	1110 0111 nouvelle fenêtre

Clé de déblocage incorrecte

Une nouvelle fenêtre de blocage est ouverte et la carte reste bloquée.

Fenêtre courante et suivante avant validation	**Fenêtre modifiée et nouvelle fenêtre après validation**
1000 1111	1000 1110 nouvelle fenêtre
1110 1111	1110 1110 nouvelle fenêtre

Début de la zone d'accès

ADM	1111 1111 1111 1111 1111 1111 1111 1111
ADM + YYh	0000 0111 1000 1110 **0111** 1111 1111 1111
ADC - 8h	1111 1111 1111 1111 1111 1111 1111 1111

Fin de la zone d'accès

La fenêtre courante est dans le 5ème quartet du mot situé à l'adresse ADM + YYh. La fenêtre précédente était en blocage.

La clé de déblocage était correcte et a permis de prendre une nouvelle fenêtre en accès 0111.

La carte est opérationnelle.

Début de la zone d'accès

ADM	1111 1111 1111 1111 1111 1111 1111 1111
ADM + YYh	0000 0111 1000 **1110** 1111 1111 1111 1111
ADC - 8h	1111 1111 1111 1111 1111 1111 1111 1111

Fin de la zone d'accès

La fenêtre courante est dans le 4ème quartet du mot situé à l'adresse ADM + YYh. La fenêtre précédente était en blocage.

La clé de déblocage était incorrecte et la nouvelle fenêtre est en blocage 1110.

La carte est bloquée.

Figure 4.15 - Exemples de déblocages.

Remplissage de la zone d'accès

Lorsque elle est pleine, la zone d'accès est suivant les modèles :

- recyclée (modèles SCOT 50 à SCOT 110 DES sauf un cas d'exception décrit dans le paragraphe "Saturation" ci-après),

- saturée (modèles SCOT 10 et SCOT 20 DES).

Ces deux cas sont décrits ci-après.

Recyclage de la zone d'accès

Les zones d'accès des modèles SCOT 50 à SCOT 110 DES peuvent être recyclées.

La zone d'accès est recyclée partiellement et totalement évitant ainsi la saturation.

Recyclage partiel

Dès qu'une première écriture a lieu dans la première fenêtre d'un mot, le mot précédent est recyclé, c'est-à-dire tous ses bits remis à 1.

Recyclage total

A condition que le dispositif de sécurité (décrit dans le paragraphe "Saturation" page suivante) soit mis en oeuvre, dès que l'écriture a lieu dans le dernier octet (donc dans l'avant-dernière fenêtre), cette fenêtre est recopiée dans la première fenêtre de la zone d'accès et le dernier mot est recyclé c'est-à-dire tous ses bits remis à 1.

Conditions particulières du recyclage total

Le système d'exploitation relit, octet par octet, tous les mots de la zone d'accès en remontant de la fin vers le début (vers ADM) et s'arrête au premier octet non vierge (2 fenêtres).

Cette méthode assure que la zone d'accès est bien entièrement vierge.

Exemple d'un extrait de mémoire :

avant recyclage partiel

ADM + YYh	0000 0111 1000 1110 0111 1000 0000 0000 1111 1111 1111 1111 1111 1111 1111 1111

après recyclage partiel

ADM + YYh	1111 1111 1111 1111 1111 1111 1111 1111 0111 1111 1111 1111 1111 1111 1111 1111

Figure 4.16 - Exemple de recyclage partiel.

Exemple d'un extrait de mémoire : premier mot et dernier mot de la zone d'accès

avant recyclage total

ADM	1111 1111 1111 1111 1111 1111 1111 1111
	.....
ADC - 8h	0000 0111 1000 1110 0111 1000 **0111** **1111**

après recyclage total

ADM	**0111** 1111 1111 1111 1111 1111 1111 1111
	.....
ADC - 8h	1111 1111 1111 1111 1111 1111 1111 1111

Figure 4.17 - Exemple de recyclage total.

Saturation

La carte est saturée lorsque la zone d'accès est remplie et qu'elle ne peut pas être recyclée.

Saturation : modèles SCOT 10 et SCOT 20 DES

La saturation intervient lors de la première écriture dans l'avant-dernière fenêtre. Le recyclage n'est pas possible.

Saturation : modèles SCOT 50 à SCOT 110 DES

Le dispositif de sécurité de la zone d'accès mis en oeuvre sur ces modèles est le suivant :

lorsque deux cas de blocage interviennent successivement en fin de zone d'accès, celle-ci ne peut pas être recyclée.

Pour faciliter l'explication, le dernier mot de la zone d'accès est représenté avec ses 8 fenêtres ci-dessous :

S	T	U	V	W	X	Y	Z

les 4 dernières fenêtres sont W, X, Y, Z, la dernière étant la fenêtre Z.

Si l'état de

- la fenêtre X est 1XX0 (cas de blocage)
- la fenêtre Y est 1110 (cas de blocage)

comme le montre l'exemple :

W	X	Y	Z
10X1	1XX0	1110	1111

la carte est saturée : elle ne peut plus être utilisée sauf pour des accès non protégés.

- 5 -

DIALOGUE CARTE - CAD

5 DIALOGUE CARTE - CAD

5.1 Introduction

Le dialogue CAD - Carte s'effectue à l'aide d'ordres. Ce chapitre présente la nature des informations échangées, leur format et le protocole d'échange.
La remise à zéro décrite dans ce chapitre est une fonction particulière, non incluse dans le jeu d'ordres, qui initialise le dialogue.
La norme 7816/3 est respectée par la famille SCOT.

Fonctions de dialogue

Le dialogue consiste à échanger des informations dans le but d'effectuer dans la carte :

- écriture
- lecture
- présentation de clé ou de code
- validation de clé ou de code
- recherche
- calcul de certificat
- lecture de résultat
- effacement (excepté SCOT 10 et SCOT 20 DES).

Eléments de dialogue

Les informations échangées sont formatées en octets. Un échange est constitué de 1 à n octets.

Sens du dialogue

Le sens du dialogue est défini de la manière suivante :

- **Entrant** signifie échange du CAD vers la carte
- **Sortant** signifie échange de la carte vers le CAD.

En réalité, au cours du déroulement d'un ordre, des échanges s'effectuent dans les deux sens. Le qualificatif Entrant ou Sortant s'applique au sens de transmission des données (lues, écrites dans la carte etc.) et non aux éléments nécessaires à l'exécution de l'ordre lui-même (initialisation de l'ordre, compte-rendu).

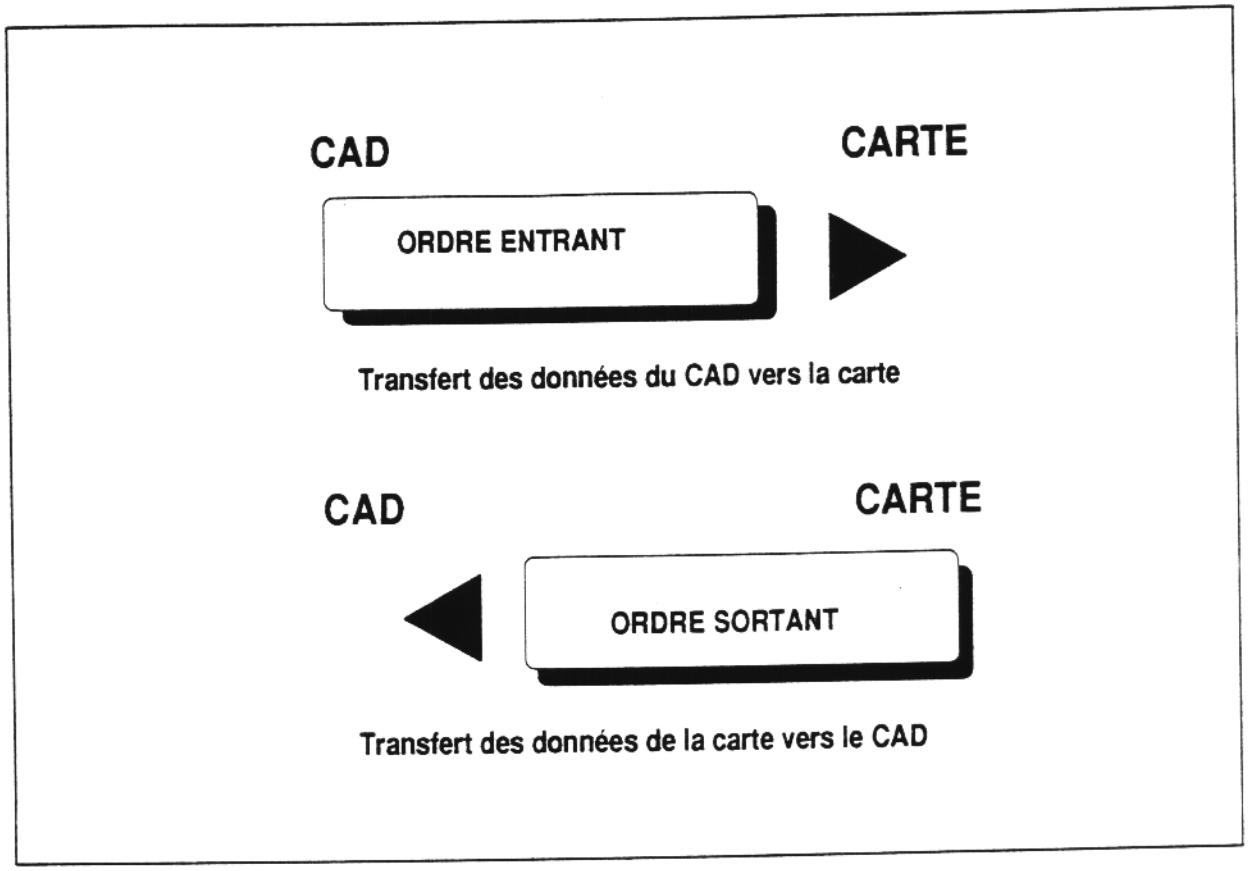

Figure 5.1 - Représentation de l'ordre entrant et de l'ordre sortant.

Mode du dialogue

Les échanges entre le CAD et la carte se font selon deux modes :

- le mode simple
- le mode asservi

Mode simple

Ce mode désigne l'échange en un seul train d'octets.

Mode asservi

Ce mode désigne l'échange en plusieurs trains d'octets sous le contrôle du système d'exploitation.

Octet d'acquittement

Dans ces deux modes d'échange, un octet d'acquittement est envoyé par le système d'exploitation au CAD.

L'octet d'acquittement renseigne sur le mode de dialogue comme le montre le tableau suivant où INS est le code hexadécimal de l'ordre transmis (exemple INS = D0h).

Valeur de l'octet d'acquittement	Mode et tension VPP
INS	Simple
$\overline{\text{INS}}$	Asservi
INS + 1	Simple + VPP
$\overline{\text{INS + 1}}$	Asservi + VPP

Tension de programmation VPP

Cette tension est demandée au CAD par les modèles SCOT 10 et SCOT 20 DES pour les ordres de validation, les ordres d'écriture et l'ordre de demande de nombre aléatoire.

5.2 Déroulement d'un ordre

Le déroulement d'un ordre est partagé en trois phases :

- phase d'initialisation
- phase d'exécution
- phase de fin.

Phase d'initialisation

L'initialisation consiste à l'envoi par le CAD des 5 octets décrits dans la section suivante "Eléments d'un ordre".

Phase d'exécution

Les étapes de l'exécution d'un ordre entrant sont :

- vérification des conditions d'exécution de l'ordre,
- réception des données envoyées par le CAD.
- exécution de la fonction de l'ordre.

Les étapes de l'exécution d'un ordre sortant sont :

- vérification des conditions d'exécution de l'ordre,
- exécution de la fonction de l'ordre,
- émission des données par la carte vers le CAD.

Phase de fin

La fin consiste au renvoi par la carte au CAD de 2 octets dits mots d'état ou STATUS (décrits dans la section "Eléments d'un ordre").

ME1 renseigne sur la syntaxe des 5 premiers octets de l'ordre exécuté.

ME2 renseigne sur le résultat de l'exécution de l'ordre.

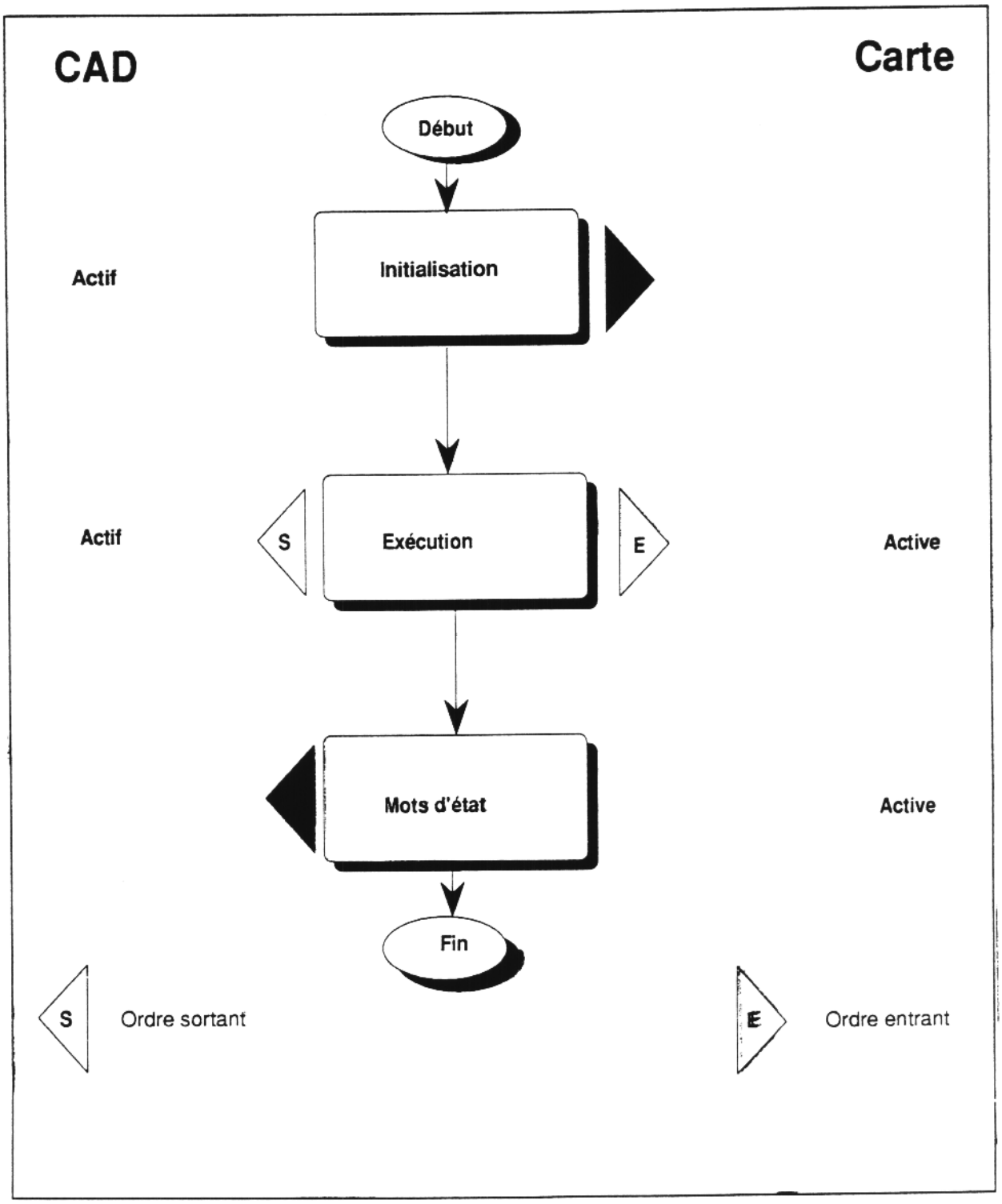

Figure 5.2 - Schéma simplifié du déroulement d'un ordre.

5.3 Eléments d'un ordre

Un ordre est matérialisé par un ensemble d'octets envoyés par le CAD à la carte. L'exécution peut entraîner un dialogue avec échange de données dans le sens entrant ou sortant terminé par un compte-rendu envoyé par la carte.

Format d'un ordre

Un ordre est constitué de 5 octets accompagnés ou non de données (DATA).

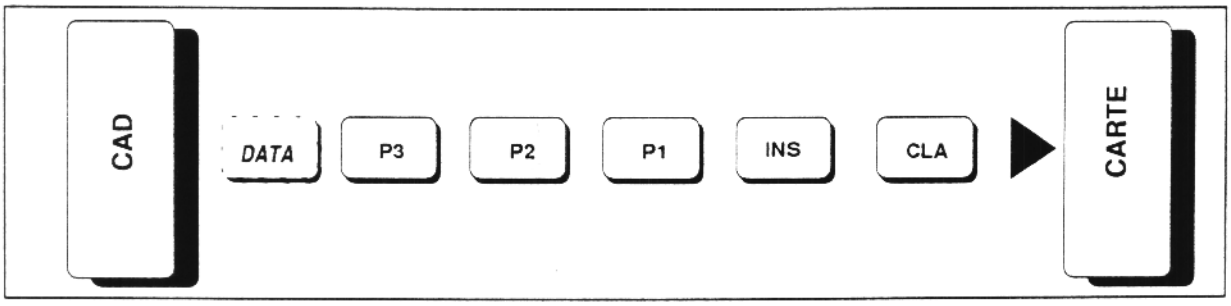

Figure 5.3 - Composition d'un ordre

CLA

Définit la classe des instructions.
CLA = BCh pour les systèmes d'exploitation SCOT.

INS

Code hexadécimal de l'ordre dans la classe des instructions.
Le bit de poids faible est toujours à 0 :

INS = XYh avec Yh = [0, 2, 4, 6, 8, A, C, E].

De plus, le quartet de poids fort X ne peut être égal ni à 6 ni à 9.

P1, P2

Eléments complétant l'ordre, par exemple pour les ordres de lecture et écriture : adresse absolue de lecture ou écriture.

P3

Longueur en octets des données à transférer (s'il y a lieu) pendant l'exécution de l'ordre.

P3 = [0 à 255] soit en hexadécimal [00h à FFh]
P3 = 0, dans le cas d'un ordre sortant, provoque le transfert de 256 octets de la carte au CAD.

DATA

Les données éventuelles sont fournies dans l'entité DATA.

Suivant les ordres DATA peut contenir :

- données à écrire dans la mémoire,
- argument à rechercher,
- adresse de fin d'effacement,
- clé,
- données pour calcul de certificat,
- code porteur.

Lorsque DATA n'existe pas, ceci est signalé dans les exemples par la mention "aucune".

CLA	= BCh	Classe d'instruction
INS	= B0h	Code opératoire de la lecture
P1	= 10h	Adresse poids forts
P2	= D0h	Adresse poids faibles
P3	= 08h	Longueur des données à lire
DATA	= Aucune	

Cet exemple provoque la lecture de 8 octets à l'adresse 10D0h.

Figure 5.4 - Exemple d'initialisation d'un ordre de lecture.

Compte-rendu de la carte

Mots d'états

La conclusion de l'exécution d'un ordre ou de la remise à zéro est matérialisée par l'envoi par la carte de 2 octets au CAD :

- ME1
- ME2.

Ces mots d'état ont la signification décrite dans le tableau ci-après.

ME1	**ME2**
6Eh erreur de classe d'instruction	sans signification
6Dh erreur de code opératoire	sans signification
90h ordre exécuté	significatif (voir ci-après)

Octet ME2

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

La valeur 1 est significative :

IF = 1 - carte saturée (zone d'accès saturée) ;

IT = 1 - carte bloquée ;

IE2 = 1 - carte en erreur code porteur (2 erreurs successives) ;

IE1 = 1 - carte en erreur code porteur (1 erreur) ;

CCF = 1 - cas de déblocage : code porteur erroné ;
- argument absent lors d'une recherche ;

CF = 1 - clé ou code porteur faux lors d'une validation ;
- accès dans une zone inaccessible :
  en recherche,
  ou en effacement (sauf SCOT 10 et SCOT 20 DES) ;

ER = 1 - tentative d'écriture sur un mot déjà validé ;
- erreur d'effacement ;
- octet de sécurité (défaut dans la carte).

ME2 = 00h	➡ Fonctionnement normal de la carte.
ME2 = 40h	➡ Carte bloquée.
ME2 = 80h	➡ Carte saturée.

Figure 5.5 - Exemples de mot d'état ME2.

5.4 Remise à zéro

A l'introduction de la carte dans le CAD, celui-ci applique au contact RAZ de la carte un signal électrique entraînant l'exécution de la fonction "Remise à zéro" conformément à la norme ISO 7816-3.

Rôle de la remise à zéro

Le microcalculateur, avant de recevoir un ordre du CAD, doit s'initialiser et spécifier au CAD ses caractéristiques propres.

Format de la réponse à remise à zéro

La carte envoie 9 octets au CAD :

4 octets "système" significatifs de l'interface carte,

5 octets "application" significatifs du système d'exploitation de la carte.

