NORME INTERNATIONALE

ISO/CEI 7816-4

Première édition
1995-09-01

Technologies de l'information — Cartes d'identification — Cartes à circuit(s) intégré(s) à contacts —

Partie 4:
Commandes intersectorielles pour les échanges

Information technology — Identification cards — Integrated circuit(s) cards with contacts —

Part 4: Interindustry commands for interchange

Numéro de référence
ISO/CEI 7816-4:1995(F)

Sommaire

Annexes

Avant-propos

L'ISO (Organisation internationale de normalisation) et la CEI (Commission électrotechnique internationale) forment le système spécialisé de la normalisation mondiale. Les organismes nationaux membres de l'ISO ou de la CEI participent au développement de Normes internationales par l'intermédiaire des comités techniques créés par l'organisation concernée afin de s'occuper des domaines particuliers de l'activité technique. Les comités techniques de l'ISO et de la CEI collaborent dans des domaines d'intérêt commun. D'autres organisations internationales, gouvernementales ou non gouvernementales, en liaison avec l'ISO et la CEI participent également aux travaux.

Dans le domaine des technologies de l'information, l'ISO et la CEI ont créé un comité technique mixte, l'ISO/CEI JTC 1. Les projets de Normes internationales adoptés par le comité technique mixte sont soumis aux organismes nationaux pour vote. Leur publication en tant que Normes internationales requiert l'approbation de 75 % au moins des organismes nationaux votants.

La Norme internationale ISO/CEI 7816-4 a été élaborée par le comité technique mixte ISO/CEI JTC 1, *Technologies de l'information.*

L'ISO/CEI 7816 comprend les parties suivantes, présentées sous le titre général *Technologies de l'information — Cartes d'identification — Cartes à circuit(s) intégré(s) à contacts*:

— *Partie 1: Caractéristiques physiques*

— *Partie 2: Dimensions et emplacements des contacts*

— *Partie 3: Signaux électroniques et protocoles de transmission*

— *Partie 4: Commandes intersectorielles pour les échanges*

— *Partie 5: Système de numérotation et procédure d'enregistrement d'identificateurs d'applications*

— *Partie 6: Éléments de données intersectoriels*

Les annexes A et B font partie intégrante de la présente partie de l'ISO/CEI 7816. Les annexes C, D, E et F sont données uniquement à titre d'information.

Introduction

La présente partie de l'ISO/CEI 7816 fait partie d'une série de normes décrivant les paramètres des cartes à circuit(s) intégré(s) à contacts, ainsi que l'utilisation de ces cartes pour les échanges internationaux.

Il s'agit de cartes d'identification destinées à l'échange d'informations entre le monde extérieur et le circuit intégré contenu dans la carte. En résultat d'un échange, la carte délivre des informations (résultats de calcul, données mémorisées) et/ou modifie son contenu (mémorisation de données ou d'événement).

Technologies de l'information — Cartes d'identification — Cartes à circuit(s) intégré(s) à contacts —

Partie 4:
Commandes intersectorielles pour les échanges

1 Domaine d'application

La présente partie de l'ISO/CEI 7816 spécifie

— le contenu des messages, commandes et réponses, transmis par le dispositif d'interface à la carte et vice versa,

— la structure et le contenu des octets historiques émis par la carte lors de la réponse à la remise à zéro,

— la structure de fichiers et de données, telle qu'elle est visible à l'interface lors du traitement de commandes intersectorielles pour les échanges,

— des méthodes d'accès à des fichiers et à des données dans la carte,

— une architecture de sécurité définissant des droits d'accès à des fichiers et à des données dans la carte,

— des méthodes de messagerie de sécurité,

— des méthodes d'accès aux algorithmes traités par la carte. Ces algorithmes ne sont pas décrits.

Elle ne décrit pas la mise en œuvre dans la carte et/ou dans le monde extérieur.

Elle permet encore la normalisation d'autres commandes intersectorielles et d'autres architectures de sécurité.

2 Références normatives

Les normes suivantes contiennent des dispositions, qui par suite de la référence qui en est faite, constituent des dispositions valables pour la présente partie de l'ISO/CEI 7816. Au moment de la publication, les éditions indiquées étaient en vigueur. Toute norme est sujette à révision et les parties prenantes des accords fondés sur la présente partie de l'ISO/CEI 7816 sont invitées à rechercher la possibilité d'appliquer l'édition la plus récente des normes indiquées ci-après. Les membres de la CEI et de l'ISO disposent du registre des Normes internationales en vigueur à un moment donné.

ISO 3166: 1993, *Codes pour la représentation des noms de pays.*

ISO/CEI 7812-1 : 1993, *Cartes d'identification — Identification des émetteurs — Partie 1 : Système de numérotation.*

ISO/CEI 7816-3 : 1989, *Cartes d'identification — Cartes à circuit(s) intégré(s) à contacts — Partie 3 : Signaux électroniques et protocoles de transmission.*

Amendement 1 : 1992 à l'ISO/CEI 7816-3 : 1989, — *Protocole de type T=1, transmission de blocs asynchrones en mode semi-duplex.*

Amendement 2: 1994 à l'ISO/CEI 7816-3: 1989 — *Révision de la sélection du type de protocole.*

ISO/CEI 7816-5: 1994, *Cartes d'identification — Cartes à circuit(s) intégré(s) à contacts — Partie 5: Système de numérotation et procédure d'enregistrement pour les identificateurs d'applications.*

ISO/CEI 7816-6: —[1], *Cartes d'identification — Cartes à circuit(s) intégré(s) à contacts — Partie 6: Éléments de données intersectoriels.*

ISO/CEI 8825: 1990[2], *Technologies de l'information — Interconnexion de systèmes ouverts — Spécification de règles de base, pour coder la notation de syntaxe abstraite numéro une (ASN.1).*

ISO/CEI 9796: 1991, *Technologies de l'information — Techniques de sécurité — Schéma de signature numérique rétablissant le message.*

ISO/CEI 9797: 1994, *Technologies de l'information — Techniques de sécurité — Mécanisme d'intégrité des données utilisant une fonction de contrôle cryptographique employant un algorithme de chiffrement par blocs.*

ISO/CEI 9979: 1991, *Techniques cryptographiques de données — Procédures pour l'enregistrement des algorithmes cryptographiques.*

ISO/CEI 10116: 1991, *Technologies de l'information — Modes d'opérations d'un algorithme de chiffrement par blocs de n bits.*

ISO/CEI 10118-1: 1994, *Technologies de l'information — Techniques de sécurité — Fonctions de hachage — Partie 1: Généralités.*

ISO/CEI 10118-2: 1994, *Technologies de l'information — Techniques de sécurité — Fonctions de hachage — Partie 2: Fonctions utilisant un algorithme de chiffrement par blocs de n bits.*

3 Définitions

Pour les besoins de la présente partie de l'ISO/CEI 7816, les définitions suivantes s'appliquent.

