NORME INTERNATIONALE

ISO/CEI 7816-4

Première édition
1995-09-01

AMENDEMENT 1
1997-12-15

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

Partie 4: Commandes intersectorielles pour les échanges

AMENDEMENT 1: Impact de la messagerie de sécurité sur les structures des messages APDU

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

Part 4: Interindustry commands for interchange

AMENDMENT 1: Impact of secure messaging on the structures of APDU messages

Numéro de référence
ISO/CEI 7816-4:1995/Amd.1:1997(F)

Sommaire

Avant-propos

L'ISO (Organisation internationale de normalisation) et la CEI (Commission électrotechnique internationale) forment ensemble un système consacré à la normalisation internationale considérée comme un tout. 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 différents 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 approbation, avant leur acceptation comme Normes internationales. Les Normes internationales sont approuvées conformément aux procédures qui requièrent l'approbation de 75 % au moins des organismes nationaux votants.

L'Amendement 1 à la Norme internationale ISO/CEI 7816-4:1995 a été élaboré par le comité technique mixte ISO/CEI JTC 1, *Technologies de l'information*, sous-comité SC 17, *Cartes d'identification et dispositifs associés*.

Introduction

Les cartes à circuit(s) intégré(s) à contacts sont des cartes d'identification destinées à l'échange d'informations entre le monde extérieur et le circuit intégré contenu dans la carte. Au cours de chaque échange d'informations, la carte délivre des informations (résultats de calculs, données stockées) et/ou modifie son contenu (stockage de données, mémorisation d'événements).

La partie 4 de l'ISO/CEI 7816 fait partie d'une série de normes qui décrivent les paramètres de ces cartes, ainsi que leur emploi pour les échanges internationaux.

Le présent amendement fixe l'impact de la messagerie de sécurité sur les structures des messages APDU.

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

Partie 4:
Commandes intersectorielles pour les échanges

AMENDEMENT 1: Impact de la messagerie de sécurité sur les structures des messages APDU

Dans le tableau 19, remplacer la dernière ligne par les deux lignes suivantes.

'96', '97'	— Valeur de L_e dans la commande non sécurisée
'99'	— Informations d'état (par exemple, SW1 SW2)

Dans le tableau 21, remplacer la valeur 'BA' par les deux suivantes.

'AC', 'BC'

Insérer le paragraphe suivant.

5.7 Impact de la messagerie de sécurité sur les structures des messages APDU

Les structures des messages APDU sont spécifiées en 5.3. Selon 5.3.1, la commande APDU comprend un préfixe de commande obligatoire sur quatre octets suivi conditionnellement d'un corps de commande (voir les figures 3 et 4); le décodage du corps de commande est spécifié en 5.3.2 (voir la figure 5 et le tableau 5). Selon 5.3.3, la réponse APDU comprend un corps de réponse conditionnel suivi d'un suffixe de réponse obligatoire sur deux octets (voir la figure 6). La figure 8 montre les structures des messages APDU.

Préfixe de commande	Corps de commande
CLA INS P1 P2 (quatre octets)	[Champ L_c] [Champ de données] [Champ L_e] (L octets, représentés par B_1 à B_L)

Corps de réponse	Suffixe de réponse
[Champ de données] (L_r octets de données)	SW1 SW2 (deux octets)

Figure 8 — Structures des messages APDU

L'article 6 spécifie commandes et réponses APDU pour des commandes intersectorielles de base. L'article 7 spécifie commandes et réponses APDU pour des commandes intersectorielles orientées transmission. Les articles 6 et 7 ne décrivent pas l'impact de la messagerie de sécurité (voir 5.6) sur les structures des messages APDU. Les significations sémantiques des champs de longueur et des champs de données dans les articles 6 et 7 peuvent donc sembler en contradiction avec leurs significations syntaxiques en 5.3.

Le présent paragraphe spécifie l'impact de la messagerie de sécurité telle que spécifiée en 5.6 sur les structures des messages APDU telles que spécifiées en 5.3, de façon à éviter l'éventuel malentendu mentionné ci-dessus.

Pour sécuriser une commande APDU où CLA a une valeur appropriée selon le tableau 9, à savoir '0X', '8X', '9X' ou 'AX', il faut y mettre à 1 le bit b4 de CLA, ce qui est indiqué par CLA* dans la figure 9 et dans l'annexe F; s'il y a un corps de commande, il faut le décoder selon 5.3.2 puis l'encapsuler comme suit.