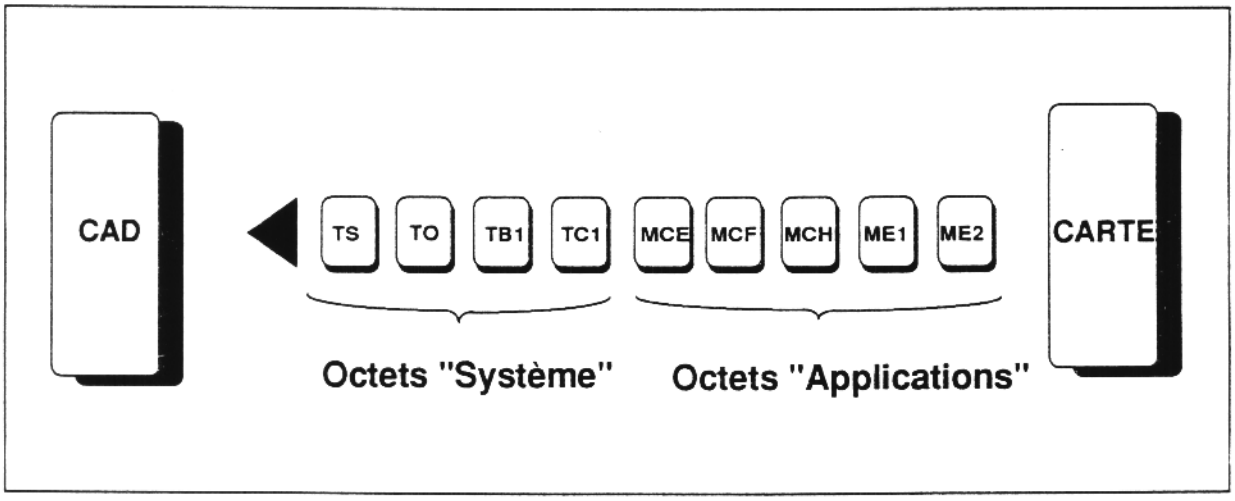

Figure 5.6 - Octets de réponse à remise à zéro.

Octets système

TS = 3Fh Spécifie que les données sont transmises :

- poids forts en tête,
- parité paire,
- fréquence 3,579545 Mhz.

TO = 65h Spécifie la présence des octets système TB1, TC1 et qu'il y a 5 octets caractérisant l'application.

TB1 Définit la tension et l'intensité maximales de courant de programmation.

SCOT 10, SCOT 20 DES TB1 = 2Fh (VPP = 15 V)
SCOT 100, SCOT 110 DES TB1 = 25h (VPP = 5 V)
SCOT 50, SCOT 60 DES TB1 = 25h (VPP = 5 V)

TC1 Définit l'intervalle maximal séparant l'émission par le CAD de deux octets.

TC1 = 00h pour la famille SCOT.

Remarque :

TA1 et TD1, normalement prévus par la norme, ne sont pas renvoyés par la carte ; le CAD doit donc adopter des valeurs par défaut définies par la norme.

Octets d'application

Ces octets permettent à l'application de connaître :

- l'identification de la carte en présence,
- la phase de vie dans laquelle se trouve la carte,
- le compte-rendu exact de la dernière fenêtre active de la zone d'accès.

MCE	MCF	MCH	ME1	ME2

Figure 5.7 - Octets "application".

Octet MCE

Identifie le numéro du composant présent dans la carte.

MCE = 11h SCOT 10, SCOT 20 DES
MCE = 21h SCOT 100, SCOT 110 DES
MCE = 24h SCOT 50, SCOT 60 DES

Octet MCF

Numéro du système d'exploitation.

MCF = 9 pour les systèmes d'exploitation de la famille SCOT.

Octet MCH

Octet des verrous, renseigne sur l'état des verrous (donc la phase de vie de la carte) et le niveau de protection de la zone de transactions.

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

Figure 5.8 - Octets des verrous MCH.

Logique des bits : le bit positionné = 1 ; le bit non positionné = 0.

ILU	= 1	Phase code porteur 2A actif terminée
ILC	= 1	Phase de personnalisation terminée
ILF	= 1	Phase de fabrication terminée
IIV	= 1	Carte invalidée
IEP	= 1	Zone de travail 1 (transactions) protégée en écriture
ILP	= 1	Zone de travail 1 (transactions) protégée en lecture

Les bits IEC (bits 1 et 0) indiquent la protection en effacement de la zone de travail (zone de travail 1 dans l'option deux zones de travail). Ces bits sont significatifs pour les modèles SCOT 50 à SCOT 110 DES sinon ils sont à la valeur 0.

IEC	= 00	Effacement interdit
	= 01	Effacement soumis au code porteur actif
	= 10	Effacement soumis à la clé 1B
	= 11	Effacement soumis à la clé 1A

Profil des indicateurs pour chaque phase de vie.

Phase de vie de la carte	ILU	ILC	ILF	IIV
Phase de personnalisation	0	0	1	0
Phase utilisation code porteur 2A	0	1	1	0
Phase utilisation code porteur 2B	1	1	1	0
Carte invalidée	X	1	1	1

5.5 Identification d'une carte

L'application identifie le modèle de carte dans la famille SCOT et ses caractéristiques.

Caractéristiques de la carte

- Adresse de fin de mémoire.
- Nombre de zones de travail.
- Type d'algorithme.
- Conditions de protection en lecture, écriture, effacement.

Modèle de carte

Pour détecter le modèle d'une carte, l'application envoie un ordre de remise à zéro puis un ordre de lecture de résultat. La réponse obtenue est l'adresse du premier mot non accessible et les caractéristiques de la carte.

Cette adresse (virtuelle) est caractéristique du modèle de carte, elle est désignée par ADMAX.

ADMAX : est définie dans la section "Description de la mémoire" du chapitre "FAMILLE SCOT".

Exécution d'une remise à zéro

Exécution d'une lecture de résultat

La carte renvoie un résultat R

L'analyse de ce résultat permet de connaître :

- l'adresse de fin de mémoire,
- l'option 1 ou 2 zones de travail,
- l'algorithme,
- l'indication de protection des zones de travail en lecture et écriture.

Figure 5.9 - Reconnaissance du modèle d'une carte.

La description du résultat R, obtenu après une remise à zéro, est donnée dans la section "Lecture de résultat : INS = C0h" du chapitre "JEU D'ORDRES".

- 6 -

JEU D'ORDRES

6 JEU D'ORDRES

6.1 Introduction

Le système d'exploitation dispose d'un jeu d'ordres élémentaires décrits dans ce chapitre.
Cette section décrit la présentation utilisée pour chaque ordre.
L'objectif de chaque ordre est donné dans cet encadrement de début de section.

TYPE et MODE

Le type peut être :

- entrant
- ou sortant.

Le mode peut être :

- simple
- ou asservi.

Ces notions, relatives au sens et au mode d'échange entre le CAD et la carte, sont décrites dans la section "Introduction" du chapitre "DIALOGUE CARTE - CAD".

VPP

Sur certains modèles de carte, une tension particulière "VPP", dite de programmation, est demandée au CAD par certains ordres. Ceci est indiqué à droite du tableau concernant le type et le mode.

Validité

Les ordres ne sont pas tous disponibles pour certains modèles de la famille SCOT. Cette rubrique précise la validité pour chaque modèle.

Fonction

Cette rubrique décrit le fonctionnement de l'ordre.

Conditions d'utilisation

Cette rubrique décrit les conditions nécessaires au fonctionnement et en particulier selon l'état de la carte et selon les modèles.

Réponse de la carte

Cette rubrique indique tous les cas possibles de réponse de la carte :

- mutisme,
- octets ME1, ME2.

La notation X dans les valeurs de ME2 indique une quelconque des valeurs : 0, 1, 2, 4, 8 significatives de l'état de la fenêtre courante.

Le compte-rendu de la carte est décrit fonctionnellement dans la section "Eléments d'un ordre" du chapitre "DIALOGUE CARTE - CAD".

Remarque

Parfois une remarque introduit un fait particulier concernant l'ordre.

Exemple

L'encadré de la page en regard décrit un ou deux exemple(s) numérique(s) d'exécution de l'ordre.

Particularités

Certains ordres contiennent d'autres rubriques utiles pour une bonne utilisation de l'ordre comme :

- des tables d'adresses autorisées,
- la description très détaillée de la réponse de la carte.

ANNEXES

Le lecteur trouve dans les annexes des récapitulatifs concernant :

- les temps d'exécution des ordres,
- les mots d'état,
- l'accessibilité des zones,
- les caractéristiques des ordres.

6.2 Lecture : INS = B0h

Ordre utilisé pour lire dans une zone accessible en lecture protégée ou non protégée.

TYPE	MODE
SORTANT	SIMPLE

Validité : **toute la famille.**

Initialisation

CLA	=	BCh
INS	=	B0h
P1	=	Poids forts de l'adresse quartet de début de lecture
P2	=	Poids faibles de l'adresse quartet de début de lecture
P3	=	Nombre d'octets à lire : 1 à 256 (pour en lire 256, P3 = 00h)
DATA	=	Aucune

Fonction exécutée

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

Conditions d'utilisation

Pour lire un nombre entier de mots à partir d'un mot donné, les conditions suivantes sont nécessaires :

- l'adresse quartet de lecture doit être multiple de 8,
- P3 = nombre d'octets à lire doit être multiple de 4 ou = 0.

Dans les zones en lecture libre : aucune autre condition n'est requise.

Dans les zones protégées :

il est nécessaire d'avoir préalablement présenté une clé (ou un code) (ordre 10h, 20h, 30h, 18h, 28h ou 38h), et avoir eu un résultat positif à la demande de "Validation de clé (ou code) en lecture" (ordre 40h). Ainsi la lecture dans une zone protégée quelconque est possible autant de fois qu'il est nécessaire.

Si le domaine de lecture demandé recouvre en partie une zone inaccessible en lecture, les octets correspondants au dépassement sont transmis à 0.

En cas d'invalidation de la carte, la lecture protégée est soumise à la clé émetteur.

La détermination des domaines autorisés en lecture est détaillée dans le tableau ci-après.

Domaines autorisés en lecture

- Phase d'utilisation -

Option	**Conditions**			**Domaines**
1 seule Zone de Travail	Sans clé	LP1 = 1 ——— LP1 = 0	Pour tout LU	**[ADT, ADMAX[** ——— **[ADL, ADMAX[**
1 seule Zone de Travail	Avec clé	Pour tout LP1	LU = 1 ——— LU = 0	**[ADM-10h, ADMAX[** **[ADM, ADMAX[**
2 Zones de Travail	Sans clé	LP2 LP1 1 1 0 1 0 0 1 0	Pour tout LU	**[ADC, ADMAX[** **[ADT, ADMAX[** **[ADL, ADMAX[** **[ADC, ADT[** ou **[ADL, ADMAX[**
2 Zones de Travail	Avec clé	Pour tout LP2 et LP1	LU = 1 ——— LU = 0	**[ADM-10h, ADMAX[** **[ADM, ADMAX[**

Figure 6.1 - Tableau des domaines autorisés en lecture.

Réponse de la carte

Les octets lus
ME1 = 90h
ME2 = 00h

Mutisme : - 'P1P2' n'adresse pas un mot accessible en lecture,

- carte invalidée et clé émetteur fausse ou non présentée.

Extrait de la mémoire utilisé dans les exemples ci-dessous

1050h 33 05 06 11h
1058h 35 54 52 41h

Lecture des deux premiers mots de la zone de lecture, à l'adresse 1050h.

CLA	= BCh
INS	= B0h
P1	= 10h
P2	= 50h
P3	= 08h
DATA	= Aucune

Réponse de la carte

Les 2 mots lus	= 33 05 06 11 35 54 52 41h
ME1	= 90h
ME2	= 00h

Lecture de 5 octets à partir de l'adresse quartet 1053h.

CLA	= BCh
INS	= B0h
P1	= 10h
P2	= 53h
P3	= 05h
DATA	= Aucune

Réponse de la carte

Les 5 octets lus	= 50 61 13 55 45h
ME1	= 90h
ME2	= 00h

Figure 6.2 - Exemples d'utilisation de "Lecture".

6.3 Ecriture : INS = D0h

Ordre utilisé pour positionner à 0 les bits d'un mot dans une zone accessible en écriture protégée ou non protégée.

TYPE	MODE
ENTRANT	SIMPLE

SCOT 10, SCOT 20 DES : VPP NECESSAIRE

Validité : **toute la famille.**

Initialisation

CLA	=	BCh
INS	=	D0h
P1	=	Poids forts de l'adresse quartet de début d'écriture
P2	=	Poids faibles de l'adresse quartet de début d'écriture
P3	=	04h
DATA	=	32 bits du mot à écrire

Fonction exécutée

Ecriture, à une adresse mot, d'un ou plusieurs bits. La configuration binaire de 32 bits fournie en données indique les bits à positionner à 0.

Conditions d'utilisation

L'adresse est une adresse mot donc multiple de 8.

L'écriture est irréversible : tout bit positionné à 0 ne peut revenir à l'état 1.

Il est impossible d'écrire dans un mot validé (bit V positionné : voir l'ordre "Validation en écriture").

Suivant la spécificité de la zone à écrire :

- non protégée en écriture
- protégée en écriture

le bit V peut être positionné à 0 lors de l'écriture (premier cas), ou il doit être positionné séparément par un ordre de "Validation en écriture" (deuxième cas).

Enfin, l'écriture n'étant pas contrôlée par le système d'exploitation, l'application doit relire les mots afin de s'assurer qu'ils sont corrects.

La détermination des domaines autorisés en écriture est détaillée dans le tableau ci-après.

Domaines: autorisés en écriture

- Phase d'utilisation -

Option	Verrou	Condition	Domaines
1 seule Zone de Travail	LU = 1 uniquement	Code porteur	**[ADM - 10h, ADM[**
	Pour tout LU	F(EP1)	**[ADT, ADL[**
2 Zones de travail	LU = 1 uniquement	Code porteur	**[ADM - 10h, ADM[**
	Pour tout LU	F(EP2) F(EP1)	**[ADC, ADT[** **[ADT, ADL[**

Figure 6.3 - Tableau des domaines autorisés en écriture.

Réponse de la carte

ME1 = 90h

ME2 = 00h écriture correcte,

= 01h mot déjà validé.

Mutisme : - P3 # 04h,

- 'P1P2' adresse un mot inaccessible en écriture,
- 'P1P2' n'est pas un multiple de 8,
- carte invalidée,
- carte saturée.

Positionnement de bits 2 par 2 à des instants différents à partir du premier mot de la zone de transaction (les bits V et C ne sont pas positionnés à 0).

CLA	= BCh
INS	= D0h
P1	= 06h
P2	= 70h
P3	= 04h
DATA	= CF FF FF FFh

Réponse de la carte

ME1	= 90h
ME2	= 00h

Positionnement des deux bits suivants.

CLA	= BCh
INS	= D0h
P1	= 06h
P2	= 70h
P3	= 04h
DATA	= F3 FF FF FFh

Réponse de la carte

ME1	= 90h
ME2	= 00h

Positionnement des deux bits suivants.

CLA	= BCh
INS	= D0h
P1	= 06h
P2	= 70h
P3	= 04h
DATA	= FC FF FF FFh

Réponse de la carte

ME1	= 90h
ME2	= 00h

Valeur résultante du mot d'adresse 0670h :

[0670h]	= C0 FF FF FFh

Figure 6.4 - Exemples d'utilisation de "Ecriture".

6.4 Recherche d'un mot sur argument : INS = A0h

Ordre utilisé pour rechercher, à partir d'une adresse donnée, un mot dont les 16 bits de poids forts sont égaux à une valeur donnée appelée argument.

TYPE	MODE
ENTRANT	SIMPLE

Validité : **toute la famille.**

Initialisation

CLA	=	BCh
INS	=	A0h
P1	=	Poids forts de l'adresse de début de recherche
P2	=	Poids faibles de l'adresse de début de recherche
P3	=	02h
DATA	=	Argument sur 2 octets

Fonction exécutée

Le système d'exploitation recherche le premier mot à partir de l'adresse 'P1P2' dont les 16 bits de poids forts sont égaux à DATA.

Conditions d'utilisation

L'adresse doit être multiple de 8.

Cet ordre ne s'exécute jamais seul, il doit être suivi d'un ordre de lecture de résultat.

Dans les zones en lecture libre :

aucune condition n'est requise.

Dans les zones protégées en lecture :

il est nécessaire d'avoir préalablement présenté une clé ou un code (ordre 10h, 20h, 30h, 18h, 28h ou 38h), et avoir eu un résultat positif à la demande de validation de clé ou de code en lecture (ordre 40h). Ainsi la recherche dans une zone protégée quelconque est possible autant de fois qu'il est nécessaire.

Si la carte est invalidée, une présentation de clé émetteur est nécessaire.

La détermination des domaines de recherche autorisés est détaillée dans le tableau ci-après. Ce tableau est identique à celui des domaines autorisés en lecture.

Domaines autorisés en recherche

- Phase d'utilisation -

Option	**Conditions**			**Domaines**
1 seule Zone de Travail	Sans clé	LP1 = 1 LP1 = 0	Pour tout LU	**[ADT, ADMAX[** **[ADL, ADMAX[**
1 seule Zone de Travail	Avec clé	Pour tout LP1	LU = 1 LU = 0	**[ADM-10h, ADMAX[** **[ADM, ADMAX[**
2 Zones de Travail	Sans clé	LP2 LP1 1 1 0 1 0 0 1 0	Pour tout LU	**[ADC, ADMAX[** **[ADT, ADMAX[** **[ADL, ADMAX[** **[ADC, ADT[** ou **[ADL, ADMAX[**
2 Zones de Travail	Avec clé	Pour tout LP2 et LP1	LU = 1 LU = 0	**[ADM-10h, ADMAX[** **[ADM, ADMAX[**

Figure 6.5 - Tableau des domaines autorisés en recherche.

Réponse de la carte

ME1	=	90h	
ME2	=	00h :	argument trouvé,
	=	X4h :	l'adresse de début de recherche est dans une zone protégée en lecture et aucune clé ou code n'a préalablement été présentée et validée ; ou zone inaccessible,
	=	X8h :	argument non trouvé.
Mutisme :	-	'P1P2' n'est pas un multiple de 8,	
	-	P3 # 02h,	
	-	carte invalidée et clé émetteur fausse ou non présentée.	

Recherche du mot dont les 16 bits de poids forts = 0CABh à partir de l'adresse 1050h

CLA	= BCh
INS	= A0h
P1	= 10h
P2	= 50h
P3	= 02h
DATA	= 0CABh

Réponse de la carte

ME1	= 90h
ME2	= 00h

L'exécution à la suite d'un ordre "Lecture de résultat" permet d'obtenir l'adresse trouvée.

Figure 6.6 - Exemple d'utilisation de "Recherche d'un mot sur argument".

6.5 Recherche du premier mot vierge : INS = A0h

Ordre utilisé pour rechercher à partir d'une adresse donnée, un mot dont aucun bit n'est positionné.

TYPE	MODE
ENTRANT	SIMPLE

Validité : **toute la famille.**

Initialisation

CLA	=	BCh
INS	=	A0h
P1	=	Poids forts de l'adresse de début de recherche
P2	=	Poids faibles de l'adresse de début de recherche
P3	=	00h
DATA	=	Aucune

Fonction exécutée

Le système d'exploitation recherche à partir de 'P1P2' le 1er mot égal à FFFFFFFFh.

Conditions d'utilisation

L'ordre de "Lecture de résultat" exécuté à la suite fournit l'adresse trouvée.

L'adresse fournie doit être un multiple de 8.

La détermination des adresses de recherche autorisées est détaillée dans le tableau de la section "Recherche d'un mot sur argument".

Réponse de la carte

ME1	=	90h	
ME2	=	00h :	mot vierge trouvé,
	=	X4h :	l'adresse de début de recherche est dans une zone protégée en lecture et aucune clé ou code n'a préalablement été présentée et validée ; ou zone inaccessible,
	=	X8h :	mot non trouvé.
Mutisme :	-	P3 # 00h,	
	-	'P1P2' n'est pas un multiple de 8.	

Recherche du premier mot vierge à partir de l'adresse 1050h

CLA	= BCh
INS	= A0h
P1	= 10h
P2	= 50h
P3	= 00h
DATA	= Aucune

Réponse de la carte

ME1	= 90h
ME2	= 00h

L'exécution à la suite d'un ordre "Lecture de résultat" permet d'obtenir l'adresse trouvée.

Figure 6.7 - Exemple d'utilisation de "Recherche du premier mot vierge".

6.6 Recherche du premier mot non vierge : INS = A8h

Ordre utilisé pour rechercher l'adresse du premier mot dont un bit au moins est positionné.

TYPE	MODE
ENTRANT	SIMPLE

Validité : **toute la famille.**

Initialisation

CLA = BCh
INS = A8h
P1 = Poids forts de l'adresse du début de recherche
P2 = Poids faibles de l'adresse du début de recherche
P3 = 00h
DATA = Aucune

Fonction exécutée

La carte recherche à partir de l'adresse 'P1P2' le premier mot différent de FFFFFFFFh.

Conditions d'utilisation

L'ordre de "Lecture de résultat" exécuté à la suite fournit l'adresse trouvée.

L'adresse fournie doit être un multiple de 8.

La détermination des adresses de recherche autorisées est détaillée dans le tableau de la section "Recherche d'un mot sur argument".