3.1 chemin: Concaténation d'identifiants de fichier, sans séparateur. Si le chemin commence par l'identifiant du fichier maître, il s'agit d'un chemin absolu.

3.2 couple commande-réponse: Ensemble de deux messages: une commande suivie d'une réponse.

3.3 données de gestion de fichier: Toute information concernant un fichier, à l'exception des paramètres de contrôle du fichier (par exemple, date de péremption, étiquette d'application).

3.4 élément de données: Information visible à l'interface, pour laquelle sont définis un nom, une description du contenu logique, un format et un codage.

3.5 enregistrement: Train d'octets traité comme un tout par la carte et référencé par un numéro d'enregistrement ou par un identifiant d'enregistrement.

3.6 fichier dédié: Fichier contenant des informations de contrôle de fichier et, le cas échéant, de la mémoire disponible. Il peut être le parent de EFs et/ou de DFs.

3.7 fichier élémentaire: Ensemble d'unités de données ou d'enregistrements partageant le même identifiant de fichier. Il ne peut pas être parent d'un autre fichier.

3.8 fichier élémentaire de travail: Fichier élémentaire utilisé pour stocker des données qui ne sont pas interprétées par la carte.

3.9 fichier élémentaire interne: Fichier élémentaire utilisé pour stocker les données interprétées par la carte.

3.10 fichier maître: Fichier dédié unique et obligatoire, représentant la racine de la structure de fichiers.

3.11 fichier parent: Fichier dédié situé juste avant un fichier donné dans l'arborescence.

3.12 fichier répertoire: Fichier élémentaire défini dans la partie 5 de l'ISO/IEC 7816.

3.13 fichier réponse à la remise à zéro: Fichier élémentaire indiquant des caractéristiques de fonctionnement de la carte.

3.14 fournisseur: Autorité qui détient ou qui a obtenu le droit de créer un fichier dédié dans la carte.

3.15 identifiant d'enregistrement: Valeur associée à un enregistrement et qui peut être utilisée pour le référencer. Dans un EF, plusieurs enregistrements peuvent avoir le même identifiant d'enregistrement.

3.16 identifiant de fichier: Valeur binaire sur deux octets, utilisée pour adresser un fichier.

3.17 message: Train d'octets transmis à la carte par le dispositif d'interface ou vice versa, à l'exception des caractères orientés transmission définis à la partie 3 de l'ISO/CEI 7816.

3.18 mot de passe: Données devant être présentées à la carte par son utilisateur à la demande de l'application.

3.19 nom de DF: Train d'octets identifiant de façon unique un fichier dédié dans la carte.

3.20 numéro d'enregistrement: Numéro attribué en séquence à chaque enregistrement pour l'identifier de façon unique dans le EF auquel il appartient.

3.21 objet de données: Information visible à l'interface, comprenant une étiquette, une longueur et une valeur (c'est à dire, un élément de données). Dans la présente partie de l'ISO/CEI 7816, les objets de données ont pour références BER-TLV, COMPACT-TLV et SIMPLE-TLV.

3.22 paramètres de contrôle de fichier: Attributs logiques, structurels et sécuritaires d'un fichier.

3.23 unité de données: Le plus petit ensemble de bits pouvant être référencé sans ambiguïté.

---
1) En cours de publication.

2) En cours de révision.

4 Abréviations et notations

Pour les besoins de la présente partie de l'ISO/CEI 7816, les abréviations suivantes s'appliquent.

APDU	Unité de données du protocole d'application
ATR	Réponse à la remise à zéro
BER	Règles de base pour coder l'ASN.1
CLA	Octet de classe
DIR	Répertoire
DF	Fichier dédié
EF	Fichier élémentaire
FCI	Information de contrôle de fichier
FCP	Paramètre de contrôle de fichier
FMD	Données de gestion de fichier
INS	Octet d'instruction
MF	Fichier maître
P1-P2	Octets de paramètre
PTS	Sélection de type de protocole
RFU	Réservé à un usage futur
SM	Messagerie de sécurité
SW1-SW2	Octets d'état
TLV	Étiquette, longueur, valeur
TPDU	Unité de données du protocole de transmission

Pour les besoins de la présente partie de l'ISO/CEI 7816, les notations suivantes s'appliquent.

'0' à '9' and 'A' à 'F'	Les seize nombres hexadécimaux
(B_1)	Valeur de l'octet B_1
B_1 ll B_2	Concaténation des octets B_1 (le plus significatif) et B_2 (le moins significatif)
(B_1 ll B_2)	Valeur de la concaténation des octets B_1 et B_2
#	Numéro

5 Organisations de base

5.1 Structures des données

Le présent article contient des informations sur la structure logique des données, visible à l'interface lors du traitement de commandes intersectorielles pour les échanges. L'ISO/CEI 7816 ne couvre pas l'emplacement des données ainsi que diverses informations de structure autres que celles présentées ici.

5.1.1 Organisation des fichiers

La présente partie de l'ISO/CEI 7816 assume les deux catégories suivantes de fichiers :

— fichier dédié (DF),

— fichier élémentaire (EF).

L'organisation logique des données dans un carte est constituée de l'arborescence structurelle suivante de fichiers dédiés.

— Le DF à la racine est appelé fichier maître (MF). Le MF est obligatoire.

— Les autres DFs sont facultatifs.

Les 2 types suivants de EFs sont définis.

— EF interne — Ces EFs sont destinés à stocker des données interprétées par la carte, c'est à dire des données analysées et utilisées par la carte à des fins de gestion et de contrôle.

— EF de travail — Ces EFs sont destinés à stocker des données qui ne sont pas interprétées par la carte, c'est à dire des données qui sont utilisées exclusivement par le monde extérieur.

La figure 1 montre un exemple d'organisation logique des fichiers dans une carte.

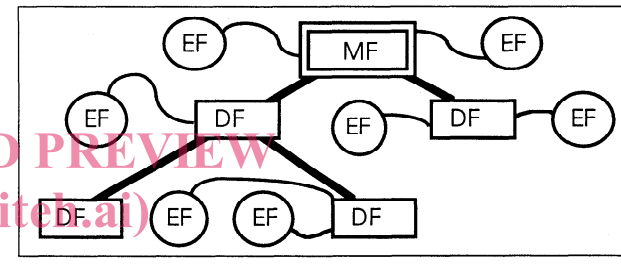

Figure 1 — Organisation logique de fichiers (exemple)

5.1.2 Méthodes de référence des fichiers

Lorsqu'un fichier ne peut être implicitement sélectionné, au moins l'une des méthodes suivantes doit permettre de le sélectionner.

— **Référence par identifiant de fichier** — Tout fichier peut être référencé par un identifiant codé sur 2 octets. Si le MF est référencé par un identifiant de fichier, la valeur '3F00' (valeur réservée) doit être utilisée. La valeur 'FFFF' est RFU. La valeur '3FFF' est réservée (voir référence par chemin). Afin de sélectionner sans ambiguïté tout fichier par son identifiant, les EFs et DFs immédiatement sous un DF donné doivent tous avoir des identifiants différents.