— Lorsqu'il y a un champ de données, il faut acheminer les L_c octets de données

- soit dans un objet de données à valeur en clair ('80', '81', 'B2', 'B3', voir le tableau 19),
- soit dans un objet de données pour la confidentialité (de '84' à '87', voir le tableau 22).

— Lorsqu'il y a un champ L_e, il faut acheminer la valeur de L_e dans un objet de données pour L_e ('96' ou '97', voir le tableau 19); le champ de valeur y code un nombre entier positif non signé sur un ou deux octets; la valeur nulle et l'objet vide signifient tous deux le maximum.

De la même façon, il faut encapsuler la réponse APDU comme suit.

— Lorsqu'il y a un champ de données, il faut acheminer les L_r octets de données

- soit dans un objet de données à valeur en clair ('80', '81', 'B2', 'B3', voir le tableau 19),
- soit dans un objet de données pour la confidentialité (de '84' à '87', voir le tableau 22).

— Si nécessaire, il faut acheminer le suffixe de réponse dans un objet de données pour informations d'état ('99', voir le tableau 19); l'objet vide signifie SW1 SW2 = '9000'.

La figure 9 montre les structures des messages APDU sécurisés.

— Tout nouveau champ de données peut acheminer d'autres objets de données SM, par exemple, un objet de données de contrôle cryptographique ('8E') à la fin. L'annexe F donne des exemples explicatifs.

— Le nouveau champ L_c donne la longueur du nouveau champ de données de la commande sécurisée.

— Le nouveau champ L_e doit être vide quand aucun champ de données n'est prévu dans la réponse APDU sécurisée; sinon il ne doit comporter que des zéros.

— Le nouveau suffixe de réponse code l'état de l'entité réceptrice après traitement de la commande sécurisée. On peut l'encapsuler pour le protéger.

Préfixe de commande	Corps de commande
CLA* INS P1 P2 (quatre octets)	[Nouveau champ L_c] { [Nouveau champ de données] = [T-L_c-Octets de données] [T-'01' ou '02'-L_e] } [Nouveau champ L_e]

Corps de réponse	Suffixe de réponse
[Nouveau champ de données] = [T-L_r-Octets de données] [T-'02'-SW1 SW2]	Nouvel SW1 SW2 (deux octets)

Figure 9 — Structures des messages APDU sécurisés

NOTES

1 Les longueurs de 1 à 127 sont codées de la même façon dans les champs de longueur BER-TLV et dans les champs de longueur APDU. Les codages sont différents pour 128 et plus.

2 Comme exprimé ci-dessus, les nouveaux champs de données peuvent acheminer d'autres objets de données SM.

3 Quand on sécurise un message, il n'est pas toujours apparent que les données à protéger soient structurées en BER-TLV. Les étiquettes '80', '81', '86' et '87' sont alors recommandées.

Remplacer l'annexe F existante (deux pages) par la révision suivante (trois pages).

Annexe F

(informative)

Utilisation de la messagerie de sécurité

F.1 Abréviations

Pour les besoins de la présente annexe, les abréviations suivantes s'appliquent.

CC élément de contrôle cryptographique
CG cryptogramme
CH préfixe de commande (CLA INS P1 P2)
CR référence de contrôle
FR référence de fichier
KR référence de clé
L longueur
LE valeur de L_e dans la commande non sécurisée (un ou deux octets codant un nombre entier positif non signé; la valeur nulle signifie le maximum)
PB octets de remplissage ('80' suivi de 0 à k-1 fois '00' où k est la longueur de bloc)
PI octet indicateur de remplissage
PV valeur en clair
RD descripteur de réponse
T étiquette
II concaténation

F.2 Élément de contrôle cryptographique

Selon 5.7, l'utilisation d'éléments de contrôle cryptographique (voir 5.6.3.1) est indiquée pour les 4 cas définis au tableau 4 et à la figure 4. Dans les exemples, la valeur de L_{CC} est quatre. CLA* indique l'utilisation de la messagerie de sécurité, c'est-à-dire que le bit b4 est mis à 1 dans CLA qui vaut '0X', '8X', '9X' ou 'AX' conformément au tableau 9.

— Cas 1 — Pas de données, pas de données

Voici une paire de commande-réponse non sécurisée.

Préfixe de commande	Corps de commande
CLA INS P1 P2	Vide

Corps de réponse	Suffixe de réponse
Vide	SW1 SW2

— Cas 1.a — État ne devant pas être protégé

Voici la commande APDU sécurisée.