Réponse de la carte

ME1	=	90h	
ME2	=	00h :	mot non vierge trouvé,
	=	X4h :	l'adresse de début de recherche est dans une zone protégée en lecture et aucune clé ou code n'a préalablement été présentée et validée ; ou zone inaccessible,
	=	X8h :	mot non vierge inexistant.
Mutisme :	-	P3 # 00h,	
	-	'P1P2' n'est pas un multiple de 8.	

Recherche du premier mot non vierge à partir de l'adresse 1050h

CLA	= BCh
INS	= A8h
P1	= 10h
P2	= 50h
P3	= 00h
DATA	= Aucune

Réponse de la carte

ME1	= 90h
ME2	= 00h

L'exécution à la suite d'un ordre "Lecture de résultat" permet d'obtenir l'adresse trouvée.

Figure 6.8 - Exemple d'utilisation de "Recherche du premier mot non vierge".

6.7 Lecture de résultat : INS = C0h

Ordre utilisé pour lire un résultat conséquent à un ordre précédemment exécuté. Cet ordre peut aussi être utilisé pour connaître la taille de la mémoire.

TYPE	MODE
SORTANT	SIMPLE

Validité : **toute la famille.**

Initialisation

CLA = BCh
INS = C0h
P1 = 00h
P2 = 00h
P3 = 08h
DATA = Aucune

Fonction exécutée

Le résultat de la lecture dépend de l'ordre exécuté précédemment. Dans tous les cas, sauf après un calcul de certificat, il restitue l'adresse ADMAX (indique ainsi la taille de la mémoire).

Si cet ordre fait suite à **un calcul de certificat** :

le système d'exploitation envoie au lecteur le résultat R (8 octets) de la fonction de calcul ;

Si cet ordre fait suite à **un ordre de recherche** :

le système d'exploitation envoie au CAD l'adresse du mot recherché et son contenu.

Si cet ordre fait suite à **un autre ordre ou une remise à zéro,**

le système d'exploitation envoie au CAD :

- la première adresse non accessible,
- l'option de la carte (1 ou 2 zones de travail),
- le numéro d'algorithme (6 = D.E.S., 7 ou 0 = TELEPASS),
- les conditions régissant la protection en lecture, en écriture et en effacement de la zone de travail 2.

Voir après les exemples la description détaillée des réponses à cet ordre pour chaque cas.

Conditions d'utilisation

Cet ordre doit faire suite à l'exécution d'un autre ordre ou d'une remise à zéro.

Réponse de la carte

8 octets constituant le résultat

ME1	=	90h
ME2	=	00h

Mutisme : - P3 # 08h.

Lecture du résultat R de l'exemple de calcul de certificat

CLA	= BCh
INS	= C0h
P1	= 00h
P2	= 00h
P3	= 08h
DATA	= Aucune

Réponse de la carte

R	= 51 F2 22 16 B2 11 A2 5Ch
ME1	= 90h
ME2	= 00h

Extrait de la mémoire utilisé pour l'exemple ci-dessous

10B0h 0C AB 20 10h

Lecture du résultat de la commande de recherche sur argument

CLA	= BCh
INS	= C0h
P1	= 00h
P2	= 00h
P3	= 08h
DATA	= Aucune

Réponse de la carte

R = 10 B0 19 38 0C AB 20 10h

R composé de la manière suivante :

Adresse du mot contenant l'argument	= 10B0h
ADMAX	= 1938h
Contenu du mot	= OC AB 20 10h

ME1	= 90h
ME2	= 00h

Figure 6.9 - Exemples d'utilisation de "Lecture de résultat".

Réponse après une remise à zéro (8 octets) ou un ordre quelconque (sauf recherche réussie ou certificat)

Octet numéro	1	2	3	4	5	6	7	8
	00h	00h	—ADMAX—		00h	00h	TA	PZT2

ADMAX (octets 3 et 4)

ADMAX est l'adresse de fin de mémoire + 8h. Valeurs suivant les modèles :

Modèle	ADMAX
SCOT 50, SCOT 60 DES SCOT100, SCOT 110 DES SCOT10, SCOT 20 DES	0A00h 1938h 41D8h

TA Type d'algorithme et option (octet 7)

0	0	0	0	IZ2	———	NA	———

IZ2 = 1 Indique 2 zones de travail
IZ2 = 0 Indique 1 zone de travail

NA (sur 3 bits) = 110 Algorithme D.E.S.
NA (sur 3 bits) = 111 ou 000 Algorithme TELEPASS

PZT2 Protections de la zone de travail 2 (octet 8) significatives si IZ2 = 1

0	0	0	0	IEP2	ILP2	--IEC2--	

IEP2 = 1 Zone de travail 2 protégée en écriture
IEP2 = 0 Zone de travail 2 libre en écriture

ILP2 = 1 Zone de travail 2 protégée en lecture
ILP2 = 0 Zone de travail 2 libre en lecture

IEC2 (2 bits)

IEC2 = 00 Zone de travail 2 interdite en effacement
IEC2 = 01 Zone de travail 2 protégée en effacement par le code porteur actif
IEC2 = 10 Zone de travail 2 protégée en effacement par la clé 1B
IEC2 = 11 Zone de travail 2 protégée en effacement par la clé 1A

Réponse après un ordre de recherche réussie (8 octets)

Octet numéro 1	2	3	4	5	6	7	8
——AD——		——ADMAX——		Contenu du mot trouvé			

AD (2 octets) Adresse du mot trouvé

ADMAX (2 octets) Adresse de fin de mémoire + 8h

Contenu du mot (4 octets)

Remarque

Dans le cas où la recherche s'est faite dans une zone libre et sans présentation de clé alors que la zone suivante est protégée, le résultat donne, à la place de ADMAX, l'adresse de fin de zone dans laquelle la recherche s'effectue.

Par exemple : recherche dans la zone de travail 2, la zone de travail 1 étant protégée.

ADC

ADT

Zone de travail 2
Zone de travail 1

La recherche donnerait ADT comme adresse de fin de mémoire à la place de ADMAX.

Réponse après un ordre "Calcul de certificat

8 octets donnant le résultat du calcul de certificat.

6.8 Ecriture des verrous : INS = 50h

Ordre utilisé pour positionner à 0 le ou les verrous dans la zone de fabrication.

TYPE	MODE
ENTRANT	SIMPLE

SCOT 10, SCOT 20 DES : VPP NECESSAIRE

Validité : **toute la famille.**

Initialisation

CLA	=	BCh
INS	=	50h
P1	=	00h
P2	=	00h
P3	=	02h
DATA	=	2 octets D1 et D2

Fonction exécutée

Le verrou désigné par l'octet D1 est positionné.

Conditions d'utilisation

L'octet D1 est le masque (profil binaire) indiquant le verrou à positionner ; le bit à positionner doit être à 0.

L'octet D2 n'est pas utilisé par le système d'exploitation.

La validité de l'exécution de cet ordre peut être vérifiée par l'exécution d'un ordre de lecture du mot contenant les verrous.

Valeur de l'octet D1 pour chaque verrou

La personnalisation et l'application ne peuvent écrire que 3 verrous.

La personnalisation écrit :

- le verrou LC

L'application peut écrire :

- le verrou LU
- le verrou IV à l'un ou l'autre des emplacements prévus.

Valeur de l'octet D1	Verrou positionné
BFh	LC
7Fh	LU
EFh	IV
F7h	IV

Exemple :

Le verrou LC est positionné par le profil BFh.

Masque utilisé :

1	0	1	1	1	1	1	1

Emplacement dans l'octet des verrous.

LU	LC	LF	IV	IV	RUF	RUF	RUF

Réponse de la carte

ME1 = 90h
ME2 = 00h

Mutisme : - P3 # 02h.

Positionnement du verrou LU

CLA	= BCh
INS	= 50h
P1	= 00h
P2	= 00h
P3	= 02h
DATA	= 7F FFh

Réponse de la carte

ME1	= 90h
ME2	= 00h

Positionnement du verrou IV

CLA	= BCh
INS	= 50h
P1	= 00h
P2	= 00h
P3	= 02h
DATA	= EF FFh

Réponse de la carte

ME1	= 90h
ME2	= 00h

Figure 6.10 - Exemples d'utilisation de "Ecriture des verrous".

6.9 Effacement de domaine : INS = 0Eh

Ordre utilisé pour effacer des mots dans la zone de travail.

TYPE	MODE
ENTRANT	SIMPLE

Validité : **toute la famille sauf SCOT 10 et SCOT 20 DES.**

Initialisation

CLA	=	BCh
INS	=	0Eh
P1	=	Poids forts de l'adresse de début d'effacement
P2	=	Poids faibles de l'adresse de début d'effacement
P3	=	02h
DATA	=	Adresse du dernier mot à effacer + 8h

Fonction exécutée

Une zone étant autorisée en effacement par une clé, le domaine désigné est effacé.

L'effacement consiste à remettre à 1 tous les bits des mots concernés.

Conditions d'utilisation

L'effacement ne peut agir que sur une seule zone ; ceci signifie qu'il ne peut pas y avoir de chevauchement.

La zone autorisée en effacement est fonction de la phase de vie de la carte.

Cet ordre doit être précédé de la séquence d'ordres suivante :

- un ordre de présentation de clé ou de code,
- un ordre de validation de lecture ou d'écriture.

L'unité d'effacement est le mot.

La détermination des domaines autorisés en effacement est détaillée dans le tableau ci-après.

Domaines autorisés en effacement

- Phase d'utilisation -

Option	**Protection d'effacement**	**Clé ou code**	**Domaines d'effacement**
1 seule Zone de Travail	EC1		
	1 1		**Interdit**
	1 0	Code porteur	**[ADT, ADL[**
	0 1	Clé 1B	**[ADT, ADL[**
	0 0	Clé 1A	**[ADT, ADL[**
2 Zones de Travail			
Zone de Travail 1	EC1		
	1 1		**Interdit**
	1 0	Code porteur	**[ADT, ADL[**
	0 1	Clé 1B	**[ADT, ADL[**
	0 0	Clé 1A	**[ADT, ADL[**
Zone de Travail 2	EC2		
	1 1		**Interdit**
	1 0	Code porteur	**[ADC, ADT[**
	0 1	Clé 1B	**[ADC, ADT[**
	0 0	Clé 1A	**[ADC, ADT[**

Figure 6.11 - Tableau des domaines autorisés en effacement.

Réponse de la carte

ME1	=	90h	
ME2	=	X4h	'P1P2' n'adresse pas un mot d'un domaine autorisé à l'effacement, le type de la clé présentée permettant l'effacement ou la clé elle-même n'était pas correcte,
	=	01h	incident d'effacement (bit V non effacé).

Mutisme :
- 'P1P2' n'est pas un multiple de 8,
- carte saturée,
- carte invalidée,
- l'effacement est interdit totalement,
- DATA = adresse du 1er mot à ne plus effacer :
  - est inférieure ou égale à 'P1P2',
  - dépasse le domaine autorisé en effacement,
  - n'est pas une adresse multiple de 8 ;
- P3 # 02h.

Extrait de mémoire utilisé pour l'exemple :

1050h	65 06 11 35h
1058h	2A FC EB 38h
1060h	54 05 B5 15h
1068h	C6 52 AB 32h
1070h	04 A6 23 10h

Effacement d'un domaine compris entre les adresses 1050h et 1070h (incluses)

Ces adresses doivent appartenir à la même zone de travail.

CLA	= BCh
INS	= 0Eh
P1	= 10h
P2	= 50h
P3	= 02h
DATA	= 10 78h

Réponse de la carte

ME1	= 90h
ME2	= 00h

Figure 6.12 - Exemple d'utilisation de "Effacement de domaine".

6.10 Demande de nombre aléatoire : INS = C4h

Ordre utilisé pour demander un nombre aléatoire à la carte en vue de chiffrement de clé.

TYPE	MODE
SORTANT	SIMPLE

SCOT 20 DES : VPP NECESSAIRE

Validité : **SCOT 20 DES, SCOT 110 DES.**

Initialisation

CLA	=	BCh
INS	=	C4h
P1	=	00h
P2	=	00h
P3	=	08h
DATA	=	Aucune

Fonction exécutée

A la réception de cet ordre, la carte envoie un nombre aléatoire (64 bits) au CAD.

Ce nombre est ensuite utilisé par le CAD pour chiffrer les clés.

Conditions d'utilisation

La carte doit avoir l'algorithme D.E.S..

Réponse de la carte

ME1 = 90h
ME2 = 00h

Mutisme :

- la carte n'est pas en phase d'utilisation,
- algorithme de la carte # D.E.S.,
- P3 # 08h,
- pointeurs ADS et AD2 non cohérents,
- le jeu secret n'est pas composé de 3 mots validés.

Demande de nombre aléatoire

CLA	= BCh
INS	= C4h
P1	= 00h
P2	= 00h
P3	= 08h
DATA	= Aucune

Réponse de la carte

R	= 56 EC 32 10 52 FA AC 27h
ME1	= 90h
ME2	= 00h

Figure 6.13 - Exemple d'utilisation de "Demande de nombre aléatoire".

6.11 Présentation en clair de clé ou code : INS = 20h, 10h ou 30h

Ordre utilisé, en préalable, pour réaliser les opérations suivantes :

- lire dans des zones protégées en lecture,
- valider l'écriture d'un mot écrit dans une zone protégée en écriture,
- effacer un domaine.

TYPE	MODE
ENTRANT	SIMPLE

Validité : **toute la famille.**

Initialisation

CLA	=	BCh	
INS	=	20h	: présentation d'une clé de fabrication (phase de personnalisation), d'un code 2i (code 2A, code 2B), ou clé de déblocage
	=	10h	: présentation de la clé 1A
	=	30h	: présentation de la clé 1B
P1	=	00h	
P2	=	00h	
P3	=	longueur de la clé ou du code en octets 08h ou 04h (code 2i) 0Ch ou 10h (clé de déblocage) 08h (clé 1A ou 1B)	
DATA	=	clé ou code au format interne à la carte	

Fonction exécutée

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

Au fur et à mesure de la réception de la clé ou du code, la carte compare terme à terme les octets reçus aux octets de la clé ou du code correspondant stocké en zone secrète. Le résultat de la comparaison est mémorisé, mais non communiqué à l'issue de cet ordre.

Conditions d'utilisation

Une carte étant sous tension, des clés peuvent être présentées successivement. C'est la dernière clé ou le dernier code présenté qui, lors de la première demande de validation (en écriture ou lecture) suivant l'ordre de présentation, est pris en compte.

La mise hors tension d'une carte "annule" le résultat de la "Présentation d'une clé ou d'un code". Lors de la mise sous tension suivante, il est nécessaire de présenter à nouveau une clé ou un code.

Lorsque la carte est bloquée, il est impossible de présenter une clé ou un code porteur, seule une clé de déblocage est acceptée.

Réponse de la carte

ME1 = 90h
ME2 = 00h

Mutisme :

- le nombre de mots validés composant la clé concernée en zone secrète ne correspond pas au nombre d'octets reçus par la carte,
- carte bloquée,
- ordre 30h : pointeur de clé 1B incohérent,
- ordre 20h : pointeur de code 1A incohérent,
- P3 # 08h (toute clé ou code sauf clé de déblocage),
- P3 # 04h (code porteur),
- P3 # 0Ch ou 10h (clé de déblocage).

Cas particulier de la clé de déblocage

Le mode de transmission est hétérogène :

- mode asservi pour la transmission du code porteur actif,
- mode simple pour la transmission de la clé 1A.

Réponse de la carte

ME1 = 90h
ME2 = 40h : carte bloquée.

Mutisme : - carte non bloquée,
- la carte n'est pas en phase d'utilisation.

C'est la validation qui réalise effectivement le déblocage.

Présentation du code 2A

CLA	= BCh
INS	= 20h
P1	= 00h
P2	= 00h
P3	= 04h
DATA	= 12 54 3F FFh

Réponse de la carte

ME1	= 90h
ME2	= 00h

Présentation de la clé 1A

CLA	= BCh
INS	= 10h
P1	= 00h
P2	= 00h
P3	= 08h
DATA	= 3A AA AA AA 3A AA AA AAh

Réponse de la carte

ME1	= 90h
ME2	= 00h

Figure 6.14 - Exemples d'utilisation de "Présentation en clair de clé ou code".

6.12 Présentation chiffrée de clé : INS = 28h, 18h ou 38h

Ordre utilisé pour présenter une clé sous une forme indéchiffrable.

TYPE	MODE
ENTRANT	SIMPLE

Validité : **SCOT 20 DES, SCOT 110 DES.**

Initialisation

CLA	=	BCh
INS	=	28h : présentation chiffrée d'une clé de déblocage
	=	18h : présentation chiffrée de la clé 1A
	=	38h : présentation chiffrée de la clé 1B
P1	=	00h
P2	=	00h
P3	=	08h (pour les ordres 18h et 38h)
	=	0Ch ou 10h (pour l'ordre 28h ; en effet la clé de déblocage est la concaténation de la clé 1A et du code porteur valide)
DATA	=	clé au format interne à la carte

Fonction exécutée

Une carte étant sous tension, des clés peuvent être présentées successivement. C'est la dernière clé présentée qui, lors de la première demande de validation (en écriture ou lecture) suivant l'ordre de présentation, est prise en compte.

La mise hors tension d'une carte "annule" le résultat de la "Présentation d'une clé". Lors de la mise sous tension suivante, il est nécessaire de présenter à nouveau une clé.

Conditions d'utilisation

L'ordre "Demande de nombre aléatoire" doit avoir été exécuté préalablement.

Si la carte est bloquée, les ordres 18h et 38h sont refusés par la carte. Si la carte est en accès ou en erreur, l'ordre 28h est refusé par la carte.

Réponse de la carte

ME1 = 90h
ME2 = 00h

Mutisme :
- algorithme de la carte # D.E.S.,
- nombre aléatoire non demandé par l'application,
- le nombre de mots validés composant la clé concernée en zone secrète ne correspond pas au nombre d'octets reçus par la carte,
- carte bloquée et ordre 18h ou 38h,
- carte non bloquée et ordre 28h,
- P3 # 0Ch ou 10h (ordre 28h),
- P3 # 08h (ordre 18h ou 38h),
- ordre 38h : ADS - 10h = AD1.

Cas particulier de la clé de déblocage (ordre 28h)

Voir le paragraphe "Cas particulier de la clé de déblocage" de la section "Présentation en clair de clé ou de code" de ce chapitre.

Présentation de la clé 1A

CLA	= BCh
INS	= 18h
P1	= 00h
P2	= 00h
P3	= 08h
DATA	= 17 28 A2 5C 49 00 17 FFh

Réponse de la carte

ME1	= 90h
ME2	= 00h

Figure 6.15 - Exemple d'utilisation de "Présentation chiffrée d'une clé".

6.13 Validation de clé ou code en lecture : INS = 40h

Ordre utilisé à la suite d'une "Présentation de clé ou code" pour réaliser les opérations suivantes :

- lire dans les zones protégées en lecture (ZA, ZC, ZT_i si $LP_i = 0$),
- recycler une carte bloquée,
- effacer un domaine.

TYPE	MODE
ENTRANT	SIMPLE

SCOT 10, SCOT 20 DES : VPP NECESSAIRE

Validité : **toute la famille.**

Initialisation

CLA	=	BCh
INS	=	40h
P1	=	00h
P2	=	00h
P3	=	00h
DATA	=	Aucune

Fonction exécutée

La carte, en fonction du résultat de la comparaison effectuée lors de la "Présentation de clé ou code en clair ou chiffrée", positionne un bit dans la zone d'accès et fournit le résultat au CAD.

Conditions d'utilisation

La "Présentation de clé ou code en clair ou chiffrée" préalable à cette validation doit avoir été effectuée à l'aide d'un des ordres 20h, 10h, 30h, 28h, 18h ou 38h.

Dans le cas contraire, la validation produit un résultat identique à celui d'une validation avec un code faux et entraîne un risque de blocage.

Réponse de la carte

ME1	=	90h	
ME2	=	00h :	clé bonne,
	=	14h :	code faux première tentative,
	=	24h :	code faux deuxième tentative,
	=	44h :	code faux troisième tentative ou clé fausse, carte bloquée,
	=	4Ch :	code porteur faux au minimum dans une clé de déblocage,
	=	X5h :	incident d'écriture,
	=	80h :	carte saturée.

Mutisme :
- carte déjà saturée,
- P3 # 00h,
- carte ayant enregistré 1 ou 2 erreurs de code porteur et la clé présentée est une clé de type 1,
- carte bloquée et aucune clé n'a été présentée préalablement,
- carte invalidée et la clé 1A n'a pas été présentée préalablement.

Validation de code 2A

CLA	= BCh
INS	= 40h
P1	= 00h
P2	= 00h
P3	= 00h
DATA	= Aucune

Réponse de la carte

ME1	= 90h
ME2	= 00h

Validation d'un mauvais code, premier essai

CLA	= BCh
INS	= 40h
P1	= 00h
P2	= 00h
P3	= 00h
DATA	= Aucune

Réponse de la carte

ME1	= 90h
ME2	= 14h

Figure 6.16 - Exemple d'utilisation de "Validation en lecture".

6.14 Validation en écriture : INS = 70h

Ordre utilisé pour positionner à 0 le bit V d'un mot dans une zone accessible en écriture protégée ou non protégée.