— **Référence par chemin** — Tout fichier peut être référencé par un chemin (concaténation d'identifiants de fichier). Le chemin commence par l'identifiant du MF ou du DF courant et se termine par l'identifiant du fichier à référencer. Si d'autres identifiants figurent sur le chemin, ce sont ceux des DF parents successifs. Les identifiants de fichier sont toujours classés en allant du parent vers l'enfant. Si l'identifiant du DF courant n'est pas connu, la valeur '3FFF' (valeur réservée) peut être utilisée au début du chemin. Le chemin permet une sélection sans ambiguïté de tout fichier, à partir du MF ou du DF courant.

— **Référence par identifiant court de EF** — Tout EF peut être référencé par un identifiant court codé sur 5 bits et prenant les valeurs de 1 à 30. La valeur 0 fait référence au fichier EF couramment sélectionné. Les identifiants courts de EF ne peuvent pas être utilisés dans un chemin, ni comme un identifiant de fichier (par exemple, dans une commande SELECT FILE).

— **Référence par nom de DF** — Tout DF peut être référencé par un nom codé sur 1 à 16 octets. Pour que la sélection par nom de DF ne soit pas ambiguë (par exemple, en sélectionnant par identifiant d'application, tels que défini à la partie 5 de l'ISO/CEI 7816), chaque nom de DF doit être unique dans une carte donnée.

5.1.3 Structures des fichiers élémentaires

Les structures suivantes de EFs sont définies.

- — Structure transparente — Le EF est visible à l'interface comme une séquence d'unités de données.
- — Structure d'enregistrements — Le EF est visible à l'interface comme une séquence d'enregistrements identifiables individuellement.

Les attributs suivants sont définis pour les EFs structurés en enregistrements.

- — Taille des enregistrements: fixe ou variable.
- — Organisation des enregistrements: en séquence (structure linéaire) ou en anneau (structure cyclique).

La carte doit assumer au moins l'une des 4 méthodes suivantes de structuration de EFs:

- — EF transparent.
- — EF linéaire à enregistrements de taille fixe.
- — EF linéaire à enregistrements de taille variable.
- — EF cyclique à enregistrements de taille fixe.

La figure 2 montre ces 4 structures de EFs.

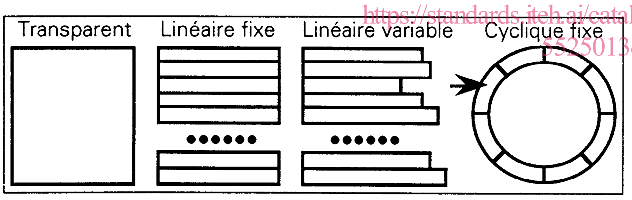

Figure 2 — Structures de EFs

NOTE — La flèche de la figure référence le dernier enregistrement écrit.

5.1.4 Méthodes de référence des données

Les données peuvent être référencées en tant qu'enregistrements, unités de données ou objets de données. Les données sont censées être stockées dans une séquence unique et continue d'enregistrements (dans un EF à structure d'enregistrements) ou d'unités de données (dans un EF à structure transparente). La référence à un enregistrement ou à une unité de données en dehors d'un EF constitue une erreur.

La méthode de référence des données, la méthode de numérotation des enregistrements ainsi que la taille des unités de données constituent des caractéristiques dépendantes du EF. La carte peut fournir des indications dans l'ATR, dans le fichier ATR ainsi que dans toute information de contrôle de fichier. Si la carte fournit des indications en différents endroits, l'indication devant être retenue pour un EF donné est celle qui se situe au plus près de celui-ci dans le chemin à partir du MF jusqu'au EF.

5.1.4.1 Référence par enregistrements

Dans chaque EF à structure d'enregistrements, chaque enregistrement peut être référencé par un identifiant d'enregistrement et/ou par un numéro d'enregistrement. Les identifiants d'enregistrement et les numéros d'enregistrement sont représentés par des entiers non signés sur 8 bits, pouvant prendre les valeurs de '01' à 'FE'. La valeur '00' est réservée à des usages spéciaux, la valeur 'FF' est RFU.

La référence par identifiant d'enregistrement suppose la gestion d'un pointeur d'enregistrement. Une remise à zéro de la carte, une commande SELECT FILE ou toute commande portant un identifiant court et valide de EF peut agir sur le pointeur d'enregistrement. La référence par numéro d'enregistrement ne doit pas agir sur le pointeur d'enregistrement.

— **Référence par identifiant d'enregistrement** — Chaque identifiant d'enregistrement est attribué par une application. Si un enregistrement prend la forme d'un objet de données SIMPLE-TLV dans le champ de données d'un message (voir 5.4.4), l'identifiant d'enregistrement est constitué du premier octet de l'objet de données. Dans un EF à structure d'enregistrements, plusieurs enregistrements peuvent avoir le même identifiant, auquel cas les données contenues dans les enregistrements peuvent être utilisées pour les distinguer les uns des autres.

Chaque fois qu'une référence est faite par un identifiant d'enregistrement, une indication doit spécifier la position logique de l'enregistrement cible: la première, dernière, prochaine ou précédente occurrence par rapport au pointeur d'enregistrement.

- — Dans chaque EF à structure linéaire, les positions logiques doivent être attribuées en séquence lors de l'écriture ou de l'ajout, c'est-à-dire suivant l'ordre de création. Le premier enregistrement créé s'y trouve donc en première position logique.
- — Dans chaque EF à structure cyclique, les positions logiques doivent être attribuées en séquence dans l'ordre inverse, c'est-à-dire que le dernier enregistrement créé se trouve en première position logique.

De plus, les règles suivantes s'appliquent aux structures linéaires et aux structures cycliques.

- — La première occurrence doit être l'enregistrement correspondant à l'identifiant spécifié, et situé en première position logique. La dernière occurrence doit être l'enregistrement correspondant à l'identifiant spécifié, lequel est situé en dernière position logique.
- — Lorsqu'il n'y a pas d'enregistrement courant, la prochaine occurrence doit être l'équivalent de la première occurrence, la précédente occurrence doit être l'équivalent de la dernière occurrence.
- — Lorsqu'il y a un enregistrement courant, la prochaine occurrence doit être l'enregistrement le plus proche de même identifiant et situé dans une position logique supérieure à l'enregistrement courant. L'occurrence précédente doit être l'enregistrement le plus proche de même identifiant et situé dans une position logique inférieure à celle de l'enregistrement courant.

— La valeur '00' doit référencer le premier, dernier, prochain ou précédent enregistrement dans la séquence de numérotation, indépendamment de l'identifiant d'enregistrement.

— **Référence par numéro d'enregistrement** — Dans chaque EF à structure d'enregistrements, les numéros d'enregistrement sont uniques et séquentiels.

— Dans chaque EF à structure linéaire, les numéros d'enregistrement doivent être attribués en séquence lors de l'écriture ou de l'ajout, c'est-à-dire suivant l'ordre de création. Le premier enregistrement (enregistrement numéro un, # 1) est donc le premier créé.