Préfixe de commande	Corps de commande
CLA* INS P1 P2	Nouveau champ L_c (un octet = '06') II Nouveau champ de données (six octets)

Nouveau champ de données = Un objet de données = T_{CC} II L_{CC} II CC

Données couvertes par CC (b3=1 dans CLA*) = Un bloc = CH II PB

Voici la réponse APDU sécurisée.

Corps de réponse	Suffixe de réponse
Vide	Nouvel SW1 SW2

— Cas 1.b — État devant être protégé

Voici la commande APDU sécurisée.

Préfixe de commande	Corps de commande
CLA* INS P1 P2	Nouveau champ L_c (un octet ='06') II Nouveau champ de données (six octets) II Nouveau champ L_e (un octet = '00')

Nouveau champ de données = Un objet de données = T_{CC} II L_{CC} II CC

Données couvertes par CC (b3=1 dans CLA*) = Un bloc = CH II PB

Voici la réponse APDU sécurisée.

Corps de réponse	Suffixe de réponse
Nouveau champ de données	Nouvel SW1 SW2

Nouveau champ de données = Deux objets de données = T_{SW} (b1=1) II L_{SW} II SW (= Nouvel SW1 SW2) II T_{CC} II L_{CC} II CC

Données couvertes par CC = Un bloc = T_{SW} (b1=1) II L_{SW} II SW II PB

— Cas 2 — Pas de données, données

Voici une paire de commande-réponse non sécurisée.

Préfixe de commande	Corps de commande
CLA INS P1 P2	Champ L_e

Corps de réponse	Suffixe de réponse
Champ de données	SW1 SW2

Voici la commande APDU sécurisée.

Préfixe de commande	Corps de commande
CLA* INS P1 P2	Nouveau champ L_c || Nouveau champ de données || Nouveau champ L_e (un ou deux octets = '00')

Nouveau champ de données = Deux objets de données =
T_{LE} (b1=1) || L_{LE} || LE ||
T_{CC} || L_{CC} || CC

Données couvertes par CC =
- Un bloc si b3=0 dans CLA* =
  T_{LE} (b1=1) || L_{LE} || LE || PB
- Deux blocs si b3=1 dans CLA* =
  CH || PB ||
  T_{LE} (b1=1) || L_{LE} || LE || PB

Voici la réponse APDU sécurisée.

Corps de réponse	Suffixe de réponse
Nouveau champ de données	Nouvel SW1 SW2

Nouveau champ de données = Trois objets de données =
T_{PV} (b1=1) || L_{PV} || PV ||
[T_{SW} (b1=1) || L_{SW} || SW (= Nouvel SW1 SW2)] ||
T_{CC} || L_{CC} || CC

Données couvertes par CC = Un bloc ou plus =
T_{PV} (b1=1) || L_{PV} || PV || [T_{SW} (b1=1) || L_{SW} || SW] || PB

— Cas 3 — Données, pas de données

Voici une paire de commande-réponse non sécurisée.

Préfixe de commande	Corps de commande
CLA INS P1 P2	Champ L_c || Champ de données

Corps de réponse	Suffixe de réponse
Vide	SW1 SW2

— Cas 3.a — État ne devant pas être protégé

Voici la commande APDU sécurisée.

Préfixe de commande	Corps de commande
CLA* INS P1 P2	Nouveau champ L_c || Nouveau champ de données

Nouveau champ de données = Deux objets de données =
T_{PV} (b1=1) || L_{PV} || PV ||
T_{CC} || L_{CC} || CC

Données couvertes par CC =
- Un bloc ou plus si b3=0 dans CLA* =
  T_{PV} (b1=1) || L_{PV} || PV || PB
- Deux blocs ou plus si b3=1 dans CLA* =
  CH || PB ||
  T_{PV} (b1=1) || L_{PV} || PV || PB

Voici la réponse APDU sécurisée.

Corps de réponse	Suffixe de réponse
Vide	Nouvel SW1 SW2

— Cas 3.b — État devant être protégé

Voici la commande APDU sécurisée.

Préfixe de commande	Corps de commande
CLA* INS P1 P2	Nouveau champ L_c || Nouveau champ de données || Nouveau champ L_e (un ou deux octets = '00')

Nouveau champ de données = Deux objets de données =
T_{PV} (b1=1) || L_{PV} || PV ||
T_{CC} || L_{CC} || CC

Données couvertes par CC =
- Un bloc ou plus si b3=0 dans CLA* =
  T_{PV} (b1=1) || L_{PV} || PV || PB
- Deux blocs ou plus si b3=1 dans CLA* =
  CH || PB ||
  T_{PV} (b1=1) || L_{PV} || PV || PB

Voici la réponse APDU sécurisée.