TYPE	MODE
ENTRANT	SIMPLE

SCOT 10, SCOT 20 DES : VPP NECESSAIRE

Validité : **toute la famille.**

Initialisation

CLA	=	BCh
INS	=	70h
P1	=	Poids forts de l'adresse du mot à valider
P2	=	Poids faibles de l'adresse du mot à valider
P3	=	00h
DATA	=	Aucune

Fonction exécutée

Deux cas se présentent :

Validation d'un mot dans une zone protégée en écriture

Le système d'exploitation contrôle que le type de la clé présentée est en accord avec les deux bits C, CA du mot à valider.

Si ce contrôle est positif et que le résultat de la présentation de clé était correct, le bit V est positionné.

Si ce contrôle est positif et que le résultat de la présentation de clé est incorrect, un bit de la zone d'accès est positionné.

Si ce contrôle est négatif, l'ordre est abandonné.

Validation d'un mot dans une zone non protégée en écriture

Le bit V est positionné à 0 sans autre procédure de contrôle.

Conditions d'utilisation

La validation n'est possible que sur un mot.

Le mot ne doit pas être déjà validé.

L'adresse est une adresse mot donc multiple de 8.

Dans le cas de "Validation en écriture" en zone protégée, l'ordre de "Présentation de clé" doit avoir été exécuté préalablement (ordres 20h, 10h, 30h, 28h, 18h ou 38h) correspondant à la configuration des bits C, CA.

Réponse de la carte

ME1	=	90h	
ME2	=	00h	clé ou code bon et mot validé,
	=	01h	'P1P2' adresse un mot déjà validé,
	=	14h	code faux, première tentative,
	=	24h	code faux, deuxième tentative,
	=	44h	code faux, troisième tentative, ou clé fausse, la carte est bloquée,
	=	80h	carte saturée.

Mutisme :
- 'P1P2' adresse un mot inaccessible en écriture,
- 'P1P2' n'est pas un multiple de 8,
- P3 # 00h,
- carte invalidée,
- carte saturée.

Présentation préalable de la clé 1B, avec les bits C = 1 et CA = 0

puis validation d'un mot écrit dans l'exemple de la section "Ecriture : INS = D0h".

CLA	= BCh
INS	= 70h
P1	= 06h
P2	= 70h
P3	= 00h
DATA	= Aucune

Réponse de la carte

ME1	= 90h
ME2	= 00h

Figure 6.17 - Exemple d'utilisation de "Validation en écriture".

6.15 Calcul de certificat : INS = 80h

Ordre utilisé pour activer la fonction de chiffrement TELEPASS ou D.E.S. afin de certifier une information écrite dans la mémoire (1 mot).

TYPE	MODE
ENTRANT	SIMPLE

Validité : **toute la famille.**

Initialisation

CLA	=	BCh
INS	=	80h
P1	=	00h
P2	=	00h
P3	=	08h
DATA	=	6 octets constituant E, suivis des 2 octets constituant ADR.

Remarque :

Cet ordre est appelé parfois :

ORDRE HABILITATION ou ORDRE DE CALCUL.

Fonction exécutée

Les données externes sont utilisées pour effectuer le calcul algorithmique, le résultat est mémorisé pour être lu grâce à un ordre de lecture ultérieur.

Conditions d'utilisation

Le mot à certifier doit être dans une zone accessible en lecture.

Si la zone est protégée en lecture, il est nécessaire d'avoir préalablement présenté et validé une clé ou un code en lecture.

Les adresses autorisées sont les mêmes que celles des ordres de recherche ou de lecture.

Rappel

La formulation de la fonction TELEPASS ou D.E.S. est :

R = F (E, ADR, [ADR], S)

Réponse de la carte

ME1 = 90h
ME2 = 00h

Mutisme :
- 'ADR' adresse un mot inaccessible en lecture,
- le jeu secret n'est pas composé de 3 mots validés,
- P3 # 08h,
- pointeurs ADS et AD2 non cohérents,
- carte invalidée.

Exécution de la fonction TELEPASS sur le mot d'adresse 10B0h
avec E = AB CD FF 00 00 00h

CLA	= BCh
INS	= 80h
P1	= 00h
P2	= 00h
P3	= 08h
DATA	= AB CD FF 00 00 00 10 B0h

Réponse de la carte

ME1	= 90h
ME2	= 00h

Figure 6.18 - Exemple d'utilisation de "Calcul de certificat".

6.16 Changement de code porteur : INS = D2h

Ordre utilisé pour changer le code porteur en mémoire.

TYPE	MODE
ENTRANT	SIMPLE

Validité : **SCOT 60 DES, SCOT 110 DES.**

Initialisation

CLA	=	BCh
INS	=	D2h
P1	=	00h
P2	=	00h
P3	=	04h
DATA	=	nouveau code (1 mot avec bit V et bit C positionnés)

Fonction exécutée

Le premier mot du code 2A est modifié en mémoire.

Le système d'exploitation vérifie la validité de l'écriture.

Cette modification peut être faite autant de fois que nécessaire.

Conditions d'utilisation

Préalablement à cet ordre, il faut avoir présenté et validé le code porteur 2A.

La carte doit être en phase d'utilisation code porteur 2A :

- le verrou LC doit être positionné (LC = 0),
- le verrou LU doit être non positionné (LU = 1).

Voir la section "Phases de vie" du chapitre "FAMILLE SCOT".

Réponse de la carte

ME1	=	90h	
ME2	=	00h	changement nouveau code porteur correct,
	=	01h	erreur d'écriture du code porteur,
	=	04h	code 2A faux ou présentation de clé de type 1.

Mutisme :
- code porteur 2B actif (verrou LU positionné),
- P3 # 04h,
- bit C du nouveau code = 1,
- bit V du nouveau code = 1.

Changement de code porteur

CLA	= BCh
INS	= D2h
P1	= 00h
P2	= 00h
P3	= 04h
DATA	= 3B 5E 4C 15h

Réponse de la carte

ME1	= 90h
ME2	= 00h

Le nouveau code porteur 2A est correct et enregistré en mémoire.

Figure 6.19 - Exemple d'utilisation de "Changement de code porteur".

- 7 -

OPERATIONS

7 OPERATIONS

7.1 Lecture protégée

Cette opération est utilisée pour effectuer une lecture en mémoire protégée.

Fonction exécutée

Cette opération consiste à exécuter successivement les ordres :

- présentation en clair (ordres 10h, 30h) ou chiffrée (ordres 18h, 38h) de clé de type 1 (clé 1A, clé 1B) ou présentation (ordre 20h) de code (code 2A, code 2B),
- demande de validation en lecture avec l'ordre 40h,
- lecture de données avec l'ordre B0h.

Conditions d'utilisation

Voir les conditions dans le chapitre "JEU D'ORDRES" pour chaque ordre.

Extrait de la mémoire utilisé pour l'exemple

0810h	6	5	0	6	1	1	3	5
0818h	5	4	5	2	A	B	4	2
0820h	0	C	A	B	2	3	1	0

Effectuer une lecture protégée avec un code tel que :
Code 2A (ou 2B) = 12 54 3F FFh

de 5 octets à l'adresse 0811h

Présentation du code

CLA	= BCh
INS	= 20h
P1	= 00h
P2	= 00h
P3	= 04h
DATA	= 12 54 3F FFh

Réponse de la carte

ME1	= 90h
ME2	= 00h

Demande de validation en lecture

CLA	= BCh
INS	= 40h
P1	= 00h
P2	= 00h
P3	= 00h
DATA	= Aucune

Réponse de la carte

ME1	= 90h
ME2	= 00h ➠ code bon

Demande de lecture

CLA	= BCh
INS	= B0h
P1	= 08h
P2	= 11h
P3	= 5h
DATA	= Aucune

Réponse de la carte

Les 5 octets lus = 50 61 13 55 45h

ME1	= 90h
ME2	= 00h

Figure 7.1 - Exemple d'utilisation de "Lecture protégée".

7.2 Ecriture protégée

Cette opération est utilisée pour effectuer une écriture en mémoire protégée.

Fonction exécutée

Cette opération consiste à exécuter successivement les ordres :

- écriture de données avec l'ordre D0h,
- présentation en clair (ordres 10h, 30h) ou chiffrée (ordres 18h, 38h) de clé de type 1 (clé 1A, clé 1B) ou présentation (ordre 20h) de code (code 2A, code 2B),
- demande de validation en écriture avec l'ordre 70h.

Conditions d'utilisation

Voir les conditions dans le chapitre "JEU D'ORDRES" pour chaque ordre.

Extrait de la mémoire avant l'écriture

08F0h	F	F	F	F	F	F	F	F

Extrait de la mémoire après l'écriture

08F0h	8	F	F	F	F	F	F	F

Effectuer une écriture protégée avec une clé telle que :

Code 2A (ou B) = 12 54 3F FFh

de 1 mot à l'adresse 08F0h

Demande d'écriture

CLA	= BCh
INS	= D0h
P1	= 08h
P2	= F0h
P3	= 04h
DATA	= 8F FF FF FFh

Réponse de la carte

ME1	= 90h
ME2	= 00h

Présentation de la clé

CLA	= BCh
INS	= 20h
P1	= 00h
P2	= 00h
P3	= 04h
DATA	= 12 54 3F FFh

Réponse de la carte

ME1	= 90h
ME2	= 00h

Demande de validation en écriture

CLA	= BCh
INS	= 70h
P1	= 08h
P2	= F0h
P3	= 00h
DATA	= Aucune

Réponse de la carte

ME1	= 90h
ME2	= 00h ➡ code bon

Figure 7.2 - Exemple d'utilisation de "Ecriture protégée".

7.3 Effacement

Cette opération est utilisée pour effectuer un effacement en mémoire.

Fonction exécutée

Cette opération consiste à exécuter successivement les ordres :

- présentation en clair (ordres 10h, 30h) ou chiffrée (ordres 18h, 38h) de clé de type 1 (clé 1A, clé 1B) ou présentation (ordre 20h) de code (code 2A, code 2B),
- validation de clé ou code avec l'ordre 40h ou 70h,
- effacement avec l'ordre 0Eh.

Conditions d'utilisation

Voir les conditions dans le chapitre "JEU D'ORDRES" pour chaque ordre.

Extrait de la mémoire utilisé pour l'exemple avant l'effacement

08F0h	8	F	F	F	F	F	F	F
08F8h	5	C	F	4	5	9	7	2
0900h	6	C	5	7	7	2	3	0

Après effacement

08F0h	F	F	F	F	F	F	F	F
08F8h	F	F	F	F	F	F	F	F
0900h	6	C	5	7	7	2	3	0

Effectuer un effacement avec une clé telle que :

Code 2A (ou B) = 12 54 3F FFh

de 2 mots à partir de l'adresse 08F0h

Présentation du code

CLA	= BCh
INS	= 20h
P1	= 00h
P2	= 00h
P3	= 04h
DATA	= 12 54 3F FFh

Réponse de la carte

ME1	= 90h
ME2	= 00h

Demande de validation en écriture

CLA	= BCh
INS	= 40h
P1	= 00h
P2	= 00h
P3	= 00h
DATA	= Aucune

Réponse de la carte

ME1	= 90h
ME2	= 00h ➠ code bon

Demande d'effacement

CLA	= BCh
INS	= 0Eh
P1	= 08h
P2	= F0h
P3	= 02h
DATA	= 0900h

Réponse de la carte

ME1	= 90h
ME2	= 00h

Figure 7.3 - Exemple d'utilisation de "Effacement".

7.4 Déblocage d'une carte

Cette opération est utilisée pour débloquer une carte bloquée.

Fonction exécutée

Cette opération consiste à exécuter successivement les ordres :

- présentation de la concaténation du code 2A (ou code 2B) et de clé 1A avec l'ordre "Présentation en clair" 20h ou "Présentation chiffrée" 28h,

- demande de validation en lecture avec l'ordre 40h.

Conditions d'utilisation

Voir les conditions dans le chapitre "JEU D'ORDRES" pour chaque ordre.

Débloquer une carte telle que :

Code 2A (ou 2B) = 12 54 3F FFh

Clé 1A = 3A AA AA AA 3A AA AA AAh

Présentation de la clé de déblocage

CLA	= BCh
INS	= 20h
P1	= 00h
P2	= 00h
P3	= 00h
DATA	= 12 54 3F FF 3A AA AA AA 3A AA AA AAh

Réponse de la carte

ME1	= 90h
ME2	= 40h

Demande de validation en lecture

CLA	= BCh
INS	= 40h
P1	= 00h
P2	= 00h
P3	= 00h
DATA	= Aucune

Réponse de la carte

ME1	= 90h
ME2	= 00h ➡ code bon

La carte est débloquée.

Figure 7.4 - Exemple d'utilisation de "Recyclage d'une carte".

7.5 Changement de code porteur

Cette opération est utilisée pour effectuer le changement de code porteur.

Fonction exécutée

Cette opération consiste à exécuter successivement les ordres :

Cas de SCOT 60 DES et SCOT 110 DES avec LU non positionné

- Présentation de code 2A avec l'ordre 20h.
- Demande de validation en lecture avec l'ordre 40h.
- Demande de changement de code porteur (code 2A) avec l'ordre D2h.

Autres cas

- Demande d'écriture du nouveau code porteur (code 2B) avec l'ordre D0h.
- Présentation de code 2A avec l'ordre 20h.
- Demande de validation en écriture avec l'ordre 70h.
- Positionnement du verrou LU avec l'ordre 50h.

Conditions d'utilisation

Les conditions d'utilisation sont différentes suivant les modèles :

Modèles SCOT 60 DES et SCOT 110 DES

Le code porteur peut être changé indéfiniment tant que le verrou LU n'est pas positionné.

Si le code présenté au bout de 3 essais, est mauvais la carte reste bloquée.

Modèles SCOT 10, SCOT 20 DES, SCOT 50 et SCOT 100

Le code porteur peut être changé 1 seule fois : code 2A remplacé par code 2B et le verrou LU est positionné.

Changer le code porteur 2A en code 2B d'une carte telle que :

Code 2A initial = 12 54 3F FFh

Ecriture du nouveau code porteur

CLA	= BCh
INS	= D0h
P1	= 02h adresse
P2	= 60h code 2B
P3	= 04h
DATA porteur	= 37 5C 55 29h nouveau code

Réponse de la carte

ME1	= 90h
ME2	= 00h

Présentation de code (code initial)

CLA	= BCh
INS	= 20h
P1	= 00h
P2	= 00h
P3	= 04h
DATA	= 12 54 3F FFh

Réponse de la carte

ME1	= 90h
ME2	= 00h

Demande de validation en écriture

CLA	= BCh
INS	= 70h
P1	= 02h
P2	= 60h
P3	= 00h
DATA	= Aucune

Réponse de la carte

ME1	= 90h
ME2	= 00h ➡ le code présenté est bon

Positionnement du verrou LU

CLA	= BCh
INS	= 50h
P1	= 00h
P2	= 00h
P3	= 02h
DATA	= 7F FFh

Réponse de la carte

ME1	= 90h
ME2	= 00h

Le code porteur actif devient le code 2B.

Figure 7.5 - Exemple d'utilisation de "Changement de code porteur" : code 2A en code 2B.

Changer le code porteur 2A d'une carte en nouveau code 2A :

Présentation de code (code initial = 12 54 3F FFh)

CLA	= BCh
OR	= 20h
P1	= 00h
P2	= 00h
P3	= 04h
DATA	= 12 54 3F FFh

Réponse de la carte

ME1	= 90h
ME2	= 00h

Validation de code 2A

CLA	= BCh
INS	= 40h
P1	= 00h
P2	= 00h
P3	= 00h
DATA	= Aucune

Réponse de la carte

ME1	= 90h
ME2	= 00h ➡ code bon

Changement de code porteur : code 2A final = 22 14 5F 3Fh

CLA	= BCh
INS	= D2h
P1	= 00h
P2	= 00h
P3	= 04h
DATA	= 22 14 5F 3Fh

Réponse de la carte

ME1	= 90h
ME2	= 00h

Le nouveau code porteur 2A est correct et enregistré en mémoire.

Figure 7.6 - Exemple d'utilisation de "Changement de code porteur" : code 2A en nouveau code 2A.

7.6 Recherche de mot

Cette opération est utilisée pour effectuer une recherche en mémoire d'un mot donné.

Fonction exécutée

La séquence d'ordres à exécuter pour effectuer une recherche dépend de la zone de recherche.

Recherche en Zone Libre

- Recherche avec l'ordre A0h ou A8h.
- Lecture de résultat avec l'ordre C0h.

Recherche en Zone Protégée

- Présentation en clair (ordres 10h, 30h) ou chiffrée (ordres 18h, 38h) de clé de type 1 (clé 1A, clé 1B) ou présentation (ordre 20h) de code (code 2A, code 2B),
- Validation de clé ou code en lecture avec l'ordre 40h.
- Recherche avec l'ordre A0h.
- Lecture de résultat avec l'ordre C0h.

Conditions d'utilisation

Voir les conditions dans le chapitre "JEU D'ORDRES" pour chaque ordre.

Extrait de la mémoire utilisé pour l'exemple

10A8h	0	C	A	C	3	0	2	8
10B0h	0	C	A	B	2	0	1	0
10B8h	0	C	A	B	2	3	1	0

Effectuer une recherche en zone libre :

Demande de recherche à partir de l'adresse 1050h

du mot dont les 16 bits de poids forts = 0CABh

CLA	= BCh
INS	= A0h
P1	= 10h
P2	= 50h
P3	= 02h
DATA	= 0C ABh

Réponse de la carte

ME1	= 90h
ME2	= 00h

Lecture du résultat de la recherche

CLA	= BCh
INS	= C0h
P1	= 00h
P2	= 00h
P3	= 08h
DATA	= Aucune

Réponse de la carte

R = 10 B0 19 38 0C AB 20 10h

R composé de la manière suivante :

Adresse du mot contenant l'argument = 10B0h

Dernière adresse de la mémoire + 8h : ADMAX = 1938h

Contenu du mot = 0C AB 20 10h

ME1	= 90h
ME2	= 00h

Figure 7.7 - Exemple d'une opération de "Recherche de mot".

Remarque *L'exemple présenté met en valeur le fait que l'adresse trouvée par le système d'exploitation est la première contenant l'argument recherché dans l'ordre croissant des adresses ; cependant ce n'est pas la seule adresse contenant cet argument.*

7.7 Identification de la carte

Cette opération est utilisée pour identifier une carte dans la famille SCOT et connaître ses caractéristiques.

Fonction exécutée

Cette opération consiste à exécuter successivement :

- remise à zéro,

- lecture de résultat avec l'ordre C0h.

Conditions d'utilisation

Voir les conditions dans le chapitre "JEU D'ORDRES" pour chaque ordre.

Rappel de la structure du mot obtenu

Octet numéro 1	2	3	4	5	6	7	8
00h	00h	——ADMAX——		00h	00h	TA	PZT2

Signification de TA

TA = 0Eh	2 zones de travail	D.E.S.
TA = 07h	1 zone de travail	TELEPASS
TA = 00h	1 zone de travail	TELEPASS

Signification de PZT2

PZT2 n'est significatif que pour TA = 0Fh ou 0Eh.

Voir la section "Lecture de résultat" du chapitre "JEU D'ORDRES".

Effectuer une remise à zéro

Effectuer une lecture de résultat :

CLA	= BCh
INS	= C0h
P1	= 00h
P2	= 00h
P3	= 08h
DATA	= Aucune

Réponse de la carte

R = 00 00 41 D8 00 00 0E 00

R composé de la manière suivante :

ADMAX = 41D8h	modèle SCOT 20 DES ou SCOT 10
TA = 0Eh	option 2 zones de travail et algorithme D.E.S. (SCOT 20 DES)
PZT2 = 00h	zone de travail 2 libre en lecture et écriture et interdite en effacement

ME1	= 90h
ME2	= 00h

Le modèle de carte en présence est SCOT 20 DES.

Figure 7.8 - Exemple d'opération "Identification de la carte".

7.8 Certification

Cette opération est utilisée pour assurer la présence et l'intégrité du contenu d'un mot à une adresse donnée.

Fonction exécutée

La séquence d'ordres à exécuter pour effectuer une certification dépend de la zone où elle s'effectue.

Certification en Zone Libre

- Calcul de certificat avec l'ordre 80h.
- Lecture de résultat avec l'ordre C0h.

Certification en Zone Protégée

- Présentation en clair (ordres 10h, 30h) ou chiffrée (ordres 18h, 38h) de clé de type 1 (clé 1A, clé 1B) ou présentation (ordre 20h) de code (code 2A, code 2B),
- Validation de clé ou code en lecture avec l'ordre 40h.
- Calcul de certificat avec l'ordre 80h.
- Lecture de résultat avec l'ordre C0h.

Conditions d'utilisation

Voir les conditions dans le chapitre "JEU D'ORDRES" pour chaque ordre.

Extrait de la mémoire utilisé pour l'exemple

10B0h	0	C	A	B	2	0	1	0

Effectuer une certification en zone libre :

Calcul du certificat du contenu de l'adresse 10B0h

CLA	= BCh
INS	= 80h
P1	= 00h
P2	= 00h
P3	= 08h
DATA	= AB CD FF 00 00 00 10 B0h

Réponse de la carte

ME1	= 90h
ME2	= 00h

Lecture du résultat du calcul de certificat

CLA	= BCh
INS	= C0h
P1	= 00h
P2	= 00h
P3	= 08h
DATA	= Aucune

Réponse de la carte

R	= 51 F2 22 16 B2 11 A2 5Ch
ME1	= 90h
ME2	= 00h

Figure 7.9 - Exemple d'une opération de "Certification".