— Dans chaque EF à structure cyclique, les numéros d'enregistrement doivent être attribués en séquence dans l'ordre inverse, c'est-à-dire que le premier enregistrement (enregistrement numéro un, # 1) est le dernier créé.

De plus, la règle suivante s'applique aux structures linéaires et aux structures cycliques.

— La valeur '00' doit référencer l'enregistrement courant, c'est-à-dire celui fixé par le pointeur d'enregistrement.

5.1.4.2 Référence par unités de données

Dans chaque fichier EF à structure transparente, chaque unité de données peut être référencée par un déplacement (par exemple, dans une commande READ BINARY, voir 6.1). Celui-ci prend la forme d'un entier non signé, codé sur 8 ou 15 bits selon l'option spécifiée dans la commande respective. Prenant la valeur 0 pour la première unité de données du EF, le déplacement s'accroît de 1 pour chaque unité de données suivante.

Par défaut, c'est-à-dire si la carte ne fournit aucune indication, la taille de l'unité de données est de un octet.

NOTES

1 Un EF structuré en enregistrements peut accepter la référence par unités de données, et si tel est le cas, les unités de données peuvent contenir des informations de structure en plus des données (par exemple, des numéros d'enregistrement dans une structure linéaire).

2 Dans un EF structuré en enregistrements, il se peut que la référence par unités de données ne donne pas le résultat escompté car l'ordre de stockage des enregistrements n'est pas connu (dans une structure cyclique par exemple).

5.1.4.3 Référence par objets de données

Chaque objet de données (tel que défini dans 5.4.4) débute par une étiquette qui le référence. Les étiquettes sont décrites dans la présente partie de l'ISO/CEI 7816 ainsi que dans d'autres parties de la même norme.

5.1.5 Information de contrôle de fichier

L'information de contrôle de fichier (FCI) est constituée du train d'octets de données disponible dans la réponse à une commande SELECT FILE. L'information de contrôle de fichier peut être présente pour n'importe quel fichier.

Le tableau 1 montre trois gabarits destinés au transport de l'information de contrôle de fichier lorsqu'elle est codée en objets de données BER-TLV.

— Le gabarit FCP est destiné au transport de paramètres de contrôle de fichier (FCP), c'est–à–dire tout objet de données défini dans le tableau 2.

— Le gabarit FMD est destiné au transport de données de gestion de fichier (FMD), c'est–à–dire les objets de données BER-TLV spécifiés dans d'autres articles de la présente partie de l'ISO/CEI 7816 ou dans d'autres parties de cette même norme (par exemple, l'étiquette d'application définie dans la partie 5 et la date de péremption d'application définie dans la partie 6).

— Le gabarit FCI est destiné au transport de paramètres de contrôle de fichier et de données de gestion de fichier.

Tableau 1 — Gabarits pour FCI

T	V
'62'	Paramètres de contrôle de fichier (gabarit FCP)
'64'	Données de gestion de fichier (gabarit FMD)
'6F'	Information de contrôle de fichier (gabarit FCI)

Les options de sélection de la commande SELECT FILE (voir tableau 59) permettent de préciser lequel des 3 gabarits est requis. Si l'option FCP ou FMD est positionnée, l'utilisation du gabarit correspondant est obligatoire. Si l'option FCI est positionnée, l'utilisation du gabarit FCI est facultative.

Une partie de l'information de contrôle de fichier peut aussi se trouver dans un EF de travail sous le contrôle d'une application. L'identifiant du EF est donné sous l'étiquette '87'. Quand de l'information de contrôle de fichier se trouve dans un EF de travail, son codage requiert l'emploi d'un gabarit, FCP ou FCI.

Des informations de contrôle de fichier qui ne sont pas codées conformément à la présente partie de l'ISO/CEI 7816, peuvent être introduites comme suit.

— '00' ou toute valeur supérieure à '9F' — Le codage du train d'octets qui suit est privé.

— Étiquette = '53' — Le champ de valeur de l'objet de données est constitué de données libres non codées en TLV.

— Étiquette = '73' — Le champ de valeur de l'objet de données est constitué d'objets de données libres codés en BER-TLV.

Tableau 2 — Paramètres de contrôle de fichier

T	L	V	S'applique à
'80'	2	Nombre d'octets de données dans le fichier, à l'exception des informations de structure	EFs transparents
'81'	2	Nombre d'octets de données dans le fichier, y compris les informations de structure s'il y en a	Tout fichier
'82'	1	Octet de description de fichier (voir le tableau 3)	Tout fichier
	2	Octet de description de fichier suivi de l'octet de codage de données (voir le tableau 86)	Tout fichier
	3 ou 4	Octet de description de fichier suivi de l'octet de codage de données et de la longueur maximum des enregistrements	EFs à structure d'enregistrement
'83'	2	Identifiant de fichier	Tout fichier
'84'	1 à 16	Nom de DF	DFs
'85'	var.	Information privée	Tout fichier
'86'	var.	Attributs de sécurité (codage non décrit dans la présente partie de l'ISO/IEC 7816)	Tout fichier
'87'	2	Identifiant d'un EF contenant une extension de la FCI	Tout fichier
'88' à '9E'		RFU	
'9F XY'		RFU	

Tableau 3 — Octet de description de fichier

b8	b7	b6	b5	b4	b3	b2	b1	Signification
0	x	-	-	-	-	-	-	**Accès au fichier**
0	0	-	-	-	-	-	-	— Fichier non partageable
0	1	-	-	-	-	-	-	— Fichier partageable
0	-	x	x	x	-	-	-	**Type du fichier**
0	-	0	0	0	-	-	-	— EF de travail
0	-	0	0	1	-	-	-	— EF interne
0	-	0	1	0	-	-	-	— Réservés
0	-	0	1	1	-	-	-	aux
0	-	1	0	0	-	-	-	EFs
0	-	1	0	1	-	-	-	de type
0	-	1	1	0	-	-	-	privé
0	-	1	1	1	-	-	-	— DF
0	-	-	-	-	x	x	x	**Structure du EF**
0	-	-	-	-	0	0	0	— Aucune précision
0	-	-	-	-	0	0	1	— Transparent
0	-	-	-	-	0	1	0	— Linéaire fixe, sans précision
0	-	-	-	-	0	1	1	— Linéaire fixe, SIMPLE-TLV
0	-	-	-	-	1	0	0	— Linéaire variable, sans précision
0	-	-	-	-	1	0	1	— Linéaire variable, SIMPLE-TLV
0	-	-	-	-	1	1	0	— Cyclique, sans précision
0	-	-	-	-	1	1	1	— Cyclique, SIMPLE-TLV
1	x	x	x	x	x	x	x	RFU

"Partageable" signifie que le fichier accepte au moins des accès simultanés sur différents canaux logiques.

5.2 Architecture de sécurité de la carte

Le présent article décrit les éléments suivants:

— états de sécurité,

— attributs de sécurité,

— mécanismes de sécurité.