Corps de réponse	Suffixe de réponse
Nouveau champ de données	Nouvel SW1 SW2

Nouveau champ de données = Deux objets de données =
T_{SW} (b1=1) || L_{SW} || SW (= Nouvel SW1 SW2) ||
T_{CC} || L_{CC} || CC

Données couvertes par CC = Un bloc =
T_{SW} (b1=1) || L_{SW} || SW || PB

— Cas 4 — Données, données

Voici une paire de commande-réponse non sécurisée.

Préfixe de commande	Corps de commande
CLA* INS P1 P2	Champ L_c || Champ de données || Champ L_e

Corps de réponse	Suffixe de réponse
Champ de données	SW1 SW2

Voici la commande APDU sécurisée.

Préfixe de commande	Corps de commande
CLA* INS P1 P2	Nouveau champ L_c || Nouveau champ de données || Nouveau champ L_e (un ou deux octets = '00')

Nouveau champ de données = Trois objets de données =
T_{PV} (b1=1) || L_{PV}|| PV ||
T_{LE} (b1=1) || L_{LE} || LE ||
T_{CC} || L_{CC} || CC

Données couvertes par CC =
- Un bloc ou plus si b3=0 dans CLA* =
  T_{PV} (b1=1) || L_{PV} || PV || T_{LE} (b1=1) || L_{LE} || LE || PB
- Deux blocs ou plus si b3=1 dans CLA* =
  CH || PB ||
  T_{PV} (b1=1) || L_{PV} || PV || T_{LE} (b1=1) || L_{LE} || LE || PB

Voici la réponse APDU sécurisée.

Corps de réponse	Suffixe de réponse
Nouveau champ de données	Nouvel SW1 SW2

Nouveau champ de données = Trois objets de données =
T_{PV} (b1=1) || L_{PV} || PV ||
[T_{SW} (b1=1) || L_{SW} || SW (= Nouvel SW1 SW2)] ||
T_{CC} || L_{CC} || CC

Données couvertes par CC = Un bloc ou plus =
T_{PV} (b1=1) || L_{PV} || PV || [T_{SW} (b1=1) || L_{SW} || SW] || PB

F.3 Cryptogrammes

L'utilisation de cryptogrammes avec et sans remplissage (voir 5.6.4) est indiquée dans des champs de données (commande APDU aussi bien que réponse APDU). Au lieu des objets de données à valeur en clair comme dans les exemples précédents, il faut utiliser des objets de données pour la confidentialité comme suit.

— Cas a — Données en clair non codées en BER-TLV

Champ de données =
$T_{PI\ CG}$ || $L_{PI\ CG}$ || PI || CG

Données acheminées par CG = Un bloc ou plus =
Données non codées en BER-TLV
puis des octets de remplissage selon PI

— Cas b — Données en clair codées en BER-TLV

Champ de données =
T_{CG} || L_{CG} || CG

Données acheminées par CG = Train d'octets masqués =
Objets de données codés en BER-TLV (remplissage selon l'algorithme et son mode d'opération)

F.4 Références de contrôle

L'utilisation de références de contrôle (voir 5.6.5.1) est indiquée.

Champ de données de la commande =
T_{CR} || L_{CR} || CR
où CR = T_{FR} || L_{FR} || FR || T_{KR} || L_{KR} || KR

F.5 Descripteur de réponse

L'utilisation de descripteurs de réponse (voir 5.6.5.2) est indiquée.

Champ de données de la commande =
T_{RD} || L_{RD} || RD
où RD = T_{PV} || '00' || T_{CC} || '00'

Champ de données de la réponse =
T_{PV} || L_{PV} || PV || T_{CC} || L_{CC} || CC

F.6 Commande ENVELOPE

L'utilisation de la commande ENVELOPE (voir 7.2) est indiquée.

Champ de données de la commande =
$T_{PI\ CG}$ || $L_{PI\ CG}$ || PI || CG

Données acheminées par CG =
Commande APDU (commençant par CH)
puis des octets de remplissage selon PI

Champ de données de la réponse =
$T_{PI\ CG}$ || $L_{PI\ CG}$ || PI || CG

Données acheminées par CG =
Réponse APDU
puis des octets de remplissage selon PI