- 8 -

PERSONNALISATION CARTE

8 PERSONNALISATION CARTE

8.1 Introduction

Personnaliser une carte consiste à la préparer en vue de son utilisation dans le cadre d'une application donnée. Chaque application adopte un scénario propre de personnalisation. Ce chapitre décrit les différentes étapes de la personnalisation.

But de la personnalisation

Les données de base de l'application utilisées par le système d'exploitation SCOT sont inscrites en memoire,

dans la zone secrète :

- les clés émetteurs primaire et secondaire, le code porteur,
- le jeu secret,
- la zone d'accès ;

dans la zone confidentielle, la zone de lecture et la zone de transactions :

- des données propres à l'application ;

dans la zone de fabrication :

- des données complémentaires telles que

  . pointeurs de zones avec CCR,
  . type d'application,
  . bits EPi, LPi et ECi,
  (éventuels : si non écrits en prépersonnalisation).

Conditions de personnalisation

Les cartes à personnaliser sont fournies par le constructeur sous forme d'un lot de cartes prépersonnalisées et accompagnées d'une carte spécifique, appelée carte LOT, indispensable pour les opérations à exécuter.

Moyens de personnalisation

Le personnalisateur doit disposer d'une machine de personnalisation composée d'un système informatique auquel sont couplés deux ou trois CAD.

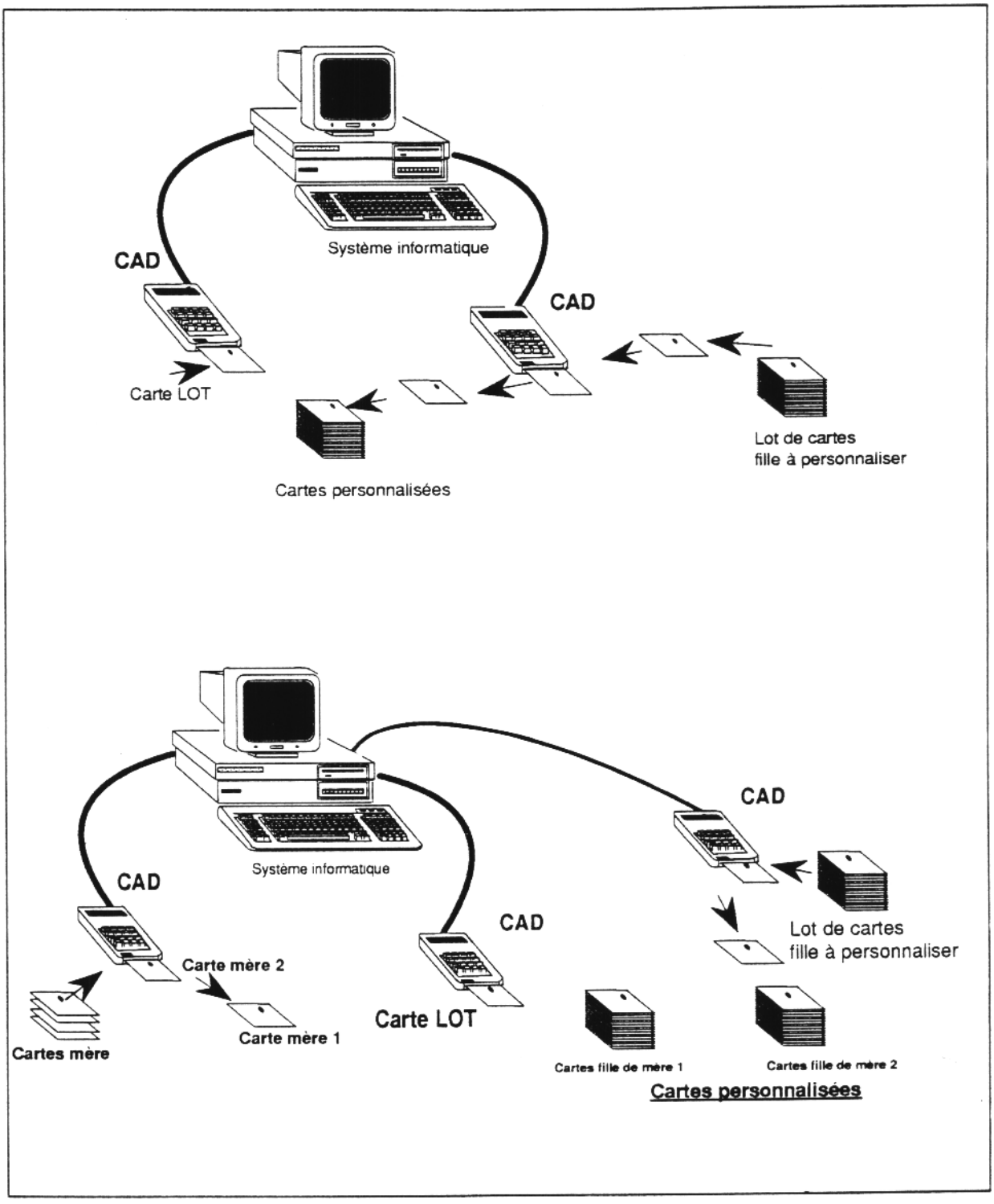

Figure 8.1 - Exemples de chaînes de personnalisation.

8.2 Procédure de personnalisation des cartes

La carte est prépersonnalisée par le constructeur, le personnalisateur ajoute les informations nécessaires au fonctionnement de la carte dans le cadre de son application.

Etat de la carte avant personnalisation

Sa mémoire contient un minimum d'informations propres à chacune comme le montre la figure ci-dessous.

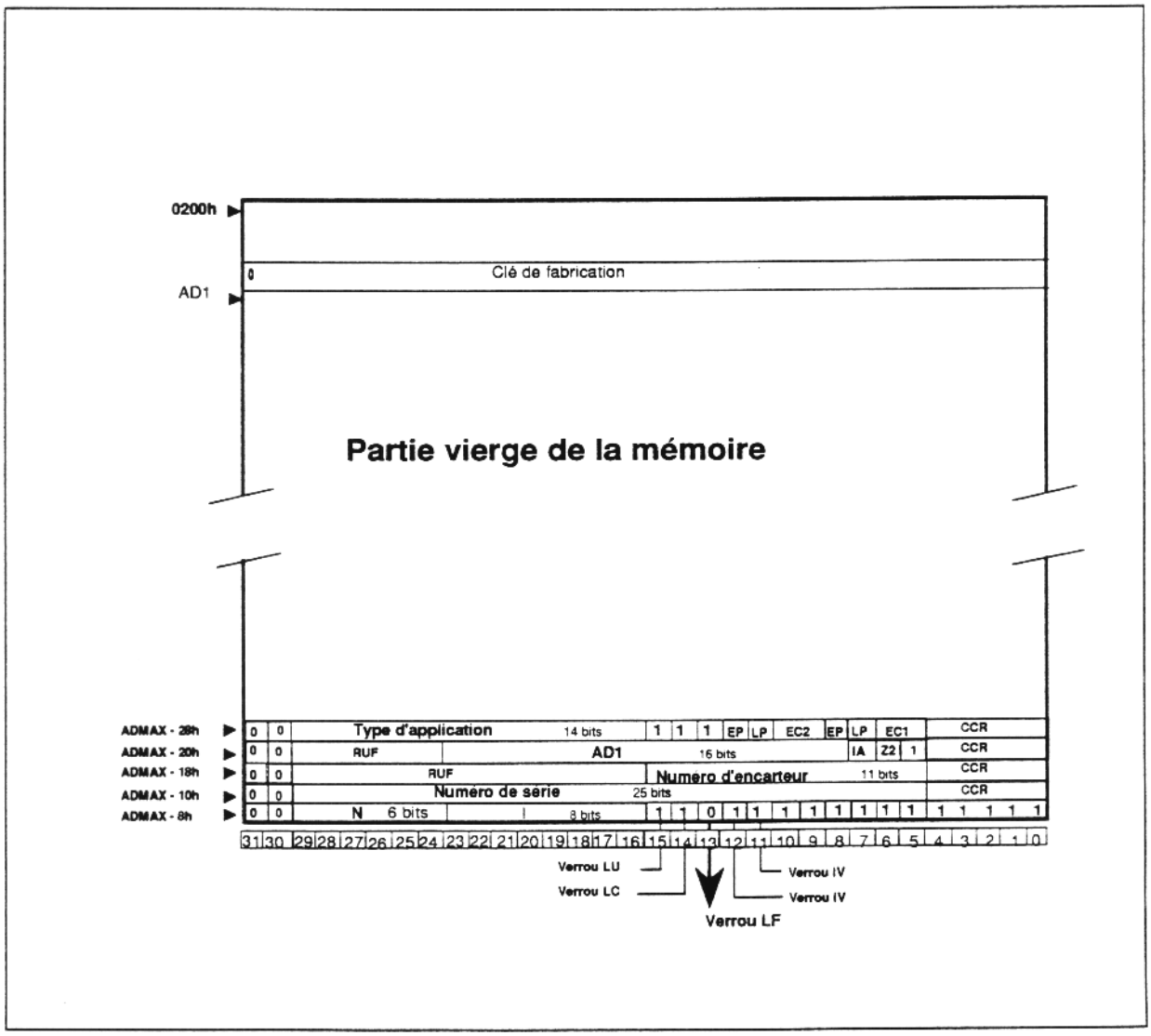

Figure 8.2 - Etat de la mémoire avant la personnalisation.

Eléments de la mémoire

Clé de fabrication (32 bits)
clé propre à chaque carte.

N (6 bits) numéro d'identification de la carte lot.

I (8 bits) numéro de diversification propre à chaque carte.

Numéro de série (25 bits)
unique pour chaque carte.

Numéro d'encarteur (11 bits)
numéro commun à toutes les cartes livrées par un encarteur donné.

AD1 (16 bits) adresse du premier mot de la mémoire utilisable par le personnalisateur, par la suite adresse du début de la zone secrète.

LF (1 bit) verrou positionné indiquant la fin de la phase de fabrication.

Protection de la mémoire d'une carte prépersonnalisée

La mémoire (de AD1 à ADMAX - 8h) est :

- libre en lecture,
- protégée en écriture et en effacement par la clé de fabrication (3 essais possibles).

Personnalisation : séquence d'actions à effectuer

- calcul de la clé de fabrication,

- présentation de cette clé de fabrication,

- calcul, écriture et validation :

  * des clés émetteurs et du code porteur,
  * du jeu secret,
  * des pointeurs correspondants ;

- détermination de la taille de la zone d'accès,

- personnalisation des zones :

  * zone confidentielle,
  * zone de transactions,
  * zone de lecture ;

- écriture dans la zone de fabrication des pointeurs correspondants.

8.3 Calcul de clé de fabrication

La clé de fabrication a été inscrite durant la phase de fabrication du composant. Cette clé, indispensable pour personnaliser une carte, est calculée puisqu'elle ne peut pas être lue.

Nécessité de la clé de fabrication

L'écriture, dans la mémoire des cartes à personnaliser, des données de base de l'application utilisées par le système d'exploitation SCOT, nécessite la présentation de la clé de fabrication.

Séquence de calcul de la clé de fabrication

Pour calculer la clé de fabrication, le système informatique, exécute la séquence d'actions suivante :

- lecture dans la carte à personnaliser des 16 bits de poids forts de ADMAX - 8h contenant N et I (N est commun à toutes les cartes du lot, I est variable),
- vérification de la valeur N : comparaison avec le numéro inscrit à l'adresse 09B8h de la mémoire de la carte LOT.
- formatage de l'entrée E (48 bits) de la fonction TELEPASS comme l'indique la figure ; E est ensuite concaténé avec les 16 bits de l'adresse du mot pour être exploité par la fonction TELEPASS,
- exécution de la fonction TELEPASS par la carte LOT,
- formatage du résultat R obtenu qui constitue la clé de fabrication au format interne de la carte (voir figure dans les pages suivantes).

Rappel :

La formulation de la fonction TELEPASS est :

R = F(E, ADR, [ADR], S)

E nombre (calculé par la machine de personnalisation),
ADR adresse du mot (donnée par la machine de personnalisation),
[ADR] contenu de l'adresse ADR (de la carte LOT),
S jeu secret (de la carte LOT),
R résultat de la fonction (64 bits).

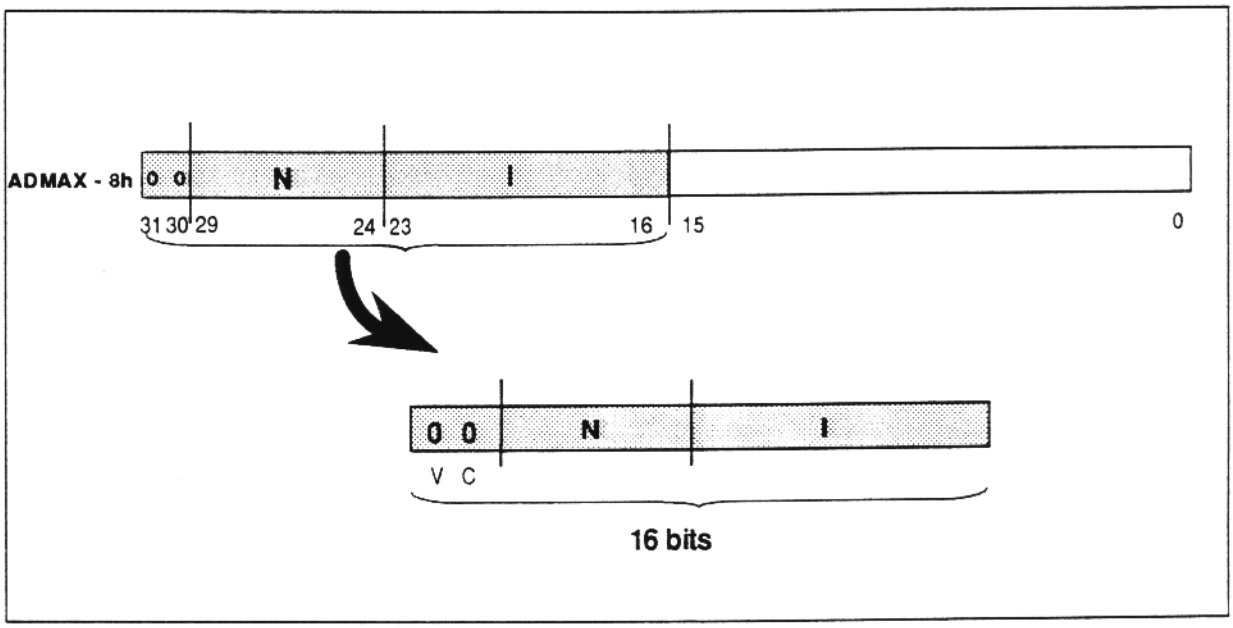

Figure 8.3 - Lecture et prélèvement de numéro N d'identification et du numéro I d'identification de secret.

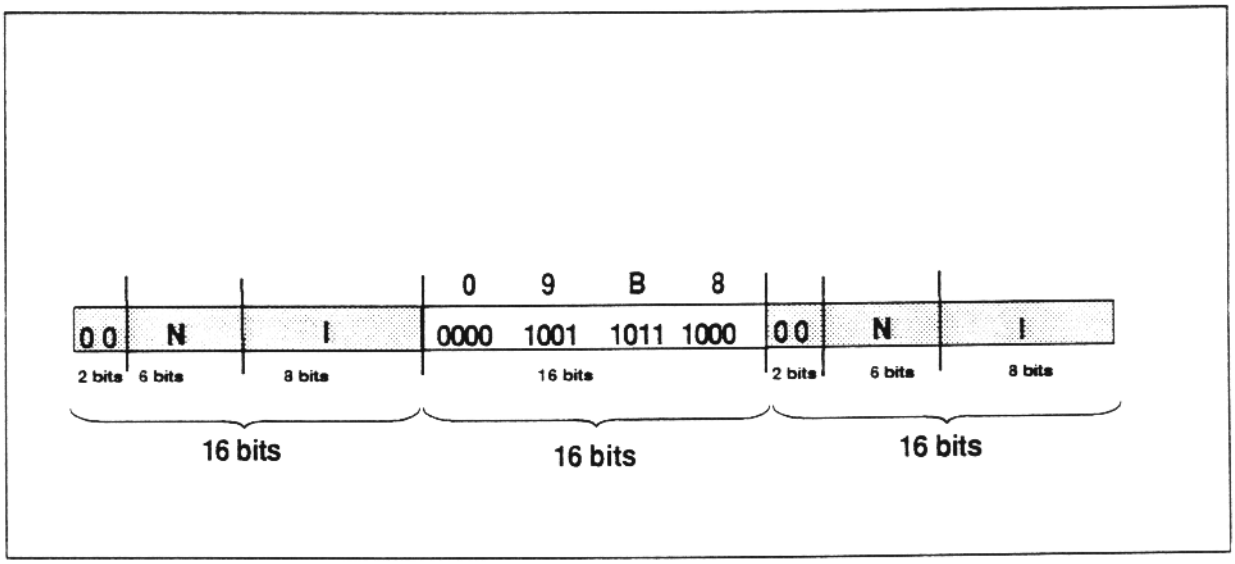

Figure 8.4 - Formatage de l'entrée E de la fonction TELEPASS.

Formatage définitif

A l'aide du résultat R de la fonction TELEPASS :

le champ R de 64 bits étant considéré comme la concaténation de deux champs R1 et R2 de 32 bits chacun, la clé de fabrication est le résultat de la fonction "OU exclusif" de ces deux valeurs avec forçage du bit de poids fort à 0,

comme l'indique la figure ci-dessous.

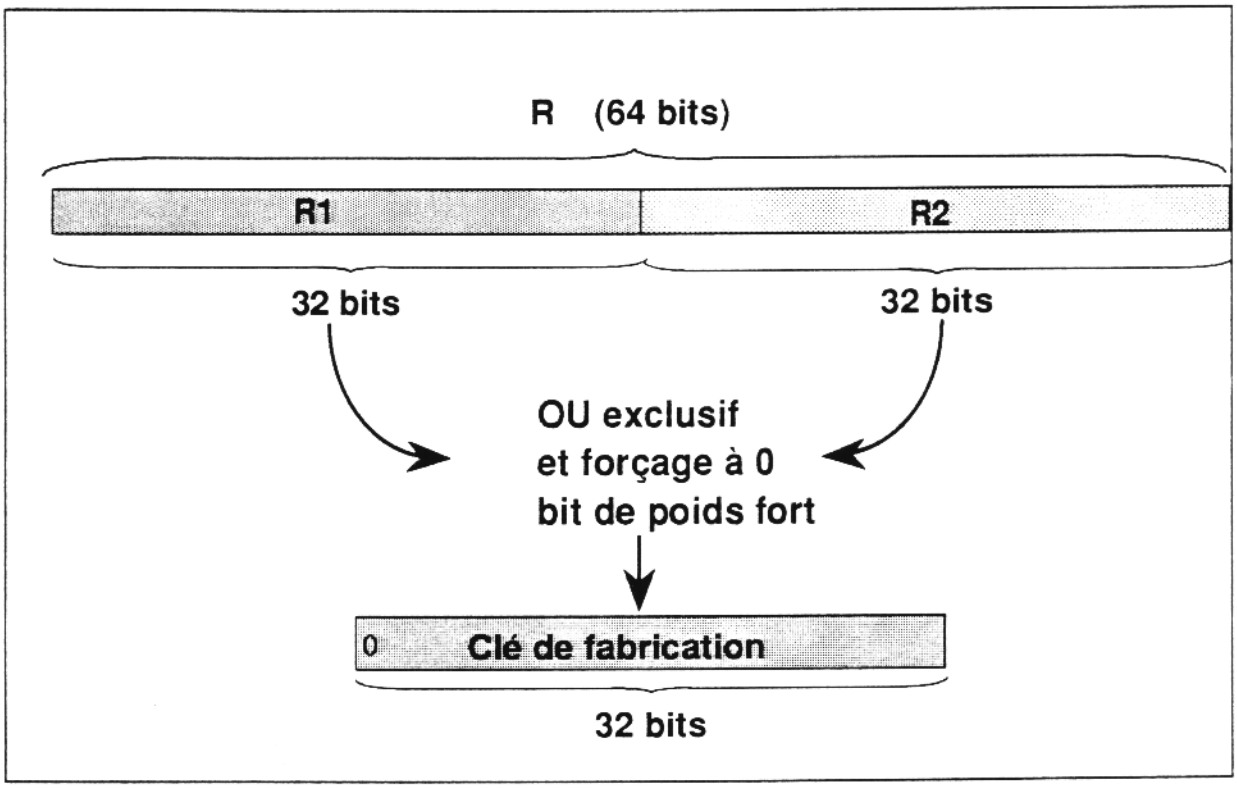

Figure 8.5 - Formatage du résultat de la fonction TELEPASS pour l'obtention de la clé de fabrication.

La clé ainsi obtenue peut être utilisée par l'ordre "Présentation de clé" (INS = 20h).