Lors de l'exécution de commandes et/ou lors de l'accès à des fichiers, les attributs de sécurité sont comparés à l'état de sécurité.

5.2.1 États de sécurité

L'état de sécurité courant représente l'état atteint après la complète exécution

— de la réponse à la remise à zéro (ATR) et, le cas échéant, de la sélection d'un type de protocole (PTS),

— et/ou d'une ou plusieurs commandes exécutant le cas échéant des procédures d'authentification.

L'état de sécurité peut également résulter de l'achèvement d'une procédure de sécurité visant à identifier les entités concernées, si elles existent. Cette identification peut consister par exemple à

— prouver la connaissance d'un mot de passe (par exemple à l'aide de la commande VERIFY),

— prouver la connaissance d'une clé (par exemple à l'aide d'une commande GET CHALLENGE suivie d'une commande EXTERNAL AUTHENTICATE).

— utiliser la messagerie de sécurité (par exemple en authentification de message).

Trois états de sécurité sont considérés.

— État de sécurité global — Il peut être modifié par l'achèvement d'une procédure d'authentification liée au MF (authentification à l'aide d'un mot de passe ou d'une clé attachés au MF, par exemple).

— État de sécurité spécifique à un fichier — Il peut être modifié par l'achèvement d'une procédure d'authentification liée au DF (authentification à l'aide d'un mot de passe ou d'une clé attachés au DF, par exemple) ; il peut être maintenu, retrouvé ou perdu après une sélection de fichier (voir 6.10.2) ; la portée de cette modification peut être limitée à l'application à laquelle appartient la procédure d'authentification.

— État de sécurité spécifique à une commande — Il existe uniquement pendant l'exécution d'une commande comprenant une authentification à l'aide de la messagerie de sécurité (voir 5.6). Ce type de commande peut n'avoir aucune incidence sur les autres états de sécurité.

Lorsque le concept de canaux logiques est utilisé, l'état de sécurité spécifique à un fichier peut dépendre du canal logique (voir 5.5.1).

5.2.2 Attributs de sécurité

Lorsqu'ils existent, les attributs de sécurité définissent les actions autorisées ainsi que les procédures à exécuter pour accomplir ces actions.

Les attributs de sécurité peuvent être associés à chaque fichier. Ils fixent les conditions de sécurité devant être satisfaites pour opérer sur le fichier. Les attributs de sécurité d'un fichier dépendent de

— sa catégorie (DF ou EF),

— de paramètres facultatifs contenus dans les informations de contrôle du fichier et/ou dans celles du ou des fichiers parents.

NOTE — Des attributs de sécurité peuvent aussi être associés à d'autres objets (par exemple des clés).

5.2.3 Mécanismes de sécurité

La présente partie de l'ISO/CEI 7816 définit les mécanismes de sécurité suivants.

— **Authentification d'entité par mot de passe** — La carte compare des données provenant du monde extérieur à des données secrètes internes. Ce mécanisme permet de protéger les droits de l'utilisateur.

— **Authentification d'entité par clé** — L'entité à authentifier doit prouver qu'elle connaît une clé, grâce à une procédure d'authentification (une commande GET CHALLENGE suivie d'une commande EXTERNAL AUTHENTICATE, par exemple).

— **Authentification de données** — À l'aide de données internes, secrètes ou publiques, la carte vérifie des données redondantes reçues du monde extérieur. Ou encore, à l'aide de données internes secrètes, la carte calcule un élément de données (élément de contrôle cryptographique ou signature numérique) et l'insère dans les données transmises au monde extérieur. Ce mécanisme permet de protéger les droits d'un fournisseur.

— **Chiffrement de données** — À l'aide de données internes secrètes, la carte déchiffre un cryptogramme reçu dans un champ de données. Ou encore, à l'aide de données internes, secrètes ou publiques, la carte calcule un cryptogramme et l'insère dans un champ de données pouvant contenir d'autres informations. Ce mécanisme peut être utilisé comme service de confidentialité, tel que la gestion de clé ou l'accès conditionnel. Outre le mécanisme de cryptogramme, la confidentialité des données peut être obtenue par masquage. Dans ce cas, la carte produit un train d'octets masquants et l'ajoute par ou exclusif avec des octets de données reçus du monde extérieur ou transmis vers celui-ci. Ce mécanisme peut être utilisé pour protéger la confidentialité et pour réduire les possibilités de filtrage de messages.

Le résultat d'une authentification peut être consigné dans un EF interne, en fonction des besoins de l'application.

5.3 Structure des messages APDU

Une étape dans un protocole d'application est constituée de l'envoi d'une commande, du traitement de cette commande dans l'entité réceptrice et de la transmission de la réponse. Une réponse spécifique correspond donc à une commande spécifique, ces deux éléments étant appelés couple commande-réponse.

Une unité de données du protocole d'application (APDU) contient un message, de commande ou de réponse, transmis par le dispositif d'interface à la carte ou vice versa.

Dans un couple commande-réponse, les messages de commande et de réponse peuvent contenir des données, ce qui se traduit par les quatre cas figurant au tableau 4.

Tableau 4 — Présence de données dans un couple commande-réponse

Cas	Données de commande	Données attendues en réponse
1	Aucune donnée	Aucune donnée
2	Aucune donnée	Données
3	Données	Aucune donnée
4	Données	Données

5.3.1 Commande APDU

La commande APDU, illustrée par la figure 3 (voir aussi le tableau 6) et définie dans la présente partie de l'ISO/CEI 7816, est constituée de

— un préfixe obligatoire de 4 octets (CLA INS P1 P2),

— un corps conditionnel de longueur variable.

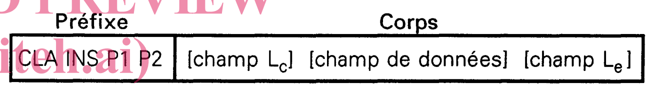

Figure 3 — Structure de la commande APDU

Le nombre d'octets présents dans le champ de données de la commande APDU est indiqué par L_c.

Le nombre maximal d'octets attendu dans le champ de données de la réponse APDU est indiqué par L_e (longueur des données attendues). Lorsque le champ L_e ne contient que des zéros, le nombre maximal d'octets de données disponibles est requis.

La figure 4 montre les 4 structures de commandes APDU, en fonction des 4 cas définis au tableau 4.

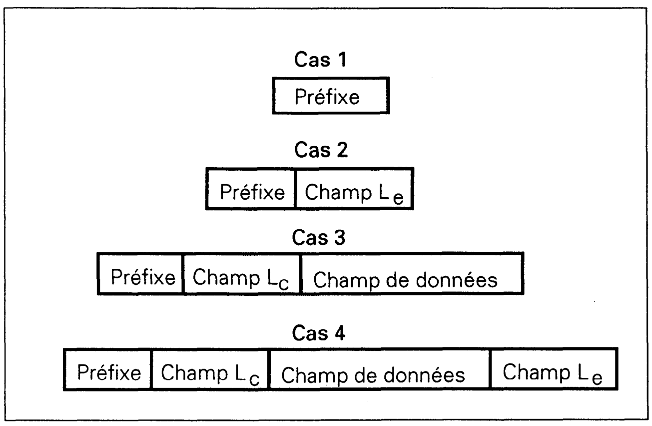

Figure 4 — Les 4 structures de commandes APDU

Dans le cas 1, la longueur L_c est nulle, ce qui implique que le champ L_c et le champ de données sont vides. La longueur L_e est nulle aussi, ce qui implique que le champ L_e est vide. Le corps de la commande est donc vide.