8.4 Ecriture des pointeurs et calcul de CCR

Les pointeurs sont les adresses délimitant les zones de la carte en phase d'utilisation. L'écriture de chaque pointeur, dans la zone de fabrication, doit être complétée par le calcul et l'écriture du CCR.

Pointeurs

Le pointeur désigne l'adresse absolue quartet du premier mot d'une zone.

Un pointeur a une taille de 16 bits.

Les pointeurs sont déterminés au moment de la mise en place des éléments qu'ils pointent.

Exemple : le pointeur ADS est mis en place au moment de l'écriture du jeu secret.

Les pointeurs de zones sont calculés en fonction de la longueur désirée pour chaque zone.

Si une zone est inexistante, les pointeurs peuvent être confondus mais doivent être inscrits en zone de fabrication comme si la zone existait.

Les pointeurs sont inscrits en mémoire comme indiqué sur la figure.

octet 1	octet 2	octet 3	octet 4
0011 1111	Poids forts du pointeur	Poids faibles du pointeur	'111CCR'

Figure 8.6 - Emplacement d'un pointeur dans le mot (zone de fabrication).

Exemple :

Pointeur 0280h

octet 1	*octet 2*	*octet 3*	*octet 4*
0011 1111	*0000 0010*	*1000 0000*	*111 10011*
	poids forts du pointeur	*poids faibles*	*CCR de 0280h = 10011*

Calcul du CCR (code correcteur d'erreur)

Le code correcteur d'erreur (5 bits) est calculé de la manière suivante.

Le polynome $G(x) = x^5 + x^2 + 1$ est utilisé comme générateur de division : sa représentation binaire est 100101.

Exemple

Supposons que le pointeur inscrit soit 0280h.

Sa représentation binaire est 0000 0010 1000 0000.

Cette valeur multipliée par 2^5 (ajout de 5 bits = 0 en poids faibles), est l'opérande de la division.

Une série de "OU exclusif" est ensuite exécutée avec le polynome G(x) en cadrant le bit de poids fort de G(x) sous le premier bit de poids fort significatif de l'opérande, jusqu'à trouver une valeur sur 5 bits qui constitue le CCR.

```
  0     2     8     0

0000 0010 1000 0000 00000
       10 0101
-------------------------
       00 1101 0000 00000
          1001 01
-------------------------
          0100 0100 00000
           100 101
-------------------------
           000 1110 00000
               1001 01
-------------------------
                0111 01000
                 100 101
-------------------------
                 011 11100
                  10 0101
-------------------------
                  01 10110
                   1 00101
-------------------------
                   0 10011   ➡  code CCR calculé de 0280h
```

Remarque

Le calcul de CCR s'applique en principe sur les 27 bits de poids forts du mot contenant le pointeur. Dans l'exemple precedent le calcul aurait lieu sur :

0011 1111 0000 0010 1000 0000 111

8.5 Mise en place de la zone secrète et de la zone d'accès

Les cartes doivent être personnalisées par l'écriture de clés émetteur, d'un code porteur et d'un jeu secret propre à chaque carte ou constant.

Diversification clés émetteur code porteur et jeu secret

Diversifier les clés, le code porteur et le jeu secret consiste à produire ces éléments de façon unique pour chaque carte.

Procédure de diversification

Une procédure possible pour calculer les clés émetteur, le code porteur et le jeu secret de façon unique pour chaque carte, est de réaliser ce calcul à partir d'un paramètre déjà unique à chaque carte :

par exemple le numéro de série.

Ce calcul peut aussi être réalisé par l'exécution d'une fonction TELEPASS ou D.E.S. sur une carte Bull CP8 dédiée à cet usage appelée carte mère.

Les cartes personnalisées à partir de cette carte mère sont les cartes filles.

Choix de la carte mère

La carte mère est choisie en fonction du type de cartes filles à personnaliser :

- une carte mère avec algorithme TELEPASS pour personnaliser les cartes SCOT 10, SCOT 50, SCOT 100 ;
- une carte mère avec algorithme D.E.S. pour personnaliser les cartes SCOT 20 DES, SCOT 60 DES, SCOT 110 DES.

Carte mère

La carte mère est caractérisée par :

- un jeu secret mère connu du seul émetteur habilité à personnaliser des cartes pour une application donnée,

- quatre mots situés en zone de transactions (ou autre) à l'adresse désignée sur la figure par W, utilisés pour différencier les résultats R de la fonction TELEPASS ou D.E.S pour obtenir :

  .l'un le jeu secret,
  .l'un une clé 1A,
  .l'un une clé 1B,
  .l'un un code porteur.

Carte fille

Les clés, le code porteur et le jeu secret de chaque carte fille sont fonction de :

- la carte elle-même par son numéro de série,

- la carte mère par le **JEU SECRET MERE** et de **mots** situés dans la zone de transactions.

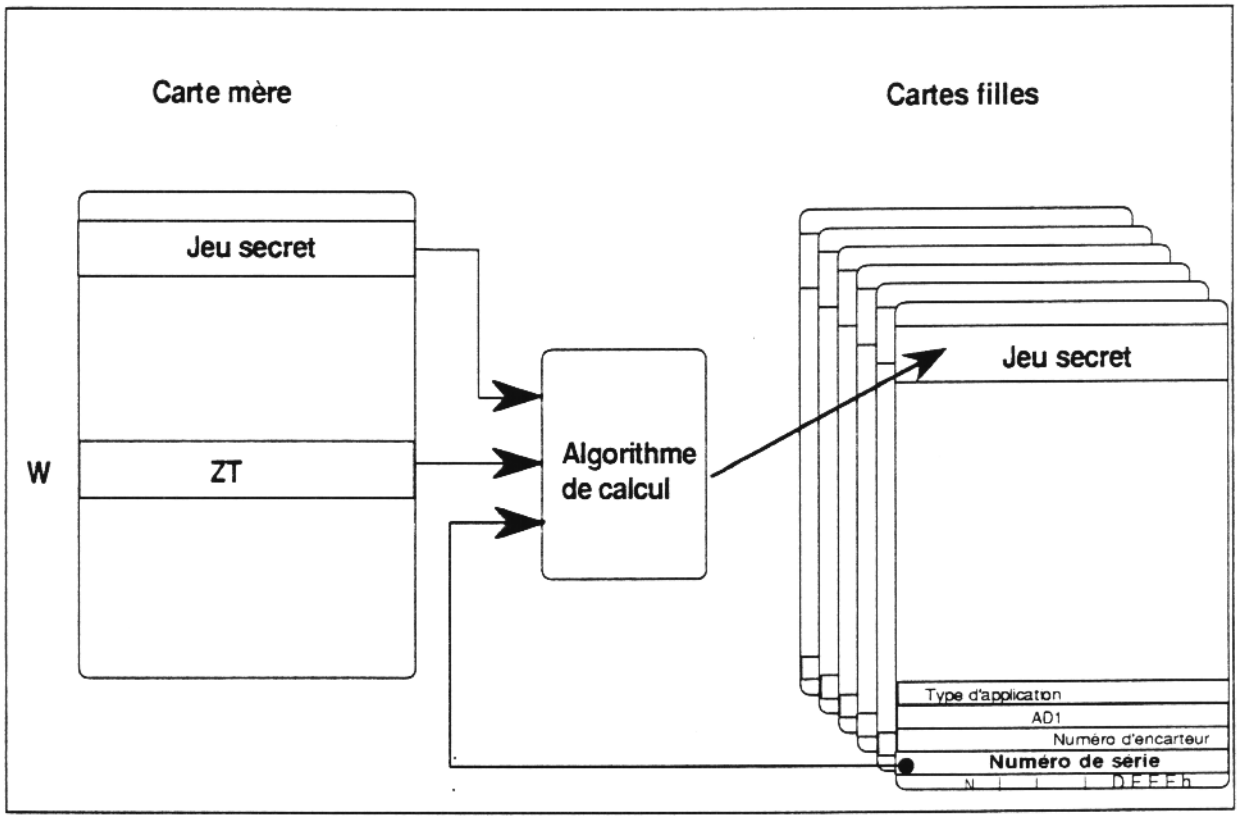

Figure 8.7 - Principe général de diversification.

Calcul des clés, du code porteur et du jeu secret d'une carte fille

- lecture dans la carte fille des 11 bits constituant le numéro d'encarteur et des 26 bits du numéro de série,

- formatage des données d'entrée externes de la fonction TELEPASS ou D.E.S. à faire exécuter par la carte mère,

- formatage du résultat R obtenu afin de générer les clés, le code porteur et le jeu secret définitifs.

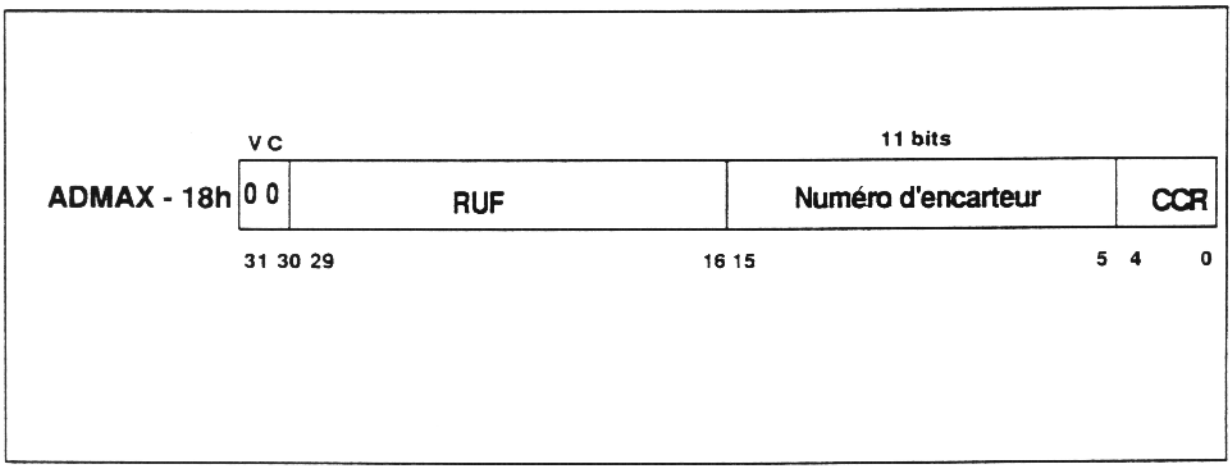

Figure 8.8 - Visualisation du numéro d'encarteur dans la mémoire de la carte.

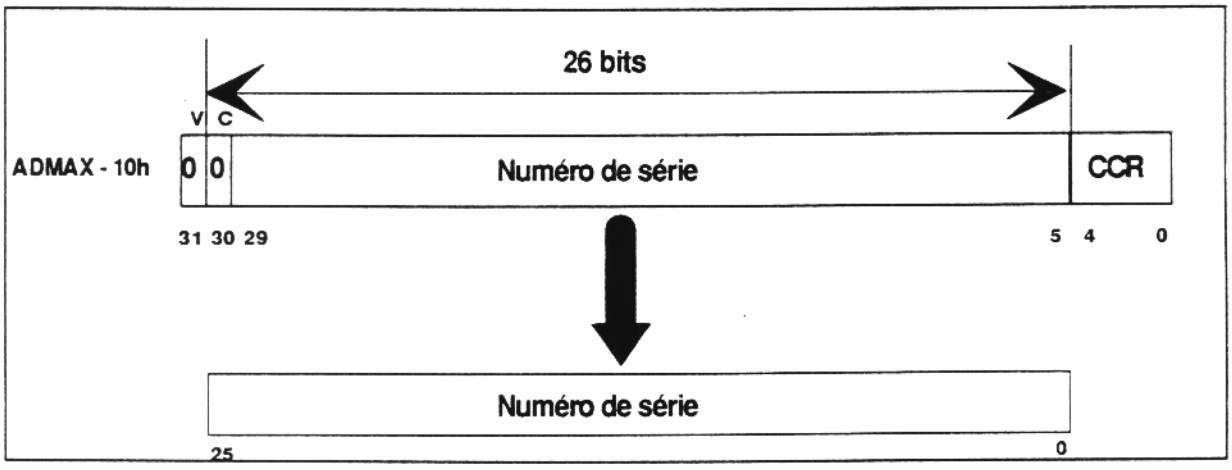

Figure 8.9 - Visualisation du numéro série dans la mémoire de la carte.

Formatage de l'entrée E de la fonction TELEPASS ou D.E.S.

Les 48 bits de données formant la valeur E d'entrée dans la fonction TELEPASS ou D.E.S. sont formatés comme le montre la figure ci-dessous.

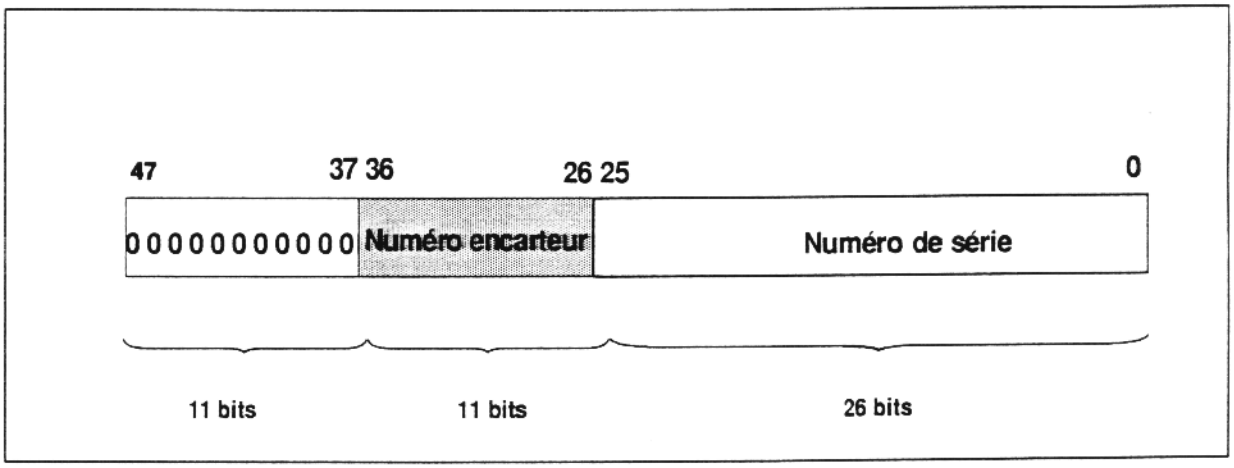

Figure 8.10 - Formatage de l'entrée E de la fonction TELEPASS ou D.E.S..

Choix de ADR utilisé pour la fonction TELEPASS ou D.E.S.

ADR	0888h	0890h	0898h	08A0h
Nom symbolique	W0	W1	W2	W3
Elément de la carte fille obtenu	Jeu secret	Clé 1A	Clé 1B	Code 2A

Dans chacun des cas, ADR pointe sur un des quatre mots de la carte mère. Les contenus de ces mots sont différents et choisis arbitrairement.

Calcul final

La fonction TELEPASS ou la fonction D.E.S. exécutée par la carte mère, délivre un résultat R.

Fabrication du jeu secret

* Après une fonction TELEPASS

Le jeu secret est constitué de 3 mots tels que :

1er mot R1 = 32 bits de poids forts de R
2ème mot R2 = 32 bits de poids faibles de R
3ème mot OU exclusif de R1 et R2.

Dans chacun de ces mots, les deux bits de poids forts sont positionnés à 0 :

bits V et C positionnés à 0.

* Après une fonction D.E.S.

Si le résultat R est constitué de 8 octets tels que :

R0	R1	R2	R3
R4	R5	R6	R7

le jeu secret est composé de 3 mots comme suit :

3Fh	**R0**	**R1**	**R2**
3Fh	**R3**	**R4**	**R5**
3Fh	**R6**	**R7**	**FFh**

Clés 1A/B et code porteur 2A

Après une fonction TELEPASS ou D.E.S., les clés et le code porteur sont constitués, par exemple, de deux mots comme suit :

1er mot R1 = 32 bits de poids forts de R

2ème mot R2 = 32 bits de poids faibles de R

Ecriture des clés, du code porteur et du jeu secret

Ces éléments sont calculés et sont inscrits dans la zone secrète et les pointeurs correspondants sont inscrits en zone de fabrication :

- ADS

- AD2

- ADM

puis le calcul de CCR associé est exécuté et inscrit pour chacun de ces pointeurs.

Zone d'accès : détermination de la taille

Le personnalisateur réserve n mots vierges à partir de ADM, il en déduit l'adresse ADC.

Il inscrit le pointeur ADC puis calcule et inscrit le CCR associé.

Tailles minimales et maximales de la zone d'accès :

Modèles	Taille minimale	Taille maximale
SCOT 10 et SCOT 20 DES	1 mot	2025 mots
SCOT 50 et SCOT 60 DES	2 mots	238 mots
SCOT 100 ET SCOT 110 DES	2 mots	525 mots

8.6 Personnalisation des zones

Les cartes doivent être personnalisées par l'écriture dans la zone de transactions, la zone de lecture et la zone confidentielle des données propres à l'application.

Zones de travail

Le personnalisateur établit en fonction de son application, le nombre, la taille et le rôle des zones. Il inscrit les pointeurs manquants :

- ADT

- ADL

et calcule et inscrit les CCR associés.

Ecriture du verrou LC

Le personnalisateur positionne le verrou **LC** marquant la fin de la phase de personnalisation.

Les données propres à l'application sont ensuite mises en place.

Mise en place des données de l'application

Il écrit en zone(s) de travail en fonction des protections d'écriture (EPi) et après présentation des clés émetteur ou du code porteur.

Les deux figures ci-contre montrent l'état de la mémoire avant et après cette dernière étape.

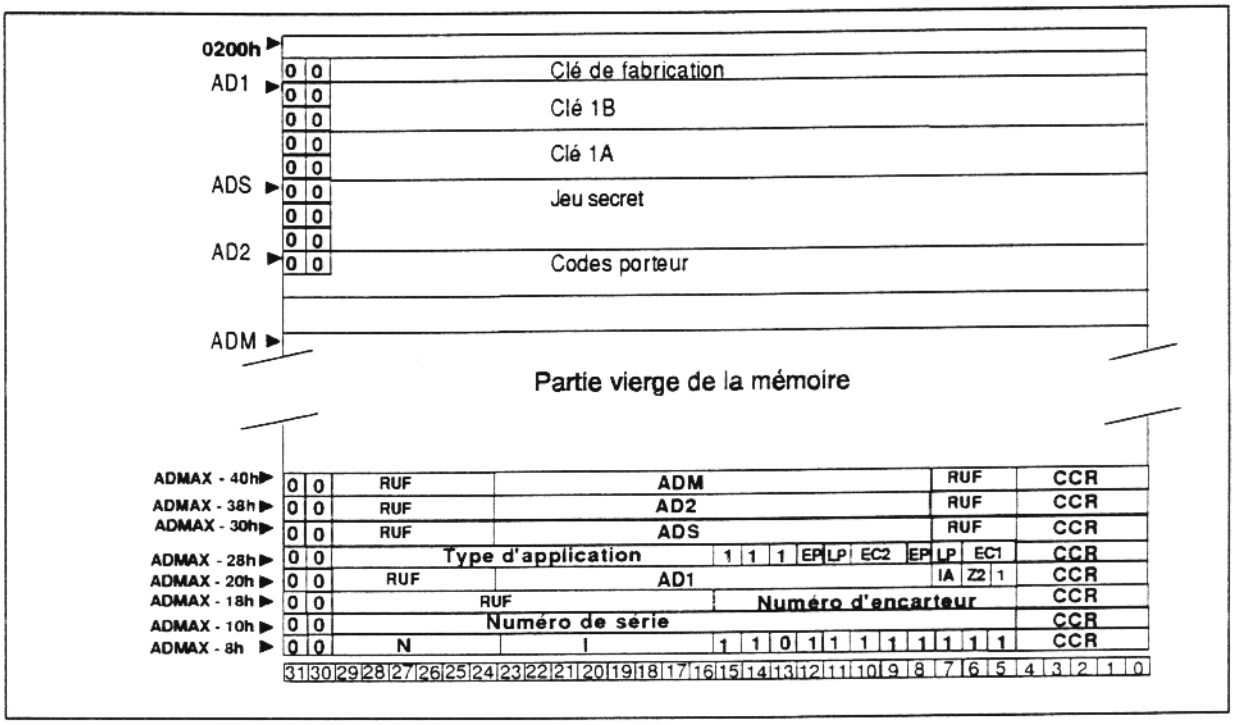

Figure 8.11 - Etat de la mémoire avant insertion des données de l'application.

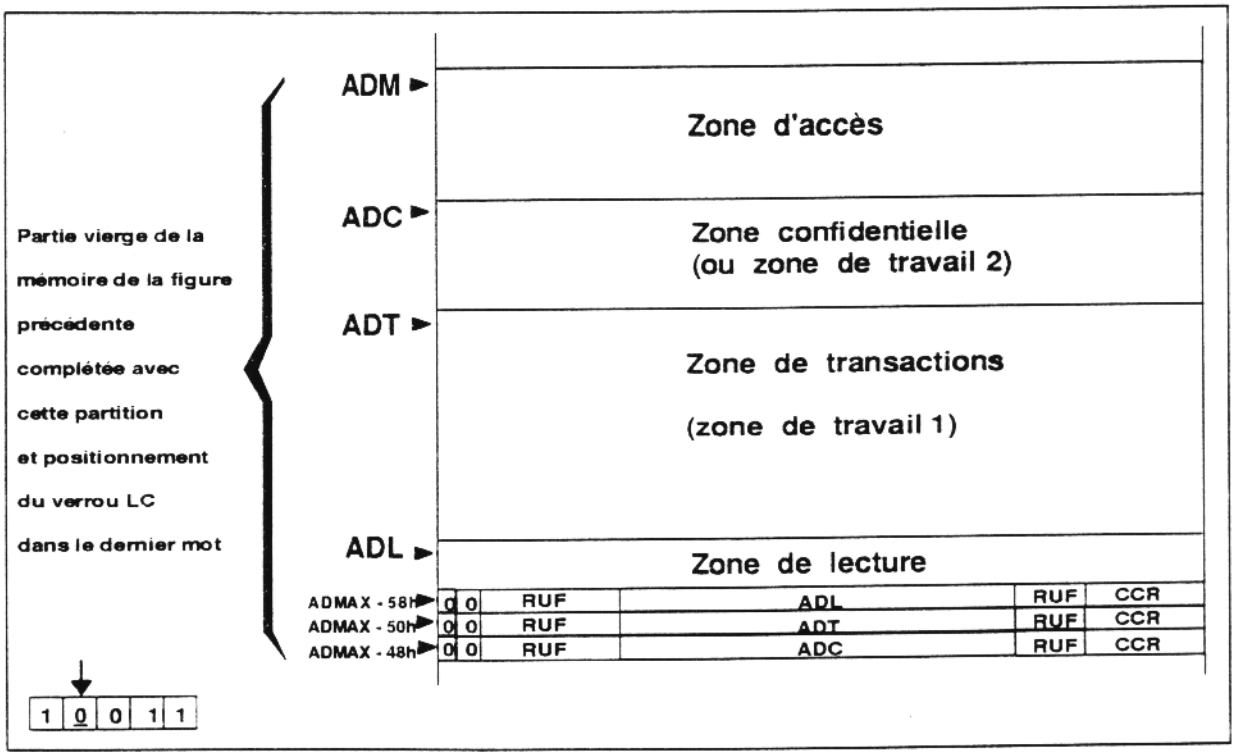

Figure 8.12 - Etat de la mémoire après insertion des données de l'application.

- ANNEXES -

ANNEXES

Annexe A - Performances

Les temps d'exécution des ordres sont indiqués pour chaque modèle dans un tableau.

Les temps sont donnés en millisecondes avec une précision d'une unité.

Le temps d'exécution d'un ordre est le temps écoulé entre le moment où la carte reçoit le premier octet et le moment où elle renvoie le dernier octet.

Temps d'exécution des ordres en phase de personnalisation

Performance en ms	SCOT 10 SCOT 20 DES (SPOM11)	SCOT 50 SCOT 60 DES (SPOM24)	SCOT 100 SCOT 110 DES (SPOM21)
B0h **Lecture** à partir de 0300h 4 octets 64 octets 256 octets	 20 122 448	 18 118 434	 20 119 435
D0h **Ecriture** 4 octets (=FFh)	24	28	29
A0h **Recherche du premier mot vierge** à partir de 0228h mot non trouvé	2219	263	773
C0h **Lecture de résultat**	24	22	24
50h **Ecriture des verrous** (Verrou LC)	25	35	36
0Eh **Effacement domaine** 1 mot en 0500h	sans objet	27	28
20h **Présentation de clé de fabrication**	18	17	18
40h **Validation de clé ou code en lecture**	19	23	25
70h **Validation en écriture** en 0300h	20	24	25
Remise à zéro	28	26	51

Temps d'exécution des ordres en phase d'utilisation

Pour ces exemples de mesures, la zone d'accès est de 4 mots.

Performance en ms	**SCOT 10** **SCOT 20 DES** (SPOM11)	**SCOT 50** **SCOT 60 DES** (SPOM24)	**SCOT 100** **SCOT 110 DES** (SPOM21)
B0h **Lecture** à partir de 0300h 4 octets 64 octets 256 octets	 22 123 450	 20 119 434	 21 121 437
D0h **Ecriture** un mot en 300h	28	36	33
A0h **Recherche d'un mot sur argument** à partir du début de zone de travail mot inexistant	2192	206	760
A8h **Recherche du premier mot non vierge**	mémoire vierge 0298h à 4180h 2213	mémoire vierge 0298h à 09A8h 248	mémoire vierge 0298h à 18E0h 754
C0h **Lecture de résultat**	25	23	24
50h **Ecriture** **des verrous** (Verrou IV)	25	36	37
0Eh **Effacement domaine** 1 mot 10 mot 20 mot 200 mots	sans objet	33 140 260 2426	30 139 259 2433

Performance en ms	**SCOT 10** **SCOT 20 DES** (SPOM11)	**SCOT 50** **SCOT 60 DES** (SPOM24)	**SCOT 100** **SCOT 110 DES** (SPOM21)
C4h **Calcul de nombre aléatoire** (après une RAZ)	49 56	sans objet	44
10h, 30h, 20h **Présentation en clair de clé ou code** clé 1A clé 1B code clé déblocage	27 28 22 41	25 26 20 39	27 27 22 41
18h, 38h, 28h **Présentation chiffrée de clé** clé 1A clé 1B clé de déblocage	46 47 60	sans objet	46 46 59
40h **Validation de clé ou code en lecture**	25	33	35
70h **Validation en écriture** Zone d'accès vierge	29 35	41 51	41 52
80h **Calcul de certificat** TELEPASS D.E.S.	93 60	87 128	92 59
D2h **Changement code porteur**	sans objet	52 (SCOT 60 DES)	54 (SCOT 110 DES)

Remise à zéro	32	35	61

Annexe B - Mots d'état des systèmes d'exploitation de la famille SCOT

Cette section récapitule pour chacun des ordres les valeurs des mots d'état.

Mots d'état

Les mots d'état sont décrits fonctionnellement dans la section "Eléments d'un ordre" du chapitre "DIALOGUE CARTE - CAD".

Convention d'écriture

Dans cette section, lorsqu'un digit est représenté par la lettre X, sa valeur dépend de l'état de la carte :

Etat de la carte	Valeur de X
Carte en accès	X = 0h
Carte en erreur porteur (1 erreur)	X = 1h
Carte en erreur porteur (2 erreurs)	X = 2h
Carte en état de blocage	X = 4h
Carte saturée	X = 8h

Cas de mutisme et mots d'état ME2 significatifs d'erreur pour chaque ordre

REMISE A ZERO	

Mutisme :

* Un des pointeurs de la zone de fabrication (de AD1 à ADL) n'est pas validé.

ME2 = 10h

* Carte en erreur (1 erreur).

ME2 = 20h

* Carte en erreur (2 erreurs).

ME2 = 40h

* Carte bloquée.

ME2 = 80h

* Carte saturée.

LECTURE	B0h

Mutisme :

* 'P1P2' n'adresse pas un mot accessible en lecture (règles non respectées).

* Carte invalidée et clé émetteur non présentée.

ECRITURE	D0h

Mutisme :

* 'P1P2' adresse un mot non accessible en écriture.

* 'P1P2' n'est pas une adresse multiple de 8.

* P3 # 04h.

* Carte invalidée.

* Carte saturée.

ME2 = 01h

* 'P1P2' pointe un mot déjà validé.

RECHERCHE sur argument	A0h
RECHERCHE 1er mot vierge	A0h
RECHERCHE 1er mot non vierge	A8h

Mutisme :

* 'P1P2' n'est pas une adresse multiple de 8.
* P3 # 00h ou P3 # 02h et INS = A0h.
* P3 # 00h et INS = A8h.
* Carte invalidée et clé émetteur non présentée.

ME2 = X4h

* 'P1P2' pointe un mot dont les règles de lecture ne sont pas respectées.

ME2 = X8h

* Le mot recherché n'a pas été trouvé.

LECTURE DE RESULTAT	C0h

Mutisme :

* P3 # 08h.

ECRITURE DES VERROUS	50h

Mutisme :

* P3 # 02h.

EFFACEMENT DE DOMAINE	0Eh

Mutisme :

* 'P1P2' n'est pas une adresse multiple de 8.
* DATA (1er mot à ne plus effacer) est inférieure ou égale à 'P1P2'.
* DATA dépasse la zone autorisée à être effacée.
* DATA n'est pas une adresse multiple de 8.
* P3 # 02h.
* Carte saturée.
* Carte invalidée.
* Les conditions d'effacement interdisent totalement l'effacement.

ME2 = X4h

* 'P1P2' n'adresse pas un mot appartenant à un domaine autorisé à l'effacement.
* La clé requise par les conditions d'effacement n'a pas été présentée correctement.

ME2 = 01h

* Incident d'effacement (bit V non effacé).

Nota : Dans la suite du texte, les fonctionnalités marquées de "*" ne sont développées que dans SCOT 20 DES et SCOT 110 DES ; cela signifie que si un tel ordre est envoyé aux autres modèles, les cartes répondent ME1 = 6Dh.

*

DEMANDE DE NOMBRE ALEATOIRE	C4h

Mutisme :

* Algorithme exploité est TELEPASS.
* Le jeu secret n'est pas composé de 3 mots validés.
* Pointeurs ADS et AD2 non cohérents.
* P3 # 08h.

PRESENTATION CLE EMETTEUR 1A	10h

Mutisme :

* Le nombre de mots validés composant la clé 1A en zone secrète ne correspond pas au nombre d'octets reçus par la carte.
* P3 # 08h.
* Carte bloquée.

PRESENTATION CLE EMETTEUR 1B	30h

Mutisme :

* Le nombre de mots validés composant la clé 1B en zone secrète ne correspond pas au nombre d'octets reçus par la carte.
* P3 # 08h.
* Le pointeur ADS - 10h est inférieur ou égal au pointeur AD1 + 8h.
* Carte bloquée.

PRESENTATION CODE PORTEUR	20h

Mutisme :

* Le nombre de mots validés composant le code porteur en zone secrète ne correspond pas au nombre d'octets reçus par la carte.
* P3 # 08h ou P3 # 04h.
* Le pointeur ADM-10h est inférieur ou égal au pointeur AD2 + 8h.
* Carte bloquée.

PRESENTATION DE CLE DE DEBLOCAGE	20h

Mutisme :

* Le nombre de mots validés composant le code porteur et la clé 1A en zone secrète ne correspond pas au nombre d'octets reçus par la carte.
* P3 # 0Ch ou P3 # 10h.
* Carte non bloquée.

* | PRESENTATION CHIFFREE DE CLE 1A | 18h

Mutisme :

- Algorithme de la carte # D.E.S..
- Nombre aléatoire non fourni auparavant par la carte.
- Le nombre de mots validés composant la clé 1A en zone secrète ne correspond pas au nombre d'octets reçus par la carte.
- P3 # 08h.
- Carte bloquée.

* | PRESENTATION CHIFFREE DE CLE 1B | 38h

Mutisme :

- Algorithme de la carte # D.E.S..
- Nombre aléatoire non fourni par la carte.
- Le nombre de mots validés composant la clé 1B en zone secrète ne correspond pas au nombre d'octets reçus par la carte.
- Le pointeur ADS - 10h est inférieur ou égal au pointeur AD1 + 8h.
- P3 # 08h.
- Carte bloquée.

* | PRESENTATION CHIFFREE CLE DEBLOCAGE | 28h

Mutisme :

- Algorithme de la carte # D.E.S..
- Nombre aléatoire non fourni par la carte.
- Le nombre de mots validés composant le code porteur et la clé 1A en zone secrète ne correspond pas au nombre d'octets reçus par la carte.
- P3 # 0Ch ou P3 # 10h.
- Carte non bloquée.

VALIDATION DE LECTURE	40h

Mutisme :

* Carte déjà saturée.
* Carte en 1 ou 2 erreurs porteur et la clé présentée précédemment est une clé émetteur.
* P3 # 00h.
* Carte bloquée et aucune clé n'a été présentée auparavant.
* Carte invalidée et la clé émetteur 1A ou 1B n'a pas été présentée au préalable.

ME2 = 14h

* Première présentation de code porteur erroné.

ME2 = 24h

* Deuxième présentation de code porteur erroné.

ME2 = 44h

* Carte en état de blocage.
* Troisième présentation de code porteur erroné.
* Première présentation de clé émetteur (1A ou 1B) erronée.
* Clé émetteur 1A erronée lors de la présentation de la clé de déblocage.

ME2 = 4Ch

* Code porteur (au minimum) faux lors d'un déblocage.

ME2 = 80h

* Carte saturée.

ME2 = X5h

* Incident d'écriture.

VALIDATION D'ECRITURE	70h

Mutisme :

* 'P1P2' adresse un mot non accessible en écriture.
* 'P1P2' n'est pas une adresse multiple de 8.
* P3 # 00h.
* Carte invalidée.
* Carte déjà saturée.

ME2 = 01h

* 'P1P2' adresse un mot déjà validé.

Dans le cas où la zone de travail est protégée en écriture :

Mutisme :

* Les bits système (C, CA) ne correspondent pas à la clé présentée.
* Carte en 1 ou 2 erreurs porteur et le bit C vaut 1.
* Carte bloquée et aucune présentation de clé ou code n'a eu lieu.

ME2 = 14h

* Première présentation de code porteur erroné.

ME2 = 24h

* Deuxième présentation de code porteur erroné.

ME2 = 44h

* Carte en état de blocage.
* Troisième présentation de code porteur erroné.
* Première présentation de clé émetteur (1A ou 1B) erronée.
* Clé émetteur 1A erronée lors de la présentation de la clé de déblocage.

ME2 = 4Ch

* Code porteur (au minimum) faux lors d'un déblocage.

ME2 = 80h

* Carte saturée.
* La taille de la zone d'accès est nulle ou de 1 mot.

ME2 = X5h

* Incident d'écriture.

CALCUL DE CERTIFICAT	80h

Mutisme :

* 'ADR' adresse un mot dont les conditions de lecture ne sont pas respectées.
* P3 # 08h.
* Le jeu secret n'est pas composé de 3 mots validés.
* Pointeurs ADS et AD2 non cohérents.
* Carte invalidée.

Valable pour SCOT 60 DES et SCOT 110 DES

CHANGEMENT DE CODE PORTEUR	D2h

Mutisme :

* P3 # 04h.
* Code porteur 2B actif.
* Bit C du nouveau code = 1.
* Bit V du nouveau code = 1.

ME2 = 04h

* Code porteur 2A faux.

ME2 = 01h

* Incident d'écriture.

Annexe C - Disponibilité des ordres en fonction des indicateurs

Cette section récapitule pour chacun des ordres sa validité en fonction des indicateurs.

Indicateurs (Rappel)

Indicateurs IEx, IT et IF

Ces indicateurs sont inclus dans le mot d'état ME2.

IEx indique l'état de la carte :

- IE2 = 1 signifie carte en erreur code porteur (2 erreurs successives)
- IE1 = 1 signifie carte en erreur code porteur (1 erreur)

IT = 1 signifie carte bloquée

IF = 1 signifie carte saturée

Ces indicateurs sont décrits dans la section "Eléments d'un ordre" du chapitre "DIALOGUE CARTE - CAD" dans le paragraphe "Compte-rendu de la carte".

Indicateurs IIV

L'indicateur IIV est inclus dans l'octet MCH.

IIV = 1 signifie carte invalidée

Cet indicateur est décrit dans la section "Remise à zéro" du chapitre "DIALOGUE CARTE - CAD" dans le paragraphe "Octets d'application".

Notations pour le tableau ci-après

OUI : l'ordre est disponible,

Erreur : l'ordre est refusé, la carte renvoie un code d'erreur,

NON : l'ordre est rejeté par la carte entraînant le mutisme.

Ordre disponible	INS	IEx	IT	IF	IIV
Lecture	B0h	OUI	OUI	OUI	OUI
Ecriture	D0h	OUI	OUI	NON	NON
Recherche d'un mot sur argument	A0h	OUI	OUI	OUI	OUI
Recherche du premier mot vierge	A0h	OUI	OUI	OUI	OUI
Recherche premier mot non vierge	A8h	OUI	OUI	OUI	OUI
Lecture de résultat	C0h	OUI	OUI	OUI	OUI
Ecriture des verrous	50h	OUI	OUI	OUI	OUI
Effacement domaine	0Eh	Erreur	Erreur	NON	NON
Demande de nombre aléatoire	C4h	OUI	OUI	OUI	OUI
Présentation en clair de clé ou code	10h 30h 20h	OUI	NON	OUI	OUI
Présentation clé de déblocage	20h 28h	NON	OUI	f(IT)	f(IT)
Présentation chiffrée de clé	18h 38h	OUI	NON	OUI	OUI
Validation de clé ou code	40h	OUI	OUI	NON	OUI
Validation en écriture	70h	OUI	OUI	NON	NON
Calcul de certificat	80h	OUI	OUI	OUI	NON
Changement code porteur	D2h	Erreur	Erreur	Erreur	Erreur

Annexe D - Accessibilité des zones en fonction des protections

Accessibilité en lecture

Option : 2 Zones de Travail

Zones	Adresses	LP2 = 1 LP1 = 1	LP2 = 1 LP1 = 0	LP2 = 0 LP1 = 1	LP2 = 0 LP1 = 0
ZS	[0200h, ADM[	Interdite	Interdite	Interdite	Interdite
ZA	[ADM, ADC[	Protégée	Protégée	Protégée	Protégée
ZT2 (ZC)	[ADC, ADT[	Libre	Libre	Protégée	Protégée
ZT1	[ADT, ADL[	Libre	Protégée	Libre	Protégée
ZL + ZF	[ADL, ADMAX[	Libre	Libre	Libre	Libre

Option : 1 zone de travail

Le tableau est identique à celui qui précède excepté la zone confidentielle (ZC) qui n'est plus, comme ci-dessus, une zone de travail.

ZC	**[ADC, ADT[**	Protégée	Protégée	Protégée	Protégée

Accessibilité en écriture

Option : 2 zones de travail

Zones	Adresses	EP2 = 1 EP1 = 1	EP2 = 1 EP1 = 0	EP2 = 0 EP1 = 1	EP2 = 0 EP1 = 0
ZS	[0200h, ADM[	Interdite	Interdite	Interdite	Interdite
ZA	[ADM, ADC[	Interdite	Interdite	Interdite	Interdite
ZT2 (ZC)	[ADC, ADT[	Libre	Libre	Protégée	Protégée
ZT1	[ADT, ADL[	Libre	Protégée	Libre	Protégée
ZL + ZF	[ADL, ADMAX[	Interdite **sauf verrous**	Interdite **sauf verrous**	Interdite **sauf verrous**	Interdite **sauf verrous**

Option : 1 zone de travail

Le tableau est identique à celui qui précède excepté la zone confidentielle (ZC) qui n'est plus, comme ci-dessus, une zone de travail.

ZC	[ADC, ADT[	Interdite	Interdite	Interdite	Interdite

Accessibilité en effacement

Option : 2 zones de travail

Zones	Adresses	Effacement
ZS	[0200h, ADM[	Interdit
ZA	[ADM, ADC[	Interdit
ZT2 (ZC)	[ADC, ADT[	f(EC2)
ZT1	[ADT, ADL[	f(EC1)
ZL + ZF	[ADL, ADMAX[	Interdit

Signification des indicateurs ECi : f(ECi)

ECi = 11 effacement interdit
ECi = 10 effacement protégé par le code porteur actif
ECi = 01 effacement protégé par la clé 1B
ECi = 00 effacement protégé par la clé 1A

Option : 1 zone de travail

Le tableau est identique à celui qui précède excepté la zone confidentielle (ZC) qui n'est plus, comme ci-dessus, une zone de travail.

ZC	[ADC, ADT[	Interdit

Annexe E - Liste récapitulative des ordres

Cette section récapitule pour chacun des ordres :

- les valeurs des Eléments de l'ordre,
- la valeur de l'octet d'acquittement selon les modèles.

Eléments des ordres

Les Eléments de l'ordre sont décrits dans le chapitre "DIALOGUE CARTE - CAD" dans la section "Eléments d'un ordre".

Ordre	INS	'P1P2'	P3	DATA	Type S Sortant E Entrant
Lecture	B0h	Adresse début de lecture	Nombre octets		S
Ecriture	D0h	Adresse du mot à écrire	04h	4 octets à écrire	E
Recherche argument	A0h	Adresse de début de recherche	02h	Argument 2 octets	E
Recherche mot vierge	A0h	" "	00h		E
Recherche mot non vierge	A8h	" "	00h		E
Lecture résultat	C0h	00 00h	08h		S
Ecriture verrou	50h	00 00h	02h	2 octets	E
Effacement	0Eh	Adresse de début d'effacement	02h	Adresse de fin d'efface-ment	E

Ordre	INS	'P1P2'	P3	DATA	Type S Sortant E Entrant
Nombre aléatoire	C4h	00 00h	08h		S
Présentation en clair **code porteur** **Clé débloc** **Clé 1A** **Clé 1B**	 20h 20h 10h 30h	 00 00h 00 00h 00 00h 00 00h	 04h ou 08h 0Ch ou 10h 08h 08h	 Code Clé débl. Clé 1A Clé 1B	 E E E E
Présentation clé chiffrée **Clé débloc** **Clé 1A** **Clé 1B**	 28h 18h 38h	 00 00h 00 00h 00 00h	 0Ch ou 10h 08h "	 Clé débl. Clé 1A Clé 1B	 E E E
Validation lecture	40h	00 00h	00h		E
Validation écriture	70h	Adresse du mot à valider	00h		E
Calcul certificat	80h	00 00h	08h	E = 6 octets + Adr = 2 octets	E
Changement Code porteur	D2h	00 00h	04h	Nouveau code = 4 octets	E

Octet d'acquittement

L'octet d'acquittement est décrit dans le chapitre "DIALOGUE CARTE - CAD" dans la section "Introduction", paragraphe "Mode du dialogue".