Dans le cas 2, la longueur L_c est nulle, ce qui implique que le champ L_c et le champ de données sont vides. La longueur L_e n'est pas nulle, ce qui implique que le champ L_e est présent. Le corps de la commande est donc constitué d'un champ L_e.

Dans le cas 3, la longueur L_c n'est pas nulle, ce qui implique que le champ L_c est présent et que le champ de données est constitué des L_c octets suivants. La longueur L_e est nulle, ce qui implique que le champ L_e est vide. Le corps de la commande est donc constitué d'un champ L_c suivi d'un champ de données.

Dans le cas 4, la longueur L_c n'est pas nulle, ce qui implique que le champ L_c est présent et le champ de données constitué des L_c octets suivants. La longueur L_e n'est pas nulle, ce qui implique que le champ L_e est également présent. Le corps de la commande est donc constitué d'un champ L_c suivi d'un champ de données puis d'un champ L_e.

5.3.2 Conventions pour décoder les corps de commande

Dans le cas 1, le corps de commande APDU est vide. Une telle commande ne comporte aucun champ de longueur.

Dans les cas 2, 3 et 4, le corps de commande APDU est constitué d'un train de L octets, appelés B_1 à B_L, comme l'illustre la figure 5. Un tel corps comporte 1 ou 2 champs de longueur et B_1 fait toujours partie du premier.

Corps de commande APDU

B_1 ... B_L (L octets)

Figure 5 — Corps non vide

La carte indique, parmi ses capacités (voir 8.3.6), que dans les commandes APDU le champ L_c et le champ L_e

— doivent être courts (un octet, valeur par défaut),

— ou bien peuvent être étendus (instruction explicite).

Par conséquent, les cas 2, 3 et 4 sont courts (1 octet par champ de longueur) ou étendus (B_1 a pour valeur '00' et la valeur de chaque longueur est codée sur 2 autres octets).

Le tableau 5 montre le décodage des commandes APDU, selon les quatre cas définis dans le tableau 4 et la figure 4, en tenant compte de l'extension possible de L_c et de L_e.

Tableau 5 — Décodage des commandes APDU

Conditions			Cas	
L = 0	-	-	1	
L = 1	-	-	Court 2	(2S)
L = 1+(B_1) ;	(B_1) ≠ 0 ;	-	Court 3	(3S)
L = 2+(B_1) ;	(B_1) ≠ 0 ;	-	Court 4	(4S)
L = 3 ;	(B_1) = 0 ;	-	Étendu 2	(2E)
L = 3+(B_2 ‖ B_3) ;	(B_1) = 0 ;	(B_2 ‖ B_3) ≠ 0	Étendu 3	(3E)
L = 5+(B_2 ‖ B_3) ;	(B_1) = 0 ;	(B_2 ‖ B_3) ≠ 0	Étendu 4	(4E)

Toute autre commande APDU est incorrecte.

Conventions pour décoder L_e

Si la valeur de L_e est codée sur un ou deux octets dans lesquels les bits ne sont pas nuls, cette valeur est égale à celle du ou des octets, qui se situe dans la fourchette de 1 à 255 (ou 65 535). Une valeur nulle dans tous les octets correspond à la valeur maximale de L_e : 256 (ou 65 536).

Les 4 premiers cas s'appliquent à toutes les cartes.

Cas 1 — L = 0 ; le corps est vide.

- Aucun octet pour L_c qui vaut 0.
- Pas d'octet de données.
- Aucun octet pour L_e qui vaut 0.

Cas 2S — L = 1.

- Aucun octet pour L_c qui vaut 0.
- Pas d'octet de données.
- B_1 code L_e qui vaut de 1 à 256.

Cas 3S — L = 1 + (B_1) et (B_1) ≠ 0.

- B_1 code L_c (≠ 0) qui vaut de 1 à 255.
- B_2 à B_L sont les L_c octets de données.
- Aucun octet pour L_e qui vaut 0.

Cas 4S — L = 2 + (B_1) et (B_1) ≠ 0.

- B_1 code L_c (≠ 0) qui vaut de 1 à 255.
- B_2 à B_{L-1} sont les L_c octets de données.
- B_L code L_e qui vaut de 1 à 256.

Pour les cartes acceptant l'extension de L_c et L_e (voir 8.3.6, capacités des cartes), les trois cas suivants s'appliquent en plus.

Cas 2E — L = 3 et (B_1) = 0.

- Aucun octet pour L_c qui vaut 0.
- Pas d'octet de données.
- Le champ L_e est constitué de 3 octets où B_2 et B_3 codent L_e qui vaut de 1 à 65 536.

Cas 3E — L = 3 + (B_2 ‖ B_3), (B_1) = 0 et (B_2 ‖ B_3) ≠ 0.

- Le champ L_c est constitué des 3 premiers octets où B_2 et B_3 codent L_c (≠ 0) qui vaut de 1 à 65 535.
- B_4 à B_L sont les L_c octets de données.
- Aucun octet pour L_e qui vaut 0.

Cas 4E — L = 5 + (B_2 ‖ B_3), (B_1) = 0 et (B_2 ‖ B_3) ≠ 0.

- Le champ L_c est constitué des 3 premiers octets où B_2 et B_3 codent L_c (≠ 0) qui vaut de 1 à 65 535.
- B_4 à B_{L-2} sont les L_c octets de données.
- Le champ L_e est constitué des 2 derniers octets B_{L-1} et B_L qui codent L_e valant de 1 à 65 536.

Pour chaque protocole de transmission défini dans la partie 3 de l'ISO/CEI 7816, une annexe rattachée à cette partie (une annexe par protocole) spécifie le transport des messages APDUs d'un couple commande-réponse, pour chacun des sept cas évoqués ci-dessus.

5.3.3 Réponse APDU

Illustrée par la figure 6 (voir aussi le tableau 7), la réponse APDU définie dans la présente partie de l'ISO/CEI 7816, est constituée de

— un corps conditionnel de longueur variable,

— un suffixe obligatoire de 2 octets (SW1 SW2).

Corps	Suffixe
[Champ de données]	SW1 SW2

Figure 6 — Structure des réponses APDU

Le nombre d'octets présents dans le champ de données de la réponse APDU est appelé L_r.

Le suffixe code l'état de l'entité réceptrice après traitement du couple commande-réponse.

NOTE — Si la commande est interrompue, la réponse APDU se limite à un suffixe codant une condition d'erreur sur 2 octets d'état.