Ordre	INS	VPP nécessaire	MODE S = simple A = asservi	OCTET d'acquittement
Lecture	B0h		S	B0h
Ecriture Modèles SCOT 10 et SCOT 20 DES	D0h	oui	S S	D0h D1h
Recherche d'un mot sur argument	A0h		S	A0h
Recherche du premier mot vierge	A0h		S	A0h
Recherche premier mot non vierge	A8h		S	A8h
Lecture de résultat	C0h		S	C0h
Ecriture des verrous Modèles SCOT 10 et SCOT 20 DES	50h	oui	S S	50h 51h
Effacement domaine Sauf modèles SCOT 10 et SCOT 20 DES	0Eh		S	0Eh
Demande de nombre aléatoire Modèle SCOT 20 DES	C4h	oui	S S	C4h C5h

Ordre	INS	VPP nécessaire	MODE S = simple A = asservi	OCTET d'acquittement
Présentation en clair de clé ou code Clé 1A Clé 1B Code porteur	 10h 30h 20h		 S S S	 10h 30h 20h
Présentation en clair clé de déblocage Code 2A Clé 1A	20h		 A S	 DFh 20h
Présentation chiffrée de clé Modèles SCOT 20 DES et SCOT 110 DES Clé 1A Clé 1B	 18h 38h		 S S	 18h 38h
Présentation chiffrée clé de déblocage code 2A (en clair) clé 1A (chiffrée)	28h		 A S	 D7h 28h
Validation de clé ou code Modèles SCOT 10 et SCOT 20 DES	40h	oui	S S	40h 41h
Validation en écriture Modèles SCOT 10 et SCOT 20 DES	70h	oui	S S	70h 71h
Calcul de certificat	80h		S	80h
Changement code porteur Modèles SCOT 60 DES et SCOT 110 DES	D2h		S	D2h

- INDEX DES -

- MOTS ET EXPRESSIONS -

INDEX DES MOTS ET EXPRESSIONS DE CE MANUEL

PAGE

A

Accès à la carte 35
ADR en personnalisation
    Donnée d'entrée de TELEPASS ou D.E.S. 159
Adresse
    AD1 (rôle en phase de personnalisation) 150
    Adresse du mot recherché 104
    Définition 7
Adresse
    AD1 24
    AD2 24
    ADC 24
    ADL 24
    ADM 24
    ADMAX - 8h 24
    ADS 24
    ADT 24
Algorithme
    Algorithme cryptographique D.E.S. 50
    Algorithme cryptographique TELEPASS 49
    Identification 17
Aspect physique de la carte 3
Asservi
    Mode asservi 87
Authentification
    Authentification d'une carte 59
    Définition 9

B

Bit
    Bit C et Bit CA 22
    Bit non positionné 21
    Bit positionné 21
    Bit V de validation 22
Bits système 22
Blocage
    Cas de blocage 69
    Définition 11

C

C
Voir Bit 22
CA
Voir Bit 22
CAD
Définition 7
Calcul de certificat
Ordre 14, 126
Caractéristiques de la carte 86
Carte bloquée 69
Carte fille 157
Carte LOT 147
Carte mère 157
Cartes prépersonnalisées 147
Cartes SCOT
Zones et adresses des zones 23
CCR 24
Calcul du CCR 155
Certificat 58
Contrôle de certificat 59
Certification
Définition 9
Opération 14, 145
Certification d'un mot 58
Changement de code porteur
Opération 14, 137
Ordre 14, 128
Chiffrement
Définition 9
CLA 78
Clé
Clé de déblocage 53
Clé émetteur 1A 53
Clé émetteur 1B 53
Définition 9
Gestion des clés et du jeu secret 53
Nombre de tentatives de présentation 53
Présentation chiffrée 54
Présentation en clair 54
Clé "diversifiée" 54
Clé de fabrication 150
Calcul en phase personnalisation 151
Formatage définitif en phase personnalisation 153
Code porteur
Code 2A 53
Code 2B 53
Définition 9
Nombre de tentatives de présentation 53
Compte-rendu de la carte 80
Conditions d'utilisation d'un ordre 88
Connexions de la carte 4

D

D.E.S.
Mise en oeuvre 51
Voir Algorithme 49
Déblocage d'une carte
Opération 14, 135
Déblocage de la carte
Cas de déblocage 69
Demande de nombre aléatoire
Ordre 13, 115
Déroulement d'un ordre 76
Dialogue Carte CAD
Eléments de dialogue 73
Fonctions de dialogue 73
Introduction 73
Mode du dialogue 75
Sens du dialogue 73
Diversification 54
Diversification clés, code et jeu secret
Personnalisation 156
Domaines
autorisés en écriture 95
autorisés en effacement 113
autorisés en lecture 91
autorisés en recherche 98

E

EC1 ..... 37, 40, 44
EC2 ..... 37, 40, 44
ECi 24
Ecriture
Mise en oeuvre de l'écriture libre 41
Mise en oeuvre de l'écriture protégée 41
Ordre 12, 93
Principe 40
Ecriture des verrous
Ordre 13, 109
Ecriture protégée
Opération 14, 131
Ecritures en zone d'accès 64
Effacement
Mise en oeuvre 45
Opération 14, 133
Principe 44
Effacement de domaine
Ordre 13, 112
Encartage
Voir le terme Fabrication 8
Entrant
Ordre entrant 73
Type entrant 87
Entrée/Sortie
Point de connexion 4
EPi
Indicateur de protection 24

F

Fabrication
Définition 8
Famille SCOT 15
Evolution 16
Fenêtre 62
Fenêtre courante 62
Fenêtre en accès 66
Fenêtre en blocage 66
Fenêtre en erreur 66
Fin de vie 29
Fonction d'un ordre 87
Fonction D.E.S.
Définition 7
Fonction TELEPASS
Définition 7
Utilisation en phase personnalisation 151
Fonction TELEPASS ou D.E.S.
Utilisation en phase personnalisation 158

H

Horloge
Point de connexion 4

I

I
Numéro de diversification 150
Numéro de diversification de secret 24
IA
Indicateur d'algorithme 24
Identification de la carte 86
Opération 14, 143
Identification du modèle de carte 17
IEC 85
IEP 85
IIV 85
ILC 85
ILF 85
ILP 85
ILU 85
Indicateur d'algorithme
IA 24
Indicateur d'option
Z2 24
Indicateur de protection
EC1 24
EC2 24
EP1 24
EP2 24
LP1 24
LP2 24
INS 78
INS = 0Eh 112
INS = 20h, 10h ou 30h 117
INS = 28h, 18h ou 38h 120
INS = 40h 122
INS = 50h 109
INS = 70h 124
INS = 80h 126
INS = A0h 97, 100
INS = A8h 102
INS = B0h 90
INS = C0h 104
INS = C4h 115
INS = D0h 93
INS = D2h 128
Invalidation 29
Définition 8
Verrou IV 24
IV
Verrou 24

J

Jeu d'ordres
Introduction 87
Jeu secret
Définition 9
Gestion du jeu secret 53

L

LC
Verrou 24
Lecture
Lecture libre 38
Lecture protégée 38
Ordre 12, 90
Principe 37
Lecture de résultat
Ordre 13, 104
Lecture protégée
Opération 14, 129
LF
Verrou 24
LPi
Indicateur de protection 24
LU
Verrou 24

M

Machine de personnalisation 148
Masque
Voir "Système d'exploitation" 6
Masse
Point de connexion 4
ME1
Mot d'état 76
ME2
Détail 80
Mot d'état 76
Mémoire
Mémoire EEPROM ou EPROM
Définition 6
Mémoire RAM
Définition 6
Mémoire ROM
Définition 6
Taille des mémoires 16
Mémoire de travail (Mémoire RAM) 4
Mémoire utilisateur (Mémoire EEPROM ou EPROM) 4
Mise en oeuvre de D.E.S. 51
Mise en oeuvre de la lecture 38
Mise en oeuvre de TELEPASS 51
Mode asservi 75
Mode d'adressage d'un mot 22
Mode d'écriture dans un mot 21
Mode de présentation des clés 54
Mode simple 75
Modèle de carte 86

Mot
Définition 7
Mode d'adressage d'un mot 22
Mode d'écriture dans un mot 21
Mot de la mémoire 21
Taille utile d'un mot 22
Mots d'états 80
Mutisme de la carte 68
Définition 11
Mutisme et mot d'erreur ME2 pour chaque ordre
Calcul de certificat 176
Changement de code porteur 176
Demande de nombre aléatoire 171
Ecriture 169
Ecriture des verrous 170
Effacement de domaine 171
Lecture 169
Lecture de résultat 170
Présentation chiffrée clé déblocage 173
Présentation chiffrée de clé 1A 173
Présentation chiffrée de clé 1B 173
Présentation clé émetteur 1A 172
Présentation clé émetteur 1B 172
Présentation code porteur 172
Présentation de clé de déblocage 172
Recherche 1er mot non vierge 170
Recherche 1er mot vierge 170
Recherche sur argument 170
Remise à zéro 169
Validation d'écriture 175
Validation de lecture 174

N

N
Numéro d'identification de lot de cartes 24
Utilisation en personnalisation 150
Nombre de zones de travail
Identification 17
Numéro d'encarteur 24, 150, 158
Numéro de série 24, 150, 158

O

Octet d'acquittement 75
Octet MCE
Réponse à remise à zéro 84
Octet MCF
Réponse à remise à zéro 84
Octet MCH
Réponse à remise à zéro 85
Octets d'application
Réponse à remise à zéro 84
Octets système
Réponse à remise à zéro 83

Opérations
Séquences d'ordres 14
Ordre
Asservi 89
CLA 78
Conditions d'utilisation 89
DATA 79
Définition 7
Eléments d'un ordre 78
Entrant 7, 89
Fonction 89
Format d'un ordre 78
INS 78
P1, P2 78
P3 79
Phase d'exécution 76
Phase d'initialisation 76
Phase de fin 76
Réponse de la carte 89
Simple 89
Sortant 7, 89
TYPE et MODE 89
Validité 89
VPP 89
Ordres
Liste 12
Ordres disponibles pour chaque modèle de carte 17

P

P1 78
P2 78
P3 79
Partition de la zone de fabrication pour chaque modèle 26
Partition détaillée de la mémoire
Eléments communs 25
Personnalisation 147
Calcul final clés et jeu secret 160
Définition 8
Phase d'utilisation 29
Phase de fabrication 28
Phase de personnalisation 28
Phase de vie de la carte
Définition 9
Pointeur
Définition 7
Porteur 5
Définition 9
Prépersonnalisation
Voir le terme Fabrication 8
Présentation chiffrée de clé
Ordre 13, 120
Présentation en clair de clé ou code
Ordre 13, 117
Procédures de sécurité 47

Protections
d'écriture 40
d'effacement 44
de lecture des zones de travail 37
Définition 9
indicateur EC1 44
indicateur EC2 44
indicateur EP1 40
indicateur EP2 40
indicateur LP1 37
indicateur LP2 37
Protection de la mémoire en phase personnalisation 150
Signification des indicateurs ECi 44, 181
Signification des indicateurs EPi 40
Signification des indicateurs LPi 37
Protections de la zone confidentielle
Identification 17

Q

Quartet 22

R

RAZ
Format de la réponse à remise à zéro 82
Point de connexion 4, 82
Rôle de la remise à zéro 82
Recherche d'un mot sur argument
Ordre 12, 97
Recherche de mot
Opération 14, 141
Recherche du premier mot non vierge
Ordre 12, 102
Recherche du premier mot vierge
Ordre 12, 100
Recyclage partiel
Zone d'accès 71
Recyclage total
Zone d'accès 71
Remise à zéro 82
Réponse de la carte 36
Réponse de la carte pour chaque ordre 88
Résultat de calcul de certificat 104
RUF 24

S

Saturation 73
    Définition 11
Simple
    Mode simple 87
Sortant
    Ordre sortant 73
    Type sortant 87
Système d'exploitation (masque)
    Définition 6
Système d'exploitation (Mémoire ROM) 4

T

Taille de la mémoire
    Identification 17
Taille des Clés et codes 53
Taille des mémoires 16
Taille utile d'un mot 22
TELEPASS
    Mise en oeuvre 51
    Voir Algorithme 49
Tension de programmation VPP 75
Type d'application 24
TYPE et MODE d'un ordre 87

U

Unité centrale 4
Utilisation
    Définition 8

V

V
    Voir Bit 22
Validation de clé ou code en écriture
    Influence sur la zone d'accès 64
Validation de clé ou code en lecture
    Influence sur la zone d'accès 64
    Ordre 13, 122
Validation en écriture
    Abandon de validation 42
    Fonctionnement 42
    Ordre 13, 124
Validité d'un ordre 87
VCC
    Point de connexion 4
Verrou
    Définition 8
    LC 162
    LF 150
Verrou à positionner 109

Verrous 24
Verrou d'invalidation (IV) 29
Verrou d'utilisation (LU) 29
Verrou de fabrication (LF) 28
Verrou de personnalisation (LC) 28
Vie de la carte
Définition 5
VPP
Tension de programmation 75
VPP nécessaire pour un ordre 87

Z

Z2
Indicateur d'option 24
Zone
Définition 7
Zone confidentielle
Définition 10
Détail 19
En phase de personnalisation 147
Zone d'accès
Définition 10
Détail 19
détermination de la taille 161
Fenêtre courante 62
Recyclage 71
Remplissage 71
Saturation 73
Structure 62
Taille de la zone d'accès 161
Zone de fabrication
Définition 10
Détail 20
En phase de personnalisation 147
Zone de lecture
Définition 10
Détail 19
En phase de personnalisation 147
Zone de transactions
Définition 10
Détail 19
En phase de personnalisation 147
Zone de travail
Définition 10
Détail 19
Zone de travail 2 19
Zone secrète
Définition 10
Détail 19
En phase de personnalisation 147
Utilisation du jeu secret 49
Zones
Caractéristiques de chaque zone 18
Droits d'accès 20

- TABLE DES FIGURES -

TABLE DES FIGURES

PAGE

Figure 1.1 - Exemples d'utilisation des conventions d'écriture 2

Figure 1.2 - Aspect physique de la carte 3

Figure 1.3 - Architecture du circuit monolithique 4

Figure 1.4 - Phases de vie de la carte 5

Figure 2.1 - Comparatif des mémoires des cartes SCOT 16

Figure 2.2 - Partition de la mémoire 18

Figure 2.3 - Aspect d'un mot de la mémoire 21

Figure 2.4 - Exemple de positionnement de bits 21

Figure 2.5 - Zones et adresses des zones des cartes SCOT 23

Figure 2.6 - Partition de la mémoire des cartes SCOT 25

Figure 2.7 - Partitions de la zone de fabrication suivant les modèles 26

Figure 2.8 - Schéma des phases de vie et positionnement des verrous 27

Figure 2.9 - Diagramme de la "Vie d'une carte" 30

Figure 2.10 - Eléments de la mémoire spécifiques de la phase de fabrication 31

Figure 2.11 - Eléments de mémoire spécifiques de la phase de personnalisation 32

Figure 2.12 - Eléments de la mémoire spécifiques de la phase d'utilisation 33

Figure 2.13 - Eléments de la mémoire spécifiques de la fin de vie 34

Figure 3.1 - Moyen d'accès à la carte 36

Figure 3.2 - Diagramme de la "Lecture protégée" 39

Figure 3.3 - Rappel : aspect du mot standard protégé en écriture 41

Figure 3.4 - Diagramme de l'"Ecriture protégée" 43

Figure 3.5 - Diagramme de l'"Effacement" 46

Figure 4.1 - Schéma synthétique des mécanismes sécuritaires 48
Figure 4.2 - Représentation de l'"Algorithme TELEPASS" 49
Figure 4.3 - Représentation de l'"Algorithme D.E.S." 50
Figure 4.4 - Représentation du chiffrement 55
Figure 4.5 - Schéma de la présentation de clé en clair 56
Figure 4.6 - Schéma de la présentation de clé chiffrée 57
Figure 4.7 - Représentation du calcul de certificat 58
Figure 4.8 - Diagramme général de la certification 59
Figure 4.9 - Diagramme du calcul de certificat D.E.S 60
Figure 4.10 - Diagramme du calcul du certificat TELEPASS 61
Figure 4.11 - Schéma de la zone d'accès au début de la phase d'utilisation 63
Figure 4.12 - Exemples de l'état de la zone d'accès 66
Figure 4.13 - Exemple de l'état de la zone d'accès après validation de clés 68
Figure 4.14 - Exemple de mutisme (validation de clé émetteur) 68
Figure 4.15 - Exemples de déblocages 70
Figure 4.16 - Exemple de recyclage partiel 72
Figure 4.17 - Exemple de recyclage total 72

Figure 5.1 - Représentation de l'ordre entrant et de l'ordre sortant 74
Figure 5.2 - Schéma simplifié du déroulement d'un ordre 77
Figure 5.3 - Composition d'un ordre 78
Figure 5.4 - Exemple d'initialisation d'un ordre de lecture 79
Figure 5.5 - Exemples de mot d'état ME2 81
Figure 5.6 - Octets de réponse à remise à zéro 82
Figure 5.7 - Octets "application" (Rappel) 84
Figure 5.8 - Octets des verrous MCH 85
Figure 5.9 - Reconnaissance du modèle d'une carte 86

Figure 6.1 - Tableau des domaines autorisés en lecture 91

Figure 6.2 - Exemples d'utilisation de "Lecture" 92

Figure 6.3 - Tableau des domaines autorisés en écriture 95

Figure 6.4 - Exemples d'utilisation de "Ecriture" 96

Figure 6.5 - Tableau des domaines autorisés en recherche 98

Figure 6.6 - Exemple d'utilisation de "Recherche d'un mot sur argument" 99

Figure 6.7 - Exemple d'utilisation de "Recherche du premier mot vierge" 101

Figure 6.8 - Exemple d'utilisation de "Recherche du premier mot non vierge" 103

Figure 6.9 - Exemples d'utilisation de "Lecture de résultat" 106

Figure 6.10 - Exemples d'utilisation de "Ecriture des verrous" 111

Figure 6.11 - Tableau des domaines autorisés en effacement 113

Figure 6.12 - Exemple d'utilisation de "Effacement de domaine" 114

Figure 6.13 - Exemple d'utilisation de "Demande de nombre aléatoire" 116

Figure 6.14 - Exemples d'utilisation de "Présentation en clair de clé ou code" 119

Figure 6.15 - Exemple d'utilisation de "Présentation chiffrée d'une clé" 121

Figure 6.16 - Exemple d'utilisation de "Validation en lecture" 123

Figure 6.17 - Exemple d'utilisation de "Validation en écriture" 125

Figure 6.18 - Exemple d'utilisation de "Calcul de certificat" 127

Figure 6.19 - Exemple d'utilisation de "Changement de code porteur" 129

Figure 7.1 - Exemple d'utilisation de "Lecture protégée" 130

Figure 7.2 - Exemple d'utilisation de "Ecriture protégée" 132

Figure 7.3 - Exemple d'utilisation de "Effacement" 134

Figure 7.4 - Exemple d'utilisation de "Recyclage d'une carte" 136

Figure 7.5 - Exemple d'utilisation de "Changement de code porteur" code 2A en code 2B 139

Figure 7.6 - Exemple d'utilisation de "Changement de code porteur" code 2A en nouveau code 2A 140

Figure 7.7 - Exemple d'une opération de "Recherche de mot" 142

Figure 7.8 - Exemple d'opération "Identification de la carte" 144

Figure 7.9 - Exemple d'une opération de "Certification" 146

Figure 8.1 - Exemples de chaînes de personnalisation 148

Figure 8.2 - Etat de la mémoire avant la personnalisation 149

Figure 8.3 - Lecture et prélèvement de numéro N d'identification et du numéro I d'identification de secret 152

Figure 8.4 - Formatage de l'entrée E de la fonction TELEPASS 152

Figure 8.5 - Formatage du résultat de la fonction TELEPASS pour l'obtention de la clé de fabrication 153

Figure 8.6 - Emplacement d'un pointeur dans le mot (zone de fabrication) 154

Figure 8.7 - Principe général de diversification 157

Figure 8.8 - Visualisation du numéro d'encarteur dans la mémoire de la carte 158

Figure 8.9 - Visualisation du numéro série dans la mémoire de la carte 158

Figure 8.10 - Formatage de l'entrée E de la fonction TELEPASS ou D.E.S. calcul des clés et jeu secret fille 159

Figure 8.11 - Etat de la mémoire avant insertion des données de l'application 163

Figure 8.12 - Etat de la mémoire après insertion des données de l'application 163