5.4 Conventions pour coder les préfixes de commande, les champs de données et les suffixes de réponse

Le tableau 6 montre le contenu de la commande APDU.

Tableau 6 — Contenu de la commande APDU

Code	Nom	Longueur	Description
CLA	Classe	1	Classe d'instruction
INS	Instruction	1	Code d'instruction
P1	Paramètre 1	1	Paramètre 1 d'instruction
P2	Paramètre 2	1	Paramètre 2 d'instruction
Champ L_c	Longueur	variable 1 ou 3	Nombre d'octets présents dans le champ de données de la commande
Champ de données	Données	variable $= L_c$	Train d'octets transmis dans le champ de données de la commande
Champ L_e	Longueur	variable ≤ 3	Nombre maximal d'octets attendus dans le champ de données de la réponse

La tableau 7 montre le contenu de la réponse APDU.

Tableau 7 — Contenu de la réponse APDU

Code	Nom	Longueur	Description
Champ de données	Données	variable $= L_r$	Train d'octets reçu dans le champ de données de la réponse
SW1	Octet d'état 1	1	État après traitement de la commande
SW2	Octet d'état 2	1	Précision sur le traitement de la commande

Les articles suivants fixent les conventions pour coder l'octet de classe, l'octet d'instruction, les octets de paramètres, les octets de données et les octets d'état.

Sauf indication contraire, les bits RFU de ces octets sont mis à zéro et les octets RFU à '00'.

5.4.1 Octet de classe

Comme le montrent conjointement les tableaux 8 et 9, l'octet de classe (CLA) d'une commande est utilisé pour indiquer

— dans quelle mesure la commande et la réponse sont conformes à la présente partie de l'ISO/CEI 7816,

— et le cas échéant (voir tableau 9), le format de la messagerie de sécurité et le numéro du canal logique.

Tableau 8 — Codage et signification de CLA

Valeur	Signification
'0X'	Structure et codage de la commande et de la réponse conformes à la présente partie de l'ISO/IEC 7816 (pour coder 'X', voir le tableau 9)
'10' à '7F'	RFU
'8X', '9X'	Structure de la commande et de la réponse conforme à la présente partie de l'ISO/IEC 7816. Sauf pour 'X' (pour le coder, voir le tableau 9), le codage et la signification de la commande et de la réponse sont privés.
'AX'	Sauf indication contraire dans le contexte de l'application, structure et codage de la commande et de la réponse conformes à la présente partie de l'ISO/IEC 7816 (pour coder 'X', voir le tableau 9)
'B0' à 'CF'	Structure de la commande et de la réponse conforme à la présente partie de l'ISO/IEC 7816
'D0' à 'FE'	Structure et codage privés pour la commande et la réponse
'FF'	Réservé à PTS

Tableau 9 — Codage et signification du quartet 'X' lorsque CLA = '0X', '8X', '9X' ou 'AX'

b4	b3	b2	b1	Signification
x	x	-	-	**Format de la messagerie de sécurité (SM)**
0	x	-	-	• **Pas de SM ou SM non conforme à 5.6**
0	0	-	-	— Pas de SM ou pas d'indication de SM
0	1	-	-	— Format de SM privé
1	x	-	-	• **Messagerie de sécurité conforme à 5.6**
1	0	-	-	— Préfixe de commande non authentifiée
1	1	-	-	— Préfixe de commande authentifiée (voir 5.6.3.1 pour l'authentification du préfixe)
-	-	x	x	**Numéro de canal logique** (conforme à 5.5) (b2 b1 = 00 quand le canal # 0 est sélectionné ou que les canaux logiques ne sont pas utilisés)

5.4.2 Octet d'instruction

L'octet d'instruction (INS) d'une commande doit être codé de façon à permettre sa transmission avec tous les

protocoles définis dans la partie 3 de l'ISO/CEI 7816. Le tableau 10 montre les codes INS qui en conséquence ne sont pas corrects.

Tableau 10 — Codes INS incorrects

b8	b7	b6	b5	b4	b3	b2	b1	Signification
x	x	x	x	x	x	x	1	— Valeurs impaires
0	1	1	0	x	x	x	x	— '6X'
1	0	0	1	x	x	x	x	— '9X'

Le tableau 11 montre les codes INS définis dans la présente partie de l'ISO/CEI 7816. Lorsque la valeur de CLA est comprise entre '00' et '7F', les autres valeurs des codes INS doivent être attribuées par l'ISO/CEI JTC1 SC17.

Tableau 11 — Codes INS définis dans la présente partie de l'ISO/CEI 7816

Valeur	Nom de commande	Article
'0E'	ERASE BINARY	6.4
'20'	VERIFY	6.12
'70'	MANAGE CHANNEL	6.16
'82'	EXTERNAL AUTHENTICATE	6.14
'84'	GET CHALLENGE	6.15
'88'	INTERNAL AUTHENTICATE	6.13
'A4'	SELECT FILE	6.11
'B0'	READ BINARY	6.1
'B2'	READ RECORD(S)	6.5
'C0'	GET RESPONSE	7.1
'C2'	ENVELOPE	7.2
'CA'	GET DATA	6.9
'D0'	WRITE BINARY	6.2
'D2'	WRITE RECORD	6.6
'D6'	UPDATE BINARY	6.3
'DA'	PUT DATA	6.10
'DC'	UPDATE RECORD	6.8
'E2'	APPEND RECORD	6.7

5.4.3 Octets de paramètres

Les octets de paramètres P1-P2 d'une commande peuvent prendre n'importe quelle valeur. Les octets de paramètres ne donnant aucune précision doivent être mis à '00'.

5.4.4 Octets des champs de données

Chaque champ de données doit revêtir l'une des trois structures suivantes.

— Chaque champ de données codé en TLV doit être composé de un ou plusieurs objets de données codés en TLV.

— Chaque champ de données non codé en TLV doit être composé de un ou plusieurs éléments de données, selon les spécifications de la commande à laquelle il se rapporte.

— La structure des champs de données codés de façon privée n'est pas décrite dans l'ISO/IEC 7816.

La présente partie de l'ISO/CEI 7816 accepte dans les champs de données les deux types suivants d'objets de données codés en TLV:

— objets de données BER-TLV,

— objets de données SIMPLE-TLV.

L'ISO/CEI 7816 n'utilise ni '00' ni 'FF' comme étiquette.

Chaque objet de données BER-TLV doit être constitué de 2 ou 3 champs consécutifs (voir l'ISO 8825 et l'annexe D).

— Le champ d'étiquette T est constitué de un ou plusieurs octets consécutifs. Il code une classe, un type et un numéro.

— Le champ de longueur est composé de un ou plusieurs octets consécutifs. Il code un nombre entier L.

— Si L n'est pas nul, Le champ de valeur V est composé de L octets consécutifs. Dans le cas contraire, l'objet de données est vide: il n'y a pas de champ de valeur.

Chaque objet de données SIMPLE-TLV doit être constitué de 2 ou 3 champs consécutifs.

— Le champ d'étiquette T est composé d'un seul octet codant un nombre entier compris entre 1 et 254 (un identifiant d'enregistrement, par exemple). Il ne code ni classe, ni type de construction.

— Le champ de longueur est composé de 1 ou 3 octets consécutifs. Si le premier octet est compris entre '00' et 'FE', le champ de longueur est limité à un seul octet codant un nombre entier L compris entre 0 et 254. Si le premier octet est égal à 'FF', le champ comporte deux autres octets codant un nombre entier L compris entre 0 et 65 535.

— Si L n'est pas nul, le champ de valeur V est composé de L octets consécutifs. Dans le cas contraire, l'objet de données est vide: il n'y a pas de champ de valeur.

Les champs de données de certaines commandes (par exemple SELECT FILE), les champs de valeur des objets de données SIMPLE-TLV ainsi que les champs de valeur de certains objets de données BER-TLV primitifs sont destinés au codage de un ou plusieurs éléments de données.

Les champs de données de certaines autres commandes (des commandes orientées enregistrement, par exemple) ainsi que les champs de valeur des autres objets de données BER-TLV primitifs sont destinés au codage de un ou plusieurs objets de données SIMPLE-TLV.

Les champs de données de certaines autres commandes (des commandes orientées objet, par exemple) ainsi que les champs de valeur des objets de données BER-TLV construits sont destinés au codage de un ou plusieurs objets de données BER-TLV.

NOTE — Avant, entre ou après des objets de données codés en TLV, des octets de valeur '00' ou 'FF' sans signification peuvent se présenter (ils peuvent être dus, par exemple, à la modification ou à la suppression d'objets de données codés en TLV).

5.4.5 Octets d'état

Les octets d'état SW1-SW2 d'une réponse indiquent l'état du traitement dans la carte. La figure 7 montre le schéma structurel des valeurs définies dans la présente partie de l'ISO/CEI 7816.

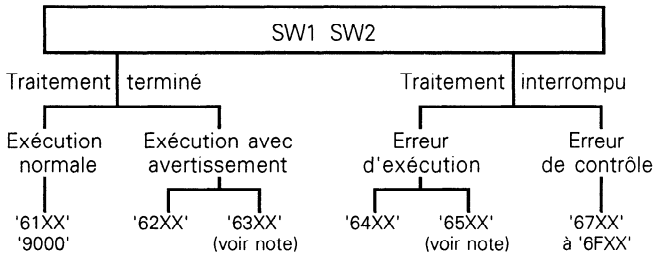

Figure 7 — Schéma structurel des octets d'état

NOTE — Lorsque SW1 = '63' ou '65', l'état de la mémoire non volatile a changé. Lorsque SW1 = '6X' sauf '63' et '65', l'état de la mémoire non volatile n'a pas changé.

En raison des spécifications de la partie 3 de l'ISO/CEI 7816, la présente partie ne définit pas les valeurs suivantes de SW1-SW2:

— '60XX';

— '67XX', '6BXX', '6DXX', '6EXX', '6FXX', dans chaque cas où 'XX' ≠ '00';

— '9XXX', si 'XXX' ≠ '000'.

Les valeurs suivantes de SW1-SW2 sont définies quel que soit le protocole (voir des exemples dans l'annexe A):

— Si une commande est interrompue avec une réponse dans laquelle SW1 = '6C', SW2 indique la valeur à attribuer au champ L_e court (longueur exacte des données requises) pour relancer la commande avant toute autre commande.

— Si une commande (qui peut correspondre aux cas 2 ou 4 du tableau 4 et de la figure 4) est traitée avec une réponse dans laquelle SW1 = '61', SW2 indique la valeur maximale à attribuer au champ L_e court (longueur des données encore disponibles) pour lancer une commande GET RESPONSE avant toute autre commande.

NOTE — Une fonctionnalité similaire à celle offerte par '61XX' peut être mise en œuvre par '9FXX' au niveau de l'application. Toutefois, des applications peuvent employer '9FXX' pour d'autres raisons.

Le tableau 12, complété par les tableaux 13 à 18, montre la signification générale des valeurs SW1-SW2 définies dans la présente partie de l'ISO/CEI 7816. Pour chaque commande, un article approprié donne des précisions.

Les tableaux 13 à 18 spécifient les valeurs de SW2 lorsque SW1 a pour valeur '62', '63', '65', '68', '69' et '6A'. Les valeurs de SW2 non définies dans les tableaux 13 à 18 sont RFU, à l'exception des valeurs comprises entre 'F0' et 'FF', qui ne sont pas définies dans la présente partie de l'ISO/CEI 7816.

Tableau 12 — Codage de SW1-SW2

SW1-SW2	Signification
	Exécutions normales
'9000'	— Pas d'autre précision
'61XX'	— SW2 indique le nombre d'octets de réponse encore disponible (voir le texte ci-dessous)
	Exécution avec avertissement
'62XX'	— État de la mémoire non volatile inchangé (plus de précision dans SW2, voir le tableau 13)
'63XX'	— État de la mémoire non volatile changé (plus de précision dans SW2, voir le tableau 14)
	Erreurs d'exécution
'64XX'	— État de la mémoire non volatile inchangé (SW2 = '00', les autres valeurs sont RFU)
'65XX'	— État de la mémoire non volatile changé (plus de précision dans SW2, voir le tableau 15)
'66XX'	Réservé au domaine de la sécurité (non défini dans la présente partie de l'ISO/IEC 7816)
	Erreurs de contrôle
'6700'	— Longueur incorrecte
'68XX'	— Fonctions dans CLA non assumées (plus de précision dans SW2, voir le tableau 16)
'69XX'	— Commande non autorisée (plus de précision dans SW2, voir le tableau 17)
'6AXX'	— Paramètres incorrects P1-P2 (plus de précision dans SW2, voir le tableau 18)
'6B00'	— Paramètres incorrects P1-P2
'6CXX'	— Longueur L_e incorrecte: SW2 indique la longueur exacte (voir le texte ci-dessous)
'6D00'	— Code d'instruction non assumé ou invalide
'6E00'	— Classe non assumée
'6F00'	— Pas de diagnostic précis

Tableau 13 — Codage de SW2 lorsque SW1 = '62'

SW2	Signification
'00'	Aucune précision
'81'	Une partie des données en retour peut être corrompue
'82'	Fin de fichier ou d'enregistrement atteinte avant lecture de L_e octets
'83'	Fichier sélectionné invalidé
'84'	Format de FCI non conforme à 5.1.5

Tableau 14 — Codage de SW2 lorsque SW1 = '63'

SW2	Signification
'00'	Aucune précision
'81'	Fichier rempli par la dernière écriture
'CX'	Compteur dans 'X' (valeur de 0 à 15) (signification exacte dépendant de la commande)

Tableau 15 — Codage de SW2 lorsque SW1 = '65'

SW2	Signification
'00'	Aucune précision
'81'	Défaillance de la mémoire